PROPUESTA METODOLÓGICA PARA LA ARMONIZACIÓN DE LA LEY 1581 DE 2012 CON EL SISTEMA DE GESTIÓN DE LA CALIDAD Y EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES PÚBLICAS COLOMBIANAS DEL ORDEN NACIONAL

Dalila Ariza Téllez
Gonzalo Gualteros Garzón
Andrea Carolina Vanegas González

UNIVERSIDAD SANTO TOMÁS
CONVENIO DE COOPERACIÓN ACADÉMICA USTA – ICONTEC
MAESTRÍA EN CALIDAD Y GESTIÓN INTEGRAL
BOGOTÁ, D. C. 2021

PROPUESTA METODOLÓGICA PARA LA ARMONIZACIÓN DE LA LEY 1581 DE 2012 CON EL SISTEMA DE GESTIÓN DE LA CALIDAD Y EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LAS ENTIDADES PÚBLICAS COLOMBIANAS DEL ORDEN NACIONAL

Trabajo de grado para optar al título de Magister en Calidad y Gestión Integral

Directora
Ingrid Carolina Moreno Rodríguez
Magíster en Gestión Documental y Administración de Archivos

CONVENIO UNIVERSIDAD SANTO TOMÁS E ICONTEC
FACULTAD DE INGENIERÍA MECÁNICA
MAESTRÍA EN CALIDAD Y GESTIÓN INTEGRAL
BOGOTÁ, D.C.2021

Nota de aceptación:

_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

DEDICATORIA

Especialmente dedicado a nuestras familias quienes con su comprensión y apoyo nos impulsaron a cumplir nuestros objetivos y al equipo que formó parte de éste proyecto por cada uno de los aportes los cuales contribuyeron a llevar a cabo este trabajo de investigación.

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

INGRID CAROLINA MORENO RODRÍGUEZ, Magíster en Gestión Documental y Administración de Archivos, docente de la maestría por su asesoría, su disponibilidad de tiempo, su compromiso y sus conocimientos los cuales fueron importantes para el desarrollo de este trabajo.

A los validadores expertos quienes con sus recomendaciones contribuyeron a la mejora del trabajo de investigación.

A las Universidad Santo Tomas y el convenio ICONTEC, por la formación.

A todos los docentes de la cohorte-40, por su apoyo y compromiso.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE GRÁFICAS

LISTA DE ANEXOS

INTRODUCCIÓN

Las entidades públicas del orden nacional, deben implementar la ley 1581 de 2012 velando por la protección de los datos personales, con el fin de asegurar los derechos y deberes de los ciudadanos, adicionalmente se hace necesario establecer, implementar, mantener y mejorar los sistemas de gestión de la calidad y de seguridad de la información entre otros, con el fin de aplicar buenas prácticas que aporten al cumplimiento de las obligaciones de las entidades.

Actualmente en la mayoría de entidades colombianas del sector público, se tienen implementadas las NTC ISO 9001 e ISO IEC 27001, sin embargo el cumplimiento de la ley 1581 no se encuentra alineado con estas normas, es preciso que se armonice la ley y los sistemas de gestión mencionados, con el fin de optimizar la gestión de las entidades del estado en función del logro de los objetivos institucionales, y así obtener mayor credibilidad y confianza por parte de los usuarios, así como ser sostenibles en el tiempo.

Teniendo como base el estudio de la ley de protección de datos personales y las normas mencionadas se identificaron los requisitos convergentes, divergentes y complementarios, haciendo uso de la estructura propuesta por el ciclo PHVA especificando algunos instrumentos que pueden ser utilizados en las entidades públicas para facilitar su implementación y contribuir con la mejora continua.

Con la propuesta de articulación de la ley con las normas objeto de estudio, se apunta a la creación de una integración de la ley y las normas antes señaladas permitan crear una cultura en la que prime la protección de los datos personales y la seguridad de la información en beneficio de los usuarios y partes interesadas.

1. PROBLEMA DE INVESTIGACIÓN

1.1. ANTECEDENTES

1.1.1 Contexto mundial

Partiendo del contexto mundial, la privacidad e intimidad de las personas es considerada un ámbito fundamental, es así como a partir de la Declaración Universal de Derechos Humanos adoptada en París por las Naciones Unidas (ONU), el 10 de diciembre de 1948, se estipulan los derechos de los individuos y la protección de los mismos.

En esta declaración se encuentra estipulado el derecho a la intimidad, el cual busca la protección de la privacidad de cada persona, en tal sentido, se hace necesario que las regulaciones estén alineadas con las tecnologías de la información, con el objeto de buscar la protección de los datos personales que se encuentran en plataformas digitales y están expuestas a posibles riesgos de mal uso de los datos (Barrera-Campos, 2020).

1.1.1.1 Sistemas de Gestión Integral. El manual The Integrated Use of Managements System Estándar (IUMSS), de la International Standard Organization (ISO), propone una metodología de integración de distintas normas acorde con la estructura de alto nivel que permite identificar los aspectos convergentes, divergentes y complementarios, a través de la identificación de cuatro etapas como son preparación, conexión, incorporación y mantenimiento; de tal manera que la aplicación de las directrices estipuladas en el manual facilita la integración de las normas. (Moreno et ál., 2021).

Teniendo en cuenta que las organizaciones colombianas cada vez buscan ser más competitivas, a través de la satisfacción de los usuarios, enmarcados en los contextos tanto externos como internos que son dinámicos, se hace necesario integrar los diferentes sistemas de gestión. Es así como el objetivo de éste trabajo de investigación, es crear una herramienta metodológica que permita la armonización entre la ley 1581 y las normas NTC ISO 9001 y 27001; por lo tanto, el IUMSS, se convierte en un modelo que permite la adaptación de estas normas. (Moreno et ál., 2021)

Por otra parte, a nivel internacional, se estableció la norma UNE 66177:2005, documento técnico que no es de carácter obligatorio, sin embargo, proporciona una guía que permite la integración de los sistemas de gestión mediante criterios

que ayudan al desarrollo, la implantación y la evaluación de un sistema integrado de gestión (Asociación Española de Normalización y Certificación, 2005).

Según Nunhes, Oliveira y Bernardo (2019), para la orientación de la integración de los sistemas de gestión se han determinado seis principios: gestión sistémica; estandarización; integración estratégica, táctica y operativa; aprendizaje organizacional; desburocratización y, mejora continua, los cuales son la base para el establecimiento y mantenimiento de la integración de los sistemas de gestión.

1.1.1.2 Sistema de Gestión de la Calidad ISO 9001. La mayoría de las entidades públicas colombianas tienen implementado el sistema de gestión de la calidad (SGC) según los requisitos establecidos en la NTC ISO 9001:2015, promoviendo en las organizaciones la eficiencia y mejora de la satisfacción de las necesidades y expectativas de los usuarios.

En 1987 se realizó la primera publicación de la ISO 9001, en el año 2015 se aplicó la estructura de alto nivel, que contribuye a facilitar la aplicación e integración de los requisitos comunes entre las normas, generando así un panorama global para la aplicación de los sistemas de gestión integral (ISO 9001:2015).

Este estándar es adaptable a cualquier tipo de organización, es por ello que cada empresa establece los procesos necesarios para el cumplimiento de sus objetivos institucionales, por tanto, la implementación de un sistema de gestión de la calidad se convierte en una medida de índole estratégico que permite la sostenibilidad y competitividad de las organizaciones a través de la mejora continua de sus procesos.

Por lo anterior, la implementación de un sistema de gestión de la calidad acorde con la ISO 9001:2015, presenta ventajas y beneficios para las entidades públicas colombianas del orden nacional, tales como: el fomento de una cultura cimentada en la mejora continua, lo cual permite mayor satisfacción del cliente proporcionando productos y/o servicios que cumplan los requisitos legales y reglamentarios; permite el tratamiento de los riesgos y oportunidades que se presenten en el contexto de la organización y el cumplimiento de sus objetivos, el resultado de ello se demuestra en la conformidad con los requisitos estipulados en el SGC (ISO 9001:2015).

El desarrollo de las políticas sobre seguridad de la información inició a finales de la década de los 60’s, cuando solo se tenían procedimientos de seguridad interna para la información gubernamental que se consideraba clasificada y debía ser protegida del público en general. En la década subsiguiente, los procesos democráticos mundiales y el desarrollo de la globalización, transformaron ese espacio reservado, a uno de transparencia de los datos (Šikman, et al., 2019).

Las normas de la serie 27000 nacen en 1995, la British Standards Institution –BSI, publicó por primera vez, la norma BS7799 que fueron elaboradas por el Departamento de Comercio e Industria (DTI) del Reino Unido. A estas normas se les llama "ISO / IEC" por ser desarrolladas y mantenidas conjuntamente por dos organismos internacionales de normas: ISO (la Organización Internacional de Normalización) y la IEC (la Comisión Electrotécnica Internacional); como una serie de buenas prácticas y requisitos de un sistema de seguridad de la información (SGI), para todo tipo de empresas. Esta norma fue adoptada como ISO 17799 en el año 2000, luego en 2005, se formalizó como ISO 27001 una vez se contó con la certificación de más 1.700 empresas en la norma (Ríos y Oscar, 2010; Carvajal, 2013).

La universidad de leyes de Harvard, en 2007, acuñó el concepto de “e-compliance”, refiriéndose a la gestión de los riesgos asociados al manejo de la información y las redes digitales en su interacción con los requisitos legales, la tecnología y el mercado (Navas y Torres, 2011).

La ISO 27001 es una norma certificable, los otros estándares brindan orientación sobre la implementación de mejores prácticas, algunos permiten orientar sobre cómo desarrollar el SGSI para industrias particulares; otros presentan una guía sobre cómo implementar procesos y controles clave de gestión de riesgos de seguridad de la información. Las normas ISO están sujetas a una revisión cada cinco años para evaluar la necesidad de actualizaciones (Rusell, 2013).

La ISO 27001 en 2013 produjo un cambio significativo con la adopción de la estructura del "Anexo SL". Si bien se realizaron algunos cambios menores en la redacción en 2017 para aclarar el requisito de mantener un inventario de activos de información, la ISO 27001:2013 sigue siendo la norma actual para que las organizaciones puedan obtener la certificación.

En Colombia fue adaptada generando la NTC ISO 27001 con la versión 2013 que es quizás, la más consultada, debido a que es certificable, muchas empresas en el país están sometidas a pruebas de riesgos de datos por manejar población sensible en informática, como contratos gubernamentales y demás información con reserva, donde esta norma juega un papel importante en la custodia de la información.

1.1.1 Contexto nacional. Basados en el contexto nacional, según Barrera-Campos (2020), se hace necesaria la protección de los datos de las personas, aunque existen normas que regulan el manejo de la información, no se tiene la certeza de la manipulación que se puede dar, teniendo en cuenta que la recolección se efectúa a través de medios digitales, lo que hace más difícil el control en cuanto al manejo de los datos.

En la normativa colombiana es necesario instituir claramente las obligaciones de las cuales es responsable el sujeto garante del tratamiento de los datos, así como el análisis de los resultados que permitan establecer la conformidad de los mismos y las buenas practicas aplicadas, relacionadas con la protección de datos personales sensibles, de tal forma que se generen estándares para el uso de criterios mínimos reglamentarios, contribuyendo a la minimización de riesgos que se generen por el indebido tratamiento de los datos (Acero González, et al., 2021).

1.1.2.1 Ley 1581 de 2012. El Hábeas Data es un híbrido de voces, "hábeas" tomada del latín que significa "tráigase", y "data" tomado del inglés, que significa "dato". Puede decirse entonces, que el Hábeas Data significa "que tengas los datos" o "que vengan los datos" o "que tengas los registros", es decir, implica tomar conocimiento de datos propios en poder de otro. (Pierini, A. et al., 2002, p.21).

Inicialmente en 1890, se discutió el derecho a la intimidad cuando los estadounidenses Samuel Warren y Louis Brandéis, célebres por su artículo The Right To Privacy que propugnaba por establecer límites jurídicos que impidieron la intromisión del periodismo en la vida privada de las personas, lograron influir ampliamente en Estados Unidos por la defensa del derecho a la privacidad (Conde Colmenero, 2014).

El marco histórico del origen de la protección de datos personales se remonta a la Constitución alemana de Weimar de 1919, la cual introdujo el concepto de datos personales de una manera muy restringida al suscribirse, únicamente, a los funcionarios públicos que conocían e intervenían la información (Masciotra, 2003).

De otra parte, la normativa internacional con la inclusión del artículo 12 en la Declaración Universal de los Derechos Humanos de 1948, reconoció el derecho a la intimidad; lo que a la postre inspiró en 1966, el artículo 17 del Pacto Internacional de Derechos Civiles y Públicos el cual lo reproduce parcialmente (Pfeffer Urquiaga, 2006).
Otro referente histórico obligado cuando se analizan los antecedentes de la regulación de datos personales es el convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, suscrito en Estrasburgo el 28 de enero de 1961, (Documento BOE-A-1985-23447), el cual buscaba extender su marco de aplicación en favor de la libertad de la información, a través de las fronteras nacionales entre los estados (Fernández, 2005).

Siguiendo el recorrido histórico, el 08 de mayo de 1979, el Parlamento Europeo aprobó la resolución que tutelaba los derechos de las personas con respecto al progreso informático, y asimismo, el gobierno español en 1984, lo ratificó e

incorporó a su derecho interno, el 15 de noviembre de 1985 (Tejerina Rodríguez, 2014).

En este mismo sentido fue aprobado el Convenio Nº 108 del 28 de enero de 1981, por parte del Consejo Europeo, como medida de protección de las personas frente al uso automatizado de sus datos personales. Este fue acogido por la Comunidad Económica Europea como un mecanismo internacional legalmente vinculante en lo concerniente a la protección de datos. Posteriormente un Tribunal Federal Alemán en 1983, fundamentándose en la garantía del libre desarrollo de la personalidad, declaró un concepto denominado derecho a la autodeterminación informativa, visto como la facultad que tiene el individuo para difundir y utilizar sus datos personales (Rebollo Delgado, 2014 citado en Cote, 2016).

De igual manera y con el ánimo de proteger la privacidad de las personas, ante los inminentes avances tecnológicos, se dio origen a la ley del Parlamento del Reino Unido de Gran Bretaña e Irlanda del Norte, denominada Data Protection Act (DPA), británica de 1984, que propende por exigir a los Estados miembros, salvaguardar la privacidad y libertades fundamentales de las personas (Fernández, 2005).

De manera complementaria surge en el Parlamento Europeo, la directiva 95/46/CE de 24 de octubre de 1995 proferida por el Consejo Europeo. Esta norma se enfoca al tratamiento de datos en cuanto a su circulación y protección se refiere, pues básicamente, la medida busca obligar a los estados miembros a proteger, mediante un marco regulador, la intimidad de las personas (Conde Ortiz, 2006).

Para concluir con este recorrido histórico, la Unión Europea, incluyó en el artículo 8 de su carta de Derechos Fundamentales proclamada en Niza en diciembre de 2000, por el Parlamento Europeo, el derecho a la protección de datos de carácter personal, como lo refiere la autora Fernández Sola (2004) en su libro Unión Europea y derechos fundamentales en perspectiva constitucional.

En Colombia la protección de datos personales nace a partir de la Constitución Política de 1991 en su artículo 15 el cual dispone: "(...) Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley (Constitución Política, 1991, Art.15).

El marco normativo de la protección de datos en Colombia se ha venido regulando bajo unos principios básicos de (veracidad-finalidad-circulación-temporalidad-interpretación-seguridad y confidencialidad), incluyendo normas que garanticen el debido cumplimiento de este derecho, y un amparo eficaz, contra la eventual afectación por su indebida utilización.

La legislación Colombiana adoptó esta iniciativa y fue reconocida en la Constitución de 1991, posteriormente apareció la Ley Estatutaria 1266 de 2008, con una orientación sectorial o especial para el sector financiero, relacionada con el riesgo crediticio, consecutivamente fue necesario expedir la Ley 1581 de 2012, ante la insuficiencia de la Ley 1266 de 2008, y la creciente necesidad de ampliar la reglamentación a todos los tipos de datos que salieran de esa órbita, y que permitiera cumplir con los estándares internacionales. Finalmente se centralizaron competencias, bajo la denominada regulación administrativa, que puso en marcha el sistema de registro de bases de datos personales RNBD bajo la responsabilidad de la Superintendencia de Industria y Comercio (Corte Constitucional, 2015, T-366, p. 18).

1.2 DESCRIPCIÓN DEL PROBLEMA

El tema de investigación se centra en la armonización de la ley 1581 de 2012, con el Sistema de Gestión de la Calidad y el Sistema de Seguridad de la Información, buscando que ésta responda a las necesidades y el cumplimiento normativo, en las entidades públicas colombianas del orden nacional.

La problemática a la cual se busca dar solución surge de la necesidad de cumplir los requisitos de la ley de protección de datos, a través de la adopción de los sistemas de gestión de la calidad y de seguridad de la información en las entidades públicas del territorio colombiano, mediante la creación de mecanismos o herramientas que permitan la aplicación de los requisitos de la ley 1581 apalancada en las normas técnicas ISO 9001 e ISO 27001, de tal manera que las entidades promuevan el manejo y la protección de los derechos de los usuarios en el uso y manejo de la información de datos personales.

La ley 1581 de 2012 o también llamada Régimen General de Protección de Datos personales, reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan obtenido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada; aplica el tratamiento de datos personales realizado en el territorio colombiano o cuando el responsable o encargado del tratamiento, no estando en territorio nacional, le aplique la legislación colombiana en concordancia con las normas y tratados internacionales.

La protección de los datos personales es de gran relevancia, ya que si estos se utilizan de manera indebida pueden ocasionar discriminación, afectando así los derechos y libertades de las personas. Sumado a esto se encuentra la importancia de la seguridad informática que permite controlar y salvaguardar los datos que se operan tanto de las personas como de la organización mediante la utilización de técnicas y medidas que ayudan a la disponibilidad, la integridad, la confidencialidad y la autenticación de la información.

Por esto es necesario que las entidades públicas colombianas del orden nacional cuenten con una metodología que permita la armonización para la aplicabilidad de la ley de protección de datos a los sistemas de gestión de la calidad y de seguridad de la información, dando cumplimiento a la legislación nacional y proporcionando a los usuarios credibilidad y confianza en el manejo de sus datos, igualmente evitando riesgos en los que se puede incurrir no sólo en sanciones pecuniarias, sino en la afectación de la salud física y mental de las personas.

Teniendo en cuenta el desarrollo de las tecnologías de la información, cada vez se hace más difícil el control de la privacidad y manejo de los datos personales y esto se presta para el uso indebido, divulgación de información no permitida y almacenamiento no controlado de los datos personales, por otra parte, para las entidades públicas colombianas del orden nacional que no cuenten con armonización de la ley 1581 con los sistemas de gestión de la calidad y de la seguridad de la información, pueden generar reprocesos.

Por lo tanto, es necesario establecer e implementar políticas y procesos documentados que optimicen los recursos, que permitan generar buenas prácticas asociadas a la disponibilidad, la integridad y la confidencialidad de la información para el manejo y protección de los datos personales establecidas en las normas técnicas ISO 9001 e ISO 27001al interior de las entidades públicas colombianas del orden nacional.
Actualmente las entidades públicas colombianas del orden nacional voluntariamente invierten recursos y esfuerzos en el cumplimiento de los requisitos que exige la NTC ISO 9001 y la NTC ISO 27001 para implementar y certificar estos modelos, sin embargo, es necesario armonizarlos con los requisitos de la ley

1581 de 2012, con el fin de contribuir a la centralización de la información, dando lugar al mejoramiento continuo y reducción de los riesgos de la seguridad de la información.

En Colombia se ha establecido el régimen general de protección de datos personales bajo la ley 1581 del 2012, como derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas, en bases de datos o archivos, lo cual da lugar a que se generen controles que permitan el buen uso y seguridad de la información en las entidades públicas colombianas del orden nacional, contribuyendo así al cumplimiento de su objetivo misional y su posicionamiento socio económico cada vez más competitivo y cambiante.

Así como el estado colombiano ha declarado la legislación relacionada con la ley de protección de datos personales, a su vez el ICONTEC como instancia de normalización en el territorio nacional, ha adaptado y homologado normas técnicas colombianas como referentes para el cumplimiento de requisitos, procesos y actividades de los sistemas de gestión de la calidad y seguridad de la información.

Las entidades públicas colombianas del orden nacional en concordancia con el cumplimiento legal reúnen esfuerzos para adoptar e implementar modelos de buenas prácticas para la estandarización de sus procesos, esto implica que debe existir cohesión e interrelación entre la legislación, como es el caso del sistema de gestión de la calidad y el sistema de seguridad de la información para el cumplimiento de los requisitos de manera articulada, evitando redundancia, dispersión y reprocesos en el manejo y uso de la información.

Por lo anterior, aunque en las entidades públicas colombianas del orden nacional cuenten con la implementación de la ley de protección de datos personales, hace falta la armonización con el Sistema de Gestión de Calidad y el Sistema de Seguridad de la Información, para lograr que la información de datos personales sea eficaz, eficiente, disponible, integral y confidencial con el fin de satisfacer las necesidades y los requerimientos legales. La implementación de estos modelos de gestión promueve en las entidades públicas el diseño de plataformas que permitan la aplicación de nuevas tecnologías para el tratamiento de la información y comunicación, de tal manera que se genera mayor competitividad y retos innovadores que permitan estar a la vanguardia tanto en el entorno nacional como internacional.

Mediante esta investigación se busca proponer una metodología que le permita a las entidades públicas colombianas del orden nacional, articular la ley 1581 con los modelos de gestión de la calidad y de la seguridad de la información, contribuyendo así, a evitar la materialización de riesgos que se generen por

incumplimiento de estas como, por ejemplo, incurrir en sanciones de tipo penal, económico y social que afecten el desarrollo de la entidad y que deterioren su imagen.

1.3 FORMULACIÓN DEL PROBLEMA

¿Cómo elaborar una propuesta metodológica de armonización de la Ley 1581 de 2012, con los sistemas de gestión de la calidad bajo los lineamientos de la NTC ISO 9001:2015 y de seguridad de la información, según los requisitos de la NTC ISO 27001:2015 para organizaciones públicas colombianas del orden nacional?

2. JUSTIFICACIÓN

Para las entidades públicas colombianas del orden nacional es de gran utilidad este trabajo de investigación porque permite la armonización de una ley colombiana y dos normas técnicas como un factor clave para la optimización de los recursos y la generación de acciones encaminadas a la protección y seguridad de la información, así como también identificar el tratamiento que se le debe dar a la información confidencial y a los datos personales, lo cual es importante para el avance y el mejoramiento continuo en el contexto de las entidades públicas colombianas del orden nacional y su cultura de la calidad.

Por otra parte, aunque la adopción de las normas de gestión de la calidad y seguridad de la información es decisión de las entidades, las armonizaciones de estas nos proporcionan un modelo que permite de manera adecuada el cumplimiento de los preceptos legales en materia de protección de datos y a su vez el manejo de la seguridad de la información evitando que se materialicen riesgos que pueden llegar a afectar la seguridad, la confidencialidad y la integridad de la información.

El derecho a la protección de los datos personales y la intimidad es un derecho de tipo fundamental consagrado en la constitución colombiana que tienen todas las personas a conocer, actualizar y rectificar los datos que se hayan recogido sobre ellas en archivos físicos o bases de datos digitales y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma, pero a pesar de esto, hoy en día se enfrentan constantes irregularidades tanto en la captura, procedimientos, tratamiento y conservación de los datos de las personas naturales y jurídicas (Constitución Política de Colombia, 1991).

Es normal que todas las entidades públicas del orden nacional utilicen información personal en distintos procesos para el desarrollo de su actividad, en su día a día se recogen datos personales, de forma verbal y escrita, a través de página web, correo electrónico, formularios físicos o digitales etc.; desconociendo en muchas ocasiones que dichos datos y su posterior tratamiento debe cumplir con las disposiciones legales en materia de manejo, procesamiento, almacenamiento, uso de las bases de datos, tecnología y seguridad, so pena de incurrir en sanciones importantes.

Los sistemas de gestión de la calidad y seguridad de la información, en las entidades públicas del orden nacional, entrelazan información fundamental al momento de formalizar la implementación de normas legales. Para que estas

implementaciones puedan funcionar adecuadamente se requiere que la documentación sirva de base para tomar decisiones, planear actividades y generar la proyección de la organización, en este sentido, la armonización entre los sistemas de gestión de la calidad, seguridad en la información y normas legales está dirigido a identificar, racionalizar, simplificar, mejorar y optimizar tiempos y recursos, de aquí se resalta la relevancia de esta investigación que podrá ser guía de análisis para futuros trabajos reglamentarios en el ejercicio de la academia.
Las entidades públicas colombianas del orden nacional están llamadas a cumplir las disposiciones legales y reglamentarias. Como resultado de esta investigación se pretende obtener una metodología que oriente las actividades, procesos señalados en la normatividad legal vigente y los aspectos contemplados en los sistemas de gestión de la calidad y seguridad en la información.

Adicionalmente este ejercicio académico aportó a los autores en metodología de integración como investigadores en ámbito profesional y laboral como gestores de la calidad en las organizaciones donde se desempeñan y como futuros magister.

La protección de datos en la actualidad se convierte en una preocupación para las entidades públicas del orden nacional en Colombia, por lo tanto, esta investigación reviste importancia tanto para la Universidad Santo Tomas como también para los investigadores que aborden esta temática, porque plasma una propuesta metodológica para facilitar la armonización de la ley 1581 de 2012 con las normas técnicas ISO 9001 e ISO 27001. Sin duda esta armonización genera estrategias que promueven el fortalecimiento de la protección de datos personales integrado a un sistema de gestión, para evitar que se vulneren los derechos y deberes de las personas en esta materia y se afecte así su calidad de vida, además contribuye a minimizar los riesgos de índole económico para las organizaciones gubernamentales.

Acorde con la dinámica actual de la sociedad y el auge de las tecnologías de la información se hace necesario que las entidades públicas colombianas del orden nacional sean más efectivas, por tanto, la innovación es una constante para el logro de sus objetivos. El desafío de las entidades públicas colombianas del orden nacional es estar a la vanguardia de éstos cambios y de la integración de los sistemas de gestión como herramientas para lograr la mejora de los procesos la seguridad de la información y la satisfacción de los usuarios (Hernández-Vivanco et al., 2018).

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Elaborar una propuesta metodológica para la armonización de la Ley 1581 de 2012 con el Sistema de Gestión de Calidad NTC ISO 9001 y el Sistema de Seguridad de la Información NTC ISO 27001, con el propósito de dar el respectivo cumplimiento legal y normativo aplicable en las entidades públicas colombianas del orden nacional en materia de tratamiento de datos personales.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los puntos convergentes, divergentes y complementarios asociados a los requisitos de la Ley 1581 de 2012 y los requisitos de las normas NTC ISO 9001 y NTC ISO 27001.
- Elaborar una propuesta metodológica para la armonización de la ley 1581 de 2012 y las normas técnicas colombianas NTC ISO 9001 y NTC ISO 27001, para las entidades públicas colombianas del orden nacional.
- Validar la propuesta metodológica a través de la consulta a expertos.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Sistemas de Gestión Integral. Para las entidades públicas colombianas del orden nacional, los sistemas de gestión integral debe ser una constante, debido a la globalización, la innovación de las tecnologías de la información y el entorno cambiante de la sociedad, cada vez son más los retos a los que se tienen que enfrentar las entidades para lograr su sostenibilidad y competitividad en el mercado.

Por consiguiente, la gestión en las entidades públicas colombianas del orden nacional debe realizarse de manera sistémica, con el fin de cumplir con las expectativas, requisitos de los clientes y las partes interesadas, fomentando una cultura de mejora continua, para el estatus de la organización en distintos mercados con productos y/o servicios que permitan que los usuarios se mantengan en el tiempo (Tejada y Peña, 2009).

A nivel internacional la norma española UNE 66177 de 2005, (Asociación Española de Normalización y Certificación, 2005), proporciona una Guía para la integración de los sistemas de gestión, basado en la identificación del nivel de madurez de la gestión los procesos mediante el ciclo PHVA y las organizaciones buscan implementar varios sistemas de gestión, sin embargo, la mayoría de las veces funcionan de forma independiente.

En general, se busca la eficiencia y la eficacia de los recursos de las organizaciones para implementar de forma integrada los diferentes sistemas de gestión, situación que no ha sido fácil para las organizaciones, no obstante, la guía presenta los lineamientos para lograr esta integración entre los diferentes sistemas de gestión (calidad, ambiental y de seguridad y salud en el trabajo), sin embargo, es de aplicabilidad a otros sistemas de gestión que maneje la organización (Norma UNE 66177:2005).

Por otra parte, en el 2006 la British Standards Institution (Institución Británica de Normalización –BSI) publicó la primera versión de la PAS 99 actualizada en el 2012, esta norma internacional se realizó usando la guía ISO y permite la alineación de los requisitos comunes de las normas, es aplicable a todos los tipos de organización.

Dentro de los beneficios de los sistemas integrados PAS 99, se encuentran: el ahorro de recursos ya que permite que se auditen varios sistemas a la vez, elimina

reprocesos y duplicidad de tareas, identificación de objetivos comunes, establecimiento de políticas y procedimientos que integren la totalidad de las normas de gestión. Por consiguiente, la adopción de la norma PAS 99, simplifica la implementación de varios sistemas de gestión teniendo en cuenta que la estructura es general a todas las normas de sistemas de gestión.

En resumen, consta de siete elementos a saber: contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora; estructura que debe alinearse a la gestión integrada de la organización. En la tabla 1 se presenta la estructura de la norma relacionada con el ciclo PHVA (PAS 99, 2012).

Tabla 1. Estructura norma PAS 99

CICLO PHVA	
PLANEAR	1.Contexto de la organización 2.Liderazgo 3.Planificación 4.Soporte
HACER	5.Operación
VERIFICAR	6.Evaluación del desempeño
ACTUAR	7.Mejora

Fuente: Norma PAS 99:2012

Así mismo en el año 2008, el Instituto Colombiano de Normas Técnicas y Certificación (Icontec), establece la Guía Técnica Colombiana GTC 180, instaura lineamientos relacionados con el fomento y desarrollo de responsabilidad social, busca integrar todos los aspectos de la organización social, económico y ambiental con un enfoque hacia la gestión, contribuyendo así al desarrollo sostenible que redunda en el bienestar de la comunidad (GTC 180, 2008).

Finalmente, en el año 2018, la ISO estableció la Guía IUMSS (The Integrated Use of Management System Standards), la cual se aplicará en el proceso de la presente investigación, esta metodología permite la aplicación de integración de los sistemas de gestión NTC ISO 9001:2015, 27001:2015 los cuales se articularon teniendo como base la ley 1581 de 2012, con el fin de proporcionar a las

organizaciones una metodología de aplicación en la que el tratamiento de datos personales, la seguridad en la información y la gestión de la calidad formen parte de la estrategia y la cultura de las empresas colombianas (IUMSS, 2018).

4.1.2 Protección de datos. El derecho a la intimidad de las personas se refiere a lo más propio y confidencial del ser humano, es decir, la información que una persona guarda para sí misma. Esta es la facultad de proteger el espacio exclusivo del individuo, a la soledad y a conservar un círculo de vida ajeno a la intrusión de los otros. Sin embargo, la interacción inevitable con la sociedad y los avances de la tecnología, han vulnerado la intimidad del ser.

El derecho a la intimidad, de la misma manera que el resto de los derechos humanos, tiene su historia y se ha consagrado en diversos escritos como, por ejemplo, “De la libertad de los antiguos comparada a la de los modernos”, de Benjamín Constant, o también en la obra “On Liberty” de J. Stuart Smill y “The Right to Privacy” de Samuel Warren y Louis Brandeis, entre otros, han llevado a justificar la intimidad con fundamento en el derecho. Por su parte, desde la de Declaración universal de los derechos humanos de 1948, ya se viene protegiendo esa esfera íntima de la persona, puesto que en el artículo 12 se enuncia la prohibición de entrometerse de manera arbitraria en la vida privada, la familia, el domicilio o la correspondencia de otro, así como tampoco, se puede agredir su honra o reputación. Este derecho a la intimidad en un plano estático, es reconocido en gran parte de las normas de carácter constitucional, pero en el otro plano que es dinámico, es decir, en el terreno derivado del avance tecnológico, pueden ser vulnerados otros aspectos de la vida personal, como, por ejemplo, sus datos personales (García, 2007).

Es importante anotar que los datos de cualquier persona deben ser protegidos para que estos puedan ser tratados y luego, convertidos en información que pueda ser utilizada con los propósitos y por las personas que hayan sido autorizados por su titular. (García, 2007). Hondius (1983), define la protección de los datos como “aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho individual a la intimidad, respecto del procesamiento manual o automático de datos”. En el contexto de la comunidad europea, se entiende como datos personales, toda información sobre una persona físicamente identificable, es decir, toda persona cuya identidad pueda ser establecida de manera directa o indirecta, ya sea a través de un número de identificación, o también mediante elementos característicos de su fisiología, o su psiquis, incluso sus particularidades económicas, culturales o sociales (Directiva 95/46/CE, Artículo 2, 1995).

Ahora bien, gracias al desarrollo de las tecnologías de la información (TI), es posible acopiar y almacenar infinidad de datos sobre una sola persona sin límite

de espacio, así como también efectuar un inventario de su información personal y relacionarla instantáneamente con todos los datos que, sobre ella, existan en diferentes archivos, o que hayan sido recolectados en lugares distintos, sin importar la distancia a la que se encuentren (Garriga, 2004, citado en Aguilar 2018).

Es por ello que se ha visto la necesidad de adoptar políticas de seguridad en lo atinente a la recolección y circulación de la información personal, puesto que el uso inadecuado de la misma, puede quebrantar las garantías constitucionales y transgredir la intimidad de los titulares. Es aquí donde los datos personales adquieren la debida importancia, ya que arrojan lo fundamental para la identificación de una persona (Aguilar-Castañeda, 2018). Se hace conveniente abordar la protección de datos desde el punto de vista de las TI en lo referente a la recolección, procesamiento y circulación de estos, puesto que el derecho a la intimidad, dentro de una sociedad computarizada, es inalienable e impone obligaciones y deberes a quienes controlan y tienen acceso a la información de los individuos (García, 2007).

Es así como la protección de datos como derecho de las personas ha sido consagrado de manera expresa en varios países en cada una de sus respectivas constituciones, mientras que, en otros, ese derecho se ha desarrollado con la institución del hábeas data. Por ejemplo, Argentina fue el primer país de Latinoamérica en adoptar normas que protegen los datos, luego lo hicieron Perú, Chile, Paraguay, México y Colombia, entre otros, donde existe una ley de hábeas data (Vega, 2013).

Por su parte, Colombia ha venido desarrollando la protección de datos personales desde 1991, como ya se anotó, al establecer el derecho de las personas a conocer, actualizar y rectificar los datos personales que se encuentren en bases de datos o en archivos de las entidades públicas o privadas. Así mismo, obliga el respeto de este derecho por parte de los terceros que recolectan, tratan y circulan la información personal de los ciudadanos. Otras disposiciones generales del hábeas data han sido reguladas por la ley 1266 de 2008, así mismo, la forma como los operadores de los bancos de datos deben presentar la información financiera, crediticia, comercial y de servicios, está determinada por el decreto 1727 de 2009. La disposición para la protección de datos personales fue instituida por la Ley 1581 de 2012 y los decretos reglamentarios 1377 de 2013 y 886 de 2014 (Ruiz, 2018).

4.1.3 Sistemas de Seguridad en la información. ISO 27000 es un conjunto de estándares internacionales sobre la Seguridad de la Información, la familia ISO 27000 contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad

de la Información, enmarcado la metodología para la aplicación de controles de seguridad de la información, mediante la protección de la información en materia de confidencialidad, integridad y disponibilidad, generando así el desarrollo de procesos y políticas de seguridad de la información en las organizaciones. Esta norma consta de dos partes, en la primera parte ISO/CEI 17799, se hace referencia a las buenas prácticas relacionadas a la gestión y seguridad de la información, en la segunda parte BS 7799, se plantean recomendaciones para la gestión eficaz de la seguridad de la información.

El SGSI que provee la norma ISO 27001 no es infalible, puesto que la mayor responsabilidad de su ejecución y de su eficacia recae sobre el capital humano de la organización, por lo que es necesario que este sistema sea elaborado, administrado y ejecutado por personal calificado, certificado, con el compromiso y disposición suficiente para que los procesos involucrados en su implementación se lleven a cabo eficazmente.

El hecho de que los estándares ISO se revisan y evalúan cada 4 o 5 años, así se actualiza la norma ISO 27001, se garantiza que cuando pasa este periodo se inspeccionaran los riesgos y vulnerabilidades nuevas que hayan surgido o evolucionado durante este lapso de tiempo, el problema latente es la velocidad con que avanza la tecnología y con ello nuevos tipos de fraudes y peligros que pueden atentar contra la información de nuestra organización; dejando la duda si esta revisión se hace con la frecuencia requerida. Uno de los beneficios más importantes que posee el SGSI que provee la ISO 27001 y en lo que la mayoría de autores coinciden es el manejo que se le da a la información, puesto que es un requisito de la ISO 27001, que esta se ordene de tal forma que sea fácil de consultar, de guardar y por ende de proteger, dándole a la organización el plus de la facilidad y agilidad con que podríamos examinar y analizar lo que en tiempos y movimientos representa ganancias a la organización y por ende a los clientes o beneficiarios. La asignación de los recursos para el SGSI debe ser acorde con el tamaño y prioridades en la información a guardar, se deben disponer de los recursos necesarios, para que la ejecución sea óptima (Balaguer, 2014). En la figura 1, se presenta la evolución de la norma ISO 27001.

Figura 1. Evolución de la ISO 27001

Fuente: https://www.pmg-ssi.com/2014/11/iso-270012015-un-cambio-en-la-integracion-de-los-sistemas-de-gestion/

La implementación de la ISO 27001:2013, se establece bajo a estructura de alto nivel y presenta varias ventajas, entre las cuales se encuentran: la mejora la integración con otros sistemas de gestión, contribuye a la mitigación de los riesgos de seguridad en la información en conjunto, se indican todas las acciones preventivas que anteriormente no se estipulaban, establecimiento de una metodología para los flujos de información, mejora continua de los procesos de gestión de información; credibilidad y confianza de los usuarios y clientes externos como internos y control de fuga de información.

Igualmente se evidencian algunas desventajas como: que todos los requisitos son un tanto más difícil de interpretar, ya que se incorporan nuevos conceptos, no se estipula el enfoque que se da al ciclo PHVA, no se mencionan las políticas dentro del Sistema de Gestión de Seguridad de la Información, no se encuentra descripción detallada de la identificación de los riesgos.

Se puede encontrar un gran reto en la Gestión de la Seguridad de la Información con la nueva ISO 27001:2013, ya que los conceptos que debemos reforzar son: Partes interesadas, liderazgo, comunicación, sensibilización, capacidades, propietario del riego, activos, gestión de riesgos y oportunidades, entre muchos otros (ISO 27001:2013). En la tabla 2, se presenta la comparación de la norma NTC ISO 27001:2013 vs NTC 27001:2005 mostrando así la evolución de la norma.

Tabla 2. Comparativo NTC ISO 27001:2005 vs NTC ISO 27001:2013

MODIFICACIONES ISO 27001:2005 A ISO 27001:2013			
ISO 27001:2005		**ISO 27001:2013**	
NUMERAL	**ITEM**	**NUMERAL**	**ITEM**
1.	INTRODUCCIÓN	1.	INTRODUCCIÓN
2.	OBJETO	2.	OBJETO
3.	REFERENCIAS NORMATIVAS	3.	REFERENCIAS
4.	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
4.1	GENERAL	4.	CONTEXTO DE LA ORGANIZACIÓN
4.2	SGSI		
4.2.1	ESTABLECER	4.	CONTEXTO DE LA ORGANIZACIÓN
		6.	PLANIFICAR
4.2.2	IMPLEMENTAR Y OPERAR	8.	OPERACIÓN

4.2.3	MONITOREAR Y REVISAR	9.	EVALUACIÓN DEL DESEMPEÑO
4.2.4	MANTENER Y MEJORAR		
4.3	DOCUMENTAR	7.	SOPORTE
5	RESPONSABILIDAD DE LA DIRECCIÓN		
6.	AUDITORIA INTERNA	9.	EVALUACIÓN DEL DESEMPEÑO
7.	REVISIÓN POR LA DIRECCIÓN		
8.	MEJORA	10	MEJORA

Fuente: https://www.pmg-ssi.com/wp-content/uploads/2014/11/comparativa.jpg

4.1.4 Sistema de Gestión de la Calidad. La NTC ISO 9001:2015, permite que las organizaciones utilicen el enfoque a procesos, en concordancia con el ciclo PHVA y el pensamiento basado en riesgos, para armonizar los requisitos de la norma con otros sistemas de gestión.

Esta norma se complementa con la ISO 9000 Sistemas de gestión de la calidad – Fundamentos y vocabulario y la ISO 9004 Gestión para el éxito sostenido de una organización; las cuales suministran información necesaria para la comprensión y presenta las orientaciones que promueven mejores prácticas para su implementación y sostenibilidad.

Se encuentra enmarcada en los principios: enfoque al cliente, liderazgo, compromiso de las personas, enfoque a procesos, mejora, toma de decisiones basada en la evidencia y gestión de las relaciones.

Al estar basada en un enfoque a procesos promueve la eficiencia y eficacia del sistema de gestión de la calidad en las organizaciones, aumentando la satisfacción de los clientes a través del cumplimiento de los requisitos exigidos por ellos. Igualmente, la interrelación de los procesos permite el control de las actividades para el logro de los objetivos de la organización (NTC-ISO-9001:2015).

4.2 MARCO CONCEPTUAL

Con el fin de abordar el tema tratado en este trabajo, se relacionan algunos conceptos fundamentales e indispensables como: sistema de gestión, sistema de gestión de la calidad, sistemas integrados de gestión, sistema de gestión de seguridad de la información y ley de protección de datos.

4.2.1 Sistema de gestión. Según las normas ISO 9000:2015 es “conjunto de elementos interrelacionados o que interactúan”.

Acorde con Diez Figueroa y Vargas Herbozo (2019), “Un sistema de gestión es el conjunto de elementos interrelacionados de una organización o empresa utilizados para lograr los objetivos plasmados por la misma”. Estos componentes como son: procedimientos, instructivos, metodologías, guías entre otros, permiten la planificación, ejecución y control de las actividades para el logro de los objetivos.

4.2.2 Sistema de gestión de la calidad. “La calidad de los productos y servicios de una organización está determinada por la capacidad para satisfacer a los clientes, y por el impacto previsto y el no previsto sobre las partes interesadas pertinentes” (NTC-ISO 9000:2015). Esta no solo incluye el valor de la percepción y utilidad para el cliente sino además el cumplimiento de sus necesidades y expectativas.

La NTC-ISO 9000:2015 define el Sistema de Gestión de Calidad como “Parte de un sistema de gestión relacionada con calidad”. El sistema de gestión de la calidad promueve en las organizaciones un marco de referencia basado en el ciclo PHVA, mediante un enfoque a procesos y el pensamiento basado en riesgos, hacia la mejora continua para la satisfacción de las necesidades y expectativas del cliente y partes interesadas.

4.2.3 Sistemas de gestión integrados. Según Peralta Cruz y Guataqui Cervera (2017), “El Sistema Integrado de Gestión (SIG) es un proceso que tiene varias fases y que satisface los requisitos establecidos para un único sistema de gestión, con base en la política y los procedimientos, su implementación, el seguimiento, el control, las auditorías y las mejoras”. El SIG en las organizaciones contribuye para facilitar la integración de los sistemas y por ende su implementación, generando en el personal mayor confianza en su aplicabilidad.

Por otra parte, la articulación de los diferentes sistemas que componen la organización, logra que se tenga una perspectiva hacia la gestión eficaz y eficiente de los procesos, mediante la creación de estrategias claras que involucren a todo el personal de la empresa, de tal forma que se logre una permanente interacción entre las partes, con el fin de lograr el cumplimiento de los objetivos institucionales.

Por consiguiente, la propuesta metodológica de armonización o integración de la ley de tratamiento de datos personales, con los sistemas de gestión de la calidad y de seguridad de la información, se hace necesaria en las organizaciones colombianas, ya que esta herramienta permite que se generen mejores prácticas y la alineación de políticas y directrices que permitan el adecuado y seguro tratamiento de datos personales, de tal manera que se satisfagan las necesidades y expectativas de los usuarios y de igual forma se optimicen los recursos

humanos, financieros y tecnológicos en pro del logro de los objetivos de la organización (Tejada y Peña, 2009).

4.2.4 Sistema de gestión de seguridad de la información. El SGSI, parte del sistema de gestión global, basado en un enfoque hacia los riesgos de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Según la ISO/IEC 27001 el SGSI, "es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio". La seguridad de la información debe formar parte de la cultura de la organización y busca el aseguramiento de la confidencialidad, integridad y disponibilidad de los datos para minimizar los riesgos que comprometan las operaciones de la organización y amenacen la seguridad de la información.

4.2.5 Ley de protección de datos. La ley 1581 de 2012 se constituye en un marco de referencia en el que se establecen los parámetros del Régimen General de Protección de Datos en Colombia, siendo este un derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos.

Por otra parte, el decreto 1377 de 2013 establece la regulación de la ley 1581, teniendo en cuenta criterios que involucran el tratamiento de datos personales en aspectos tales como: la responsabilidad demostrada del tratamiento, la transferencia, el ejercicio de los derechos del titular de la información, las políticas de tratamiento de los responsables y encargados y la autorización del titular para su tratamiento.

Otro concepto a tener en cuenta es el de Armonización, referido al establecimiento de la intercambiabilidad de productos y procesos en normas, reglamentos técnicos y evaluaciones de la conformidad sobre un mismo asunto aprobados por distintos organismos. El objetivo del proceso es establecer requisitos idénticos en normas, reglamentos técnicos y evaluaciones de la conformidad (Ref. de la OMC modificada).

El Habeas Data, corresponde al derecho fundamental que tiene toda persona para conocer, actualizar y rectificar toda aquella información que se relacione con ella y que se recopile o almacene en centrales de información. Este derecho está regulado por el Artículo 15 de la Constitución Política de Colombia, desarrollado por la Ley 1266 de 2008.

Así mismo, según la Corte Constitucional, el núcleo esencial del habeas data se encuentra integrado por el derecho a la autodeterminación informática, entendiendo esto como la facultad de la persona, a autorizar la conservación, uso y circulación de sus datos y a la libertad, en especial la económica, ya que esta podría ser vulnerada en virtud de la circulación de datos que carezcan de veracidad o para los cuales no se haya autorizado su circulación.

Por lo anterior el Habeas significa tener, y data significa datos. Este es el derecho que poseen todas las personas de conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bancos de datos y los demás derechos libertades y garantías constitucionales, relacionadas con la recolección, tratamiento y circulación de datos personales.

De otra parte, se hace necesario, estipular la definición de los términos como:
Datos Sensibles: Son aquellos que afectan la intimidad del titular o cuyo uso indebido, puede generar su discriminación, tales como: aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos organizacionales sociales, de derechos humanos o que promuevan interés de cualquier partido político.

Información negativa son los datos que hagan referencia al tiempo de mora, tipo de cobro, estado de la cartera y de forma general, todos aquellos datos que se refieren a una situación de incumplimiento de obligaciones, estarán regidos por un término máximo de cuatro (4) años, a partir de la fecha en que sean pagadas las cuotas vencidas, o que se extinga la obligación por cualquier modo. Y de acuerdo a la Corte Constitucional, se estableció un plazo de permanencia del doble de la mora, para los deudores que presentaron mora inferior a dos (2) años y asumieron voluntariamente el pago de la obligación y plazo de permanencia será de (4) años cuando la mora máxima alcanzada fue superior a los (2) años.

Seguridadg de la Información se define como la preservación de la confidencialidad, integridad y disponibilidad de la información, además hay que considerar otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucrados.

Protección de datos personales se refiere a reservar el uso o tratamiento (Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.) de información. Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

De otro lado, el Sistema de Gestión de Calidad permite fortalecer las organizaciones para planear, realizar, controlar y buscar la mejora continua en el

desempeño de los procesos, basada en los principios de: enfoque al cliente, liderazgo, compromiso de las personas, enfoque a procesos, mejora, toma de decisiones basada en la evidencia y gestión de las relaciones.

4.3 MARCO LEGAL Y NORMATIVO

Acorde con la regulación normativa de la protección de datos y los sistemas de gestión de la calidad y de seguridad de la información para entidades públicas colombianas del nivel nacional y en referencia al objetivo del proyecto de investigación a continuación se describen las normas, leyes, decretos, resoluciones, circulares y demás que se relacionan con el tema tratado, en la tabla 3 se presenta el referente legal y normativo en el que se destacan en primera medida la constitución política, la ley 1581 de 2012 del régimen de protección de datos personales cuya aplicabilidad es reglamentada por el decreto 1377 de 2012, por otra parte las normas técnicas colombianas ISO 9001 e ISO 27001.

Tabla 3. Marco legal y normativo

N°	Norma	Descripción
1	Constitución política	Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
2	Constitución política	Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.
3	Ley 1581 de 2012	Es la ley de tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable o encargado del tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.
4	Ley estatutaria 1266 de 2008	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.
5	Ley 79 de 1993	Por la cual se regula la realización de los Censos de Población y Vivienda en todo el territorio nacional, donde se recogen datos personales.
6	Decreto 1122 de 1999	Por el cual se dictan normas para suprimir trámites, facilitar la actividad de los ciudadanos, contribuir a la eficiencia y eficacia de la Administración Pública y fortalecer el principio de la buena fe. El Decreto 1122 de 1999 fue declarado INEXEQUIBLE por la

		Corte Constitucional mediante Sentencia C-923-99 del 18 de noviembre de 1999, Magistrado Ponente Dr. Álvaro Tafur Galvis.
7	Decreto 2740 de 2004	Por el cual se establece la participación del sector educativo en el XVII censo nacional de población y VI de vivienda a realizarse en 2005.
8	Conpes 3276	El presente documento reitera la importancia y necesidad del censo como herramienta básica para el manejo eficiente de los problemas del país, y da cuenta, además, de las características esenciales del mismo. Especifica también el avance, estado actual y perspectivas de la programación adoptada; relaciona el monto de recursos ejecutado hasta el presente y la inversión pendiente para las próximas vigencias en la ejecución, producción y difusión de sus resultados.
9	Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012
10	Decreto 1074 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.
11	Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
12	Circular 003 de 2018	Modificar los numerales 2.1 y 2.4 y eliminar los numerales 2.5 al 2.7 del capítulo segundo del título V de la circular única de la Superintendencia de Industria y Comercio
13	Conpes 3920	Política Nacional de explotación de datos (Big Data)
14	Ley 1712 de 2014	Por medio del cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional.
9	NTC ISO 27001	Esta es la especificación de un sistema de gestión de seguridad de la información (SGSI), que sustituyó a la antigua norma BS7799-2

Fuente: Elaboración propia (2021).

5. METODOLOGÍA

La metodología que se plantea para el logro de los objetivos propuestos incluye el enfoque de la investigación, el alcance y fases de investigación, definición de variables o categorías, escenario de estudio, los instrumentos y técnicas usadas para la recolección de la información.

5.1. ENFOQUE DE LA INVESTIGACIÓN

La metodología empleada para el desarrollo de esta investigación responde a un enfoque de tipo mixto que se basa en la “Recolección y análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta” (Hernández - Sampieri y Mendoza, 2018, p 42). Igualmente, Creswell (2008), argumenta que la investigación mixta permite integrar en un mismo estudio, metodologías cuantitativas y cualitativas, con el propósito de que exista mayor comprensión acerca del objeto de estudio.

Es un estudio mixto secuencial con preponderancia cualitativa. Es secuencial porque conlleva la recopilación y análisis de datos tanto cuantitativos, seguido de la recopilación y el análisis de datos cualitativos y estos datos se combinan en la fase de análisis del proyecto de investigación (Hernández - Sampieri y Mendoza, 2018, p 613).

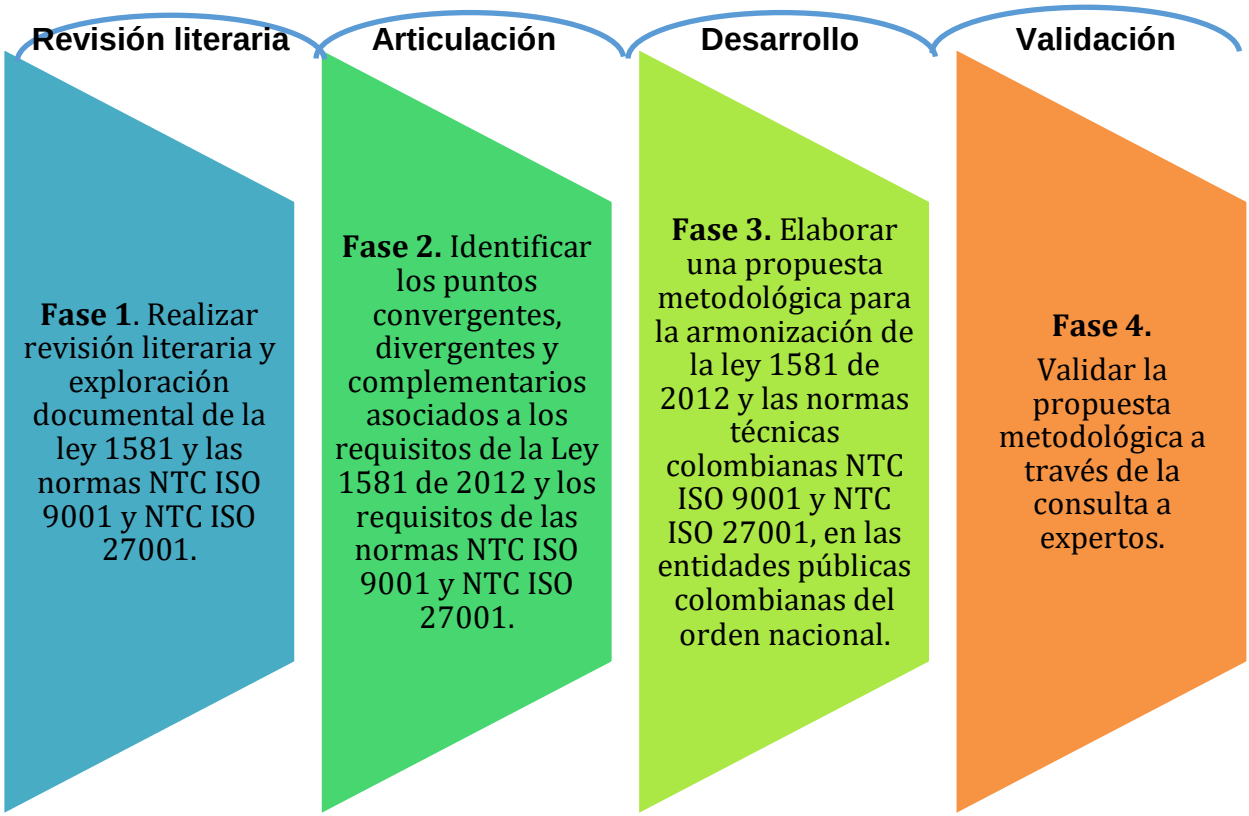
5.2 ALCANCE Y FASES DE LA INVESTIGACIÓN

Esta investigación tiene un alcance de tipo descriptivo, pues se considera como base de estudio la ley 1581 de 2012 y los puntos adyacentes a las normas NTC ISO 9001 y NTC ISO 27001, definiendo así los conceptos legales enlazados con los requisitos establecidos en las normas técnicas.

Lo anterior conlleva a elaborar una propuesta metodológica para la armonización de la ley 1581 de 2012 y las normas técnicas NTC ISO 9001 y NTC ISO 27001, en las entidades públicas colombianas del orden nacional, partiendo los puntos en convergentes, divergentes y complementarios de la ley con las normas técnicas.

5.2.1 Fases o etapas del proyecto. De acuerdo con el marco referencial y la literatura acerca del tema de investigación se plantean las fases de revisión literaria, articulación, elaboración y validación. En la figura 2, se presentan las fases del proyecto, acorde con los objetivos de la investigación.

Figura 2. Fases del proyecto



Fuente Elaboración propia

5.2.1.1 Fase 1 revisión bibliográfica. Realizar revisión literaria y exploración documental de la ley 1581 y las normas NTC ISO 9001 y NTC ISO 27001. Para esta fase del proyecto se toma como base la revisión bibliográfica y literaria realizada para el artículo "Protección de datos y su articulación con la gestión de calidad" (Acero, et al., 2021)

Donde las palabras claves para la búsqueda literaria fueron sistema de gestión y protección de datos, habeas data y seguridad de la información, Se consultaron bases de datos como Elsevier, Core, Redalyc, Scielo, Signos, Uned, Microsoft Académico, Facultad de Ciencias de la Información, Revista del Instituto Jurídico de Puebla México, Revista Jurídica Unam, Revista Latinoamericana, Serie Bibliotecología y Gestión de Información, International Data Privacy Law, repositorios de universidades latinoamericanas y europeas y normas legales nacionales, como principales herramientas para la selección de artículos insumo.
La revisión literaria se hace con el objetivo de analizar los diferentes contextos que se puedan presentar frente a la ley 1581 y la articulación con las normas NTC ISO 9001 y NTC ISO 27001, de esta forma las investigaciones que realizaron los autores contribuye a recolectar, seleccionar toda la evidencia disponible asociada

a protección de datos personales y su articulación con los sistemas de gestión de calidad y de seguridad de la información ayudando a enriquecer los ejemplos de metodologías y las aplicaciones de alguno de los lineamientos aplicables a la ley que se pueden tomar como referencia en el desarrollo de los objetivos del proyecto.

5.2.1.2 Fase 2 articulación. Se identificó los puntos convergentes, divergentes y complementarios asociados a los requisitos de la Ley 1581 de 2012 y los requisitos de las normas NTC ISO 9001 y NTC ISO 27001.

Se estructuro una matriz de armonización, ésta tiene como objetivo identificar los requisitos convergentes los cuales se definen cuando por lo menos la ley y una de las normas tienen algo en común, divergentes cuando no hay nada en común entre las tres categorías y complementarios cuando se permite la aplicación de la ley 1581 del 2012 con cualquiera de las normas NTC ISO 9001 y NTC ISO 27001, basados en la metodología del ciclo PHVA, adicionalmente permitió definir las herramientas e instrumentos que gestionaran la aplicación para la armonización de la ley y las dos normas, y así dar cumplimiento a los respectivos requisitos.

5.2.1.3 Fase 3 propuesta desarrollo. Se elaboró una propuesta metodológica para la armonización de la ley 1581 de 2012 y las normas técnicas colombianas NTC ISO 9001 y NTC ISO 27001, en las entidades públicas del orden nacional.

Mediante la información resultado de la revisión bibliográfica, y una vez realizado el análisis de la matriz de armonización se elabora la propuesta metodológica para la armonización de la ley 1581 de 2012 y las NTC ISO 9001 y 27001, en la cual se muestra el paso a paso de cómo se deben armonizar de la ley de protección de datos a las normas del sistema de gestión de la calidad y sistema de seguridad de la información, esta propuesta metodológica se realiza teniendo en cuenta el ciclo PHVA del cual se extraen los puntos más relevantes y se proponen estrategias y recomendaciones para su aplicabilidad.

5.2.1.4 Fase 4 validación. En esta fase se validó la propuesta metodológica a través de la consulta a expertos. Se realizó adaptación de un instrumento de encuesta de validación en el cual se valoran tres aspectos relacionados con la claridad, pertinencia y aplicabilidad de la propuesta metodológica, y se efectuará aplicación del instrumento con el fin de evaluar la pertinencia de la propuesta.

Luego de obtener la evaluación por parte de los expertos se consolida la información, se realiza la automatización y análisis, luego se realizan los ajustes a que haya lugar, teniendo en cuenta la calificación obtenida de los expertos.

Se presentó un panel de 5 expertos con los siguientes perfiles: un magister en Administración Pública, un especialista en sistemas de gestión de la calidad, dos magister en calidad y gestión integral, un magister en docencia e investigación con énfasis en ingeniería.

Por último, se presenta el resultado final de la propuesta y se registran las conclusiones en el documento final de la investigación.

5.3 DEFINICIÓN DE VARIABLES O CATEGORÍAS

A continuación, se presentan las variables o categorías para la armonización de la ley de protección de datos personales y las normas de sistemas de gestión de la calidad y sistema de seguridad de la información. En la tabla 4, se observan las variables objeto de estudio:

Tabla 4.Definición categorías

Categorías	**Definición de la categoría**
Ley 1581 de 2012	Es el mandato legal que ordena el desarrollo del derecho constitucional de los colombianos a conocer, actualizar y rectificar la información que exista en bases de datos (Constitución Política de Colombia, 1991).
Sistema de Gestión de la Calidad NTC ISO 9001	Es un sistema de gestión adoptado por una organización que le permite mejorar la mejora de sus productos y servicios y promueve decisiones que contribuyen al desarrollo sostenible a través de la satisfacción del cliente (ISO 9001:2015).
Sistema de Gestión de Seguridad en la Información NTC ISO 27001	Este sistema de gestión proporciona a las organizaciones los requisitos necesarios para establecer, implementar y mantener un sistema de gestión de la seguridad de la información, de acuerdo a los requisitos necesarios para la preservación de la confidencialidad, integridad y disponibilidad de la información (NTC ISO 27001).

Fuente: Elaboración propia (2021)

5.4 ESCENARIO DE ESTUDIO

La metodología propuesta se orienta a las entidades públicas colombianas del nivel nacional, con el fin de dar cumplimiento a la normativa vigente en materia de protección de datos y su articulación con los modelos de gestión de la calidad y de seguridad en la información, mediante la propuesta para la estructuración de

buenas prácticas para promover la confidencialidad, disponibilidad e integridad de la información y de esta manera proteger los datos de los usuarios.

Adicionalmente el cumplimiento de los requisitos evita riesgos de tipo económico, reputacional y otros que puedan afectar el cumplimiento de los objetivos de las entidades.

5.5 INSTRUMENTOS Y TÉCNICAS DE INVESTIGACIÓN

Acorde con los objetivos específicos señalados en el presente trabajo, se presentan los instrumentos y técnicas de investigación que se realizaron para la recopilación de la información, para lo cual se propone revisar como instrumento una matriz en la cual se comparan los requisitos de la ley 1581 y las normas técnicas colombianas ISO 9001 e ISO 27001, resultado del análisis se establece la metodología para su integración y finalmente como instrumento de validación se adaptó un instrumento para la validación por parte de expertos de la metodología propuesta. En la tabla 5 se presentan los instrumentos y técnicas de la presente investigación.

Tabla 5.Despliegue de objetivos

Objetivos	Instrumentos	Descripción o producto
Identificar los puntos convergentes, divergentes y complementarios asociados a los requisitos de la Ley 1581 de 2012 y los requisitos de las normas NTC ISO 9001 y NTC ISO 27001.	Matriz comparativa de la ley y requisitos de las normas.	Se diseñó una matriz comparativa teniendo como base la ley 1581 de 2012, a partir de la cual identificó la aplicación del ciclo PHVA y la estructura de alto nivel y sus divergencias, convergencias y complementariedades con las normas NTC ISO 9001 y 27001.
Elaborar una propuesta metodológica para la armonización de la ley 1581 de 2012 y las normas técnicas colombianas NTC ISO 9001 y NTC ISO 27001, en las entidades públicas colombianas del orden nacional.	Metodología de armonización basada en el ciclo PHVA.	Una vez elaborada la matriz de articulación, se procede a estructurar la metodología que permita a las entidades públicas colombianas del orden nacional cumplir con los requisitos de la ley de protección de datos y armonizar con los requisitos de los sistemas de gestión de la calidad y la seguridad de la información.
Validar la propuesta metodológica a través de la consulta a expertos.	Instrumento de validación con panel de expertos. Metodologías estadísticas para el análisis de resultados.	Se estableció un panel de expertos teniendo en cuenta su experiencia y conocimiento en la ley 1581 de 2012, NTC ISO 9001, NTC ISO 27001, quienes validaron la aplicabilidad de la propuesta metodológica resultado de la presente investigación.

Elaboración propia (2022)

6. RESULTADOS Y DISCUSIÓN DEL PROYECTO

Para plantear el desarrollo de la propuesta metodología de Armonización de los requisitos ley 1581, NTC-ISO 9001:2015 y NTC-ISO 27001:2015, se identificaron los puntos convergentes, divergentes y complementarios asociados a los requisitos de la Ley 1581 de 2012 y los requisitos de las normas NTC ISO 9001 y NTC ISO 27001, con el fin de clasificar los requisitos de la norma con respecto al ciclo planear, hacer, ejecutar y actuar.

Inicialmente se hizo la identificación estructurada de la ley 1581 la cual está compuesta por nueve títulos así: Título I, se describen el objeto, ámbito de aplicación y definiciones, Título II se estipulan los principios rectores, Título III se establecen las categorías especiales de datos, Título IV se enmarca en los derechos y condiciones de legalidad para el tratamiento de datos, Título V se refiere a los procedimientos para atender las consultas y/o reclamos, Titulo VI presenta los deberes de los responsables del tratamiento y encargados del tratamiento, Título VII mecanismos de vigilancia y sanción, Título VIII transferencia de datos a terceros países, Título IX otras disposiciones como normas corporativas vinculantes, régimen de transición, derogatoria y vigencia.

Una vez identificada la estructura de la ley, el análisis se orientó hacia el ciclo PHVA, donde se clasificaron los requisitos de las normas técnicas ISO 9001 e ISO 27001 dependiendo de si las actividades podrían apalancar a la ley, se identificaron criterios de convergencia, divergencia y complementariedad.

Teniendo en cuenta los criterios anteriormente mencionados, se propuso una herramienta de aplicación para cada fase del ciclo PHVA. en el planear, en el hacer, en el verificar y en el actuar.

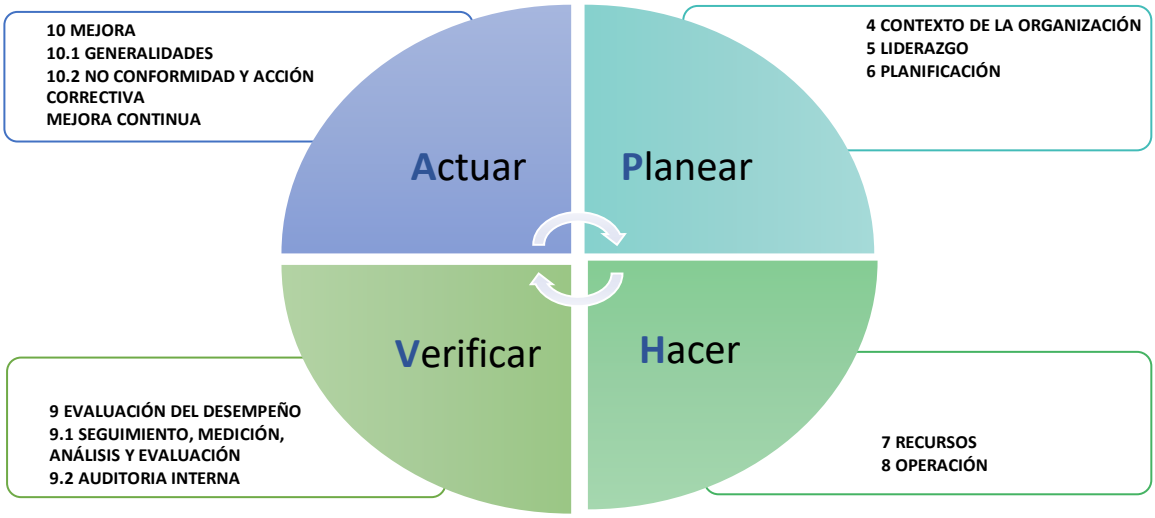
6.1. ARMONIZACIÓN DE LOS REQUISITOS LEY 1581, NTC-ISO 9001:2015 Y NTC-ISO 27001:2015

Como se mencionó anteriormente la propuesta de la metodología desarrollada se basó en el ciclo PHVA (Planear, Hacer, Verificar y Actuar); donde se proponen las herramientas por cada etapa del ciclo y se aplicó a los requisitos comunes entre la ley y las normas NTC ISO 9001:2015 y NTC ISO 27001:2013. Se hizo bajo esta forma de armonización puesto que la ley no tiene estructura de alto nivel y como se partió de la ley se observó que la estructura más idónea era por medio del ciclo de PHVA.

La estructura de alto nivel a la que corresponde las normas NTC ISO 9001:2015 y NTC ISO 27001:2013 tienen su punto de encuentro en el ciclo de esta forma: El

planear que corresponde al Contexto de la organización, Liderazgo, Planificación y Soporte del sistema; el **Hacer** corresponde a la Operación el cual se encamino al talento humano; el **Verificar** a la Evaluación del desempeño. El **actuar** a la mejora; a continuación, se muestra gráficamente esta estructura basados en la NTC ISO 9001:2015 de esta forma se estructuraron las herramientas que se proponen para el apalancamiento de la ley a través de las normas técnicas, donde aquellos requisitos divergentes y complementarios, se abordan desde los lineamientos regulatorios de cada norma específica.

Gráfica 1.Ciclo PHVA



Fuente: NTC ISO 9001:2015

Partiendo de la ley 1581 se determinaron los criterios de convergencia (por lo menos la ley y una norma tienen algo en común), divergencia (nada en común) y complementariedad (permiten aportar al cumplimiento de la aplicación de la ley); asociados a las normas, los cuales se relacionan en la matriz armonización ley 1581_ISO 9001_ISO 27001 anexo A.

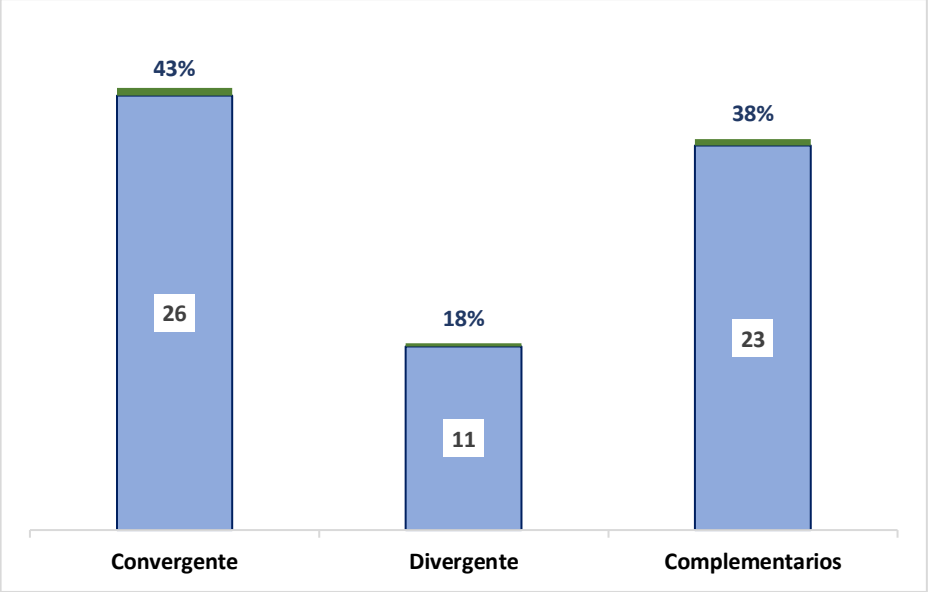
Como resultado se obtuvo un total de 60 requisitos analizados y se encontró que la ley de protección de datos converge en 26 ítems que corresponden al 43% los cuales tienen un enfoque hacia el hacer con el planear, teniendo en cuenta la tendencia de estos ítems de convergencia desde el ciclo PHVA llevaron a buscar herramientas de aplicación que fueran guía para las empresas y así realizar una visión desde el contexto de la organización hasta la planeación de los requisitos a tener en cuenta de la ley apalancados con la normas.

Se encontraron 11 ítems divergentes equivalentes al 18%, que difieren entre sí por ser específicos y técnicos de la ley y cada norma. Dentro los puntos divergentes se encuentra una tendencia hacia el hacer donde se planeó herramientas orientadas a la toma de conciencia, al sistema de comunicación que apalanque a las organizaciones a tener una política de protección de datos efectiva y clara donde la comunicación interna y externa es clara.

Finalmente se pudo evidenciar 23 ítems correspondientes al 38% son complementarios y aportan valor en la aplicación de ley 1581, en estos puntos de complementariedad se pudo observar una tendencia hacia el planear seguido del actuar donde el contexto de la organización junto con las estrategias para implementación de unas acciones de mejoran son la principal aplicación desde los elementos complementarios.

De acuerdo con la matriz comparativa de requisitos en la gráfica 2 se presenta el porcentaje de resultado acorde con los criterios establecidos:

Gráfica 2. Requisitos convergentes, divergentes y complementarios



Fuente: Matriz de armonización – Anexo A

A partir de este análisis se pudo evidenciar que es posible apalancar la ley 1581 en promedio del 80% de su contenido con las normas NTC ISO 9001:2015 y NTC ISO 27001:2013. Desde estrategias del planear y el hacer tomando los puntos convergentes y complementarios.

Tabla 6. Resultado requisitos convergentes, divergentes y complementarios

Requisitos	No.	%	P	H	V	A	Total
Convergentes	26	43%	11	12	1	2	26
Divergente	11	18%	1	7	2	1	11
Complementarios	23	38%	9	7	3	4	23
Total	**60**	100%	**21**	**26**	**6**	**7**	**60**

Fuente: Elaboración propia (2022)

Se propuso para la implementación de la metodología propuesta herramientas que permitieron dar respuesta a los requisitos desde el ciclo PHVA, teniendo en cuenta que la tendencia de la armonización estaba orientada a principios que van desde la planeación y el hacer como mayoritarios apalancadores; en la tabla 7, se presenta una relación de las herramientas para su aplicación desde los frentes del ciclo teniendo en cuenta la metodología usada.

Tabla 7. Herramientas de armonización

Ciclo PHVA	Requisitos			Herramienta
	Ley 1581	ISO 9001:2015	ISO 27001:2013	
Planear	N/A	4.1 Comprensión de la organización y de su contexto	4.1 Comprensión de la organización y de su contexto	Anexo J. Matriz DOFA
	Artículo 14	N/A	9.1 Requisitos del negocio para control de acceso.	Anexo C. Política de seguridad de la información datos personales
Hacer	Artículo 15 Reclamos	N/A	H Anexo A 18.1.4 Privacidad y protección de información de datos personales.	Anexo D. Formato Autorización de tratamiento de datos personales
				Anexo E. Lista chequeo seguridad de la información
	Artículo 26 Prohibición	7.1 Recursos 7.2. Competencia 7.3. toma de conciencia 7.4 comunicación 7.5. información documentada 5.1.1 Políticas para la	7.1 Recursos 7.2 Competencia 7.3 toma de conciencia 7.4 comunicación 7.5. información	Anexo F. Plan de formación y capacitación
				Anexo G. Proceso de comunicación

		seguridad de la información 5.2 Política	documentada 5.1.1 Políticas para la seguridad de la información 5.2 Política	
				Anexo H. Matriz del plan de comunicación interna y externa
				Anexo I. Mapa conceptual toma de conciencia
Verificar	N/A	9.2. Auditoria interna	9.2. Auditoria interna	Anexo K. Procedimiento de auditorias
				Anexo L. Formato plan de auditoria
				Anexo M. Formato Informe de auditoría
				Anexo N. Formato lista de verificación
Actuar	N/A	10. Mejora continua	10. Mejora	Anexo O. Procedimiento de planes de mejoramiento
				Anexo P. Formato del plan de mejoramiento

Elaboración propia fuente matriz de armonización

6.1.1. Planear. Los requisitos convergentes fueron los mayoritarios en la etapa del planear con un 46 % y se evidencio que la Ley se puede complementar en 38% con las normas articuladas para generar estrategias desde el planear.

Para poder hacer una planeación estratégica se identifica el contexto, en factores como el económico, el social, el ambiental, el tecnológico y en especial para esta investigación el factor legal (ley 1581), adicionalmente es importante tener presente las partes interesadas como alta dirección, funcionarios, contratistas, entidades estatales, proveedores y población beneficiaria de acuerdo a la misionalidad de la entidad, es por eso que se usó en la guía metodológica propuesta una herramienta que permite ver la realidad de las organizaciones como la matriz DOFA donde se pretende que las organizaciones identifiquen como se encuentran frente a los requisitos de la ley de protección de datos y así poder actuar frente a las debilidades, amenazas y actuar sobre ellas, aprovechar las

oportunidades y potenciar las fortalezas que puedan llegar a surgir para así establece la política con objetivos y estrategias que contemplen lineamientos asociados a la seguridad de los datos personales. De esta etapa surgen dos herramientas, la matriz DOFA y una plantilla de política de seguridad de la información que contiene los principales aspectos que las organizaciones deben tener presenten en sus objetivos organizacionales.

6.1.1.1 Matriz DOFA. Se propuso el instrumento matriz DOFA como herramienta del análisis del contexto interno y externo, donde se estableció un instructivo para su aplicación. Al hacer una relación de las debilidades, oportunidades, amenazas y fortalezas se puede tomar mejores decisiones frente a las organizaciones; es por esto se propuso en el desarrollo de la herramienta de armonización la matriz DOFA para la etapa de planear.

Figura 3. Matriz DOFA

	Factores externos		
	DOFA	OPORTUNIDADES	AMENAZAS
		Se refieren a factores externos favorables que podrían dar a una organización una ventaja competitiva. Como puede ser la facilidad para la recolección de datos entre otros	áreas que tienen el potencial de causar problemas. Difieren de las debilidades en que las **amenazas** son externas y, por lo general, están fuera de nuestro control. Pueden ser eventos como la veracidad de la información dada por los usuarios.
Factores internos	FORTALEZAS	ESTRATEGIA **FO**	ESTRATEGIA **FA**
	Aspectos positivos internos como la gestión del tratamiento de datos dentro de una organización		
	DEBILIDADES	ESTRATEGIA DO	ESTRATEGIA **DA**
	son aquellos factores que provocan una posición desfavorable frente a la aplicación de la ley, habilidades que no se poseen, actividades que no se desarrollan positivamente. Como el análisis de riesgo en un consentimiento mal elaborado.		

Fuente: Material clase Módulo Gerencia Estratégica

Ver anexo J. Matriz DOFA

6.1.1.2. Política de seguridad de la información. Las políticas de seguridad son mecanismos que permiten o restringen el acceso a la información. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y seguridad de la información. En este caso el acceso de los

titulares a la información personal. Anexo D. (Informativo), de la GTC-ISO/IEC 27003 Guía de implementación de un sistema de gestión de seguridad de la información, Estructura de las políticas de seguridad.

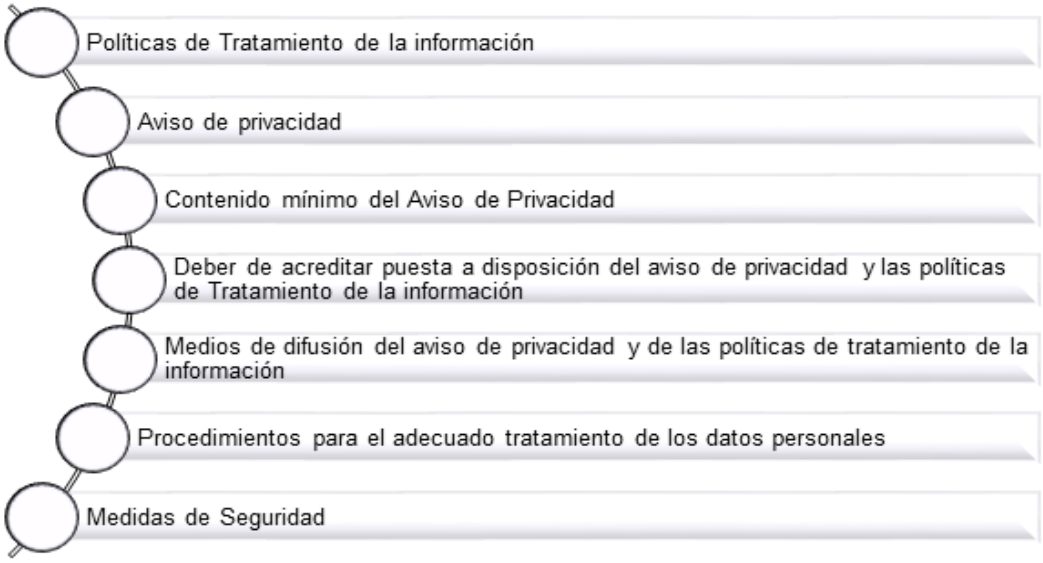
La ISO 27001 establece los requisitos para la implementación de un sistema de gestión de la seguridad de la información en una organización, en el cual se busca preservar la confidencialidad, integridad y disponibilidad de la información a través de un enfoque en gestión de riesgos, generando confianza en los usuarios.

Con respecto a la política de seguridad de la información de datos personales, estos deben tener una protección especial para su uso, se hace necesario el establecimiento de políticas de seguridad que salvaguarden la Integridad, disponibilidad, confidencialidad, autenticidad y trazabilidad de la información.

Al establecer una política de protección de datos se requiere estar alineados con la normatividad en la materia en este caso la ley 1581 y apalancarse con las normas SGC y SGSS, para de esta forma fortalecer la seguridad de la información.

Es necesario integrar la política de tratamiento de la información acorde con lo establecido en los artículos del 13 al 19, capítulo III del decreto 1377 Políticas de tratamiento, la cual debe estar escrita en un lenguaje claro, estar a disposición de los titulares y ser documentada ya sea en medio electrónico o físico. En la figura 3 se presentan los apartados que se requieren para las políticas de tratamiento:

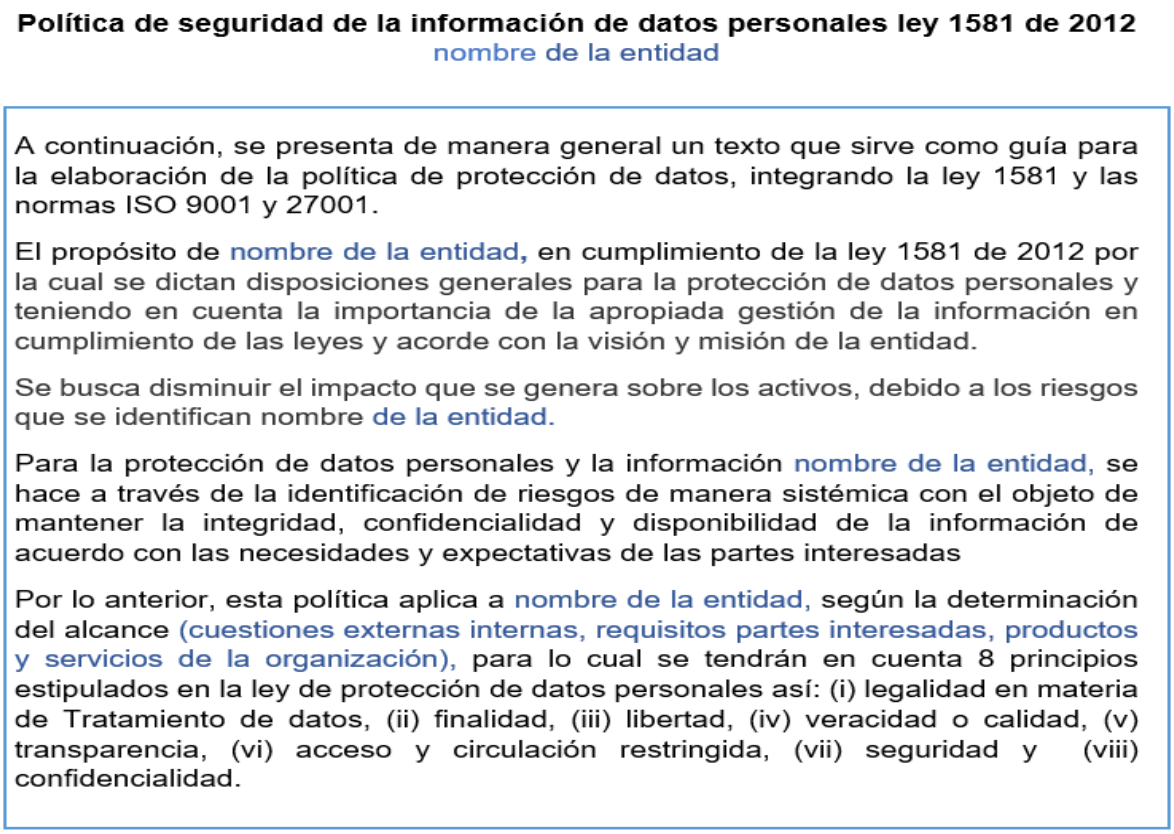
Figura 4. Políticas de Tratamiento



Fuente: Elaboración propia Decreto 1377 de 2013

En el Anexo C, Documento Política de seguridad de la información datos personales, se detallan los elementos que la conforman y se presenta un modelo de elaboración, el cual se puede adaptar acorde con el contexto de la organización.

Figura 5. Política de seguridad de la información de datos personales



Política de seguridad de la información de datos personales ley 1581 de 2012
nombre de la entidad

A continuación, se presenta de manera general un texto que sirve como guía para la elaboración de la política de protección de datos, integrando la ley 1581 y las normas ISO 9001 y 27001.

El propósito de nombre de la entidad, en cumplimiento de la ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales y teniendo en cuenta la importancia de la apropiada gestión de la información en cumplimiento de las leyes y acorde con la visión y misión de la entidad.

Se busca disminuir el impacto que se genera sobre los activos, debido a los riesgos que se identifican nombre de la entidad.

Para la protección de datos personales y la información nombre de la entidad, se hace a través de la identificación de riesgos de manera sistémica con el objeto de mantener la integridad, confidencialidad y disponibilidad de la información de acuerdo con las necesidades y expectativas de las partes interesadas

Por lo anterior, esta política aplica a nombre de la entidad, según la determinación del alcance (cuestiones externas internas, requisitos partes interesadas, productos y servicios de la organización), para lo cual se tendrán en cuenta 8 principios estipulados en la ley de protección de datos personales así: (i) legalidad en materia de Tratamiento de datos, (ii) finalidad, (iii) libertad, (iv) veracidad o calidad, (v) transparencia, (vi) acceso y circulación restringida, (vii) seguridad y (viii) confidencialidad.

Fuente: Elaboración propia basada en ley 1581

En el anexo C, se encuentra el formato editable.

6.1.2. Hacer.

Como resultado de la articulación se evidencio que los mayores requisitos articulados de la ley a las normas son de la etapa del hacer en un 43 % donde estos son en gran mayoría convergentes en un 46 % de los requisitos de la etapa del hacer y los complementarios están en un 26% del total de los 26 requisitos de esta etapa.

El hacer se fundamenta en la implementación de las acciones que se requieran para el logro de las mejoras propuestas que optimizan los resultados y subsanan posibles errores en la ejecución. Es necesario que para el control de los procesos se determine la información documentada requerida para permitir la trazabilidad de los mismos.

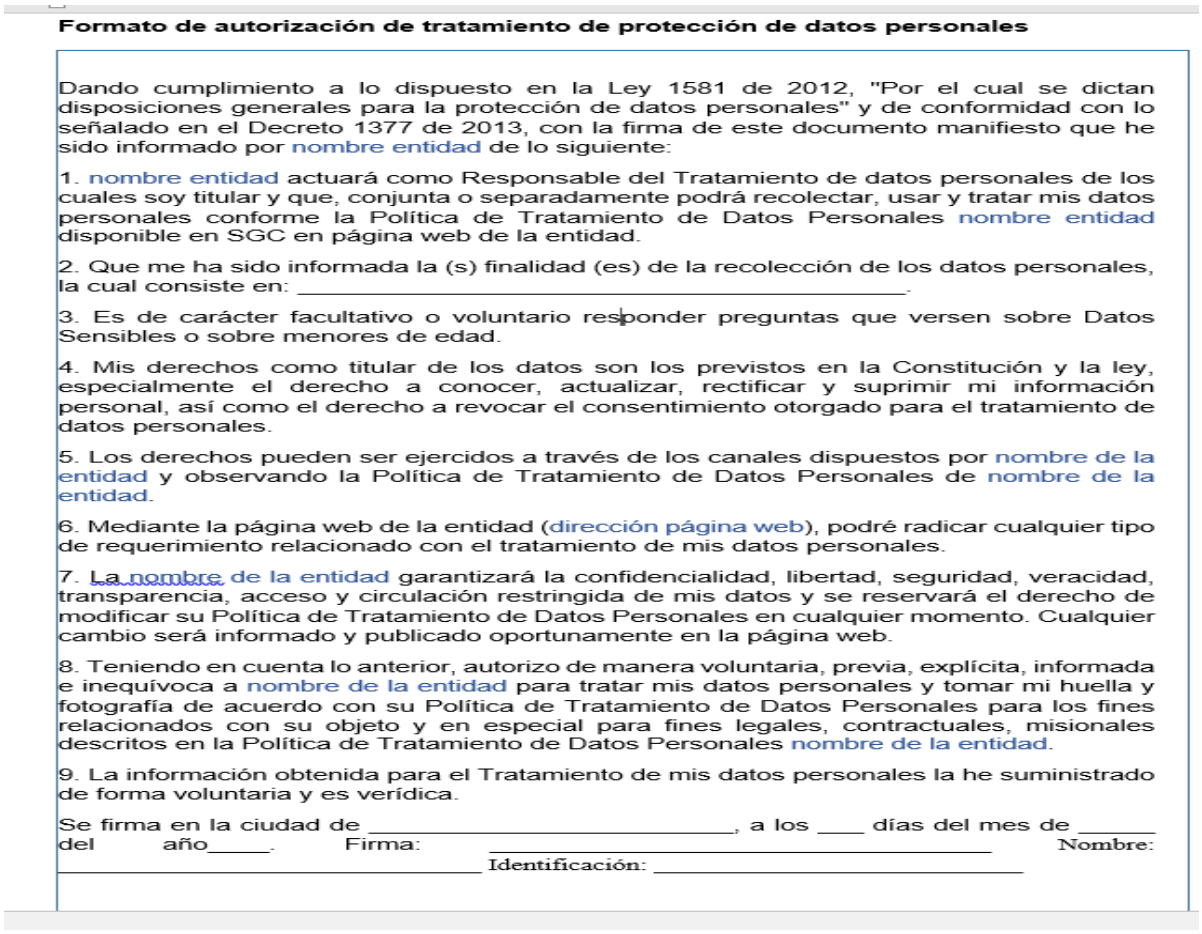
Para el hacer se presenta como herramientas seis formatos: Autorización de tratamiento de protección de datos personales, lista chequeo seguridad de la información, plan de formación y capacitación, flujo de proceso de comunicación y matriz del plan de comunicación interna y externa; las cuales ayudaran a las organizaciones a mejorar la comunicación entre los procesos sin dejar a un lado los parámetros que se deben tener en cuenta en cada uno de estos, a continuación una breve reseña de cada una.

Se requiere apoyo de la alta dirección para contar con la asignación de recursos económicos considerables, que se van a ver reflejados en el impacto de las entidades, esto a través de un enfoque basado en procesos y en riesgos de tal manera que se puedan superar los incidentes que se llegaran a presentar en el desarrollo de las tecnologías de la información.

Para dar cumplimiento a lo establecido en el artículo 15, título V de la ley 1581, procedimientos. La organización como responsable del tratamiento de datos personales tendrá que establecer el procedimiento para la solicitud de la información en el momento en que se recolectan los datos, de tal forma que se informe al titular el tratamiento de los mismos, por lo tanto, es necesario su autorización. Se propone el formato Autorización de tratamiento de protección de datos personales y la lista chequeo seguridad de la información.

6.1.2.1. Autorización de tratamiento de datos personales. Conforme con el literal g, artículo 4, título II, de la ley 1581, dentro de los principios rectores se encuentra el principio de seguridad, las organizaciones están llamadas a adoptar medidas tanto humanas, técnicas y administrativas para otorgar la seguridad a esos datos personales, enfocados a evitar la adulteración, pérdida, consulta uso o acceso no autorizado o fraudulento es decir evitar incidente de seguridad. Con el fin de contribuir tanto con la autorización de los datos y la seguridad de los mismos se propone en la figura 6, modelo de formato de autorización.

Figura 6. Autorización de tratamiento de protección de datos personales



Formato de autorización de tratamiento de protección de datos personales

Dando cumplimiento a lo dispuesto en la Ley 1581 de 2012, "Por el cual se dictan disposiciones generales para la protección de datos personales" y de conformidad con lo señalado en el Decreto 1377 de 2013, con la firma de este documento manifiesto que he sido informado por nombre entidad de lo siguiente:

1. nombre entidad actuará como Responsable del Tratamiento de datos personales de los cuales soy titular y que, conjunta o separadamente podrá recolectar, usar y tratar mis datos personales conforme la Política de Tratamiento de Datos Personales nombre entidad disponible en SGC en página web de la entidad.

2. Que me ha sido informada la (s) finalidad (es) de la recolección de los datos personales, la cual consiste en: _____.

3. Es de carácter facultativo o voluntario responder preguntas que versen sobre Datos Sensibles o sobre menores de edad.

4. Mis derechos como titular de los datos son los previstos en la Constitución y la ley, especialmente el derecho a conocer, actualizar, rectificar y suprimir mi información personal, así como el derecho a revocar el consentimiento otorgado para el tratamiento de datos personales.

5. Los derechos pueden ser ejercidos a través de los canales dispuestos por nombre de la entidad y observando la Política de Tratamiento de Datos Personales de nombre de la entidad.

6. Mediante la página web de la entidad (dirección página web), podré radicar cualquier tipo de requerimiento relacionado con el tratamiento de mis datos personales.

7. La nombre de la entidad garantizará la confidencialidad, libertad, seguridad, veracidad, transparencia, acceso y circulación restringida de mis datos y se reservará el derecho de modificar su Política de Tratamiento de Datos Personales en cualquier momento. Cualquier cambio será informado y publicado oportunamente en la página web.

8. Teniendo en cuenta lo anterior, autorizo de manera voluntaria, previa, explícita, informada e inequívoca a nombre de la entidad para tratar mis datos personales y tomar mi huella y fotografía de acuerdo con su Política de Tratamiento de Datos Personales para los fines relacionados con su objeto y en especial para fines legales, contractuales, misionales descritos en la Política de Tratamiento de Datos Personales nombre de la entidad.

9. La información obtenida para el Tratamiento de mis datos personales la he suministrado de forma voluntaria y es verídica.

Se firma en la ciudad de _____, a los ____ días del mes de _____ del año_____. Firma: _____ Nombre: _____ Identificación: _____

Fuente: Elaboración propia basada en ley 1581

En el anexo D, se encuentra el formato editable.

6.1.2.2. Lista chequeo seguridad de la información. Se propone determinar el grado de comprensión que la organización tiene sobre el tema de seguridad y protección de datos personales, por medio de la herramienta “lista de chequeo en protección de datos”.

Con la cual se obtuvo un diagnóstico en materia de seguridad de la información, en cuanto a si hay una cultura de seguridad de la información, tratamiento de los datos, tecnologías que se aplican, sistemas de Sistemas de gestión documental, medidas que se utilizan para la protección, recuperación y seguridad de la información.

Esta herramienta sirve de guía para los responsables de la protección de datos, en cuanto al diseño del programa del cumplimiento legal específico y permite tener un diagnóstico real de la organización. Tomando como fuente la NTC-ISO-IEC 27001:2013 A.9.1, en la figura 7 se muestra parcialmente el formato de lista de chequeo.

Figura 7. Lista de chequeo seguridad de la información en protección de datos personales

Entidad Pública de orden nacional			**Código**
Proceso Seguridad de la información datos personales			
Objetivo del control. Realizar diagnóstico del acceso a la seguridad de la información			
Cuestionario			
Pregunta	**SI**	**NO**	**N/A**
¿Se tienen definidas políticas para la seguridad de la información personal, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes?			
¿Se realiza revisión a intervalos planificados y se establece control a las políticas para la seguridad de la información, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas?			
¿Se cuenta con política de privacidad y tratamiento de datos?			
¿Se tienen claves de acceso a redes y a servicios en red?			
¿Se tiene establecido un proceso de gestión de acceso de usuarios ?			
¿Se cuenta con áreas seguras para prevenir el acceso físico no autorizado, el daño y a información y a las instalaciones de procesamiento de información de la organización?			
¿Se tienen disponibles los equipos y se previene la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización?			
¿Se establecen los procedimientos documentados operacionales y responsabilidades para asegurar que las operaciones sean correctas y seguras?			
¿Se asegura la protección de la información y las instalaciones contra códigos maliciosos?			
¿Se realizan backups periódicos para proteger contra pérdida de datos?			
¿Se cuenta con un software operacional que asegure la integridad de los sistemas operacionales?			
¿Se asegura la protección de los datos usados para pruebas?			
¿Se mantiene el nivel de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores?			
¿Se tiene establecido el tratamiento a la gestión de incidentes de seguridad de la información ?			
¿Se da cumplimiento a los requisitos legales y contractuales acorde con las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad?			
¿Se realizan revisiones para asegurar que la seguridad de la información esté implementada y opere acorde con las políticas y procedimientos organizacionales?			
TOTAL			

Fuente: Tomado de NTC-ISO-IEC 27001:2013 A.9.1

Esta Lista chequeo seguridad de la información, esta de forma general, pero se recomienda que para su aplicación se oriente según las necesidades de la

organización teniendo como base los criterios establecidos tanto en la NTC-ISO-IEC 27001:2013 A.9.1, en el Manual de Usuario del Registro Nacional de Base de Datos-RNBD, las disposiciones dadas por el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC y demás lineamientos legales establecidos en la materia. En el anexo D se encuentra archivo editable.

6.1.2.3. Formación y capacitación. Las personas que conforman la organización constituyen la base para la gestión de los procesos, es por esto se hace necesario el fortalecimiento de las competencias laborales velando por la calidad de vida y el bienestar de los trabajadores; la cual redunda en la mejora continua de la satisfacción de los usuarios.

En el literal c del numeral 7.2 las normas técnicas ISO 9001:2015 e ISO 27001:2013; se establece: "asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia apropiadas".

Por otra parte, para dar cumplimiento con lo establecido en el artículo 27, capítulo VI, el decreto 1377 de 2013, establece:

> "Políticas internas efectivas*. En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar:*
>
> *1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este decreto.*
>
> *2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.*
>
> *3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento.*
>
> *La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto"* (Decreto 1377 de 2013).

Teniendo en cuenta el contexto anterior frente a la protección de datos es necesario que en las organizaciones establezcan un plan de capacitación que fortalezca las necesidades de formación en las personas, contribuyendo a que estas propongan iniciativas innovadoras, promoviendo la gestión del conocimiento y por ende la mejora continua de la gestión y posicionamiento de las organizaciones enfocándonos en la metodología de armonización de las herramientas se prepusieron.

Desde el hacer de la armonización propuesta, donde se apalanca con el conocimiento de la organización se encontró en la literatura según (Barney, 1991; Dosi, Teece, & Winter, 1991; Riesco, 2006), que la gestión del conocimiento permite mayor competitividad, innovación y beneficios diferenciadores, y su desarrollo gira en torno a las etapas de la adquisición, el almacenamiento, la transformación, la distribución y la aplicación. En la figura 8, se presenta formato de plan de capacitación.

Figura 8. Plan de capacitación

Plan de capacitación empresa año

NECESIDAD	TEMA	PARTICIPANTES	CAPACITADOR Y METODOLOGIA	LUGAR E INTENSIDAD (horas)	RECURSOS (Financieros, técnicos o humanos)	FECHA		EVALUACIÓN		
						Inicial	Final	Cumplimiento	Eficacia de la actividad	
									Método	Fecha

Fuente: Material clase Gestión Integral, Profesor Guillermo Peña

En el Anexo F. Se encuentra disponible en archivo editable del formato Plan de formación y capacitación, el cual permite a las organizaciones establecer la asignación de recursos para la consecución de los objetivos esperados y realizar la evaluación de la eficacia de las actividades realizadas.

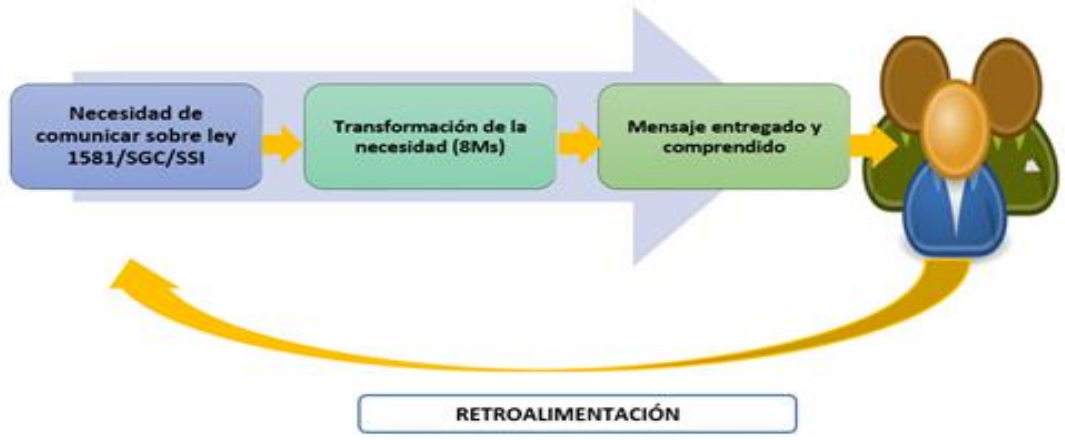
6.1.2.4. Proceso de comunicación. Es necesario establecer, implementar y mantener un proceso de comunicación, en las entidades gubernamentales del

orden nacional, soportado por un plan estratégico de comunicaciones, teniendo como eje orientador el Modelo Integrado de Planeación y Gestión (MIPG) diseñado por el Departamento Administrativo de la Función Pública (DAFP). La quinta dimensión del MIPG está orientada a la Información y comunicación tal como estipula el DAFP:

"El propósito de esta dimensión es garantizar un adecuado flujo de información interna, es decir aquella que permite la operación interna de una entidad, así como de la información externa, esto es, la vinculada a la interacción con los ciudadanos; para tales fines se requiere contar con canales de comunicación acordes con las capacidades organizacionales y con lo previsto en la Ley de Transparencia y Acceso a la Información" (MIPG, 2019, p.79).

En la figura 9 se presentan los elementos principales que debe tener un proceso de comunicación.

Figura 9. Proceso de comunicación



Fuente: Elaboración propia - Material clase Gestión Integral

6.1.2.5. Plan de comunicación interna y externa. El plan de comunicaciones permite que se implemente adecuadamente la armonización de la ley 1581 y las normas técnicas ISO 9001 e ISO 27001, enfocado hacia la estrategia de difusión entre las entidades gubernamentales del orden nacional y las partes interesadas.

Es necesario establecer, implementar y mantener un plan de comunicación acorde con el numeral 7.4 de las normas técnicas ISO 9001 e ISO 27001. El plan de comunicaciones permite que se implemente adecuadamente la armonización de la ley 1581 y las normas técnicas ISO 9001 e ISO 27001, enfocando hacia la

estrategia de difusión entre las entidades gubernamentales del orden nacional y las partes interesadas.

El plan de comunicaciones está compuesto por dos partes: en primer lugar, se define la estrategia de comunicación y en segundo lugar se establece la matriz de comunicación interna y externa. En la figura 10, se presenta un modelo de matriz de comunicación propuesta.

Figura 10. Matriz del plan de comunicación interna y externa

QUÉ [Mensaje que se debe comunicar]	QUIÉN EMITE	QUIÉN RECIBE	CANAL [Medios de Comunicación]	FRECUENCIA [Cuándo]	VERIFICAR [recepción y Comprensión]
	Quien envía la comunicación	A quien se envía la comunicación	Que canal se va a usar	Diaria semanal mensual	Verificar si la persona recibió el mensaje listado asistencia

Fuente: Elaboración propia - Material Módulo Liderazgo y Gestión del Talento Humano Profesora Eleonora Enciso Forero

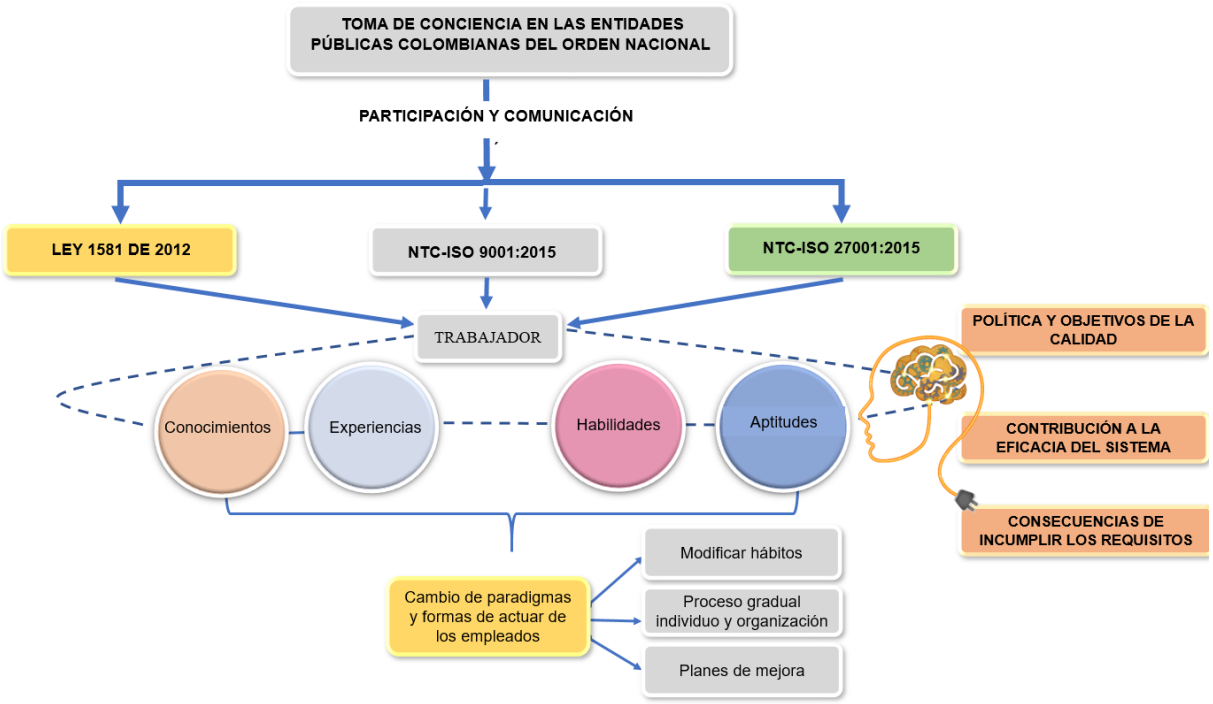
En el anexo H. Se detalla la matriz del plan de comunicación interna y externa, en la que se muestran los componentes que se requieren para una comunicación efectiva, además permite establecer controles de seguimiento de la misma.

6.1.2.6. Toma de conciencia. La toma de conciencia se logra cuando las personas que forman parte de la organización comprenden su responsabilidad frente a las actividades del quehacer diario y la forma como su proceder aporta al cumplimiento de los objetivos institucionales.

Acorde con la cultura organizacional en la que primen los principios y valores éticos, a través del cambio de paradigmas y formas de actuar de los empleados mediante la modificación de hábitos, en los que se involucre y de relevancia a la participación y la comunicación. En este campo la alta dirección juega un papel muy importante porque es quien debe dar ejemplo del compromiso con la organización.

La comunicación debe darse en un lenguaje claro y presentarse mediante diferentes herramientas para que todas las personas conozcan las política, objetivos y procesos que hacen parte de la misión de la organización; las reuniones periódicas con las personas permiten que se genere una retroalimentación y se busquen mejores maneras de hacer las cosas, siempre buscando el bienestar y satisfacción de los empleados y por ende la satisfacción de las partes interesadas como clientes y proveedores externos entre otros. En la figura 6, se presenta una propuesta de armonización conceptual en el que se indica los puntos más relevantes a tener en cuenta según el criterio de armonización propuesto para la generación de toma de conciencia en las organizaciones, basándose en los parámetros indicados en la NTC-ISO-9001:2015.

Figura 11. Mapa conceptual toma de conciencia



Fuente elaboración propia basada en NTC ISO 9001:2015

6.1.3 Verificar.

La articulación de los requisitos de la ley con las normas para la etapa de verificar arrojo como resultado que estos son complementarios en un 50%, la verificación del cumplimiento de la ley se complementa con las estrategias que pueden abordarse desde las normas.
La fortaleza de los sistemas de gestión radica en su capacidad para ofrecer información, de ello depende que las entidades puedan evaluar el cumplimiento legal, el uso de recursos y la efectividad de los resultados de su gestión, a partir de actividades de seguimiento, medición, análisis y evaluación, con el propósito de recopilar información (Resultados) para una efectiva toma de decisiones, el análisis de los hechos, las evidencias y los datos conducen a una mayor objetividad y confianza en las decisiones tomadas por la dirección de las entidades.

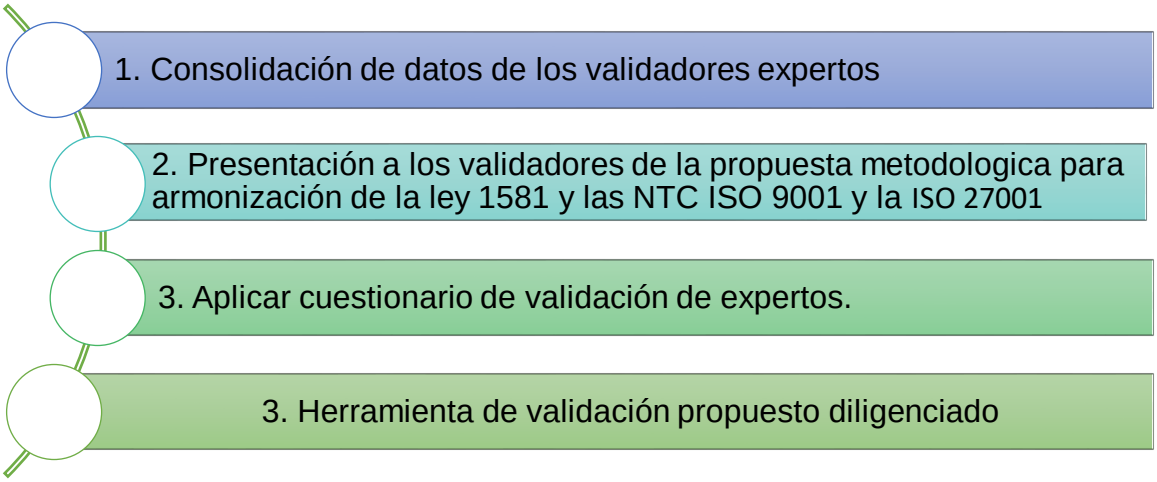
En esta etapa del verificar la investigación se centra en el ejercicio de auditoría, como herramienta principal de verificación en materia de cumplimiento legal y normativo, determinando la metodología procedimental y documentos anexos para la aplicación, tales como dentro de los que se plantean los siguientes: Procedimiento de auditorías, formato plan de auditoría, formato Informe de auditoría y formato lista de verificación

6.1.4 Actuar. Como salida de la etapa del verificar está la toma de decisiones que se convierte en entrada para la mejora.
Frente a la articulación se evidencio que los requisitos de la ley se pueden complementar en un 57 % con las normas para la toma de decisiones y se puede converger en 28% lo cual va de la mano con la herramienta propuesta para el flujo de la mejora continua.

El actuar es un proceso de cambio, de desarrollo y con posibilidades de mejorar. En este escenario es importante que las entidades dispongan de métodos y herramientas que les permita detectar y ejecutar planes de mejoramiento que los lleven a gestionar factores de éxito o fallas. Para ello se estableció un procedimiento para planes de mejoramiento y como anexo el formato para el plan de mejoramiento.

7. VALIDACIÓN DE EXPERTOS

Figura 12. Fases Metodología de validación



Fuente: Elaboración propia

Con el fin de realizar la validación de la metodología para la armonización se realizó mediante la herramienta (Anexo S) que se establece acorde con los criterios: claridad (4 ítems), pertinencia (6 ítems) y aplicabilidad (5 Ítems), los cuales son respondidos por los validadores expertos, teniendo como referente la escala de 1 al 5, en donde 1 representa estar totalmente en desacuerdo y 5 significa estar totalmente de acuerdo. La metodología fue presentada a los validadores por medio de una reunión mediada por tecnología, en la que se presentó el contenido de la misma y posteriormente el diligenciamiento del instrumento de validación por parte de cada experto.

Los expertos se seleccionaron considerando aspectos como la formación académica, experiencia profesional y laboral en temas de protección de datos personales, NTC ISO 9001 y la NTC ISO 27001 y experiencia en entidades del sector público colombiano.

El resultado de la validación en la que participaron 5 expertos, presenta las características cualitativas y cuantitativas estos se muestran en la tabla 8.

Tabla 8. Validación cuantitativa - resultados

CRITERIO EVALUADO	RESULTADO
Claridad	
1. La estructura de la propuesta metodológica se comprende fácilmente	4,4
2. La denominación de los criterios establecidos para la armonización es comprensible	4
3. Los criterios para la armonización son descritos de forma clara	4,4
4. La integración de los numerales se presenta de forma lógica	4,6
Pertinencia	
5. La propuesta metodológica cuenta con una estructura adecuada para realizar la armonización de la ley 1581 y las normas técnicas ISO 9001 e ISO 27001	4,2
6. Las herramientas son apropiados para llevar a cabo la armonización de la ley 1581 y las normas técnicas ISO 9001 e ISO 27001 en las entidades públicas colombianas del orden nacional	4,2
7. Los ítems de la propuesta metodológica dan cuenta de los requisitos de la ley 1581 de 2012 de acuerdo con las exigencias legales colombianas	4,4
8. Los ítems de la propuesta metodológica dan cuenta de los requisitos de los sistemas de gestión de la calidad de acuerdo con los referentes normativos	4,4
9. Los ítems de la propuesta metodológica dan cuenta de los requisitos de los sistemas de seguridad de la información de acuerdo con los referentes normativos	4,4
10. Los ítems de la propuesta metodológica permiten el cumplimiento de los requisitos de la ley 1581 armonizada con las normas técnicas ISO 9001 e ISO 27001	4,4
Aplicabilidad	
11. La propuesta brinda información suficiente para la armonización de la ley 1581 y las normas técnicas ISO 9001 e ISO 27001	4,2
12. La propuesta metodológica es de fácil aplicación por parte del personal que conforma las entidades públicas del orden nacional	4,2
13. La propuesta metodológica proporciona a las entidades públicas del orden nacional información confiable para la toma de decisiones orientadas a la mejora de la armonización de la ley 1581 y las normas técnicas ISO 9001 e ISO 27001	4,2
14. La propuesta metodológica proporciona información básica para la implementación de la armonización de la ley 1581 y las NTC ISO 9001 y NTC 27001	4,2
15.La propuesta de armonización de la ley 1581 y las normas técnicas ISO 9001 e ISO 27001 es aplicable a las entidades públicas del orden nacional	4,4

Fuente Anexo S Validación herramienta aplicada

Según los resultados logrados se puede concluir que los validadores consideran:

- La propuesta metodológica para la armonización de la ley de protección de datos y las normas de Gestión de la Calidad y la Seguridad de la Información se presenta de manera clara para el usuario, promedio de evaluación ítem claridad 4.35.
- La propuesta metodológica para la armonización de la ley de protección de datos y las normas de Gestión de la Calidad y la Seguridad de la Información, es pertinente para las entidades públicas del orden nacional colombiano, promedio de evaluación ítem pertinencia 4.33.
- La propuesta metodológica para la armonización de la ley de protección de datos y las normas de Gestión de la Calidad y la Seguridad de la Información, es aplicable a las entidades públicas del orden nacional en Colombia, promedio de evaluación aplicabilidad 4.24.

Por otra parte, se efectúa cálculo de Alfa de Cronbach, con los resultados que se describen en la tabla 9.

Tabla 9. Medición Alfa de Cronbach

Cronbach Alpha and Related Statistics				
Items	**Cronbach Alpha**	**Std. Alpha**	**G6(smc)**	**Average R**
All itmes	0.8791	0.8667	0.9963	0.3716
Ítem1 excluded	0.8783	0.8631	0.9957	0.3866
Ítem2 excluded	0.8884	0.8787	0.9959	0.4201
Ítem3 excluded	0.8884	0.8879	0.9961	0.442
Ítem4 excluded	0.8783	0.8631	0.9957	0.3866
Ítem5 excluded	0.8642	0.8525	1	0.3662
Ítem6 excluded	0.8639	0.8419	0.9953	0.3475
Ítem7 excluded	0.8651	0.8442	0.9953	0.3514
Ítem8 excluded	0.851	0.8407	0.9953	0.3455
Ítem9 excluded	0.851	0.8407	0.9953	0.3455
Ítem10 excluded	0.851	0.8407	0.9953	0.3455
Ítem11 excluded	0.8608	0.8436	0.9953	0.3505
Ítem12 excluded	NA	NA	NA	NA

Fuente: Recuperado de http:www.wessa.net/rwasp_cronbach.wasp

Obteniendo así una fiabilidad de 0.87 la cual se encuentra cerca de 1, es decir que los resultados alcanzados según la encuesta son eficaces para el objeto de la evaluación.

De igual forma dando uso al instrumento de validación propuesto por Hernández-Nieto, en la tabla 10 se presentan los resultados obtenidos:

Tabla 10. Resultado Validez Hernández-Nieto

	Sujeto 1	Sujeto 2	Sujeto 3	Sujeto 4	Sujeto 5	Sumatoria puntaje Sujetos	Sumatoria/valor máximo	Coeficiente validez de contenido (CVC)	Probabilidad de error	CvC-Pe
1. Criterio de claridad	18	15	18	19	17	87	4,6	0,916	1,21427E-06	0,9158
2. Criterio de pertinencia	25	24	25	29	27	130	4,5	0,897	1,21427E-06	0,8966
3. Criterio de Aplicabilidad	21	20	21	23	21	106	4,6	0,922	1,21427E-06	0,9217

Fuente: Hernández-Nieto, 2002

Acorde con el resultado se obtuvo un puntaje mayor a 0.90 lo que representa una validez y concordancia excelente, corroborando el resultado obtenido con el Alfa de Cronbach contribuyendo al objeto de estudio. La consolidación y análisis de los resultados se encuentran en el Anexo S.

Por otra parte, en las observaciones realizadas por los validadores se destacan las siguientes:

1. Es una propuesta valiosa para las organizaciones.
2. Me parece un trabajo importante de gran aplicabilidad para las entidades del sector público desarrollado de manera lógica, coherente y con herramientas de gran aplicabilidad.
3. Me parece una excelente herramienta para la armonización de las normas ISO 9001, 27001 y la ley 1581 que seguro permitirán facilitar los procesos y garantizar la agilidad organizacional en las organizaciones que tienen que cumplir con esta normatividad.
4. Importante propuesta y que las entidades públicas la utilicen para los objetivos que las normas establecen.

5. Propuesta novedosa y de utilidad para las entidades públicas.

Así mismo, a continuación, se describen las recomendaciones propuestas por los validadores:

- Cada vez que se referencie la norma "27001" se debe referenciar como ISO IEC 27001.
- Es importante como complemento al trabajo realizado revisar la norma ISO IEC 27701 la cual desarrolla precisamente el tema de privacidad de la información de identificación personal como parte del sistema de gestión de la seguridad de la información.
- Un buen programa para que su implementación sea realidad

En la presente investigación teniendo en cuenta las recomendaciones de los expertos se efectuó ajuste al documento señalando la ISO IEC 27001. En cuanto a la propuesta de complementar el trabajo con la ISO IEC 27701, si bien es cierto que es válida, no se realizaron ajustes considerando que no está dentro del alcance y su aplicabilidad implicaría realizar cambios sustanciales en la investigación. Por lo tanto se sugiere que ésta recomendación sea el escenario inicial para ampliar la metodología propuesta por futuros investigadores.

8. CONCLUSIONES

Teniendo en cuenta que la ley 1581 de 2012 es transversal a todas las organizaciones públicas del orden nacional, se puede concluir que la articulación con las normas ISO 9001:2015 e ISO-IEC-27001 puede ser de fácil aplicación si se estructura la parte documental partiendo de los sistemas de gestión de la calidad y se siguen posteriormente los lineamientos para la seguridad de la información.

Un sistema de gestión de calidad implementado eficazmente en las entidades públicas de orden nacional, se convierte en el pre requisito más importante para la aplicación de la ley 1581 de 2012 para la satisfacción de las partes interesadas, así mismo dar cumplimento a los requisitos que allí se establecen para la protección de datos con las recomendaciones de la norma de seguridad de la información ISO IEC 27001.

La Investigación presentó que la armonización de la Ley 1581 de 2012 con el Sistema de Gestión de Calidad NTC ISO 9001 y el Sistema de Seguridad de la Información NTC ISO IEC 27001 se alinean adecuadamente para la aplicación con el ciclo del PHVA donde la ley toma la forma sistemática de articulación de los procesos de la organización que lo quiera implementar y así tener control y seguridad de la información que estas normas nos presentan.

Como resultado de la articulación de los puntos convergentes, divergentes y complementarios asociados a los requisitos de la Ley 1581 de 2012 y los requisitos de las normas NTC ISO 9001 y NTC ISO 27001 se puede concluir que la ley de protección de datos se puede articular en un 80 % con estas normas.

La articulación arroja como resultado que los requisitos son en un 46% convergentes y complementarios en un 38 % lo que brinda que las estrategias propuestas en las herramientas puedan generar eficiencia en el momento de la aplicación.

En la propuesta metodológica los ítems apalancadores de la Ley 1581 de 2012 frente a las normas NTC ISO 9001 y NTC ISO 27001 están orientados hacia del HACER siendo esta la etapa que más participación tiene dentro los mecanismos que se propuso en la herramienta.

La validación de la propuesta metodológica a partir de los expertos arroja como resultado que esta herramienta de aplicación de los requisitos convergentes y complementarios a partir de mecanismos articuladores que parten del ciclo PHVA es clara, pertinente y aplicable a las entidades públicas colombianas del orden nacional.

Como resultado de la validación de expertos se obtuvo una calificación aceptable en un 86%, la cual se validó a través de las metodologías estadísticas de Cronbach con resultado de 0,87 sobre 1 de fiabilidad y la metodología de Hernández y Nieto con índices superiores a 0.90 que reflejan una validez y concordancia excelente; de tal manera que la metodología propuesta es aplicable a las entidades públicas del orden nacional.

9. RECOMENDACIONES

Se recomienda a las entidades públicas colombianas del orden nacional, iniciar con la determinación del contexto y sus partes interesadas, como fuente principal para identificar necesidades y expectativas relacionadas con la protección de los datos personales, articulado con las normas de sistemas de gestión de la calidad y sistema de seguridad de la información para lograr una base sólida en la gestión de las entidades públicas que perdure en el tiempo.

Del mismo modo las entidades públicas del orden nacional que deseen realizar la adopción de esta metodología, podrían sistematizar la herramienta a través de una plataforma tecnológica que facilite la implementación, el mantenimiento y la mejora de la gestión pública dando respuesta a las obligaciones legales y que esta se convierta en una buena práctica para otras entidades del nivel.

Se recomienda a los futuros investigadores que quieran ampliar la propuesta metodológica, que incorporen la norma ISO-IEC-27701 referente a la Gestión de la Privacidad de la información, ya que esta define requisitos para la protección de la información e identificación personal (IIP) englobando la manera en la que las organizaciones tienen que realizar la gestión de la información personal y ampara el cumplimiento de las normas de privacidad que se puedan aplicar.

Se recomienda al convenio USTA-ICONTEC socializar esta investigación de armonización entre sistemas de calidad y marco legal en sus programas académicos, con el fin de brindar herramientas que orienten a los estudiantes en la aplicabilidad de las leyes en especial la ley 1581 apalancada por los sistemas de gestión de la calidad y seguridad de la información, como modelo de aplicación de otras leyes.

10. REFERENCIAS

Acero González, W.Y., Ruiz León N.L.,Vanegas González, A.C. (2021). Protección de datos y su articulación con la gestión de calidad, *Signos. Maestría en Calidad y Gestión Integral.*

Aguilar-Castañeda, M. A. (2018). *La ley de protección de datos en Colombia: sus inicios y examen de sus principales postulados*. (Trabajo de Grado), Universidad Católica de Colombia. Bogotá, Colombia. Disponible en: https://repository.ucatolica.edu.co/handle/10983/23060?locale=es

Asociación Española de Normalización y Certificación. (2005). Norma UNE 66177: 2005. Guía para la integración de los sistemas de gestión. Cuadernos de calidad (V). https://www.aec.es/c/document_library/get_file?uuid=2f9c8623-b422-4b34-bb66-d406418bcbf5&groupId=10128

Balaguer, I. M. (2014). La nueva versión ISO 27001:2013: un cambio en la integración de los sistemas de gestión. *SGSI. Blog especializado en sistemas de gestión de seguridad de la información.* https://www.pmg-ssi.com/2014/11/iso-270012015-un-cambio-en-la-integracion-de-los-sistemas-de-gestion/

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. Journal de of management, 17(1), 99-120

Barrera-Campos, J. M. (2020). Regulación sobre protección de datos personales en el mundo digital en el Estado Colombiano. Trabajo de Grado. Universidad Católica de Colombia. Facultad de Derecho. Bogotá, Colombia

Carvajal H., Rubén. (2013). *Seguridad informática y de información*. (Tesis de grado), Universidad Tecnológica de Bolívar. Cartagena de Indias, Colombia.

Conde Colmenero, P. A. (2014). Los derechos a la intimidad y a la privacidad en el siglo XXI. España: Dykinson.

Conde Ortiz, C. (2006). La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad. España: Dykinson.

Constitución Política de Colombia (Const). Art. 15. 1991 (Colombia).

Cote P., L.F. (2016). Hábeas Data en Colombia, un Trasplante Normativo para la Protección de la Dignidad y su Correlación con la NTC/ISO/IEC 27001.

(Tesis de maestría), Universidad Santo Tomás. https://repository.usta.edu.co/bitstream/handle/11634/965/2016-CotePena,LuisFernando-Trabajodegrado.pdf?sequence=1

Corte Constitucional. Sentencia T-366. Gloria Stella Ortiz Delgado; 16 de junio de 2015.

Creswell, J. (2008). Mixed Methods Research: State of the Art. [Power Point Presentation]. University of Michigan. Recuperado de sitemaker.umich.edu/creswell.workshop/files/ creswell_lecture_slides.ppt

Decreto 1377 de 2013 por el cual se reglamenta parcialmente la Ley 1581 de 2012. 27 de junio de 2013. DO N. 48834, p,28

Departamento Administrativo de la Función Pública (DAFP). (2019). Manual Operativo del Modelo Integrado de Planeación y Gestión. Consejo para la Gestión y Desempeño Institucional, Versión 3. Colombia. Recuperado de https://www.funcionpublica.gov.co/

Diez Figueroa, A. A., y Vargas Herbozo, V. S. (2019). El ISO 37001: sistema de gestión antisoborno y el impacto financiero en las empresas del sector construcción como proveedores del estado. Universidad Peruana de Ciencias 97 Aplicadas. UPC. https://repositorioacademico.upc.edu.pe/handle/10757/62582

Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea. (1995). Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial n° L 281 de 23/11/1995 p. 0031 – 0050*

Dosi, G., Teece, D., y Winter, S. (1991). Toward a theory of corporate coherence: preliminary remarks. En G. Dosi, R. Giannetti & P. A. Toninelli (eds.), Technology and Enterprise in a Historical Perspective. Oxford: Oxford University Press

Fernández, F. (2005). El régimen jurídico del tratamiento automatizado de los datos de carácter personal de España. Chile: Red IUS et Praxis

Fernández Sola, N. (Dykinson). (2004). Unión Europea y derechos fundamentales en perspectiva constitucional. España.

García González, Aristeo. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *Boletín mexicano de*

derecho comparado, *40*(120), 743-778. Recuperado en 25 de agosto de 2021, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332007000300003&lng=es&tlng=es.

Glosario de Agricultura Orgánica de la FAO, (2009) tomado de https://boletinagrario.com/ap-6,armonizacion,4805.html

Hernández – Sampieri, R.H y Mendoza Torres, C. P. (2018). *Metodología de la* investigación: las rutas cuantitativa, cualitativa y mixta. McGraw-Hill interamericana editores, S.A. México.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (1997). Metodología de la investigación.

Hernández-Vivanco, A., Cruz-Cázares, C., y Bernardo, M. (2018). Openness and management systems integration: Pursuing innovation benefits. Journal of Engineering and Technology Management, 49, 76-90. https://doi.org/10.1016/j.jengtecman.2018.07.001

Hondius, F. W. (1983). A Decade of International Data Protection, *NILR*, 17(4), 105

Icontec. (2008). Guía Técnica Colombiana GTC 180 Responsabilidad Social. Bogotá: Icontec

Integrated Use of Management System Standards (IUMSS). (2018). ISO. https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100435_preview.pdf

ISO 27001:2013. Organismo de certificación global, NQA. Disponible en: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 17 de octubre de 2012. Congreso de Colombia. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Masciotra, M. (2003). El Habeas Data: la garantía polifuncional. Argentina: Librería Editora Platense S.R.L.

Moreno Parra, P. A., Restrepo Benavidez, B. y Sánchez Martínez, P. A. (2021). Aplicación metodológica: the integrated use of management system

standards para la integración de sistemas de gestión. *Signos, Investigación en Sistemas de Gestión*, 13(2). https://doi.org/10.15332/24631140.6668

Navas Guzmán, D. S., y Torres Nova, E. Y. (2011). Análisis de la relación entre la normatividad jurídica de la seguridad de la información en Colombia y el modelo de Sistema de Gestión de Seguridad de la Información NTC/ISO 27001. *SIGNOS - Investigación En Sistemas De gestión*, *3*(1), 61-69. https://doi.org/10.15332/s2145-1389.2011.0001.03

NTC ISO 27001:2015, (2015). Instituto Colombiano de Normas Ténicas. Sistemas de gestión de la calidad. Fundamentos y vocabulario. Icontec.

NTC ISO 9000:2015. (2015). Instituto Colombiano de Normas Técnicas. Sistemas de gestión de la calidad. Fundamentos y vocabulario.

NTC ISO 9001:2015, (2015). Instituto Colombiano de Normas Técnicas. Sistemas de gestión de calidad. Requisitos. https://colaboracion.dnp.gov.co/CDT/Normograma/NORMA%20ISO%209001%202015.pdf

Nunhes, V., Oliveira, O., & Bernardo, M. (2019). Guiding principles of integrated management systems: Towards unifying a starting point for researchers and practitioners. *Journal of Cleaner Production*, 210, 977 – 993

Pass 99:2012. (2012). The British Standards Institution. www.bisgroup.com

Peralta Cruz, D. C., y Guataquí Cervera, S. (2017). Metodología de integración del sistema de gestión de la seguridad y salud en el trabajo en el sistema de gestión de calidad en las entidades públicas colombianas de orden nacional. [Tesis de Maestría en Calidad y Gestión Integral]. Universidad Santo Tomas. https://repository.usta.edu.co/handle/11634/12069?show=full

Pierini, A., Lorences, V., Tornabene, M. (2002). *Hábeas Data. Derecho a la intimidad*. Buenos Aires, Argentina. Editorial Universidad de Buenos Aires. Edición 2.

Pfeffer Urquiaga, E. (2006). Los derechos a la intimidad o privacidad, a la honra y a la propia imagen: su protección frente a la libertad de opinión e información. Chile: Red Ius et Praxis.

Rebollo Delgado, L. (2014). ProQuest ebrary. (Dykinson, Ed.) Recuperado el 19 de febrero de 2015, de http://site.ebrary.com/:

http://site.ebrary.com/lib/bibliotecaustasp/reader.action?docID=10903674&ppg=140

Riesco, M. (2006). El negocio es el conocimiento. Madrid: Díaz de Santos

Ríos, G. y Oscar A. (2010). *ISO SERIE 27000, ISO 17799*. (Trabajo de investigación), Universidad Nacional. Manizales, Colombia.

Ruiz Concha, J. (2018). *Modelo para la implementación de la ley de protección de datos personales basado en el SGSI de la norma ISO 27001*. (Trabajo de grado especialización en seguridad informática), Universidad Nacional Abierta y a Distancia. Cali, Colombia.

Russell, Julian. (2013). Guía de implantación para la seguridad de la información. NQA. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Šikman, L., Latinović, T., y Paspalj, D. (2019). Iso 27001 - Information Systems Security, Development, Trends, Technical and Economic Challenges. *Annals of the Faculty of Engineering Hunedoara - International Journal of Engineering*, 17(4), 45–48.

Tejada, F., & Peña, G. (2009). Reflexiones sobre las características constitutivas de la gestión integral. *Signos*, 1(2), 79 – 93

Tejerina Rodríguez, O. (2014). Seguridad del Estado y privacidad. Madrid, España: Editoiral Reus.

Vega Suárez, A. (2013). El cumplimiento de la normativa de protección de datos en Iberoamérica. Disponible en: https://www.abogacia.es/actualidad/opinion-y-analisis/el-cumplimiento-de-la-normativa-de-proteccion-de-datos-en-iberoamerica/