Protección de datos y su articulación con la gestión de calidad*

Data protection and its articulation with quality management

*Weimar Yesid Acero González***

Universidad Santo Tomás

*Natalia Lisset Ruiz León ****

Universidad Santo Tomás

*Andrea Carolina Vanegas González *****

Universidad Santo Tomás

Resumen

En Colombia el marco jurídico asociado a la protección de datos personales sensibles no establece con claridad obligaciones sobre el sujeto responsable del tratamiento de la información y la generación de logros y resultados conformes, por lo que es necesario el uso de herramientas que permitan estandarizar los criterios mínimos de la regulación y la mitigación de riesgos que pueden derivarse del tratamiento indebido.

---

*Artículo de revisión.

** Msc (c) en Calidad y Gestión Integral. Ingeniero de Sistemas y Telecomunicaciones. Línea de investigación en Calidad y Gestión Integral, Universidad Santo Tomás. Bogotá, Colombia. Correo electrónico: weimaracero@usantotomas.edu.co. ORCID ID: 0000-0002-9303-6058. CVLAC: xxxxxx.

*** Msc (c) en Calidad y Gestión Integral. Químico Farmacéutico. Línea de investigación en Calidad y Gestión Integral, Universidad Santo Tomás. Bogotá, Colombia. Correo electrónico: nataliaruizl@usantotomas.edu.co. ORCID ID: 0000-0003-3050-2186. CVLAC: https://scienti.minciencias.gov.co/cvlac/visualizador/generarCurriculoCv.do?cod_rh=0001826352

*** Msc (c) en Calidad y Gestión Integral. Especialista en Calidad y seguridad alimentaria. Química de Alimentos. Línea de investigación en Calidad y Gestión Integral, Universidad Santo Tomás. Bogotá, Colombia. Correo electrónico: andreavanegas@usantotomas.edu.co. ORCID ID: 0000-0003-0076-4687. CVLAC: https://scienti.minciencias.gov.co/cvlac/visualizador/generarCurriculoCv.do?cod_rh=0001341845.

Con el propósito de buscar conductas orientadoras, este artículo realiza un análisis sobre la articulación de la Ley colombiana de protección de datos personales y la norma técnica de los sistemas de gestión de calidad desde el tratamiento, administración controlada, autorizada y trazable tanto del cliente interno como del cliente externo y la importancia de la información documentada asociada a la gestión de calidad.

Palabras clave: protección, dato sensible, sistema de gestión, hábeas data.

Abstract

In Colombia, the legal framework associated with the protection of sensitive personal data does not clearly establish obligations on the subject responsible for the processing of information and the generation of compliant achievements and results, so it is necessary to use tools to standardize the minimum criteria of the regulation and mitigation of risks that may arise from improper treatment.

With the purpose of looking for guiding conducts, this article makes an analysis on the articulation of the Colombian Law of protection of personal data and the technical norm of the quality management systems from the treatment, controlled, authorized and traceable administration of both the internal client and the external client and the importance of the documented information associated to the quality management.

Keywords: protection, data, data protection, data management system, habeas data

Introducción

Actualmente en Colombia se encuentran establecidos principios legales para el tratamiento de datos personales. Esta legislación ratifica el derecho fundamental que tienen los individuos

a conocer, actualizar y rectificar los datos recolectados sobre los mismos, en bancos de datos o registros. En la recolección, tratamiento y circulación de datos se busca la protección del individuo y la garantía de sus derechos facilitando la mejora continua**,** mediante la evaluación periódica y el fortalecimiento del ambiente de control en las empresas colombiana (Ley Estatutaria 1581, 2012).

Las bases de datos con información personal detallada de los colaboradores y los clientes constituyen un valor agregado para las organizaciones (Gené et al., 2018). El contar con datos normalizados en su rol de encargado de la administración de la información permite dar cumplimiento a lo establecido en la ley colombiana. Perfilar los clientes a la oferta comercial que brinda el negocio, contar con la documentación básica requerida, identificar sus problemas de seguridad, riesgos y vulnerabilidades también hace parte de la estandarización que genera valor y robustez.

Las fuentes de información de una empresa nacional se almacenan de forma descentralizada. Dentro de estas podemos encontrar: e-mail; sistemas de administración; asistentes de información; equipos de cómputo asignados al personal; teléfonos móviles de los colaboradores; mensajería instantánea; administrador de procesos; informática en la nube; plataformas sociales; sitios web; intranet; organización documental, etcétera. Estas entradas de información deben ser sometidas al control interno desde el punto de vista tecnológico aplicando políticas, estrategias y procedimientos y estableciendo la información documentada asociada a los sistemas de calidad (Nahabetián B., 2015) (Castañeda, s. f.).

La asignación de la implementación de la protección de datos personales asociada al sistema de gestión en las compañías nacionales no debería estar sujeto solo a las áreas de tecnología y aseguramiento de la calidad. Son fundamentales para la automatización del manejo de la información, pero indudablemente no es suficiente. Es indispensable que desde el direccionamiento estratégico se lidere el manejo de la información, siendo necesaria su participación y transversalidad a efectos de alcanzar la participación de todas las áreas de la compañía (Monsalve, 2017).

En Colombia, el artículo 15 de la Constitución Política manifiesta el derecho fundamental de la protección de datos así:

"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" (Constitución Política de Colombia, 2016).
En cumplimiento al pronunciamiento de la Corte Constitucional, el Congreso de Colombia expidió la Ley 1266 de 2008 por la cual se reglamentó el hábeas data para las personas naturales y jurídicas en relación con la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Actualmente, el hábeas data es una facultad autónoma y los instrumentos que aseguran su aplicación requieren del organismo administrativo autorizado y designado para ejercer eficazmente inspección y supervisión a los sujetos ya sean públicos o privados gestores del manejo de los datos personales (Rojas, 2014). En el año 2006 se estableció la Ley 1581 de 2012 la cual concede a la Superintendencia de Industria y Comercio (SIC) la creación de una delegación, que garantice

la efectiva ejecución del precepto normativo. Con la entrada en vigencia de esta Ley se incluyó el Registro Nacional de Bases de Datos (RNBD), cuya inscripción es administrada por la SIC siempre y cuando comprenda datos personales (Normativa Protección de Datos Personales, 2012).

Dentro de las compañías colombianas, los perfiles que ejercen los colaboradores no cuentan con una autorización total para acceder a los datos personales que se manejan dentro de la operación diaria. Por ello, la definición de roles y responsabilidades sobre los procesos que compromete el uso de este tipo de información, ya que es esencial para asegurar y restringir el acceso y su circulación; el tratamiento solo puede ser ejecutado por el individuo autorizado por el titular o por los previstos en la Ley (Ley Estatutaria 1581, 2012; Franco & Quintanilla, 2020).

Sin necesidad de vulnerar los derechos del Titular de la información, se puede generar responsabilidad sobre el administrador de los datos, en el momento en que no pueda demostrar ante la Superintendencia de Industria y Comercio - SIC el cumplimiento de las imposiciones determinadas por la ley. Para ello la SIC, por medio de la delegada para la protección de datos con su equipo de investigación administrativa, comprueba que las políticas acogidas por los administradores de la información apoyen un sistema conforme al desarrollo organizacional y su articulación interna para el progreso de la política, capacitación, esquemas de formación y atención de los titulares (Decreto 1074 Único Reglamentario del Sector Comercio, Industria y Turismo, 2015). Para lo cual, soportados en la norma verificarán que las medidas adoptadas sean apropiadas y efectivas para garantizar los derechos de los titulares, para ello, se tendrán en cuenta los criterios de las empresas respecto a la naturaleza jurídica del responsable, tamaño de la empresa, naturaleza de los

datos personales, tipo de tratamiento y riesgos para los titulares (Aparicio & Pastrana, 2017; Rodríguez, 2021).

Ahora bien, el desarrollo legislativo en Colombia, no define con claridad el alcance sobre las obligaciones impuestas a las organizaciones que ejercen tratamiento sobre los datos personales para el logro de resultados conformes (Ruiz, s. f.), por lo que es necesaria la búsqueda de herramientas que definan el medio de circulación que utilizan los responsables o encargados del dato, no solo para ejercer protección sobre el titular del dato manejado, si no también para efectos de mitigación de riesgos jurídicos que pueden derivarse del tratamiento indebido.

A partir de esto se plantea como objetivo analizar la integración de la gestión de la protección de datos personales y su articulación con la gestión de la calidad en empresas nacionales con el propósito de facilitar la implementación del cumplimiento normativo y legal aplicable.

Metodología

Esta investigación corresponde a una revisión sistémica de la literatura de tipo exploratorio sobre la protección de datos personales y su articulación con el sistema de gestión de calidad en Colombia. Existen diferentes ejes de clasificación de las investigaciones; para este artículo la estructura de la metodología se presenta en las siguientes etapas:

Descripción de metodología. Etapa principal que se caracteriza por describir el proceso de construcción de la matriz de información para el análisis de forma estructurada, con una revisión sistemática, se recolecta, selecciona, evalúa y se resume toda la evidencia disponible asociada a protección de datos personales y su articulación con la gestión de la calidad.

Proceso de búsqueda y recuperación. De acuerdo con la revisión sistemática se establecieron términos claves en el proceso de búsqueda de los artículos como; 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 (Gayo, s. f.). Se aplicó el método deductivo, ya que se tomaron conclusiones generales para explicaciones particulares presentadas en los resúmenes de cada artículo. Así mismo, se analizó el contenido general de cada uno de ellos, incluyendo conclusiones, relacionando contenido como análisis de herramientas, leyes, explicaciones particulares, principios de aplicación general y/o comprobación de validez de información presentada por cada artículo.

Criterios de inclusión y exclusión. El primer paso fue la segmentación de artículos con un máximo de cinco años de publicación, posteriormente se identificaron los artículos duplicados de los cuales se realizó exclusión para lograr un análisis eficaz. Como herramienta de gestión se utilizó Microsoft Excel para la distribución y segmentación de los datos previamente definidos para la conformación de la matriz de información. Se aplicó un método analítico lo cual llevó a la identificación de los datos y cuyo objetivo era excluir o mantener el artículo en cuestión para el presente estudio.

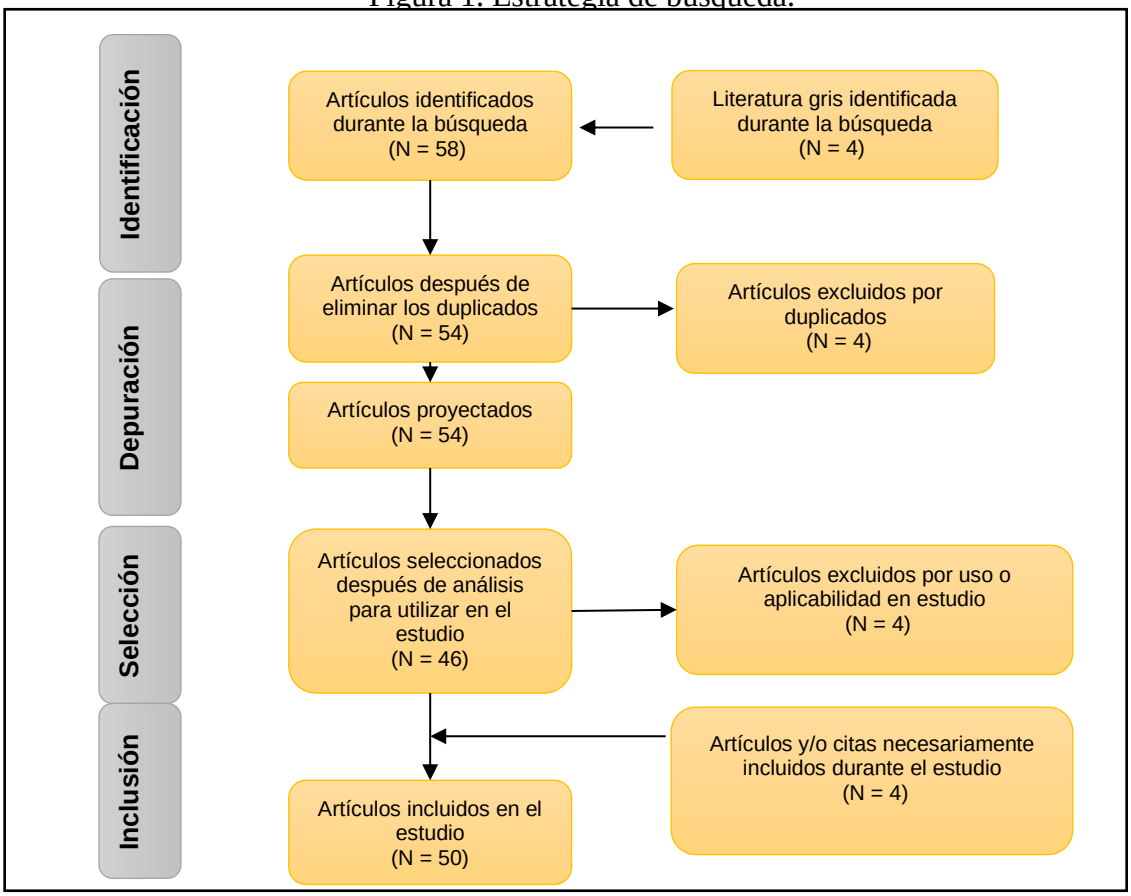
Teniendo en cuenta lo anterior, se construye el siguiente diagrama y tabla de datos como fuente para resumir cuantitativamente el resultado (ver Tabla 1 y Figura 1).

Tabla. 1. Estrategia de búsqueda.

BASE DE DATOS	NUMERO DE ARTÍCULOS	BASE DE DATOS	NUMERO DE ARTÍCULOS
Core	1	Uned	1
Elsevier	3	Universidad Autónoma de Chile	1
Facultad de Ciencias de la Información Universidad Autónoma de San Luis Potosí México.	1	Universidad Católica de Perú	1
Instituto de Administración Pública de España	1	Universidad Católica del Norte Coquimbo, Chile	1
International Data Privacy Law	1	Universidad de Costa Rica, Escuela de Bibliotecología y Ciencias de la Información	1
Microsoft Académico	1	Universidad de los Andes	2
Pontificia Universidad Católica del Perú	1	Universidad de Valencia	1
Prolegómenos Derechos y Valores	1	Universidad del Atlántico	1
Redalyc	3	Universidad del Rosario Colombia	1
Revista del Instituto de Ciencias jurídicas de Puebla México	2	Universidad mayor de Republica oriental de Uruguay	1
Revista Jurídica Unam	1	Universidad Militar Nueva Granada	1
Revista Latinoamericana	1	Universidad Nacional autónoma de México	1
Scielo	6	Universidad Piloto de Colombia	1
Serie Bibliotecología y Gestión de Información	1	Universidad Santo Tomas	1
Signos	6	Universidad Federal de Lavras, Facultad de derecho	1
Universidad Católica de Colombia	4		

Fuente: elaboración propia.

Figura 1. Estrategia de búsqueda.



Fuente: elaboración propia.

Variables de análisis. Desde el enfoque deductivo utilizado para el levantamiento de la información, como variables de selección importantes se tuvo en cuenta el año de publicación, el temario y área de aplicación de los resultados.

Más adelante, en la inclusión y exclusión de artículos para el estudio, se generó una distribución de la información de acuerdo con las siguientes variables, fundamento teórico, problemática planteada, metodología utilizada, carácter o conceptos de planeación, ejecución, verificación y monitoreo, tanto para la protección de datos personales, como para

el temario de gestión de la calidad. Por último, se define una caracterización de posible relación del artículo en cuestión, frente a la ISO 9001.

Resultados y discusión

Para la selección inicial de los artículos, se efectúo una aplicación del enfoque deductivo, donde se consideraron las variables como año de publicación, temario y área de aplicación de los resultados. En el tamizaje de búsqueda de información se identificó que el tema de investigación no cuenta con un abordaje recurrente lo cual nos lleva a realizar una primera exclusión de artículos con un tiempo superior de publicación a diez años, posteriormente un segundo filtro definiendo el máximo número de artículos con mínimo cinco años de publicación para un total de cuarenta artículos. Finalmente, se incluyeron diez artículos adicionales para un total de cincuenta, estos últimos no inferiores al año 2011 de publicación.

En la finalización del proceso de selección de la información, se identificaron 4 documentos de literatura gris y 58 artículos, de los cuales se excluyeron 4 por duplicidad y 4 por aplicabilidad, estos últimos reemplazados para finalizar con un total de cincuenta y cuatro documentos. Aunque se seleccionaron 50 artículos, luego del análisis del texto completo se incluyeron 25 que aportaron al objetivo de la revisión.

El tema y área de aplicación de los resultados planteados en los artículos, tomados de los repositorios universitarios, bibliotecas electrónicas y bases de datos académicas, fueron relevantes en la decisión de incluir o excluir cada uno de ellos. Se analizaron los resultados y las palabras claves, identificando la temática de investigación principal respecto a la protección de datos personales y su articulación con el sistema de gestión de calidad. En

cuanto a la aplicación de los resultados se revisó la problemática planteada y la metodología de desarrollo propuesta en los artículos de referencia, verificando coherencia y alineación con la armonización de una norma técnica y una ley.

Se considera el enfoque analítico desde el fundamento teórico, problemática planteada, metodología utilizada, carácter o conceptos de planeación, la ejecución, verificación y monitoreo de la protección de datos personales articulados con la gestión de la calidad (García et al., 2020). La recopilación de esta información es plasmada en la matriz de extracción en la cual se identifican los siguientes aspectos; en primera instancia para el ciclo de planeación, la protección de datos personales se orienta en parametrización de bases de datos y los sistemas de gestión de calidad construyen su enfoque en procesos. Respecto al hacer, la protección de datos se enfoca en la gestión sobre el dato personal interno y externo y en la gestión de calidad asegura la articulación de la información entre los procesos. En la verificación, el sistema de gestión de calidad permite establecer criterios de medición sobre el cumplimiento de metas específicas y la protección de datos realiza su enfoque en la integración de la información recopilada. Como parte del actuar se establecen criterios de cumplimiento mínimos evaluables para la protección de datos y en la gestión de calidad se pueden establecer diversas formas de evaluar dicho cumplimiento.

Así mismo, se realizó un análisis del aporte de cada artículo al sistema de gestión documental del ciclo planear hacer verificar actuar (PHVA), como el aporte al sistema de gestión de calidad y su articulación con los parámetros establecidos dentro de la ISO 9001:2015, donde se identifica que los datos son tratados como el producto final dentro de un sistema de gestión documental el cual debe estar guiado por las normas que le aplican a la calidad de la

información y toma de datos de las fuentes primarias, ya sea digital o física que se plasma en un archivo o que se migra a la nube.

A continuación, se presenta una síntesis de la información articulada dentro del sistema de calidad y la gestión de la protección de datos, desde el análisis de la revisión sistémica de la literatura la cual nos permite identificar las similitudes, diferencias y complementariedades partiendo del PHVA.

SGC Protección de Datos Personales	Similitudes	Diferencias	Complementariedades
Planear	Generación de guías armonizadoras de los parámetros aplicables en el sistema de gestión con respecto a la norma de protección de datos (Novoa, 2020).	La protección de datos se enfoca en la mejora de la gestión de los datos. La gestión de la calidad desde el planear se enfoca en la articulación de los procesos y su mejora continua (Nahabetián, 2015).	Al articular los procesos desde el sistema de gestión de calidad se puede realizar la trazabilidad de la gestión de los datos personales, su paso por los procesos y su administración (Silva et al., 2019).
Hacer	Parametrización de los datos para la toma de decisiones respecto al direccionamiento de los procesos dentro del sistema de gestión de la calidad (Cubillos, 2017).	Establecer lineamientos para gestionar la recolección de información interna como externa en la gestión de la protección de datos personales. En un sistema de gestión de calidad se afianza la articulación de la información interna (Nahabetián, 2015).	En el sistema de gestión de calidad se establecen límites y alertas sobre los grupos poblacionales referente a los datos que no cumplen con los parámetros de seguridad dentro de la protección de datos personales (Mendoza, 2018).
Verificar	El sistema de gestión de calidad y el documental se apoyan en normas técnicas para dar cumplimiento a los lineamientos y sea asocia con el cumplimiento legal frente al tratamiento de datos y el manejo de estos en los procesos como la ley 1581 de 2012 y la NTC ISO 9001 y 9002 (Abreo & Pinzón, 2017).	En la protección de datos personales se generan herramientas que permiten integrar la información capturada, en el sistema de gestión de calidad se establecen indicadores que permitan medir el cumplimiento de la recopilación de la información (Puentes, 2017).	Con las bases de datos estandarizadas como información documentada se puede establecer márgenes de desviación en torno al cumplimiento legal de la protección de datos personales y así permitir la generación de acciones correctivas en los procesos (Martínez, 2020)
Actuar	Se aplican unas series de herramientas tecnológicas para recolectar información que se basan en el enfoque al cliente, partes interesadas, liderazgo, responsabilidad y toma de decisiones a partir de los contextos en las organizaciones (Rojas & Martínez, s. f.)	La protección de datos personales establece criterios de cumplimiento en cuanto a información recopilada y dentro del sistema de gestión de calidad se utiliza la evaluación de desempeño como herramienta asociada a la mejora continua en un proceso determinado (Santos, 2019)	La medición periódica tanto en la protección de datos personales como en el sistema de gestión de calidad, se convierten en variables que le apuntan al cumplimiento de los requisitos legales y al control y seguimiento de indicadores de rendimiento que le apuntan a la mejora continua (Portilla, 2017) (Daissy & Guataquí, 2018)

Fuente: elaboración propia

La gestión de los datos personales, para su tratamiento requiere una armonización entre la responsabilidad social y el cumplimiento legal. Por tanto, mientras el universo de aplicación de la Ley 1581 de 2012 tiene que ser abordada siempre en función de la dignidad humana y de los derechos fundamentales, la aplicación de la NTC ISO 9001:2015 se desarrolla en relación costo beneficio entre el valor del desempeño organizacional y los requerimientos para su cumplimiento.

Para realizar un análisis documental efectivo que se pueda articular con la norma de protección de datos personales, es necesario definir los criterios de recolección de información e identificar según lo establecido en la Ley 1581 de 2012 los datos sensibles y la información que soporta el cumplimiento legal; estableciendo límites y puntos críticos que permitan generar confianza y mitigar desviaciones asociadas al sistema de gestión de calidad (Manrique, 2015).

El análisis de las fuentes recopiladas, en la etapa del planear permiten identificar que el enfoque de la protección de datos personales se basa en la gestión realizada con los datos capturados y almacenados tanto del cliente interno como externo, y en el sistema de gestión de calidad el enfoque esta dado en la articulación de los procesos. Tanto la norma como la ley le apuntan a la trazabilidad de la información en las organizaciones.

Dentro de la gestión de datos estos son tratados como el producto de venta al cliente, y entre más precisa y exacta sea la información más valioso y costoso puede ser el servicio de gestión de la información. Es por ello, por lo que la ley de protección de datos define parámetros en los que limita la violación a la privacidad que requieren las fuentes de información y el sujeto

dueño del dato, generando un control sobre la gestión documental y al mismo tiempo genera un valor económico a las organizaciones (Frigerio, 2018).

Las experiencias documentadas son fundamentales en la toma de decisiones de una organización, es por ello, que los repositorios de información juegan un papel importante cuando se articulan dentro del sistema de calidad tanto en el contexto interno como externo.

De acuerdo con la investigación se observa que uno de los mayores obstáculos de la implementación de la protección de datos personales es la falta de voluntad y de interés por parte de las organizaciones, ya que ejercer el debido tratamiento sobre el dato implica la implementación de información documentada la cual puede convertirse en necesaria para la eficacia de un sistema de gestión de calidad.

Aunque la implementación de la Ley de protección de datos personales en las organizaciones es un proceso que demanda tiempo, organización y recursos, una de las pautas iniciales es la identificación y clasificación de los datos, lo cual si se ejecuta de forma sistemática y siguiendo el ciclo PHVA se puede desarrollar eficazmente.

Según lo establecido en la ley 1581 de 2012, es necesario tener en cuenta aspectos y definiciones que deben estar relacionados en los documentos a desarrollar e implementar en las organizaciones, los cuales deben ser trazables en el tiempo, como son la autorización del titular de información para el tratamiento de sus datos personales, el ejercicio de los derechos de los titulares de información, las políticas de tratamiento de los responsables y encargados, las transferencias de datos personales, la responsabilidad demostrada frente al tratamiento de datos personales (Ley Estatutaria 1581, 2012).

Las orientaciones dadas por la Superintendencia de Industria y Comercio a efectos de lograr el cumplimiento por parte de los obligados a cumplir con la ley de protección de datos personales, permite identificar que detrás de la normativa nacional está como soporte teórico conceptual la norma NTC ISO 27001:2013, la cual se materializa mediante el diseño e implementación de un sistema de gestión de seguridad de la información. Para lograr el adecuado cumplimiento de la ley de protección de datos se debe diseñar e implementar también un sistema de calidad, constituyendo la primera NTC, por razón de los elementos comunes que le relacionan con la segunda, en una base importante para su desarrollo (Navas & Torres, 2011).

En el contexto internacional se evidencia que en países de Europa como España la protección de datos se encuentra armonizada directamente con la NTC ISO 27001:2013, la cual dirige al aseguramiento e integridad de los datos y la confidencialidad de la información. Esto hace que los derechos de privacidad sean prioridad en las organizaciones que capturan la información personal generando tranquilidad a las comunidades que comparten sus datos, ya que el estándar para los sistemas de gestión de seguridad de la información evalúa el riesgo y generan controles para su mitigación o eliminación (Quiroz, 2016). Por el contrario, en Latino América el panorama no es muy alentador en países como Ecuador y Perú (L. E. Álvarez, 2017); donde la protección de datos es un material jurídico flexible, el cual permite que la información se use y comercialice sin consentimiento previo del sujeto dueño de la misma y no se cuenta con un estamento de orden frente al cumplimiento legal como se evidencia en países Europeos (Mayorga et al., 2019), donde la verificación no consiste en la aplicación de la ley sino en la capacidad de las organizaciones para cumplirla.

En países como México y Colombia (Barrera, s. f.), existen normas claras frente a la protección de datos, en este último la Ley 1266 de 2008 regula el tratamiento de datos financieros, la Ley 1581 de 2012 la protección de datos personales y el Decreto 1377 de 2013 el cual determina los procedimientos para la aplicación de las leyes (Silva et al., 2019); más sin embargo es necesario indicar que existen vulnerabilidades sobre el derecho a la autodeterminación informática lo cual en nuestro país es más visible en el contexto bancario donde se genera una mayor circulación de la información personal (Gil, 2017). En México (Castillo & Zavala, 2019), la vulnerabilidad de la circulación de la información personal es altamente evidente en las agencias estatales donde se utilizan los datos de los ciudadanos para el tratamiento de rastreo de comportamientos sociales con el fin de perfilar al sujeto según su nivel socio económico y gestionar pagos e impuestos locales (Cotino, 2018).

Conclusiones

En la revisión de literatura se identificó que a nivel Latinoamérica el enfoque dado a la implementación de datos personales armoniza con la gestión de calidad tanto documentalmente como hacia la mejora continua de los procesos, ya que se acogen lineamientos medibles y trazables.

Durante la revisión sistemática e investigación del tema propuesto en el presente documento se observó que, si bien actualmente la gestión de los datos personales no se asocia a la información documentada del SGC, en las actividades diarias de las organizaciones nacionales existe una notable convivencia de esta articulación la cual se soporta tanto en los indicadores corporativos como en las normas presentadas por los órganos legislativos para el

cumplimiento de los lineamientos, esto a su vez impacta positivamente la gestión de calidad y la mejora continua de una organización.

El análisis expuesto indica que el uso de datos e información que se recolectan dentro de una organización, deben ser manejados como un producto donde la gestión y tratamiento eficaz de esta información aporta a la mejora continua.

En el proceso de armonización se evidenció que el sistema de gestión documental y la información documentada asociada a la gestión de calidad definen límites en el uso de los datos aún más si están vinculados a regulaciones o normatividad. Estas parametrizaciones que se establecen en la aplicación del sistema documental aportan a que la información tenga un valor mayor y se enfoque tanto en el contexto interno como externo en las organizaciones.

En Europa la ley de protección de datos lleva una estrategia de análisis de riesgos con el fin de que la información que se recoja sea transparente y confiable, sirviendo de insumo para: usarla con fines comerciales, promociones de salud y estrategias de bienestar común, adicionalmente usada para gestiones legales. Por el contrario, en América Latina la información recolectada no está parametrizada y está sujeta al tránsito libre, la cual puede ser usada en promoción de servicios muchos de ellos comerciales y no existe a la fecha en las organizaciones nacionales una trazabilidad confiable tanto en la documentación física como en las plataformas digitales.

Referencias

Abreo, N., & Pinzón, N. N. (2017). Guía para la implementación de NTC ISO 9001:2008, NTC ISO 14001:2004 y NTC OHSAS 18001:2007, basada en los hallazgos de las auditorías de certificación realizadas por el ICONTEC entre junio de 2012 y junio de 2015. *SIGNOS - Investigación en sistemas de gestión*, *9*(2), 149-158. https://doi.org/10.15332/s2145-1389.2017.0002.09

Alvarado, J. A., & Lopez, L. J. (s. f.). *Implementación de la protección de datos personales en el SGC basado en la Ley 1581 para una institución privada de la libertad*. 18.

Álvarez, D. (2016). Acceso a la información pública y protección de datos personales: ¿Puede el consejo parar la transparencia ser la autoridad de control en materia de protección de datos? *Revista de derecho (Coquimbo)*, *23*(1), 51-79. https://doi.org/10.4067/S0718-97532016000100003

Álvarez, L. E. (2017). *Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales*. 19.

Aparicio, J. A., & Pastrana, M. Á. (2017). Conceptos y legislación de transparencia sindical y protección de datos personales de los trabajadores en México. *Revista Latinoamericana de Derecho Social*, *1*(24), 175. https://doi.org/10.22201/iij.24487899e.2017.24.10815

Barrera, J. M. (s. f.). *Regulación sobre protección de datos personales en el mundo digital en el Estado*.

Castañeda, M. Á. A. (s. f.). *La Ley de protección de datos en Colombia: Sus inicios y exámen de sus principales postulados*. 56.

Castillo, J. M., & Zavala, B. (2019). Ciberseguridad y vigilancia tecnológica un reto para la protección de datos personales para los archivos. *30/06/2019*.

Constitución Política de Colombia. (2016). Biblioteca Enrique Low Murtra, 170.

Contreras, P. (2020). El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. *Estudios constitucionales*, *18*(2), 87-120. https://doi.org/10.4067/S0718-52002020000200087

Cotino, L. (2018). Confidencialidad y protección de datos en la mediación en la Unión Europea. *REVISTA IUS*, *12*(41). https://doi.org/10.35487/rius.v12i41.2018.421

Cotino, L. (2020). Inteligencia artificial, big data y aplicaciones contra la COVID-19: Privacidad y protección de datos. *IDP. Revista de Internet Derecho y Política*, *31*. https://doi.org/10.7238/idp.v0i31.3244

Cubillos, Á. (2017). La explotación de los datos personales por los gigantes de internet. *Estudios en Derecho a la Información*, *1*(3), 27. https://doi.org/10.22201/iij.25940082e.2017.3.10823

Daissy, P. C., & Guataquí, S. (2018). 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. *SIGNOS - Investigación en sistemas de gestión*, *10*(1), 39-56. https://doi.org/10.15332/s2145-1389.2018.0001.02

De la Vega, L. C., & Novoa, K. J. (2017). La protección de datos personales en Colombia. *Vis Iuris*, 38-49. https://doi.org/10.22518/vis.v4i72017.1142

Decreto 1074 Único Reglamentario del Sector Comercio, Industria y Turismo, Pub. L. No. 1074, 405 (2015).

Foral, L. (s. f.). *Comunidad Foral de Navarra*. 3.

Franco, D., & Quintanilla, A. (2020). La protección de datos personales y el derecho al olvido en el Perú. A propósito de los estándares internacionales del Sistema Interamericano de los Derechos Humanos. *Derecho PUCP*, *84*, 271-299. https://doi.org/10.18800/derechopucp.202001.009

Frigerio, C. (2018). Mecanismos de regulación de datos personales: Una mirada desde el análisis económico del derecho. *Revista Chilena de Derecho y Tecnología*, *7*(2), 45. https://doi.org/10.5354/0719-2584.2018.50578

Galvis, L. (2018). El Panóptico digital de la protección de datos personales en Colombia. *Revista Temas*, *12*, 125-140. https://doi.org/10.15332/rt.v0i12.2038

Galvis, L., & Pesca, D. A. (2019). Límites del tratamiento de los datos personales en el ámbito laboral frente al uso de las tecnologías de la información y comunicación en la era digital. *IUSTA*, *52*. https://doi.org/10.15332/25005286.5482

García, F. J., Villegas, R., Goicoechea, J. A., Muñoyerro, D., & Dopazo, J. (2020). La evaluación de impacto en protección de datos en los proyectos de investigación. *Gaceta Sanitaria*, *34*(5), 521-523. https://doi.org/10.1016/j.gaceta.2019.10.006

Gayo, M. R. (s. f.). *Big data: Hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas*. 25.

Gené, J., Gallo de Puelles, P., & de Lecuona, I. (2018). Big data y seguridad de la información. *Atención Primaria*, *50*(1), 3-5. https://doi.org/10.1016/j.aprim.2017.10.004

Gil, J. C. (2017). El debido proceso en la ley de habeas data. *CES Derecho*, 191-204. https://doi.org/10.21615/cesder.8.1.10

González, A. B., & Gamboa, O. (s. f.). *Datos personales en las relaciones laborales del sector privado*. 11.

Gonzalez, L. D. (2018). Control de nuestros datos personales en la era del big data: El caso del rastreo web de terceros. *Estudios Socio-Jurídicos*, *21*(1). https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941

Guerrero, B. (2020). Protección de datos personales en el Poder Judicial: *Revista Chilena de Derecho y Tecnología*, *9*(2), 33. https://doi.org/10.5354/0719-2584.2020.54372

Hernández, C., Fonseca, M. D. P., Hernández, J. F., & Bravo, A. (s. f.). *El consentimiento informado en la investigación médica*. 5.

Iglesias, R. G. (2013). *El Habeas data y la ley de protección de datos en Chile*. 18.

Ley Estatutaria 1581. (2012). Congreso de Colombia, 301.

Manrique, V. (2015). El derecho al olvido: Análisis comparativo de las fuentes internacionales con la regulación colombiana. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, *14*, 1-25. Recuperado de https://doi.org/10.15425/redecom.14.2015.09

Martínez, R. M. (2020). Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública. *2020*, 15.

Mayorga, T. C., García, M., Duret, J. F., Carrión, J. L., & Yarad, P. V. (2019). Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos. *Dominio de las Ciencias*, *5*(1), 518. https://doi.org/10.23857/dc.v5i1.875

Mendoza, O. A. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: Desafíos y cumplimiento. *REVISTA IUS*, *12*(41). https://doi.org/10.35487/rius.v12i41.2018.355

Monsalve, V. (2017). La protección de datos de carácter personal en los contratos electrónicos con consumidores: Análisis de la legislación colombiana y de los principales referentes europeos. *Prolegómenos*, *20*(39), 163-195. https://doi.org/10.18359/prole.2729

Nahabetián, L. (2015). Protección de datos y gestión documental: Decálogo ampliado para la sociedad de la información. *Revista de la Facultad de Derecho*, *39*, 199-225. https://doi.org/10.22187/20158

Navas, D. S., & Torres, 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), 9. https://doi.org/10.15332/s2145-1389.2011.0001.03

Departamento Nacional de Planeación. (2012). Normativa Protección de Datos Personales, 9.

Novoa, E. (2020). *El derecho a la protección de datos de personales en la prestación de servicios de cloud computing. Una perspectiva ecuatoriana*. 26.

Paños, A. (2013). *Marco legal de los servicios de anatomía patológica vigente en España*. 7.

Portilla, J. D. (2017). Gobierno de datos, un potenciador de los sistemas de gestión de calidad. *SIGNOS - Investigación en sistemas de gestión*, *9*(2), 159-172. https://doi.org/10.15332/s2145-1389.2017.0002.10

Puentes, M. (2017). Propuesta metodológica para articular la gestión documental con los requisitos de la Ley General de Archivos y la norma técnica internacional ISO 9001:2015. *SIGNOS - Investigación en sistemas de gestión*, *9*(2), 81-95. https://doi.org/10.15332/s2145-1389.2017.0002.05

Quiroz, R. (2016). El hábeas data, protección al derecho a la información y a la autodeterminación informativa. *Letras (Lima)*, *87*(126), 23-49. https://doi.org/10.30920/letras.87.126.2

Rivera, V. (2019). Realidad sobre la Privacidad de los Datos Personales en Costa Rica. *e-Ciencias de la Información*. https://doi.org/10.15517/eci.v9i2.37503

Rodríguez, J. F. (2021). Estado de alarma y protección de la privacidad en tiempos de pandemia: Licitud del tratamiento de categorías especiales de datos. *Revista de Derecho Político*, *1*(110), 299. https://doi.org/10.5944/rdp.110.2021.30337

Rojas, D., & Martinez, J. C. (s. f.). *Un SGSI Genera Valor cuando una Organización se adapta a nuevas Leyes como la 1581 de Protección de Datos Personales*. 5.

Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Novum Jus*, *8*(1), 107-139. https://doi.org/10.14718/NovumJus.2014.8.1.6

Ruiz, B. Y. (s. f.). *Regulación en materia de protección de datos personales o habeas data en Colombia*.

Santos, S. B. (2019). Reflexiones escépticas, principiológicas y económicas sobre el consentimiento necesario para la recolección y tratamiento de datos. *Derecho PUCP*, *83*, 179-206. https://doi.org/10.18800/derechopucp.201902.006

Silva, J., Solano, D., Fernandez, C., Romero, L., & Villa, J. V. (2019). Privacy Preserving, Protection of Personal Data, and Big Data: A Review of the Colombia Case. *Procedia Computer Science*, *151*, 1213-1218. https://doi.org/10.1016/j.procs.2019.04.174

Tejedor, J. C. (2014). A la búsqueda del equilibrio entre transparencia administrativa y protección de datos. Primeros desarrollos en el ámbito municipal. *Gestión y Análisis de Políticas Públicas*, 7-30. https://doi.org/10.24965/gapp.v0i12.10205

Traca, J. L., & Embry, B. (2012). The Angolan Data Protection Act: First impressions. *International Data Privacy Law*, *2*(1), 40-45. https://doi.org/10.1093/idpl/ipr024

Vargas, W. C., Moreno, A. G., Oñate, A. M., & Sanabria, M. (2020). Importancia del big data en un gestor documental para las entidades públicas de Colombia. *SIGNOS - Investigación en sistemas de gestión*, *13*(1). https://doi.org/10.15332/6345