	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
	Documento	Código	Fecha	Revisión
	FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO	F-AC-DBL-007	10-04-2012	A
Dependencia	Aprobado		Pág.	
DIVISIÓN DE BIBLIOTECA	SUBDIRECTOR ACADEMICO		1(221)	

RESUMEN - TESIS DE GRADO

AUTORES	JORGE ALBERTO CAMARGO BARBOSA
FACULTAD	DE INGENIERIAS
PLAN DE ESTUDIOS	MAESTRIA EN GOBIERNO DE TI
DIRECTOR	DRA. TORCOROMA VELAZQUEZ
TÍTULO DE LA TESIS	MODELO DE GOBIERNO DE TRATAMIENTO DE LA INFORMACIÓN PARA LA EMPRESA COLOMBIANA EN LA GLOBALIZACIÓN EN LA PROSPECTIVA DEL DESARROLLO ORGANIZACIONAL

RESUMEN (70 palabras aproximadamente)

LA ORGANIZACIÓN EMPRESARIAL SE HA CONVERTIDO EN EL PUNTO DE PARTIDA PARA EL BIENESTAR, PROGRESO Y DESARROLLO DE LAS EMPRESAS; DE ALLÍ, EL AFÁN POR CONCRETAR ACCIONES EN EL PRESENTE TRABAJO INVESTIGATIVO QUE TIENE COMO NORTE: DISEÑAR UN MODELO DE GOBIERNO DE TRATAMIENTO DE LA INFORMACIÓN PARA LA EMPRESA COLOMBIANA, COMO UN ELEMENTO FUNDAMENTAL EN LA ORGANIZACIÓN PERMITIENDO LA PROTECCIÓN DE DATOS PERSONALES, EN CUMPLIMIENTO DE LOS DERECHOS FUNDAMENTALES DE SUS TITULARES. PARTIENDO DE DICHA INTENCIONALIDAD, LA INVESTIGACIÓN TOMA UN CAMINO CENTRADO EN EL PARADIGMA CUALITATIVO APOYADO EN LOS PRECEPTOS DE LA INVESTIGACIÓN CUALITATIVA

CARACTERÍSTICAS

PÁGINAS: 221	PLANOS: 0	ILUSTRACIONES: 50	CD-ROM: 1
---------------------	------------------	--------------------------	------------------



**MODELO DE GOBIERNO DE TRATAMIENTO DE LA INFORMACIÓN PARA LA
EMPRESA COLOMBIANA EN LA GLOBALIZACIÓN EN LA PROSPECTIVA DEL
DESARROLLO ORGANIZACIONAL**

JORGE ALBERTO CAMARGO BARBOSA

Proyecto presentado como requisito para optar el título de Maestría en Gobierno de TI

Director

Dra. TORCOROMA VELAZQUEZ

Nivel de Formación

Doctor

Codirector

Dr. HUGO FERNANDO CASTRO SILVA

Nivel de Formación

Doctor

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

MAESTRIA EN GOBIERNO DE TI

Ocaña, Colombia

Mayo, 2019

Dedicatoria

Este trabajo de grado se lo dedico a DIOS y la Virgen por el amor y la sabiduría humilde que han depositado en mí para glorificarlos con el logro de los triunfos que me han regalado; a mi Madre por enseñarme a amar a DIOS y la Virgen, razón de inspiración y guía en mi camino espiritual y personal incentivándome a trabajar con esfuerzo, dedicación y con humildad en dar y en servir a la comunidad, ejemplo a seguir, tu huella en mi corazón siempre está, motivo de amor en mi vida siempre estarás. A mi Padre ejemplo de fortaleza, firmeza y honestidad, perseverancia y fe que Dios me ha querido dar para continuar el camino en su Santa Bondad. A mi Esposa la dulce mujer que Dios me ha querido dar, admiración y respeto, compañía y apoyo incondicional, mis sueños... sus sueños, mis triunfos los suyos, son uno más. A mi familia motivación y riqueza espiritual, comprensión y confianza recibida en mi vida para la meta llegar. Al Dr. Juan Carlos López Castrillón, rectitud, buen obrar, ejemplo y apoyo incondicional... Jefe, amigo que Dios puso en este camino profesional y personal. A la Universidad Francisco de Paula Santander Ocaña por construir este espacio académico y profesional en beneficio de la Región y de la Comunidad.

Agradecimientos

Agradecimientos a DIOS, la Virgen, a mis padres, a mi esposa, mi familia, al Dr. Juan Carlos López Castrillón, a mi Directora de Proyecto Torcoroma Velásquez, a mi Codirector Hugo Fernando Castro Silva y a todo el grupo Docente y Administrativo de la Maestría en Gobierno de Tecnología de la Información de la Universidad Francisco de Paula Santander Ocaña, por su apoyo incondicional y hacer posible la razón de encontrar y sentir que esta nueva página en mi vida es obra de ustedes, autores de apoyo, confianza y felicidad.

A Ustedes Infinitas Gracias y Bendiciones.

Índice

Capítulo 1. Modelo de gobierno de tratamiento de la información para la empresa colombiana en la globalización en la perspectiva del desarrollo organizacional	1
1.1 Planteamiento del problema.....	1
1.2 Formulación del problema	3
1.3 Objetivos	4
1.3.1 General.....	4
1.3.2 Específicos	4
1.4 Justificación	4
1.5 Delimitaciones	7
1.5.1 Delimitación geográfica.....	7
1.5.2 Delimitación temporal.	7
1.5.3 Delimitación conceptual.....	8
1.5.4 Delimitación operativa	8
Capítulo 2. Marco referencial	9
2.1 Marco histórico.....	9
2.2 Marco conceptual	12
2.2.1 Tratamiento de datos personales	12
2.3 Marco contextual.....	14
2.3.1 Tratamiento de datos personales en la empresa Colombiana	14
2.4 Marco teórico	16
2.4.1 Gobierno de tecnologías de la información.....	16
2.4.2 Seguridad de la información.	17
2.4.3 Sistema de gestión de seguridad de la información.	17
2.5 Marco legal	17
Capítulo 3. Metodología	19
3.1 Diseño metodológico.....	19
3.1.1 Historia de la teoría fundamentada.....	21
3.1.2 La teoría fundamentada en la empresa.....	23
3.1.3 Estrategias del método de comparación	24
3.1.4 El proceso de la teoría fundamentada.....	24
3.1.5 Estrategias para la teoría fundamentada	24
3.1.6 Criterios de la teoría fundamentada.....	25
3.1.7 Elementos de la teoría fundamentada.....	25
3.1.8 Seguimiento metodológico del proyecto	31
3.1.9 Análisis de la información.	36
Capítulo 4. Análisis de resultados.....	38
4.1 Contextualización del escenario	38
4.1.1 Colombia mayor.....	38
4.1.2 Seguro mundial	40
4.1.3 Universidad Francisco de Paula Santander Ocaña	49

	vii
4.14 BDO AUDIT	53
4.15 Ministerio TIC.....	55
4.2 Información recolectada.....	57
4.21 Categorías de análisis.....	57
4.3 Sistematización de la información.....	86
4.31 Análisis de aplicación de las categorías en las empresas.....	87
4.32 Nivel de madurez de aplicación de categorías en las empresas.....	91
4.4 Modelo de gobierno de tratamiento de la información para la empresa colombiana en la globalización como prospectiva de desarrollo organizacional	97
4.4.1 Impacto de la legislación aplicable al tratamiento de la información de datos personales y prácticas relacionadas	99
4.5 Estructuración del modelo de gobierno de tratamiento de la información para la empresa colombiana en la globalización como prospectiva de desarrollo organizacional.....	117
4.5.1 Establecimiento del modelo de gobierno de tratamiento de la información para la empresa colombiana	117
4.5.2 Contexto general del modelo	117
4.5.3 Elementos del contexto del modelo	119
4.6 Analizar la factibilidad de aplicación del modelo de gobierno de tratamiento de la información para la empresa colombiana	163
4.6.1 Aplicación del modelo de gobierno de tratamiento de la información para la empresa colombiana.....	172
5. Remembranzas de la investigación.....	184
Referencias.....	186
Apéndices.....	200

Lista de Figuras

Figura 1. Elementos de la Teoría Fundamentada.....	26
Figura 2. Modelo General Teoría de Campo.	27
Figura 3. Modelo Específico Teoría de Campo.	27
Figura 4. Proceso de muestreo teórico.	28
Figura 5. Codificación.....	29
Figura 6. Proceso de generación de categorías.	30
Figura 7. Historia de BDO Audit.....	54
Figura 8. Mapa de Procesos Colombia Mayor.....	62
Figura 9. Mapa de Procesos Colombia Mayor.....	63
Figura 10. Mapa de Procesos Seguros Mundial.....	65
Figura 11. Objetivos Estratégicos Seguros Mundial.....	65
Figura 12. Prioridades Estratégicas Seguros Mundial.	66
Figura 13. Mapa de Procesos Universidad Francisco de Paula Santander Ocaña	68
Figura 14 Mapa de Macroprocesos Ministerio TIC.....	69
Figura 15. Organigrama General Colombia Mayor	71
Figura 16 . Organigrama Regional Colombia Mayor	71
Figura 17. Estructura Empresarial Seguros Mundial.	72
Figura 18. Estructura Organizacional Universidad Francisco de Paula Santander Ocaña.....	72
Figura 19. Organigrama Despacho del Ministro Ministerio TIC.....	76
Figura 20. Organigrama Secretaría General Ministerio TIC.....	76
Figura 21. Organigrama Despacho del Viceministro Ministerio TIC.....	77

Figura 22. Organigrama Órganos de Asesoría y Coordinación Ministerio TIC	77
Figura 23. Concreción de categorías en la Empresas.....	88
Figura 24. Aplicabilidad Gobierno de TI.....	88
Figura 25. Aplicabilidad Tratamiento de la Información.	89
Figura 26. Aplicabilidad Desarrollo Organizacional.	89
Figura 27. Aplicabilidad Estructura Empresarial.....	89
Figura 28. Aplicabilidad Globalización en la Empresa	90
Figura 29. Aplicabilidad Legislación Vinculante	90
Figura 30. Aplicabilidad Normas Prácticas.	90
Figura 31. Concreción de las Categorías por Niveles de Madurez	92
Figura 32. Nivel de Madurez Gobierno de TI.....	93
Figura 33. Nivel de Madurez Tratamiento de la Información.	93
Figura 34. Nivel de Madurez Desarrollo Organizacional	94
Figura 35. Nivel de Madurez Estructura Empresarial.....	94
Figura 36. Nivel de Madurez Globalización en la Empresa	95
Figura 37. Nivel de Madurez Legislación Vinculante	95
Figura 38. Ni Nivel de Madurez Buenas Prácticas.	96
Figura 39. Concreción de categorías surgidas del apoyo estadístico.....	96
Figura 40. Objetivos del Modelo de Gobierno de Tratamiento de la Información.....	97
Figura 41. Metodología del Modelo de Gobierno de Tratamiento de la Información.....	100
Figura 42. Modelo de Resultados del Modelo de Gobierno Tratamiento de la Información. ...	110
Figura 43. Ejes Organizacionales del Modelo de Gobierno Tratamiento de la Información. ...	120
Figura 44. Ejes Proceso de Gestión de Riesgos.....	121

Figura 45 . Mapa de Riesgos.....	133
Figura 46. Elementos del Nivel Estratégico.	137
Figura 47. Modelo Acta Compromiso del Tratamiento de Datos Personales.....	151
Figura 48. Elementos del Nivel Táctico.	158
Figura 49. Elementos del Nivel Operativo.	161
Figura 50. Modelo de gobierno de tratamiento de la información para empresa colombiana...	162

Lista de tablas

Tabla 1. Modelo Metodológico.....	31
Tabla 2 Aplicación de las Categorías en las Empresas.....	87
Tabla 3 Niveles de Madurez por Categoría.....	92
Tabla 4. Matriz de Legislación Nacional Tratamiento de Datos Personales.	101
Tabla 5 Matriz de Legislación Internacional Tratamiento de Datos Personales.....	103
Tabla 6. Matriz de Buenas Prácticas de Tratamiento de la Información	109
Tabla 7 Variables de Evaluación del Riesgo.	123
Tabla 8 Criterios Evaluación del Riesgo.....	124
Tabla 9 Variables de impacto.....	124
Tabla 10 Criterios de Impacto.....	125
Tabla 11 Criterios de Aceptación de Riesgo.....	125
Tabla 12 Responsables y Funciones de la Gestión de Riesgos.	126
Tabla 13 Inventario de Activos.....	128
Tabla 14 Inventario de Amenazas.....	128
Tabla 15 Inventario de Controles.....	128
Tabla 16 Inventario de Vulnerabilidades.	129
Tabla 17 Inventario de Consecuencias.....	129
Tabla 18 Priorización de los Activos de Información.....	130
Tabla 19 Escenario de las Consecuencias.....	130
Tabla 20 Evaluación Probabilidad de Ocurrencia.....	130
Tabla 21 Evaluación Probabilidad de Impacto.	131

Tabla 22 Evaluación del Riesgo.....	132
Tabla 23 Criterios del tratamiento de riesgos.	134
Tabla 24 Criterios del tratamiento de riesgos.	134
Tabla 25 Elementos del Nivel Estratégico.....	136
Tabla 26 Estrategias de Tratamiento de Información de Datos Personales	144
Tabla 27 Métricas de Tratamiento de Información de Datos Personales.....	148
Tabla 28 Encargados de Tratamiento de Datos Personales.	152
Tabla 29 Elementos del Nivel Táctico.....	156
Tabla 30 Elementos del Nivel Operativo.....	159
Tabla 31 Partes Interesadas.....	163
Tabla 32 Inventario de Acuerdos Internacionales y Tratados de Libre Comercio.....	165
Tabla 33 Inventario de Contratación o Outsourcing de TI	165
Tabla 34 Evaluación del Contexto Jurídico.....	167
Tabla 35 Nivel de Cumplimiento del Contexto Jurídico.	168
Tabla 36 Análisis de Riesgos del Contexto Jurídico.....	168
Tabla 37 Plan de tratamiento de la información de datos personales.	169
Tabla 38 Ficha de Control de Actividades de Ejecución.....	170
Tabla 39 Ficha de Control de Seguimiento del Plan.....	171
Tabla 40 Plan de Mejora	171
Tabla 41 Partes Interesadas de Colombia Mayor.....	172
Tabla 42 Inventario de la Legislación Colombiana de Protección de Datos Personales para Colombia Mayor	174
Tabla 43 Inventario de Acuerdos Internacionales y Tratados de Libre Comercio.....	174

Tabla 44 Inventario de Contratación o Outsourcing de TI	175
Tabla 45 Evaluación del Contexto Jurídico.	176
Tabla 46 Nivel de Cumplimiento del Contexto Jurídico.	177
Tabla 47 Análisis de Riesgos del Contexto Jurídico.	178
Tabla 48 Plan de tratamiento de la información de datos personales.	179
Tabla 49 Ficha de Control de Actividades de Ejecución.	180
Tabla 50 Ficha de Control de Seguimiento del Plan.	182
Tabla 51 Plan de Mejora	183

Lista de apéndices

Apéndice A. Matriz de Operacionalización Documental	201
---	-----

Resumen

La organización empresarial se ha convertido en el punto de partida para el bienestar, progreso y desarrollo de las empresas; de allí, el afán por concretar acciones en el presente trabajo investigativo que tiene como norte: Diseñar un Modelo de Gobierno de Tratamiento de la Información para la Empresa Colombiana, como un elemento fundamental en la organización permitiendo la protección de datos personales, en cumplimiento de los derechos fundamentales de sus titulares. Partiendo de dicha intencionalidad, la investigación toma un camino centrado en el paradigma cualitativo apoyado en los preceptos de la investigación cualitativa que se apoya en la teoría fundamentada lo que conduce a repensar elementos teóricos procedimentales que permiten convertirse en herramientas para los gerentes de la actualidad que en todo momento requieren conocimientos ajustados a los cambios y transformaciones que se viven diariamente en las empresas; razón que fundamenta la investigación permitiendo dejar en su hacer un cúmulo de conocimientos aplicables en diversos escenarios de la organización empresarial que cada día exige mayor dedicación en pro de ofrecer una buena atención a los clientes y beneficiarios de los mismos.

Descriptores: organización, progreso, desarrollo, tratamiento de la información.

Abstrac

The business organization has become the starting point for the welfare, progress and development of companies; from there, the desire to specify actions in this research work that has as its goal: Design a Government Model for Information Processing for Colombian Companies, as a fundamental element in the organization allowing the protection of personal data, in compliance with the fundamental rights of their owners. Based on this intention, the research takes a path centered on the qualitative paradigm supported by the precepts of qualitative research that is based on grounded theory, which leads to rethinking procedural theoretical elements that allow them to become tools for today's managers. At all times they require knowledge adjusted to the changes and transformations that are experienced daily in companies; reason that bases the investigation allowing to leave in his do an accumulation of applicable knowledge in diverse scenarios of the business organization that every day demands major dedication in favor of offering a good attention to the clients and beneficiaries of the same ones.

Descriptors: organization, progress, development, treatment of information

Introducción

El mundo empresarial encierra un cumulo de elementos significativos dentro de lo que constituye la organización y por ende el tratamiento de la información que se maneja en cada uno de los escenarios que conforman las empresas; de allí el afán por establecer un aporte que permita canalizar acciones en función a ofrecer recursos y herramientas que contribuyan al éxito empresarial desde la perspectiva del tratamientos de la información lo que permite dar solidez a nivel corporativo para los gerentes y empresarios como para aquellos que disfrutan de sus beneficios.

El desarrollo de un modelo de tratamiento de la información de datos personales desde el contexto del gobierno de TI como una herramienta de apoyo a nivel corporativo para la empresa colombiana en razón de ser competitiva, sostenible y adaptable a las nuevas necesidades que exige la globalización y como parte de su prospectiva de su desarrollo organizacional en el cumplimiento de su misión, visión y metas establecidas. Este modelo se definirá a partir de la identificación de la legislación, normatividad y buenas prácticas vigentes sobre el tratamiento de la información y el análisis del impacto del Gobierno de TI en el tratamiento de la información de datos personales en la empresa colombiana a partir de la integración de componentes legales y buenas prácticas de seguridad y de TI. Complementario a lo anterior, se determinará la factibilidad de la aplicación del Modelo diseñado para una empresa colombiana que se enfrenta o mantiene su incentivo en ser reconocida en el tratamiento de la información de datos personales con altos niveles de calidad y seguridad de la misma en su entorno nacional e internacional.

Se presenta el modelo de gobierno de tratamiento de la información para la empresa colombiana en la globalización como prospectiva de desarrollo organizacional, a partir del estudio de la problemática actual sobre el tratamiento de los datos personales a nivel del Gobierno de TI, justificada y delimitada en el contexto de la empresa colombiana, estableciendo objetivos que permitan desarrollar esta propuesta, aplicando un método de investigación de tipo cualitativo a través de análisis documental considerando un marco referencial histórico, conceptual, contextual, teorías y aspectos legales como referencia fundamental para el desarrollo de este estudio. Así mismo, se describe la planeación administrativa para llevar a cabo el desarrollo de este proyecto.

Posteriormente, se hace presente el capítulo tres referido a lo que es la metodología de la investigación y se muestra los elementos correspondientes al paradigma de investigación que en este caso se plantea desde la perspectiva cualitativa apoyado en los preceptos que establece la teoría fundamentada apoyado en algunos elementos propios de la investigación; ahora bien, es importante señalar que allí se plantea lo concerniente al escenario y los informantes claves como también la credibilidad y validez como lo correspondiente a las técnicas e instrumentos de recolección de información como los procedimientos de análisis de la información.

Seguidamente se presenta el capítulo referido a los resultados donde se realiza un contraste de la información partiendo de la codificación abierta, axial y selectiva para posteriormente generar los aportes teóricos que permitirán la conformación de la estructura del modelo; partiendo de esos elementos se da paso al capítulo que encierra el modelo que se pretende

implementar teniendo en cuenta que se convertirá en un aporte significativo para los avances organizacionales de las empresas.

Capítulo 1. Modelo de gobierno de tratamiento de la información para la empresa colombiana en la globalización en la prospectiva del desarrollo organizacional

1.1 Planteamiento del problema

El tratamiento de la información se fundamenta en aprender a transformar la información en conocimiento, es un término que en los últimos años ha conllevado a las organizaciones y a los países a tomar medidas pertinentes en razón de dar especial cumplimiento de los derechos fundamentales que les conciernen a las personas sobre el habeas data; El Gobierno de España (1999), en el artículo 3 de la Ley Orgánica de Protección de Datos de Carácter Personal del año 1999 define el tratamiento de datos como operaciones y procedimientos técnicos de carácter automatizado o no, que permiten su gestión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. En el Modelo Gavilán de competencia (Eduteka, 2007), se habla del manejo de la información en cuatro etapas: la definición, la búsqueda y evaluación, el análisis, y por último la síntesis y uso de la información. En Colombia la Ley 1581 de 2012 (Congreso de la República de Colombia, 2017), define tratamiento como cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. Su ciclo comprende la generación, el almacenaje, el procesamiento y la transmisión (Vivancos, 2014). En el contexto normativo la Red Iberoamericana Protección de Datos (2017) define el tratamiento de información como cualquier operación o conjunto de operaciones efectuadas mediante

procedimientos físicos o automatizados realizadas sobre datos personales, para el aprovechamiento, uso o disposición de datos personales.

Investigación realizada por la firma Infométrika Ltda. para el Ministerio de Tecnologías de la Información de Colombia, cuatro de cada diez entidades públicas no han implementado sistemas de gestión de la seguridad de la información (Infométrika, 2014), lo que demuestra que ha aumentado el grado de conciencia frente a la importancia de proteger la información.

Almanza (2016), en la Revista de Sistemas de la Asociación Colombiana de Ingenieros en las Tendencias 2016 Encuesta Nacional de Seguridad Informática Retos de la Ciberseguridad, indica que el 22% de personal de seguridad de las organizaciones manifiestan no estar sujetos a una regulación o normatividad de seguridad de la información incluyendo la Ley 1581 de 2012 de protección de datos personales, Ley 1712 de 2014 de Transparencia o el CONPES de ciberseguridad. Así mismo, manifiesta que el 29% de los directivos entienden y atienden recomendaciones de seguridad, el 36% de la alta gerencia tiene compromiso por la seguridad y el 45% en realidad participan en temas de seguridad. La Superintendencia de Industria y Comercio (2017) manifiesta que ha impuesto sanciones hasta por más de \$21 mil millones de pesos por violaciones de datos personales por parte de empresas y ha impuesto más de 610 sanciones desde el 2010.

A nivel internacional, la Agencia Española de Protección de Datos (2017) ha publicado sanción a Google por tratar sin consentimiento datos personales recogidos a través de redes WiFi con los coches de su servicio Street View. Igualmente, manifiesta que en el año 2016 se presentaron 7935 denuncias por inadecuado tratamiento de datos personales en España. En los

últimos años debido a las incursiones de amenazas informáticas o humanas como es el caso de la Ingeniería social que han enfrentado las empresas, se ha venido despertando el interés de la organización y de las personas en general sobre la importancia que realmente tiene la información para la empresa o en su vida propia, especialmente, cuando han sido víctimas de un impacto sobre la integridad, la confidencialidad y disponibilidad de la misma.

Según la Policía Nacional Dirección de Investigación Criminal e Interpol (2017), en su informe de amenazas del cibercrimen 2016-2017 se manifiesta que durante los últimos 3 años a través de las plataformas dispuestas por el Centro Cibernético Policial se recibieron 15.565 incidentes informáticos (Centro Cibernético Policial, 2017). Igualmente, se manifiesta que en el 2014, del total de incidentes atendidos, el 92% afectaban a los ciudadanos del común, para el 2015 el 63% y en el 2016 el 57%, presentando una disminución del 35%.

Mientras tanto, el sector empresarial pasó de un 5% a un incremento del 28% en los reportes atendidos. Lo que indica que las amenazas frente al tratamiento de la información se están inclinando más al sector empresarial.

1.2 Formulación del problema

¿Cuáles son los elementos que debe involucrar un modelo de gobierno TI para empresas colombianas que permitan fortalecer la protección de los datos personales en cumplimiento de los derechos fundamentales de sus titulares?

1.3 Objetivos

1.3.1 General. Diseñar un Modelo de Gobierno de Tratamiento de la Información para la Empresa Colombiana, como un elemento fundamental en la organización permitiendo la protección de datos personales, en cumplimiento de los derechos fundamentales de sus titulares.

1.3.2 Específicos. Contextualizar la legislación aplicable al tratamiento de la información de datos personales y prácticas relacionadas.

Estructurar el modelo de gobierno de tratamiento de la información para la empresa colombiana en la globalización como prospectiva de desarrollo organizacional.

Analizar la factibilidad de aplicación del Modelo de gobierno de Tratamiento de la Información para la empresa colombiana.

1.4 Justificación

Las Tecnologías de la Información y la Comunicación (TIC) son una de las principales referencias vigentes de la globalización cultural. (Silva, 2008). El impacto de las TIC no se refleja únicamente en un individuo, grupo, sector o país, sino que, se extiende al conjunto de las sociedades del planeta. Los propios conceptos de "la sociedad de la información" y "la globalización", tratan de referirse a este proceso (Belloch, 2014). Así, los efectos se extenderán a todos los habitantes, grupos e instituciones conllevando importantes cambios, cuya complejidad

está en el debate social hoy en día (Beck, U. 1998). Considerando lo mencionado, la Globalización exige un contexto organizacional que conlleve un contacto directo con tecnología e información empresarial o personal de titulares.

En el contexto de TI, Colombia en inversión tecnológica sigue siendo reservada en comparación con otros países desarrollados. Solo el 0,38 por ciento del PIB Colombiano es invertido en ciencia y tecnología actualmente (Ministerio de Comercio, Industria y Turismo de Colombia, 2017). De esta manera, en los últimos años se ha realizado esfuerzos significativos en cuanto a infraestructura, conectividad y acceso a las tecnologías de la información en las diferentes regiones del país. El gobierno colombiano ha definido políticas económicas y sociales en las tecnologías de la información a través de CONPES como el 3834 política para estimular la inversión privada en ciencia, tecnología e innovación a través de deducciones tributarias (Consejo Nacional de Política Económica y Social, 2015), el CONPES 3582 política nacional de ciencia, tecnología e innovación (Consejo Nacional de Política Económica y Social, 2009), CONPES 3854 política nacional de seguridad digital (Consejo Nacional de Política Económica y Social, 2016), Estrategia de Gobierno Digital del Gobierno.

Complementario a lo anterior, en términos de tratamiento de la información ha definido la Ley 1712 de 2014 Transparencia y del Derecho de Acceso a la Información Pública Nacional (Congreso de la República de Colombia, 2014), Ley 1581 de 2012 Protección de Datos Personales (Congreso de la República de Colombia, 2012), Ley 1273 de 2009 Protección de la Información y de los Datos - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Congreso de la

República de Colombia, 2009), Ley 527 de 1999 del Acceso y Uso de los Mensajes de Datos, del Comercio Electrónico y de las Firmas Digitales (Congreso de la República de Colombia, 1999), entre otras que fortalecen y controlan el uso de las tecnologías de la información en Colombia.

Frente al tratamiento de la información en el contexto de gobierno de TI, Priebe y Markus (2015), han desarrollado un Modelo de Información Comercial a nivel metodológico que hace relación a los proyectos, datos científicos y gobernanza de Big Data Castillo (2015), en su tesis menciona la gestión de datos como una mejora soporte para tomar decisiones en los negocios. Así mismo, Lepage (2014), en Perú presenta un –Diseño de un Modelo de Gobierno de TI con Enfoque de Seguridad de Información para Empresas Prestadoras de Servicios de Salud Bajo la Óptica de Cobit 5.0|. Así mismo, a nivel de gobierno en Colombia el Ministerio de Tecnologías de la Información y las Comunicaciones (2016), ha diseñado un modelo de seguridad y privacidad de la información. En Colombia (Rincón, 2016) ha desarrollado un framework para el gobierno de la información con base en COBIT. Conforme a lo manifestado, se evidencia claramente que esta problemática ha sido abordada desde el contexto de gobierno de TI especialmente al tratamiento de la información empresarial o corporativa y no a nivel de tratamiento de datos personales, el cual le permita a la empresa proteger los derechos fundamentales de los titulares de la información.

Desde el contexto de datos personales, Gacitúa (2014), presenta en su tesis doctoral manifiesta en su tesis doctoral la importancia que tiene –El Derecho Fundamental a la Protección de Datos Personales en el Ámbito de la Prevención y Reprensión Penal Europeall. Así mismo desde el contexto de las tecnologías, la importancia que tienen la información, el gobierno de

datos en la organización y de ciberseguridad, hoy en día manifiesta la necesidad que debe tener la empresa en el manejo de su información como parte del gobierno corporativo y de la seguridad que debe ser aplicada sobre el tratamiento de la misma (IEEE, 2014). Por tal motivo, el diseño del Modelo de Tratamiento de la Información contribuirá a la empresa colombiana en términos de aspectos sociales en razón de apoyar el tratamiento de los datos personales de los titulares y el respeto de sus derechos fundamentales; a nivel tecnológico, a la adaptación de la tecnología de la empresa frente al uso adecuado tratamiento de la información de los datos personales; a nivel ambiental y cultura frente a la transformación digital del tratamiento de la información de los datos, e incluso a nivel político como una apoyo de parte del gobierno corporativo de TI al cumplimiento de estándares y tratados internacionales sobre el tratamiento de los datos personales.

1.5 Delimitaciones

1.5.1 Delimitación geográfica. A nivel geográfico el Modelo de Gobierno de Tratamiento de la Información será diseñado para la aplicación en la empresa colombiana que lo considere pertinente como una buena práctica organizacional.

1.5.2 Delimitación temporal. Este modelo se desarrolla en cumplimiento académico de la Maestría en Gobierno TI de la Universidad Francisco de Paula Santander Ocaña. Por tal motivo, la realización de este proyecto de investigación se establece para un tiempo aproximado de un (1) año.

1.5.3 Delimitación conceptual. A nivel conceptual se limita a la aplicación de buenas prácticas de gobierno de TI, seguridad y tratamiento de la información existentes conforme a los estándares internacionales y a la legislación vigente en un contexto nacional e internacional de acuerdo a los tratados de comercio establecidos que impacten o relacionen el tratamiento de datos personales.

1.5.4 Delimitación operativa. A nivel Operativo se limita a la definición de elementos que como parte de un modelo el cual apoye y fomente un tratamiento a la información en la organización en términos de la legislación y normatividad aplicable a la misma. El Modelo de Tratamiento de la Información se limita a la validación del mismo en una empresa colombiana.

Capítulo 2. Marco referencial

En cuanto a este apartado es importante señalar que está conformado por varios marcos teóricos reflejados desde el marco histórico, el conceptual, el contextual, el teórico, el legal entre otros; lo cual permite mostrar algunos elementos por donde se plantea la investigación y al igual define lo concerniente a lo que varios estudiosos lo llaman el estado del arte, a la vez se instituyen las bases legales de la investigación que posteriormente se convierten en base para el modelo que se pretende implementar, tal como se observa a continuación.

2.1 Marco histórico

En el contexto histórico el tratamiento de la información a nivel mundial y local ha trascendido a un entorno normativo que le permita mantener un control y garantizar los derechos de los ciudadanos, especialmente, en defensa del derecho de la intimidad, la honra y de la información como lo establece la Constitución Política de Colombia (1991), en su artículo 15, 20 y 21, respectivamente.

Bautista (2015), afirma que la Constitución de 1991, en relación al artículo 12 y 19 de la Declaración Universal de Derechos Humanos (Asamblea General de las Naciones Unidas, 1948), contempla como derechos fundamentales con entidad propia y dimensión bien definida de una parte del derecho a la intimidad, la honra y derecho a la información. Así mismo, manifiesta que la Sentencia del Tribunal Supremo de los Estados Unidos sobre Protección de Datos Personales (Whalen y Roe, 1977), trata el tema de la intimidad y la sistematización de información, fallo

que provocó la acción de unos ciudadanos que estimaron vulnerado su derecho a la intimidad. La Declaración de Santa Cruz de la Sierra (2003), los Jefes de Estado y de Gobierno de veintidós países iberoamericanos manifestaron que –la protección de datos personales es un derecho fundamental de las personas cita (Remolina, 2012), en su artículo sobre la aproximación constitucional de la protección de datos personales en Latinoamérica.

Así mismo, a nivel de América ya regulan la protección de datos personales, Argentina a través de la Ley 25326, Uruguay con la Ley 18331, México con la Ley Federal de Protección de Datos (LFPD), Perú con la Ley 29733 (Valbuena, 2014). A nivel de Europa, España entre otros países, ha establecido la Ley Orgánica de Protección de Datos de Carácter Personal (Gobierno de España, 1999).

A nivel de internacional la Organización de los Estados Americanos (OEA) ha definido la Ley Modelo Interamericana sobre Acceso a la Información Pública, la Ley Modelo sobre Garantías Mobiliarias, la Ley Modelo Interamericana sobre Protección de Datos Personales (en elaboración) (OEA, 2017).

La Red Iberoamericana de Protección de Datos (2017) ha constituido los Estándares de Protección de Datos Personales para los Estados Iberoamericanos. El Parlamento Europeo y el Consejo de la Unión Europea (2016), ha publicado el Reglamento General de Protección de Datos (General Data Protection Regulation, GDPR), relativo a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Calveras y Ganuza (2005) afirman que la empresa debería tener una responsabilidad social, implicando en el contexto del tratamiento de la información de datos personales un deber de manejarlos adecuadamente en sus operaciones y responder a sus clientes o titulares por la protección de los mismos.

Domínguez (2004), manifestaba que la fragmentación productiva, la globalización y la asociatividad propia de los fenómenos de integración económica y social, demandaría una transferencia internacional de datos personales (importación o exportación información).

Colombia en razón de tratamiento de información ha establecido legislación sobre esta temática. El Congreso de la República (2017), manifiesta la disposición de leyes en este contexto relacionadas con la Ley 23 (1982) por el cual se reglamentan los derechos de autor, Ley 527 (1999) referente al acceso y uso de los mensajes de datos, del correo electrónico y firmas digitales, Ley 594 (2000) reconocida como la ley general de archivos, Ley 1266 (2008) que menciona 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.

Ley 1273 (2009) por la cual se reglamenta la protección de la información y de los datos, también reconocida como ley de delitos informáticos en Colombia Ley 1581 (2012) por el cual se reglamenta la protección de datos personales en Colombia, La Ley 1712 (2014) referente a la Transparencia y del Derecho de Acceso a la Información Pública Nacional.

2.2 Marco conceptual

2.2.1 Tratamiento de datos personales. El tratamiento de datos personales como teoría en Colombia se establece a través de la Ley 1581 de 2012, el cual considera el tratamiento como la operación que se ejerce sobre los datos personales, como la recolección, uso, almacenamiento, transporte o supresión. Así mismo, la Ley define el Dato personal como aquella información que se encuentra asociada o vinculada a una o varias personas de manera que pueda ser determinada o determinable. De igual manera, considera Dato Sensible a todo dato que pueda afectar el derecho a la intimidad personal conforme al artículo 15 de la Constitución Política de Colombia de 1991, o dar pie a la discriminación.

Así, Datos Sensibles de acuerdo a la legislación colombiana en el artículo 5 de la Ley 1581 de 2012 son los datos relacionados con –el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricosl.

La Ley 1581 de 2012 fundamenta la protección de los datos personales en diferentes principios fundamentales de acuerdo a lo establecido en el artículo 4 de la presente Ley:

- El **Principio de legalidad** que hace referencia a “una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollenl.

- **Principio de finalidad** que –obedece a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.
- **Principio de libertad** mediante el cual los datos personales —sólo pueden ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
- **Principio de veracidad o calidad, el cual se fundamenta en que la información** —debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- **Principio de transparencia**, el cual –garantice el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
- **Principio de acceso y circulación restringida, donde** “el Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.

- **Principio de seguridad**, donde “la información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”.
- **Principio de confidencialidad**, el cual hace referencia a “todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma”.

2.3 Marco contextual

2.3.1 Tratamiento de datos personales en la empresa Colombiana. El trabajo se desarrollará para la empresa colombiana como apoyo a su cumplimiento legal, social, económico y organizacional del tratamiento de los datos personales que manejan en sus operaciones, frente a los requisitos que hoy en día exige la globalización en términos empresariales.

La Real Academia de la Lengua (2017), define empresa como una -Acción o tarea que entraña dificultad y cuya ejecución requiere decisión y esfuerzoll o Unidad de organización dedicada a actividades industriales, mercantiles o de prestación de servicios con fines lucrativosll. Así mismo, a nivel de nuestro país el artículo 15 del Código de Comercio dice que

–se entenderá por empresa toda actividad económica organizada para la producción, transformación, circulación, administración o custodia de bienes, o para la prestación de servicios. Dicha actividad se realizará a través de uno o más establecimientos de comercio. De igual manera, este concepto lo asocia al concepto de persona jurídica como lo manifiesta en el artículo 98 del mismo documento manifestando que –por el contrato de sociedad dos o más personas se obligan a hacer un aporte en dinero, en trabajo o en otros bienes apreciables en dinero, con el fin de repartirse entre sí las utilidades obtenidas en la empresa o actividad social. Dada una constitución de un ente como empresa en Colombia el artículo 100 del Código de Comercio define la asimilación a sociedades comerciales y legislación mercantil en Colombia, considerando que –se tendrán como comerciales, para todos los efectos legales las sociedades que se formen para la ejecución de actos o empresas mercantiles. Si la empresa social comprende actos mercantiles y actos que no tengan esa calidad, la sociedad será comercial. Las sociedades que no contemplen en su objeto social actos mercantiles, serán civiles.

En Colombia existen diferentes tipos de empresa. De acuerdo a lo establecido en la Ley 905 de 2004 se promueve el desarrollo de la micro, pequeña y mediana empresa en Colombia. Así mismo, el Ministerio de Industria y Comercio mencionan Leyes marco del Desarrollo Empresarial para las empresas en Colombia, indicando que toda empresa debe cumplir una regulación del país. Así mismo, las Superintendencias y demás entes de control desarrollan normativas para regular el sector que les compete respecto al campo de acción de la cual son responsables de controlar en el país. Consecuente con lo anterior, respecto al tema que se pretende desarrollar en este proyecto la Superintendencia de Industria y Comercio ha emitido la Ley 1581 de 2012 por el cual se regula la protección de datos personales para todas las empresas

en Colombia que son reguladas por esta entidad, razón por la cual, el marco contextual de este trabajo se enmarca a toda empresa colombiana.

2.4 Marco teórico

El proyecto se desarrollará con base a teorías soportadas en estudios realizados, regulación o buenas prácticas sobre la temática de gobierno de TI y del tratamiento de datos personales.

2.4.1 Gobierno de tecnologías de la información. En lo que respecta a teorías o buenas prácticas de Modelos de Gobierno se puede citar el Marco de Negocio para el Gobierno y la Gestión de TI de la Empresa se fundamenta en cinco (5) principios relacionados con: a) satisfacer las necesidades de las partes interesadas; b) cubrir la empresa; c) aplicar un marco de referencia integrado; d) propender un enfoque holístico a través de siete (7) categorías soportadas en: - principios, políticas, y marcos de trabajo, - proceso, - estructuras organizativas, cultura, ética y comportamiento, - información, - servicios, infraestructuras y aplicaciones, - personas, habilidades y competencias; e) mantener separado el gobierno de la gestión.

El Gobierno en la empresa como lo define COBIT en su versión 5, considera que se enfoca en la evaluación de las necesidades, condiciones y oportunidades de las partes interesadas con el fin de alcanzar las metas corporativas de manera equilibrada y acordada, constituyendo una dirección con base a la prioridad, toma de decisiones, medición del desempeño o rendimiento y el cumplimiento de la misma frente a las metas trazadas.

2.4.2 Seguridad de la información. La Seguridad de la Información de acuerdo a lo establecido por la ISO 27001 se define como la preservación de la confidencialidad, integridad y disponibilidad de la información.

2.4.3 Sistema de gestión de seguridad de la información. El Sistema de Gestión de Seguridad de la Información de acuerdo a lo descrito en la ISO 27001 es la parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la Información.

2.5 Marco legal

El proyecto respecto al gobierno de TI en el tratamiento de datos personales se fundamenta en la siguiente regulación:

- congreso de la república de Colombia. ley 1581 de 2012. ley de protección de los datos personales.
- congreso de la república de Colombia. ley 1273 de 2009. ley de protección de la información y de los datos.
- congreso de la República de Colombia. Constitución Política de Colombia de 1991. artículo 15 y 20.
- Ministerio de comercio, industria y turismo. decreto 1377 de 2013. por el cual se reglamenta parcialmente la ley 1581 de 2012.

- Ministerio de comercio, industria y turismo. decreto 886 de 2014. por el cual se reglamenta el artículo 15 de la ley 1581 de 2012, relativo al registro nacional de bases de datos.
- Congreso de la república de Colombia. ley 594 de 2000. ley general de archivos.
- Congreso de la república de Colombia. ley 1266 de 2008. ley del hábeas data.
- Congreso de la república de Colombia. ley 23 de 1982. ley de derechos de autor.
- Congreso de la república de Colombia. ley 44 de 1993. por la cual se modifica y adiciona la ley 23 de 1982 y se modifica la ley 29 de 1944.
- Congreso de la república de Colombia. ley 527 de 1999. ley de acceso y uso de los mensajes de datos, del correo electrónico y firmas digitales.
- Congreso de la república de Colombia. ley 594 de 2000. ley general de archivos.
- Congreso de la república de Colombia. ley 1520 de 2012, por la cual se establece la responsabilidad por infracciones al derecho de autor y los derechos conexos en internet.
- Congreso de la república de Colombia. ley 1712 de 2014. ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

Capítulo 3. Metodología

En cuanto a los elementos que conforman la parte metodológica es importante indicar que en esta parte del proyecto se define lo que es la ruta metodológica, entendiéndose que es un procedimiento el cual permite canalizar las acciones necesarias para concretar los objetivos; teniendo presente que el trabajo que se viene desarrollando se encuentra enmarcado en el paradigma cualitativo bajo los elementos teóricos que encierra la teoría fundamentada; lo que permite definir los aspectos a cubrir durante el desarrollo de la investigación.

3.1 Diseño metodológico

El desarrollo de este de proyecto se fundamentará en una metodología cualitativa basada en la teoría fundamentada (Strauss y Corbin, 2002), manteniendo un enfoque descriptivo, en el cual a partir del análisis documental se captará la realidad que enfrenta actualmente la empresa colombiana en el tratamiento de datos personales frente a la globalización. Según Martínez (2004), la investigación cualitativa es —...descriptiva, inductiva, fenomenológica, holista, ecológica, sistémica, humanista, de diseño flexible y destaca más la validez que la replicabilidad de los resultados de la investigaciónl (p. 8).

Por lo tanto, favorece las transformaciones necesarias para superar problemáticas específicas a partir de la participación activa de los miembros que componen dicha comunidad, quienes asumen conciencia activa de su rol mediante la autorreflexión y reconocimiento de sus necesidades. Popkewitz (1988) afirma que algunos de los principios del paradigma son: (a)

conocer y comprender la realidad como praxis; (b) unir teoría y práctica, integrando conocimiento, acción y valores; (c) orientar el conocimiento hacia la emancipación y liberación del ser humano; y (d) proponer la integración de todos los participantes. Desde esta perspectiva, el conocimiento se construye a partir de la interacción entre los seres humanos y el mundo; este conocimiento se desarrolla y es transmitido en contextos esencialmente sociales.

En este aspecto Bonilla y Rodríguez (1997) plantean que -la Investigación Cualitativa intenta hacer una aproximación global de las situaciones sociales para explorarlas, describirlas y comprenderlas de manera inductiva... a partir de los conocimientos que tienen las diferentes personas involucradas en ella... esto supone que los individuos interactúan (p.70). En este aspecto, la investigación cualitativa busca comprender la realidad por medio de la interacción de todos los actores que influyen en el proceso investigativo, desde una mirada holística del fenómeno, es decir, no busca variables que determinen una conducta particular, sino que a través de ella busca la comprensión del todo, pues la configuración global de un contexto puede cambiar al variar una de sus partes y esto va a depender de los diferentes factores que influyen en la realidad de estudio.

Para investigar cualitativamente hay que situarse dentro del contexto por lo tanto esta investigación es participativa, entrando en contacto directo con el entorno o ambiente donde se sitúa la investigación, permitiendo que se desarrolle un proceso de retroalimentación constante entre el investigador y el individuo que forman parte de la realidad estudiada, donde no interesa dimensionar magnitudes, sino explorar naturalezas, las cuales se conciben desde múltiples

perspectivas, apoyándose en los diferentes métodos cualitativos pertinentes como vía de obtención de conocimientos.

3.1.1 Historia de la teoría fundamentada. La teoría fundamentada nace en el siglo XX en la Universidad de Chicago (Estados Unidos) en la escuela de sociología como una nueva opción diferente a las teorías aplicadas hasta ese momento en este campo de acción. Glaser y Strauss quienes en el año 1967 desarrollaron la teoría fundamentada como una metodología que apoyaría teorías del comportamiento humano y social de manera empírica (Kendall, 1999).

La Teoría Fundamentada es considerada un método de investigación basada en los datos con el fin de identificar procesos sociales (Glaser y Strauss, 1967). Así mismo, a partir de un enfoque cualitativo conduce a obtener respuestas sobre lo ocurrido y la razón de los fenómenos sociales. A partir de la obra *-The discovery of grounded theory* desarrollada por Glaser y Strauss en 1967, el cual marcó cierto reconocimiento en esta época, cada uno de los autores inicia un trabajo complementario por separado de la Teoría Fundamentada. Así en 1990 Strauss trabaja con Corbin sobre la Teoría Fundamentada dando origen a una nueva obra denominada *-Basics of Qualitative research: grounded Theory, procedures and techniques*, manifestando que esta teoría se utiliza para entender mejor los fenómenos de estudio profundizando más en los mismos.

Sandoval (1997) concibe que la teoría fundamentada es una metodología que conduce al desarrollo de teoría partiendo de los datos capturados de manera sistemática y que a partir de su análisis se toma una idea de pensar sobre los mismos para llegar a lograr conceptuarlos. Glaser

(1992) define la teoría fundamentada como una metodología de análisis el cual recolecta datos utilizando métodos sistemáticos con el fin de dar origen a una teoría basada en la inducción de un área sustantiva, obteniendo como resultado una formulación de una teoría o hipótesis de manera conceptual sobre el área sustantiva u objeto de estudio evaluado.

Otros autores como Charman (2005), manifiesta que desde el punto de vista de la investigación la teoría fundamentada se concibe como un método de análisis definida con unas directrices que apoyan la investigación en su recolección sucesiva de información o datos y desarrollos conceptuales para la construcción de teorías.

Considerando las definiciones dadas anteriormente, en lo que respecta a este proyecto se alude que la teoría fundamentada es la metodología adoptada para el desarrollo del mismo donde a partir de una recolección consecutiva o permanente de información sobre el objeto de estudio que en esta investigación se relaciona con el gobierno de tratamiento de datos personales, contribuya al desarrollo de elementos que permitan establecer un modelo teórico práctico para que permita a empresa colombiana cumplir con los requisitos legales exigidos actualmente en términos de privacidad de la información de los titulares que maneja en sus operaciones, estableciendo un gobierno corporativo desde las tecnologías de la información y adoptando buenas prácticas de seguridad de la información que le permitan asegurar los datos personales, dando seguridad y confianza a sus propietarios, y como organización ser sostenible y evolutiva frente a las necesidades del contexto globalizado del mercado. La teoría fundamentada tiene afinidad con otras teorías como la teoría sustantiva en razón de enfocarse a la construcción

teórica a partir de la recolección de datos o generados de aspectos de la realidad humana sobre el objeto de estudio, manteniendo una investigación abierta y dinámica.

Así mismo, se relaciona con la teoría formal respecto al desarrollo conceptual más universal que se puede generar a partir del estudio de disciplinas científicas ya establecidas utilizando la comparación y sosteniendo una investigación cerrada y estática. La teoría formal puede partir de una recolección y análisis de datos, es decir, iniciar con la aplicación de la teoría sustantiva. Consecuente con lo anterior, la integración de una recolección de datos y un análisis de teorías que pueden conllevar a la validación de hipótesis generadas de manera permanente en el proceso de investigación. De esta manera, partiendo de una teoría sustantiva para consolidar una teoría formal, se puede considerar que la Teoría Fundamentada al manejar las dos teorías mencionadas mantiene un enfoque inductivo y deductivo sobre el estudio de los diferentes fenómenos que se consideren en una investigación. La teoría fundamentada tiene como objetivo primordial el descubrimiento de una teoría que explique de manera comprensible o acertada un fenómeno de estudio en particular (Cuñat, 2007).

3.1.2 La teoría fundamentada en la empresa. La Teoría Fundamentada es una metodología que puede ser de gran apoyo para el desarrollo empresarial. Glaser (1992) afirma que la Teoría Fundamentada ayuda al desarrollo de la investigación en temas relacionados con el comportamiento humano en la organización o diferentes entornos sociales. De esta manera como lo afirma Douglas (2004), se puede concluir que esta teoría puede aplicarse al estudio de cualquier organización ya que la creación de empresa es considerada un proceso social.

3.1.3 Estrategias del método de Comparación

- Interrogatorio sistemático para relacionar conceptos.
- Muestreo teórico.
- Categorización sistemática (codificación).
- Seguimiento de principios para lograr un desarrollo conceptual.

3.1.4 El proceso de la teoría fundamentada. Un estudio o investigación aplicando la Teoría Fundamentada debe partir de mantener inquietudes permanentes sobre el tema específico de interés. De esta manera, es importante tener las siguientes expectativas:

- Qué es lo que pasa.
- Qué sucede.

3.1.5 Estrategias para la teoría fundamentada. Se consideran las siguientes estrategias para aplicar la Teoría Fundamentada:

- Recolectar y analizar datos concurrentemente.
- Determinar procesos y productos de la investigación a partir de los datos.
- Descubrimiento y desarrollo teórico a partir de los procesos analíticos.
- Muestreo teórico a partir de los datos para refinar, elaborar y completar categorías.
- Uso sistemático de los procedimientos analíticos.
- Circularidad del proceso (desarrollo continuo).

De acuerdo a lo manifestado por Glaser y Straus (1967), este es un proceso continuo en el cual los estadios establecidos se transforman a partir de los análisis realizados de manera concurrente hasta terminar la totalidad del análisis de la investigación. De esta manera, el estudio o investigación cualitativa de acuerdo a lo mencionado se fundamenta en la recolección de datos, codificación, análisis e interpretación de la información para llegar a lograr establecer una teoría como resultado al objeto de estudio. Así, este método de investigación se comporta como un método de comparación de manera constante, en el cual existe una comparación permanente y continua entre los códigos y clasificaciones de información del objeto de estudio, integrando cada análisis anterior con los posteriores.

3.1.6 Criterios de la teoría fundamentada. La Teoría Fundamentada maneja los siguientes criterios:

- Ajuste: esto es, que encaje en la experiencia de los participantes.
- Funcionamiento: que explique la mayor variedad posible.
- Relevancia al fenómeno en estudio.
- Posibilidad de la propia teoría de modificarse, es decir, que la teoría pueda acomodarse a nuevos hallazgos. (Glaser B. Theoretical Sensitivity: Advances in the methodology of Grounded Theory, 1978).

3.1.7 Elementos de la teoría fundamentada. La Teoría Fundamentada se compone de elementos que hacen parte del proceso de investigación para el objeto de estudio. Estos son los siguientes:

- Muestreo teórico.
- Método comparativo constante.
- Codificación.
- Categorización.
- Teorías.

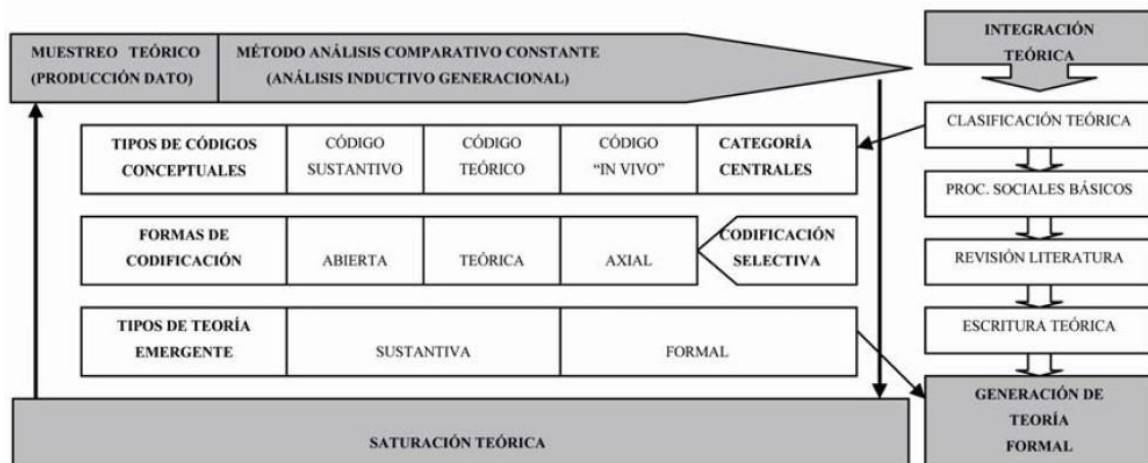


Figura 1. Elementos de la Teoría Fundamentada

Fuente. Adaptación de Carreño (1998)

Muestreo teórico. El muestreo teórico es una recolección de datos constante durante la investigación hasta lograr una saturación teórica relacionada con el objeto de estudio, el cual comprende el análisis de los datos y categorías con el fin de lograr definir una teoría como resultado final. De esta manera, se podría considerar que este tipo de muestreo es un proceso que funciona en espiral logrando identificar información durante todo el estudio o investigación. En otras palabras, en un proceso de mejora continua sobre la recolección y análisis de la información para cumplir los objetivos de la investigación. Considerando lo anterior, cabe citar la teoría del campo que complementa la teoría fundamentada y en razón del muestreo teórico tiene una relación directa frente a este proceso que en el caso de la teoría del campo se considera como una

actividad en la investigación que funciona en espiral, haciendo uno análisis, realizando una síntesis o propuesta y finalizando con una evaluación de manera continua (Kurtlewin, XXX).

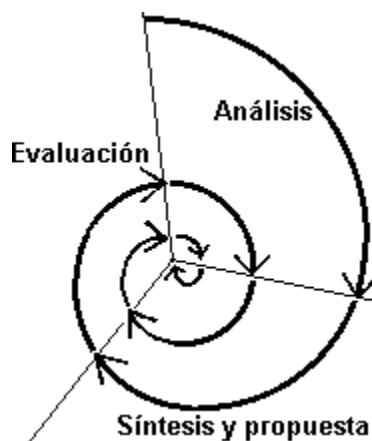


Figura 2. Modelo General Teoría de Campo.
Fuente. Kurtlewin.

De manera específica, el comportamiento de este proceso relacionado con la teoría del campo se muestra reflexión teórica permanente durante la investigación para tomar decisiones apropiadas sobre la misma. A continuación, se muestra gráficamente este proceso específico.

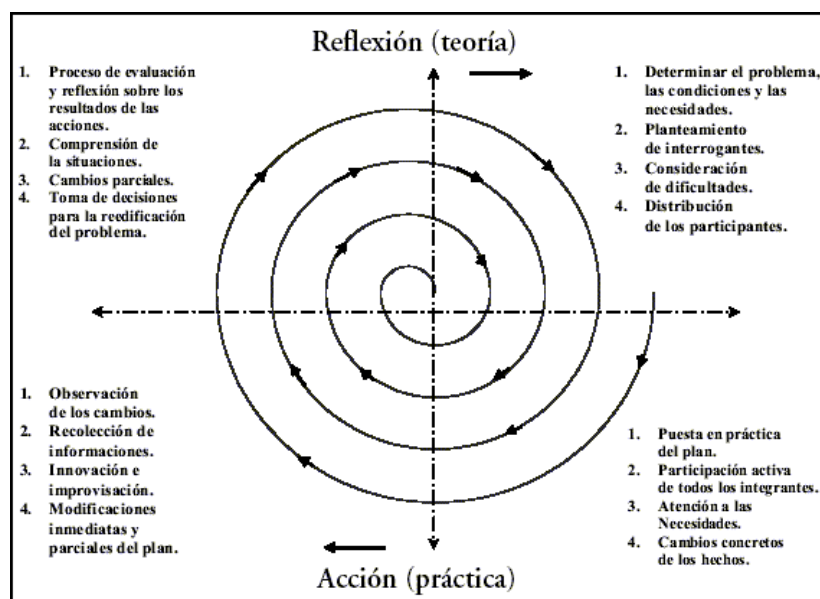


Figura 3. Modelo Específico Teoría de Campo.
Fuente. Kurtlewin.

El muestreo teórico permite establecer categorías sobre los datos encontrados que ayudan a determinar unidades de información de calidad permitiendo profundizar en una temática en particular a partir de la identificación de incidencias con la oportunidad de afianzar códigos y propiedades de los datos como parte del logro de los objetivos de la investigación. A continuación, se ilustra el proceso de muestreo teórica partiendo de la recolección de datos y siguiendo de manera constante un análisis de los datos hasta llegar a la saturación teórica del caso de estudio:



Figura 4. Proceso de muestreo teórico.
Fuente. Bisquerra (2004: 319)

Método comparativo. Este método es un proceso en el cual tiene como objetivo realizar una comparación constante de los datos obtenidos del muestreo teórico y las incidencias presentadas en el caso de estudio para lograr llegar a establecer una teoría. En este método comparativo se establecen las siguientes fases:

- Comparación de incidencias y categorización.
- Integración de categorías y propiedades.
- Conceptualización y reducción de la teoría.
- Definición de la teoría.

Codificación. La codificación es un proceso que permite la identificación de los datos a través de códigos relacionando las categorías existentes o que van emergiendo del proceso de investigación. La codificación se puede dar considerando los siguientes tipos:

- **Codificación abierta.** Esta se entiende como la parte inicial de identificación de datos que permiten determinar categorías de la información recolectada.
- **Codificación selectiva.** La codificación selectiva ya consiste en la definición de un código determinado para una variable central respecto a la categoría central del proceso, reduciendo así el número de categorías, simplificando así el proceso.
- **Codificación teórica.** Este tipo de codificación ayuda a establecer las relaciones o conexiones entre los códigos sustantivos y propiedades de las diferentes categorías como parte de integral para lograr construir o determinar una teoría.
- **Codificación axial.** La codificación axial permite la relación entre códigos de manera inductiva o deductiva en la investigación.

A continuación, se ilustra los tipos de codificación en la Teoría Fundamentada:

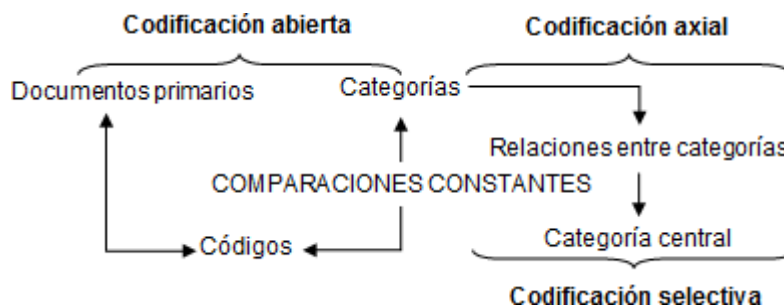


Figura 5. Codificación.

Fuente. Adaptación de Modelo de Strauss y Corbin.

Categorización. La categorización es el proceso en el cual se clasifican los datos e incidencias descubiertas y que hacen parte de una investigación. A continuación, se ilustra un proceso de generación de categorías:

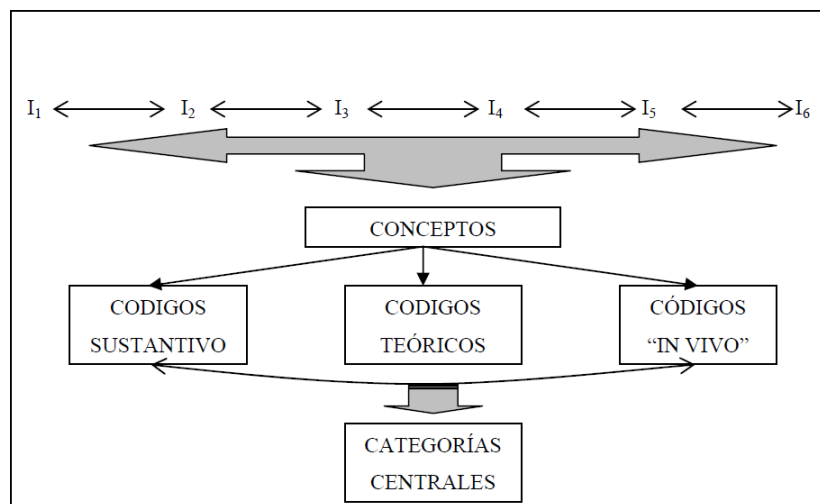


Figura 6. Proceso de generación de categorías.

Fuente. Adaptación del Modelo de Glaser (1978).

Teorías. El propósito de la Teoría Fundamentada es determinar una teoría formal a partir de una teoría sustantiva. Por tanto, estas dos teorías hacen parte del proceso de la Teoría Fundamentada.

La teoría sustantiva hace referencia a la parte inicial de la investigación donde se identifican los datos, el cual a partir de su análisis considerando la codificación y la categorización conllevan a la construcción de una teoría formal del caso de estudio.

Así, la teoría formal hace referencia a aquella que es definida a través de la identificación, estructuración y análisis de los datos previamente descubiertos como parte de la teoría sustantiva.

3.1.8 Seguimiento Metodológico del Proyecto. El seguimiento metodológico se encuentra establecido en el siguiente modelo metodológico:

Tabla 1. Modelo Metodológico.

OBJETIVOS DE LA INVESTIGACIÓN	ACTIVIDADES POR OBJETIVO	INDICADOR POR ACTIVIDAD
Obj 1. Contextualizar la legislación aplicable al tratamiento de información de datos personales y prácticas relacionadas.	Act 1. Análisis Documental para: Identificar la legislación nacional sobre el tratamiento de la información.	Ind 1. Matriz de legislación de tratamiento de datos personales.
	Act 2. Análisis documental para: Identificar la legislación internacional sobre el tratamiento de la información.	Ind 2. Matriz de legislación de tratamiento de datos personales.
	Act 3. Análisis documental para: Identificar buenas prácticas de tratamiento de la información.	Ind 3. Matriz de buenas prácticas de tratamiento de la información.
Obj 2. Estructurar el modelo de gobierno de tratamiento de información para la empresa colombiana en la globalización como prospectiva de desarrollo organizacional.	Act 1. Análisis Documental: Investigar el tratamiento de la información en las empresas colombianas.	Ind 1. Documento de tratamiento de la información en la empresa colombiana.
	Act 2. Análisis Documental: Analizar el impacto del Gobierno de TI en el tratamiento de la información en la empresa colombiana a partir de los resultados obtenidos.	Ind 2. Documento de tratamiento de la información en la empresa colombiana.
	Act 3. Diseñar el modelo de gobierno de tratamiento de la información para la empresa colombiana.	Ind 3. Modelo de gobierno de tratamiento de la información para la empresa colombiana.

Tabla 1. Continuación

	Act 3. Determinar el impacto del Gobierno de TI en el tratamiento de la información en la empresa colombiana a partir de los resultados obtenidos.	Ind 3. Informe de tratamiento de datos personales en la empresa colombiana.
Obj 3. Determinar la factibilidad de aplicación del Modelo de gobierno de TI para la empresa colombiana en la globalización.	Act 1. Diseñar caso de estudio para aplicar el modelo.	Ind 1. Caso de estudio.
	Act 2. Aplicar modelo en caso de estudio.	Ind 2. Documento aplicación caso de estudio del modelo.
	Act 3. Determinar la factibilidad del modelo a partir del resultado obtenido en su aplicación en el caso de estudio.	Ind 3. Documento aplicación caso de estudio del modelo.

Fuente. Autor del proyecto

Escenario. La selección del escenario de la investigación, es considerada como uno de los aspectos primordiales que influyen en el logro de los objetivos planteados y el éxito de la investigación. En este caso Rodríguez y Valdeoriola (s/f) expresan que: —la selección, la entrada y la retirada del escenario de la investigación son aspectos fundamentales (p. 48). En tal sentido la investigación se ejecuta en las siguientes empresas colombianas: COLOMBIA MAYOR, SEGUROS MUNDIAL, BDO AUDIT, UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA y MINISTERIO TIC.

Informantes claves. Los informantes son las personas que sirven de introductores al investigador en la comunidad investigada y sus mejores aliados durante su estancia allí. Por esta razón se requiere que sean representativos y conocedores de su grupo. A menudo se convierten en los mejores amigos del investigador, responden de él ante la comunidad, son sus fuentes primarias, y colaboran dándole consejos e información sobre cómo le ven en la comunidad.

Partiendo de dichos señalamientos se deben considerar cinco informantes bajo los siguientes criterios:

- Se entrevistarán los gerentes principales de cada una de las empresas seleccionadas a los cuales se les debe colocar un código para poder definir lo que señala cada informante.
- La información recolectada estará acompañada de la observación directa que se realice en cada una de las empresas seleccionadas.
- En caso de surgir algún informante emergente es importante señalar que se debe incluir en el momento de la codificación para el análisis respectivo.

Categorías previas. En referencia a las categorías previas de la investigación o de entrada es pertinente tener claro que en la investigación cualitativa dentro de la teoría fundamentada plantea algunas categorías preestablecidas, lo que no quiere decir que sean la únicas o las definitivas; puesto que, a medida que se avance surgirán las categorías que se convertirán en la base teórica de la investigación, en tal sentido, dicho aspecto se fundamenta en Martínez, (1994) quien señala:

Se podría partir de un grupo de categorías preestablecidas, con tal de que se utilicen con mucha cautela y como algo provisional hasta que no se confirmen, y no se deje uno llevar por la tendencia (cosa muy fácil y natural) de rotular la nueva realidad con viejos nombres. (p.9)

Como se puede apreciar el método permite un manejo ajustable del uso de las categorías siempre y cuando su aplicabilidad sea muy cautelosa para evitar cualquier trasgresión de la información o en su defecto algún sesgo de la misma. Por lo tanto, en el caso particular del trabajo se establecen algunas categorías de entrada denominadas de esta manera; por que a medida que se realicen observaciones y se apliquen los instrumentos de recolección de la

información surgirán las categorías definitivas, teniendo presente que dentro de la investigación cualitativa no se debe hablar de categorías definitivas; ya que las mismas poseen un alto grado de relatividad dependiendo en gran medida de factores externos y de la forma como sea observada, analizada e interpretada por el investigador; dentro de dichas categorías se tiene:

- Gobierno de TI.
- Tratamiento de la Información.
- Desarrollo organizacional.
- Estructura empresarial.
- Globalización en la empresa.
- Legislación vinculante.
- Normas prácticas.

Confiabilidad y validez. La credibilidad de la investigación recae en el proceso investigativo, donde el investigador recoge los datos y los procesa; posterior a ello para verificar regresa a los informantes claves y estos verifican si la interpretación realizada se encuentra ajustada a lo que es su realidad, su mundo o su cosmovisión, en ocasiones los informantes claves se convierten en garantes de los datos y las interpretaciones realizadas por la oportunidad que tienen de corregir y mejorar las apreciaciones y/o aportes que el investigador le otorga a determinado hecho, fenómeno o suceso que sea centro de atención durante la investigación.

Razón por la cual se toman los aspectos que manejan Guba y Lincoln (1985) en busca de establecer un rigor científico ajustable a las informaciones y hallazgos que se logren obtener a

medida que avance el proceso investigativo y más cuando se trata de una investigación social de carácter cualitativo. La credibilidad, es un aspecto que se encaja en la verificación de la rigurosidad metodológica de la investigación. Aunado a lo anterior se plantea la validez de los instrumentos que en esta ocasión se plantea mediante la validación de pares.

Se entiende por validación de pares que se estructuran los guiones de preguntas y se le agrega el protocolo de validación cualitativa; luego se hace la validación de pares expertos que estén vinculados con el área de conocimiento y la parte metodológica solo la complementa y orientan los metodólogos; es decir, el contenido se hace mediante pares de expertos y el apartado metodológico lo hacen dos metodólogos; esto permite corroborar una sistematización de la credibilidad y validez ajustable a lo que se quiere y enmarcado en los nuevos postulados de la investigación cualitativa.

Martínez (2009) define la validez como la fuerza mayor de la investigación cualitativa. En tal sentido, para recabar los datos, de captar cada cuento desde diferentes puntos de vista, de vivir la realidad estudiada, analizarla e interpretarla, es necesario que estén inmersos en su propia dinámica, lo cual ayuda a superar la subjetividad. (p.119) También la validez de la investigación se determina por la coherencia que se da de los resultados y la concordancia con otros estudios.

Técnicas de recolección de la información. Por tratarse de una investigación con enfoque cualitativo, bajo los preceptos de la teoría fundamentada, la recolección de la información se basará en instrumentos que faciliten la participación de los gerentes de las empresas sujeta al estudio, de manera que tanto el investigador como los informantes claves, puedan realizar este

proceso. En esta dirección, los procedimientos de recolección de información (observación y entrevista) precisan de unos mínimos planteamientos teóricos previos que los sitúe en el contexto donde van a ser utilizados. La técnica de la observación, tal como aquí se plantea, consiste en observar atentamente el caso, tomar información y registrarla para su posterior análisis, la observación es un elemento fundamental de todo proceso investigativo; en ella se apoya el investigador para obtener el mayor número de datos, por ello se tendrá en cuenta la observación no estructurada llamada también simple o libre, que es la que se realiza sin la ayuda de elementos técnicos especiales.

Otra estrategia a desarrollar dentro de la propuesta metodológica es la entrevista abierta no estructurada la cual permitirá que la gente responda a su manera y con su propia perspectiva. Es importante saber lo que se va a preguntar como lo que no tiene que preguntarse. A partir de entonces ha de preocuparse en el control de la veracidad de la información, comparando lo que se dice con lo que se puede observar o experimentar personalmente. De igual forma se tendrá en cuenta la triangulación que pretende algo parecido: se trata de combinar los distintos métodos o fuentes de datos para controlar las tendencias del observador y los relatos de los informantes.

3.1.9 Análisis de la información. El Análisis de la información obtenida en la puesta en práctica de cada uno de los instrumentos apropiados a la investigación cualitativa se efectúa comparando y estudiando cada uno de los contenidos obtenidos, para llegar a una posterior categorización, considerada por Buendía y Otros (2008) como —...conceptualización realizada a partir de la conjunción de elementos concretos que tienen características comunes». (p.184) Posteriormente, se procede a organizar de la información del diario de campo para efectuar la

triangulación de la información enfrentando instrumentos e informaciones obtenidas con el fin de extraer los datos más exactos y objetivos de la investigación efectuada, dándole validez al trabajo desarrollado, para Parra (2008) triangular significa –...comparar y constatar la consistencia de la información derivada de la misma fuente, pero en tiempos variados a través de diferentes métodos cualitativos. (p.62).

En el caso de la presente investigación se requiere aplicar la teoría fundamentada específicamente considerando el análisis microscópico que es una de las maneras de interpretar información para luego poder establecer el aporte teórico que permite: Diseñar un Modelo de Gobierno de Tratamiento de la Información para la Empresa Colombiana, como un elemento fundamental en la organización permitiendo la protección de datos personales, en cumplimiento de los derechos fundamentales de sus titulares.

Capítulo 4. Análisis de resultados

4.1 Contextualización del escenario

Como parte complementaria al análisis realizado se ha contextualizado el desarrollo de esta temática en diferentes empresas del sector público y privado del país. De esta manera, se identificaron y describieron las características de las siguientes empresas:

4.1.1 Colombia mayor

Ubicación. Bogotá.

Breve reseña histórica. El CONSORCIO COLOMBIA MAYOR es una alianza estratégica entre sociedades fiduciarias del sector público: FIDUPREVISORA S.A., FIDUCOLDEX S.A. y FIDUCENTRAL S.A., que tiene por objeto administrar los recursos del Fondo de Solidaridad Pensional, en virtud del contrato de fiducia pública No.216 de 2013, suscrito con el Ministerio del Trabajo.

En su calidad de administrador fiduciario del Fondo de Solidaridad Pensional tiene a cargo las subcuentas de solidaridad y subsistencia, con las que financia el Programa de Subsidio al Aporte en Pensión y el Programa de Solidaridad con el Adulto Mayor, Colombia Mayor.

El objeto social del CONSORCIO es la administración fiduciaria de los recursos del FONDO DE SOLIDARIDAD PENSIONAL creado por la ley 100 de 1.993 en su artículo 25 como una cuenta sin personería jurídica, adscrita al MINISTERIO DEL TRABAJO. La administración del fondo fue contratada con el Consorcio en el marco del Contrato de Fiducia Pública No. 216 con fecha de 30 de mayo 2013.

- Administración del Programa de Subsidio al Aporte en Pensión – Subcuenta de Solidaridad.
- Administración del Programa Colombia Mayor – Subcuenta de Subsistencia.

Misión. Para junio de 2017 continuaremos siendo reconocidos por el Gobierno Nacional y por la población impactada e involucrada en los Programas, como un equipo humano consolidado profesional y técnicamente capaz de administrar el negocio a largo plazo, sobre la base de nuestras creencias corporativas.

Visión. Somos un equipo humano dedicado a administrar los recursos del Fondo de Solidaridad Pensional, a través de los Programas Sociales: Colombia Mayor y Programa de Subsidio al Aporte en Pensión que atienden población vulnerable, fundamentados en nuestra experiencia y flexibilidad organizacional.

Planes y programas de organización empresarial.

- Plan de trabajo organizacional.
- Plan estratégico.

- Plan de seguridad de la información.
- Plan de continuidad del negocio.
- Plan institucional de archivo.
- Plan sistema integrado de conservación.
- Programa de gestión documental.
- Programa de auditoría.

4.1.2 Seguro mundial

Ubicación. Bogotá.

Breve reseña histórica. 1970 – 1972 Compañía Internacional de Seguros de Vida S.A. Se crea la Compañía Internacional de Seguros de Vida S.A., dedicada exclusivamente a la comercialización de seguros de personas.

1973 – 1981 Compañía Mundial de Seguros. La Organización fue adquirida por industriales de amplia y conocida trayectoria quienes designaron una nueva administración y la proyectaron en el mercado mediante una suscripción altamente técnica de los riesgos y el desarrollo y mejoramiento de los productos de acuerdo con las necesidades de los clientes, lo cual la ha situado en una posición destacada en el sector asegurador.

La sociedad cambió su razón social a Mundial de Seguros de Vida S. A. y en ese mismo año se creó la Compañía Mundial de Seguros S.A.

1981-1990 La Calidad en el Servicio. Durante este periodo la compañía evolucionó hacia un concepto que después haría parte muy importante de sus objetivos corporativos: "La Calidad en el Servicio".

Precisamente en la época donde el consumidor se hacía más exigente y las empresas trataban de aprovechar los "momentos de verdad" para brindar el mejor servicio posible, Mundial hizo parte de las empresas fundadoras de la Corporación Calidad y participó en un sin número de simposios especializados en busca de la excelencia en el servicio.

Se implementó la sistematización integral de procesos de seguros, lo cual le permitió trabajar con mayor agilidad sobre los estados financieros y la constante evaluación del negocio.

No menos importante fue el proceso de Planeación Estratégica de principios de los años 90's, donde varias de las temáticas abordadas en este estudio fueron las bases de los procesos posteriores y de las decisiones de futuro que la compañía tomaría para los años venideros.

1991-1995 La apertura del mercado. A principios de los 90's se socializó toda la información sobre las estrategias que desarrollaría la compañía y aunque el primer ejercicio de la apertura de mercado resultó ser uno en el cual muchas prácticas conocidas y utilizadas perdieron vigencia y validez, la gestión de las diferentes áreas buscó mantener siempre un alto nivel de conocimiento sobre el desenvolvimiento real de la compañía en comparación con el mercado.

Se continuaron refinando los procesos de expedición de pólizas a través del nuevo software integrado de seguros, para llevarlas a niveles de eficiencia y calidad destacadas dentro del mercado.

Se dieron importantes pasos para proyectar comercialmente a la compañía y posicionarla como un grupo asegurador de avanzada en el mercado colombiano, se cambió la imagen visual corporativa, se realizó una destacada campaña de publicidad institucional en periódicos y revistas de circulación nacional.

Se desarrollaron y lanzaron nuevos productos como las pólizas ESCUDO y CARRUS, y la actualización de todas las pólizas para brindar mayor claridad sobre ellas a nuestros asegurados.

1996 - 2000 La Especialización. La Compañía Mundial Seguros S.A. entendió la apertura del mercado asegurador como una oportunidad para crecer, progresar y servir, razón por la cual comprometió el esfuerzo y dedicación de toda la Organización en el diseño y desarrollo de un Plan Estratégico.

Este Plan determinó como estrategia la especialización en los ramos de Cumplimiento, Seguro de Vida Grupo Educativo, Aviación y SOAT.

Así, Mundial Seguros se convierte en la primera compañía especializada en el sector asegurador.

Durante las actividades desarrolladas en este periodo se profundizó en el sistema de calidad y de documentación de procesos.

Conscientes de la importancia que tiene para el futuro de la empresa estar a la vanguardia en materia de tecnología, tanto en computación como en comunicaciones, se diseñó e implementó la primera página Web de la compañía.

2001 La consolidación de la especialización. Las compañías Mundial de Seguros S.A. y Mundial de Seguros de Vida S.A., se fusionaron quedando como absorbente la Compañía Mundial de Seguros S.A. Con esta fusión la Compañía logro fortalecerse patrimonialmente y ampliar su capacidad de retención neta por riesgo, brindando así un servicio más ágil de suscripción, constituyéndose de esta manera en una entidad sólida, en la que la seriedad y profesionalismo de su gente, ha sido el mejor acceso a la confianza y respaldo, tanto en el mercado nacional como en el internacional.

En los primeros meses de 2001, la Compañía diseñó un nuevo Plan Estratégico denominado "La Consolidación de la Especialización". Este plan se apoyó en la metodología provista por el Sistema de Gestión de Calidad y Mejoramiento Continuo ISO 9001 versión 2000.

2002 – 2006 Una Compañía Especializada con Calidad Certificada. Buscando la implantación total del Sistema de Gestión de Calidad, la compañía definió con precisión la Red de Procesos de cara al cliente interno y externo, y logró el levantamiento de la documentación de

cada uno de los subprocesos que componen dicha red, la certificación ISO 9001 versión 2000 otorgada por el Icontec se obtuvo el 30 de Octubre de 2002.

Para administrar eficientemente el Sistema de Gestión de Calidad, la organización diseñó, desarrolló e implantó el sistema –Tutorl, con acceso a todos los funcionarios de la empresa y en donde se pueden encontrar la totalidad de la documentación actualizada de nuestros procesos, manuales técnicos y de suscripción, los módulos de auditoria de calidad, acciones correctivas, preventivas, quejas y reclamos, estos últimos fundamentales para la óptima administración del sistema.

2007 Una compañía con fortaleza financiera- Gracias a la fortaleza financiera de la compañía se obtuvo la calificación de AA (Doble A), por parte de Duff & Phelps, Sociedad Calificadora de Valores para la cual —AA Muy Alta fortaleza financiera‖ significa que la capacidad de empresas aseguradoras con esta calificación para el cumplimiento de pólizas y otras obligaciones contractuales es muy fuerte.

La compañía cumplió a cabalidad con lo dispuesto por la Superintendencia Financiera en desarrollar y poner en marcha el SEARS en los plazos estipulados por el ente de control.

Se realizó una revisión a fondo del Plan Estratégico que ha permitido validar las estrategias Gerenciales teniendo en cuenta las diferentes y nuevas variables que actúan sobre las fuerzas del mercado en que interactúa.

Mundial Seguros consiente de las nuevas necesidades de sus clientes complementa su portafolio de ramos especializados lanzando al mercado el Seguro de Crédito respaldado por una alianza estratégica con COFACE S.A., multinacional francesa con más de 60 años de experiencia en el ramo.

2008 – 2010 Mejoramiento continuo. Con el propósito de impulsar el mejoramiento continuo se incluyó la metodología Seis Sigma, la cual se trabajó para la revisión y simplificación de los procesos en busca de reducción de tiempos y errores en la operación.

En materia de evaluación, administración, medición y control de riesgo, la compañía cuenta con un adecuado Sistema de Administración de Riesgos de Seguros (SEARS) y trabajó durante este periodo en la implementación de las normas emanadas de la Superintendencia Financiera, relacionadas con la Administración de Riesgos Operativo (SARO) y Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo (SARLAFT), implementación que ha sido permanentemente monitoreada por la Junta Directiva.

La política de Gestión de Calidad y mejoramiento continuo se ha reflejado en mayor productividad, eficacia y se ha consolidado ahora bajo los preceptos de ISO 9001 con la versión 2008.

Con el propósito de impulsar el mejoramiento continuo, se definió y dio inicio al Plan de Mejoramiento Mundial –PMM420, con el propósito de buscar la optimización de la eficiencia de la operación de la compañía.

La compañía realizó la adquisición de la licencia de uso del programa SISE y acceso al código fuente, mejorando con ello la oportunidad y eficiencia en el proceso de evolución del sistema informático.

2011 – 2012 Renovación en seguros de personas. En coherencia con su plan estratégico, la compañía decide hacer su plan táctico para validar en el corto plazo sus estrategias y poder enfrentar con eficiencia los retos de un mercado exigente y altamente competido.

En el año 2012 la organización lanzó el Seguro de Arrendamiento, el cual puede ser adquirido por las inmobiliarias o por los propietarios de inmuebles y para el trámite de estudio de los posibles inquilinos y coarrendatarios, se ofrece la tradicional alternativa de diligenciar un formulario físico, o una innovadora plataforma web, sin ningún costo y sin desplazamientos. Comienza así el sendero de los seguros personales, estrategia clara para prestar servicios de calidad a los crecientes mercados de personas.

2013 – 2014 “Seguros Mundial” En el desarrollo del plan Estratégico –E-volución Mundial 2015 se estableció el genoma empresarial y la Causa Mundialista, igualmente se consolidaron las diferentes estrategias que trazan el rumbo de la compañía en los próximos 5 años.

En Octubre de 2013, BRC Standard & Poor's otorgó la calificación de Fortaleza Financiera en AA-, que indica que la capacidad financiera de empresas aseguradoras con esta calificación es muy fuerte para cumplir con el pago de los siniestros y de sus obligaciones contractuales.

Misión. Seguro Mundial es una organización dedicada a conocer y satisfacer las necesidades de aseguramiento y afianzamiento de sus clientes. Seguros Mundial acompaña y ofrece respaldo a las personas para la protección de su familia, su patrimonio y su vida contra los riesgos a los que están expuestos. Somos tranquilidad hacia el futuro.

Nuestra organización se proyecta como una aseguradora especializada altamente técnica, rentable y eficiente, que busca retribuir a sus accionistas y a todos sus funcionarios con las más altas recompensas económicas y humanas.

Queremos ser un agente económico productivo para la sociedad, que desarrolle a cabalidad su función social y que, además, cumpla de manera oportuna y adecuada las obligaciones adquiridas y las normas legales, dentro de la ética que nuestra actividad exige.

Nos distinguimos por el compromiso con el servicio, la seriedad y transparencia de nuestras acciones, y el profesionalismo y capacidad de liderazgo de nuestros colaboradores. Estimulamos la realización de nuestra gente a través de la participación y la creatividad.

Nuestra actitud positiva nos hace dinámicos, eficientes e innovadores, considerando el cambio como un reto permanente.

Visión. Ser la mejor compañía aseguradora especializada de Colombia

Planes y programas de organización empresarial. Desde su fundación, Seguros Mundial ha forjado su imagen de solidez y seriedad en el mercado asegurador, lo que le ha permitido participar de manera competitiva en todos los negocios inherentes a su actividad.

Entendiendo la apertura del mercado asegurador como una oportunidad para crecer, progresar y prestar un mejor servicio a cada uno de sus clientes, Seguros Mundial diseñó y desarrolló un Plan Estratégico que determinó como estrategia la especialización en los ramos de Cumplimiento, Judiciales, Aviación, SOAT, Vida Grupo Educativo, Accidentes Personales y Seguro de Crédito.

Como parte de su proyección estratégica la organización decide cambiar de nombre a -Seguros Mundialll con el consecuente cambio de la imagen corporativa brindando una extensión de marca a cada uno de nuestros productos. Esta nueva imagen -fresca y renovadorall identifica las ambiciones institucionales de servicio y la proactividad natural para atender las necesidades actuales de los colombianos.

Seguros Mundial se visualiza como una compañía especializada que quiere conocer a sus clientes y cree en ellos, proyectándolos a futuro para asegurar su familia, su empresa y sus sueños.

El Plan Estratégico de Seguros Mundial está integrado al Sistema de Gestión de Calidad que nos permite trabajar sistemáticamente para mejorar los procesos de la organización, garantizando la satisfacción de las necesidades y expectativas de nuestros clientes bajo los más

altos estándares de calidad y servicio. Seguros Mundial cuenta hoy con la Certificación ISO 9001 Versión 2008, otorgada por Icontec. Nuestro Sistema de Gestión de Calidad está implementado en la totalidad de los procesos que se desarrollan al interior de la compañía y aplica en todas las áreas que conforman la organización.

Como parte de su planeación se establece lo siguiente: Plan estratégico corporativo.

4.1.3 Universidad Francisco de Paula Santander Ocaña

Ubicación. Ocaña

Breve reseña histórica. En noviembre de 1973 se suscribió un contrato para la realización de un estudio de factibilidad denominado "Un centro de educación superior para Ocaña", que fue terminado y sugirió la creación pronta de un programa de educación a nivel de tecnología en énfasis en ciencias sociales, matemáticas y física. En diciembre de ese mismo año, el rector de la Universidad Francisco de Paula Santander, José Luis Acero Jordán, le envió copia de dicho estudio al Icfes, Instituto que conceptuó que el proyecto para abrir el centro de estudios en Ocaña, era recomendable.

Según Acuerdo No. 003 del 18 de Julio de 1974, por parte del Consejo Superior de la Universidad Francisco de Paula Santander Cúcuta, se crea la Universidad Francisco de Paula Santander Ocaña, como máxima expresión cultural y patrimonio de la región; como una entidad

de carácter oficial seccional, con Autonomía administrativa y patrimonio independiente, adscrito al Ministerio de Educación Nacional.

Su primer coordinador, el doctor Aurelio Carvajalino Cabrales, buscó un lugar adecuado para funcionar la sede, en los claustros Franciscanos al costado del templo de la Gran Convención, y con las directivas del colegio José Eusebio Caro, se acordó el uso compartido del laboratorio de física.

En 1975 comenzó la actividad académica en la entonces seccional de la Universidad Francisco de Paula Santander con un total de 105 estudiantes de Tecnología en Matemáticas y Física, y su primera promoción de licenciados en Matemáticas y Física se logró el 15 de diciembre de 1980.

La consecución de 27 hectáreas de la Hacienda El Rhin, en las riberas del Río Algodonal, en comodato a la Universidad por 50 años, que la antigua Escuela de Agricultura de Ocaña cedió a la Universidad, permitió la creación del programa de Tecnología en Producción Agropecuaria, aprobado por el Consejo Superior mediante el Acuerdo No. 024 del 21 de agosto de 1980, y luego el Icfes otorgó la licencia de funcionamiento el 17 de febrero del año siguiente. Luego se crean las Facultades.

La Facultad de Ciencias Agrarias y del Ambiente fue creada según Acuerdo 084 del 11 de septiembre de 1995, conformada por los departamentos de Ciencias Agrícolas y del Ambiente y el departamento Ciencias Pecuarias junto a los programas académicos de Tecnología

Agropecuaria (Acuerdo N° 024 del 21 de agosto de 1980), Zootecnia (Acuerdo N° N°057 y 058 del 27 de junio de 2007), e Ingeniería Ambiental (Acuerdo 089 del 9 de octubre 1995 con resolución 10542 de 8-ago-2013 del MEN).

La Facultad de Ciencias Administrativas y Económicas fue creada según Acuerdo No. 008 del 05 de marzo de 2003; está conformada por el departamento de Ciencias Administrativas y Departamento de Ciencias Contables y Financieras. Están adscritos los programas académicos de Tecnología en Gestión Comercial y Financiera (Acuerdo No, 024 del 29 de junio de 1988 con la resolución 9886 de 31-jul-2013 del MEN), Administración de Empresas (Acuerdo No, 024 del 29 de junio de 1988) y la profesionalización (Acuerdo No. 118 del 16 de noviembre de 1994 Resolución 1867 de 26-feb-2013); Contaduría Pública (Acuerdo No. 007 del 05 de marzo de 2003 y según resolución 13873 del 8-oct-2013 del MEN).

La Facultad de Ingenierías fue creada según Acuerdo 007 del 20 de febrero de 2006, conformada con los departamentos de Ingeniería Civil, Ingeniería Mecánica y el departamento de Sistemas e Informática. Con los registros calificados de los programas completos de acuerdo a la Resolución 2909 de julio 21 de 2005 para el programa de Ingeniería Civil (Resolución 6779 de 20-jun-2012) e Ingeniería Mecánica (Resolución 6233 de 7-jun-2012), Ingeniería de Sistemas (Resolución 9950 de 31-jul-2013). La creación del Técnico Profesional en Telecomunicaciones con registro calificado (Resolución 5366 de agosto 25 de 2008) y el Técnico Profesional en Informática con registro calificado (Resolución 4613 de julio 18 de 2008).

La Facultad de Educación, Artes y Humanidades de la Universidad Francisco de Paula Santander Ocaña fue creada según Acuerdo 063 del 07 de noviembre de 2006, está conformada con los departamentos de Matemáticas, Física y Computación y el Departamento de Humanidades. Según el Acuerdo No. 010, marzo 29 de 2004 se crea el plan de estudios del programa de Comunicación Social (Resolución 5363 de 10-may-2013,) y Derecho con registro calificado (Resolución 10185 de noviembre 22 de 2010). En el mes de noviembre de 2005, se suscribió el convenio de asociación No. 1744/05 con el Ministerio de Cultura, con el objeto de apoyar el proceso de estructuración académica de la Escuela de Bellas Artes.

Misión. La Universidad Francisco de Paula Santander Ocaña, institución pública de educación superior, es una comunidad de aprendizaje y autoevaluación en mejoramiento continuo, comprometida con la formación de profesionales idóneos en las áreas del conocimiento, a través de estrategias pedagógicas innovadoras y el uso de las tecnologías; contribuyendo al desarrollo nacional e internacional con pertinencia y responsabilidad social.

Visión. La Universidad Francisco de Paula Santander Ocaña para el 2019, será reconocida por su excelencia académica, cobertura y calidad, a través de la investigación como eje transversal de la formación y el uso permanente de plataformas de aprendizaje; soportada mediante su capacidad de gestión, la sostenibilidad institucional, el bienestar de su comunidad académica, el desarrollo físico y tecnológico, la innovación y la generación de conocimiento, bajo un marco de responsabilidad social y ambiental hacia la proyección nacional e internacional.

Planes y programas de organización empresarial.

- Plan de Desarrollo Institucional 2014-2019.
- Planes de mejoramiento.
- Plan de emisión de tv.
- Programas académicos.
- Programas de Gestión Ambiental.
- Programa del sistema de gestión de la seguridad y salud en el trabajo.
- Plan mantenimiento preventivo y correctivo de equipos.
- Plan de contingencia de TI.

4.1.4 BDO AUDIT

Ubicación. *Bogotá.*

Breve reseña histórica. *BDO Colombia tuvo su origen en el año 1985 al constituirse bajo el nombre de sus socios fundadores Antequera Gómez Escobar & Asociados - AGE Contadores Públicos y Consultores.*

En el año 1988 se convirtió en la firma miembro en Colombia de la red internacional de contadores BDO.

Hoy, con tres décadas de experiencia en el mercado local y más de 3,000 clientes satisfechos a lo largo de nuestra historia, se ha consolidado como una de las cinco firmas de servicios profesionales más grandes del país, con 4 oficinas en Bogotá D.C., y sucursales en Barranquilla, Cali, y Medellín.

Gracias al apoyo de entidades públicas, organismos multilaterales de crédito y compañías privadas de diversas industrias ha logrado alcanzar sus objetivos corporativos.

Dispone de un equipo multidisciplinario con más de 450 profesionales especializadas en la prestación de servicios de auditoría, consultoría, outsourcing, legal e impuestos.

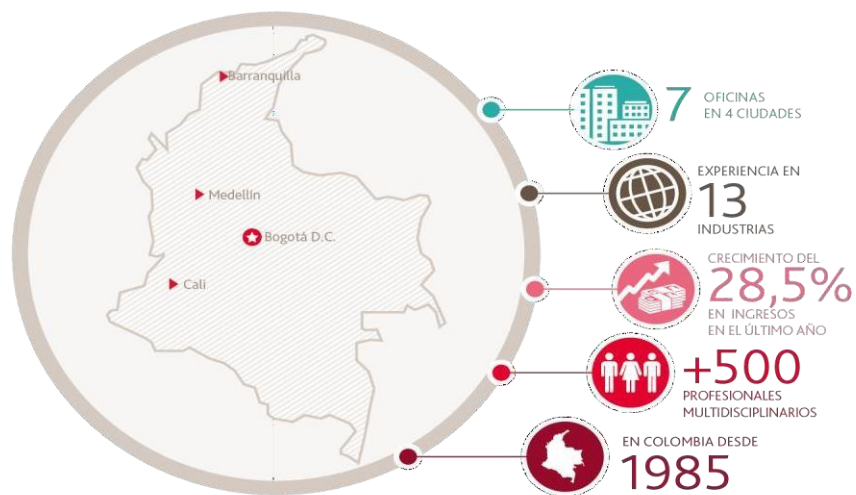


Figura 7. Historia de BDO Audit.
Fuente. BDO Audit.

Misión. Contribuir a que nuestros clientes logren sus objetivos corporativos con la experiencia, conocimiento y habilidades de nuestros profesionales, metodologías innovadoras,

mejores prácticas y recursos de nuestra red internacional, con el soporte de nuestro Sistema Integrado de Gestión.

Visión. Ser los líderes en servicio excepcional al cliente.

Planes y programas de organización empresarial

4.1.5 Ministerio TIC

Ubicación. Bogotá.

Breve reseña histórica. El Congreso de la República mediante la Ley 31 del 18 de julio de 1923, creó el Ministerio de Correos y Telégrafos, organismo encargado de fijar las políticas de planeación y desarrollo en los campos de la telegrafía y el correo.

En 1953, por Decreto 259 del 6 de febrero, el Gobierno Nacional determinó que a partir del 1 de febrero de 1953 el Ministerio de Correos y Telégrafos en adelante se denominaría Ministerio de Comunicaciones, reestructurándolo y estableciendo su funcionamiento con base en los Departamentos de Correos, de Telecomunicaciones y Giros.

En el año de 1990 por decreto 1901 del 19 de agosto, se establece la estructura orgánica para El Ministerio, se determinan las funciones de sus dependencias y se dictan disposiciones,

relacionadas con el Fondo de Comunicaciones, el Consejo Nacional de Telecomunicaciones, el Consejo Filatélico y la Comisión de Personal.

Con la Ley 72 de 1989 y el Decreto Reglamentario 1900 de 1990, se estableció la desmonopolización del sector y se segregó por primera vez en la historia de las telecomunicaciones los conceptos de redes y servicios, definiendo los servicios a prestar por el Ministerio de Comunicaciones.

La Ley 1341 de julio de 2009 genera nuevas responsabilidades para el Ministerio pues se le reconoce su papel como integrador del sector TIC, y como el encargado de apoyar el cierre de la brecha social en materia de tecnologías de comunicaciones. Es así como esta Ley cambia el nombre del Ministerio de Comunicaciones a Ministerio de Tecnologías de la Información y las Comunicaciones. Así mismo, el Decreto 091 del 19 de enero de 2010 modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones.

Misión. El Ministerio de Tecnologías de la Información y las Comunicaciones promueve el acceso, uso efectivo y apropiación masivos de las TIC, a través de políticas y programas, para mejorar la calidad de vida de cada colombiano y el incremento sostenible del desarrollo del país.

Visión. En el 2018, el Ministerio de las Tecnologías de la Información y las Comunicaciones estará preparado para enfrentar los retos de la economía digital y habrá logrado posicionar al país como referente en el desarrollo de aplicaciones sociales y contenidos digitales.

Contribuirá al desarrollo social y económico del país, al desarrollo integral de los ciudadanos y la mejora en su calidad de vida, mediante la investigación, promoción y apropiación del uso de nuevas tecnologías y la implementación de un modelo organizacional efectivo.

Planes y programas de organización empresarial. Planes de Acción 2018:

- Plan de Acción MINTIC/FONTIC 2018.
- Plan de Acción Anual 2018.
- Planes de Mejoramiento.
- Plan Anticorrupción.
- Plan Estratégico.
- Plan de Participación Ciudadana.
- Planes de desarrollo administrativo.
- Programa de Gestión Documental – PGD.
- Programa de acompañamiento a los sectores.
- Plan Estratégico de TI (PETI).
- Plan de Continuidad de TI.

4.2 Información recolectada

4.2.1 Categorías de análisis. Para el análisis de la información recolectada se han establecido las siguientes categorías:

Gobierno de TI. Gobierno de TI COLOMBIA MAYOR

El Consorcio Colombia Mayor como parte de su plan estratégico incorpora elementos de TI:

- Automatización de Procesos.
- Actualización de Bases de Datos.
- Fortalecimiento de los Canales Tecnológicos.

Gobierno de TI Seguros Mundial. SEGUROS MUNDIAL mantiene un gobierno corporativo enfocado propiamente a los productos y servicios de su negocio, acompañado de unas estrategias importantes a nivel de procesos relacionados con las tecnologías que se enfocan a:

- Implementar servicios de venta y postventa en un proceso tecnológico.
- Establecer los canales digitales para venta de servicios y productos.
- Establecer un ecosistema generador de valor.
- Tecnología adecuada.

Gobierno de TI Universidad Francisco de Paula Santander Ocaña

- Procedimiento gestión de los sistemas de TI.
- Procedimiento administración de los recursos informáticos.

- Procedimiento soporte y atención al usuario.

Gobierno de TI BDO AUDIT

- Planeación.

Gobierno de TI MINISTERIO TIC

- Política lineamientos y estándares para la gestión TI.
- Liderazgo TI – GCIO.

Estrategia de Gobierno de TI MINTIC. La estrategia de tecnología debe estar estrechamente ligada a las estrategias y políticas organizacionales del Estado o las entidades del sector. Para apoyar la construcción de un Gobierno TI es fundamental desarrollar un plan normativo y legal, las políticas organizacionales, los procesos, el modelo de gobierno y los mecanismos de compras y contratación de la entidad. Para que las TIC cumplan su papel es necesario contar con un modelo de gobierno de TI que contemple los siguientes aspectos:

- Marco legal y normativo.
- Estructura de TI y procesos.
- Toma de decisiones.
- Gestión de relaciones con otras áreas y entidades.
- Gestión de proveedores.

- Acuerdos de servicios y de desarrollos.
- Alineación con los procesos.

Estrategia de Gestión de TI. El Plan Estratégico de TI (PETI) define las estrategias de gobierno en cuanto a TI, sistemas de información, servicios tecnológicos y del uso y apropiación de los anteriores. El modelo de gestión que apoya el PETI garantiza el valor estratégico de la capacidad y la inversión en tecnología realizada por el Estado. Dicho modelo además incluye la estrategia organizacional y las necesidades del negocio de TI. Para la Estrategia se desarrollan los siguientes aspectos:

- Planeación estratégica de gestión de TI.
- Portafolio de planes y proyectos.
- Políticas de TI en cuanto a seguridad, información, acceso y uso, etc.
- Portafolio de servicios.
- Gestión financiera.
- Plan de Continuidad de TI.

Tratamiento de la Información. Tratamiento de la Información COLOMBIA MAYOR

- Política de tratamiento de información de datos personales.
- Aviso de privacidad.
- Procedimiento de quejas y reclamos.
- Formatos de autorización de datos personales.

- Metodología de gestión de riesgos.
- Políticas de seguridad de la información.

Tratamiento de la Información SEGUROS MUNDIAL

- Políticas de tratamiento de la información.
- Aviso de privacidad y autorización expresa para el tratamiento de datos personales.
- Procedimiento de peticiones y quejas (reclamos).
- Metodología de gestión de riesgos.

Tratamiento de la Información UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

La Universidad Francisco de Paula Santander Ocaña en materia de tratamiento de la información de datos personales dispone de los siguientes elementos:

- Política Protección de Datos Personales.
- Política de tratamiento de protección de datos personales TI.
- Documento de Aprobación de la Política de Protección de datos personales de la Universidad Francisco de Paula Santander Ocaña.
- Formato Autorización de uso de datos personales.
- Aviso de Privacidad de los datos personales.
- Formato de consulta, actualización, rectificación, y eliminación de datos personales.
- Documento Contrato de confidencialidad.

Tratamiento de la Información BDO AUDIT

- Política de tratamiento de datos personales del grupo empresarial BDO tratamiento de la información Ministerio TIC.
- Autorización del titular para el tratamiento de datos.
- Procedimiento para el ejercicio de sus derechos como titular de datos.
- Seguridad y privacidad de la información.

Desarrollo organizacional. Desarrollo Organizacional COLOMBIA MAYOR

Mapa de Procesos

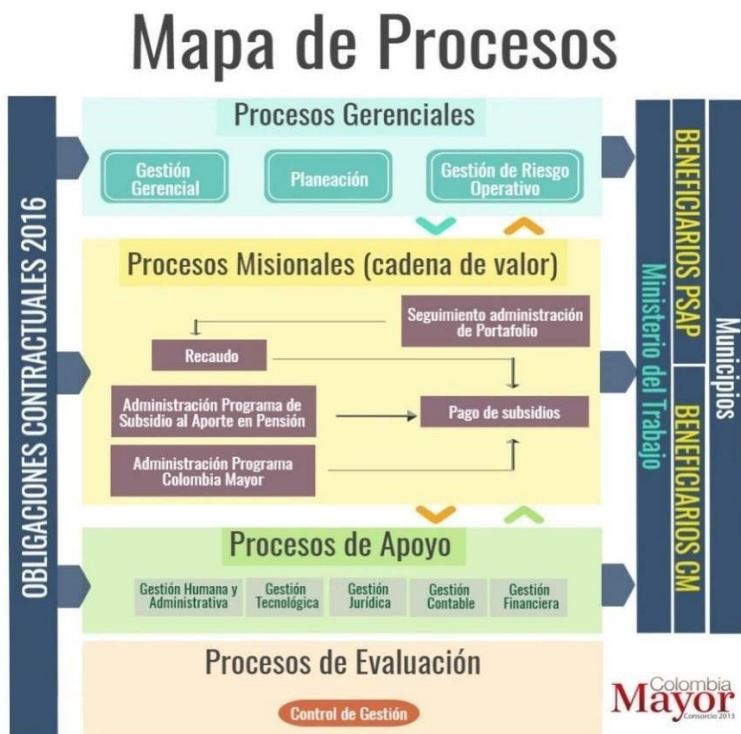


Figura 8. Mapa de Procesos Colombia Mayor.

Fuente. Colombia Mayor.

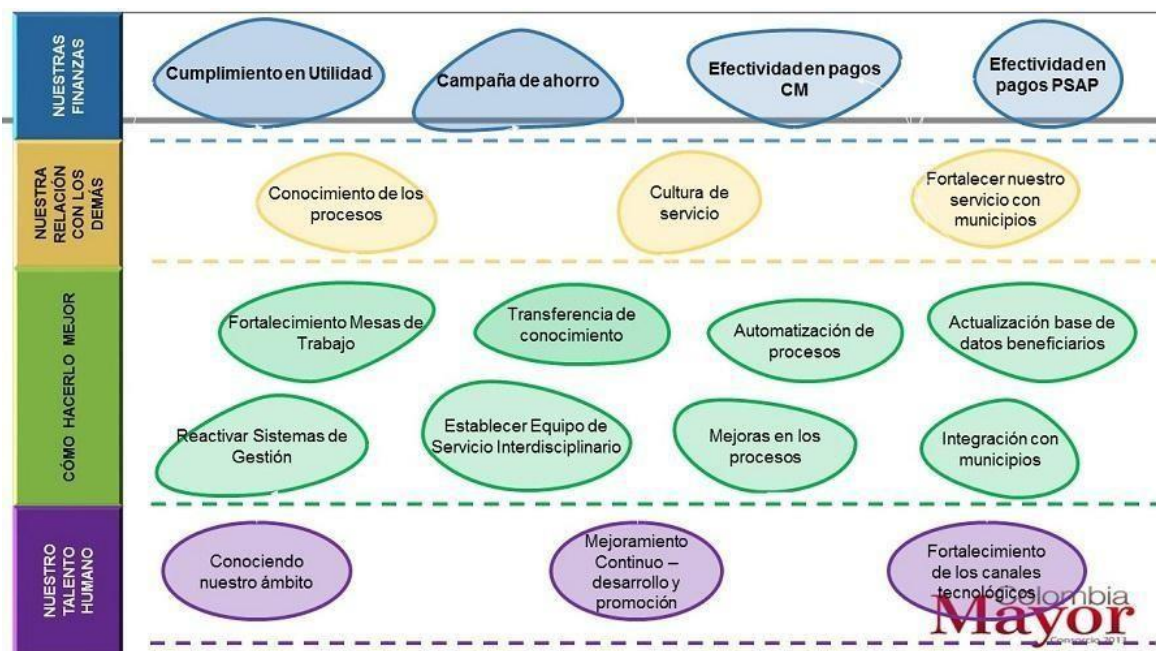


Figura 9. Mapa de Procesos Colombia Mayor.

Fuente. Colombia Mayor.

Objetivos Estratégicos

Nuestro Talento Humano

- Conociendo nuestro ámbito.
- Fortalecimiento de los canales tecnológicos.
- Mejoramiento continuo – desarrollo y promoción.

Cómo hacerlo mejor

- Actualización base de datos beneficiarios.

- Autorización de bases de datos.
- Establecer equipos de servicio interdisciplinario.
- Fortalecimiento mesas de trabajo.
- Integración con municipios.
- Mejoras en los controles de los procesos.
- Reactivar sistemas de gestión.
- Transferencia de conocimiento.

Nuestra relación con los demás

- Conocimiento de los procesos.
- Cultura de servicio.
- Fortalecer nuestro servicio con municipios.

Nuestras finanzas

- Aumentar la efectividad en pagos CM.
- Campaña de ahorro.
- Cumplimiento en utilidad.
- Mantener la efectividad en pagos PSAP.

Desarrollo Organizacional SEGUROS MUNDIAL

Mapa de Procesos



Figura 10. Mapa de Procesos Seguros Mundial.
Fuente. Seguros Mundial.

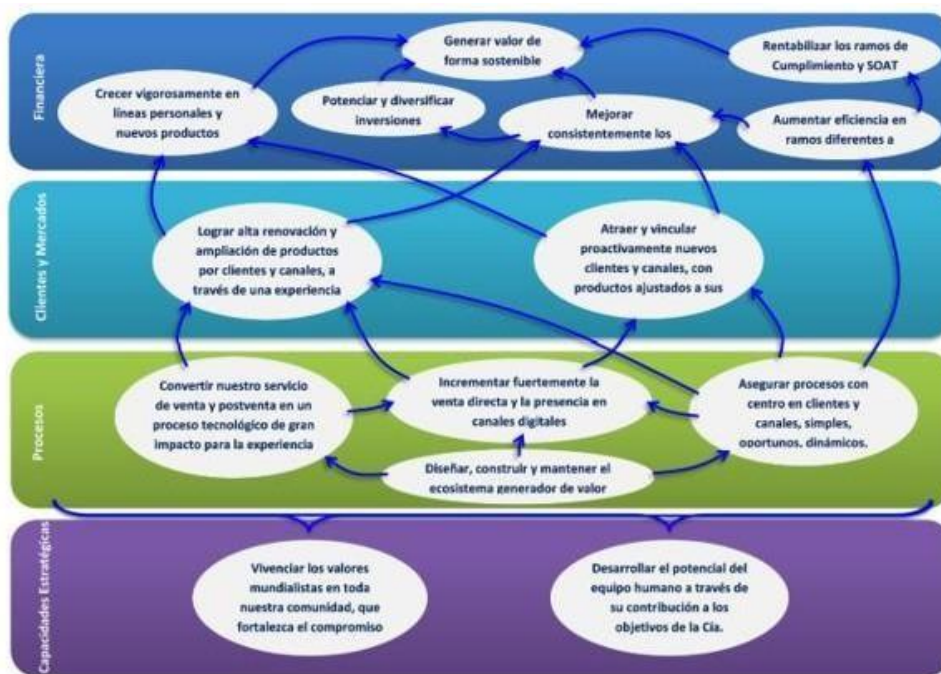


Figura 11. Objetivos Estratégicos Seguros Mundial.
Fuente. Seguros Mundial.

Valores Corporativos

- Servicio.
- Cordialidad.
- Familiaridad.
- Comunicación.
- Liderazgo.
- Trabajo en equipo.



Figura 12. Prioridades Estratégicas Seguros Mundial.

Fuente. Seguros Mundial.

Desarrollo Organizacional UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

Objetivos Institucionales

Investigación y formación académica. La investigación como eje transversal de la formación se desarrolla a través de la incorporación e implementación de las TIC en los procesos académicos, la cualificación docente, la calidad y pertinencia de la oferta, la cobertura y el desarrollo estudiantil como soporte integral del currículo, de la producción científica y la generación de conocimiento, hacia la consolidación de la Universidad como institución de investigación.

Desarrollo físico y tecnológico. Fortalecimiento de la gestión tecnológica y las comunicaciones, modernización de los recursos y adecuación de espacios físicos suficientes y pertinentes para el desarrollo de las funciones sustantivas y el crecimiento institucional.

Impacto y proyección social. Desarrollo de las capacidades institucionales promoviendo impactos positivos a la región, el medio ambiente y la comunidad, mediante la creación de alianzas estratégicas, ejecución de proyectos pertinentes, aumento de cobertura en actividades de extensión y el compromiso con la responsabilidad social.

Visibilidad nacional e internacional. Integración, transformación y fortalecimiento en las funciones de investigación, docencia y extensión para su articulación en un ambiente globalizado de excelencia y competitividad, tomando como referencia las tendencias, el estado del arte de la disciplina o profesión y los criterios de calidad reconocidos por la comunidad académica nacional e internacional.

Bienestar institucional. Generación de programas para la formación integral, el desarrollo humano y el acompañamiento institucional que permitan el mejoramiento de las condiciones de vida

de la comunidad universitaria con servicios que sean suficientes, adecuados y accesibles, que respondan a la política integral de bienestar universitario definida por la institución.

Sostenibilidad administrativa y financiera. Implementación y mantenimiento de procesos eficientes y eficaces en la planeación, ejecución y evaluación administrativa y financiera; abordando estándares de alta calidad y mejoramiento continuo en todos los niveles de la organización; generando espacios de participación, transparencia, eficiencia y control de la gestión.

Mapa de procesos

Mapa de Procesos

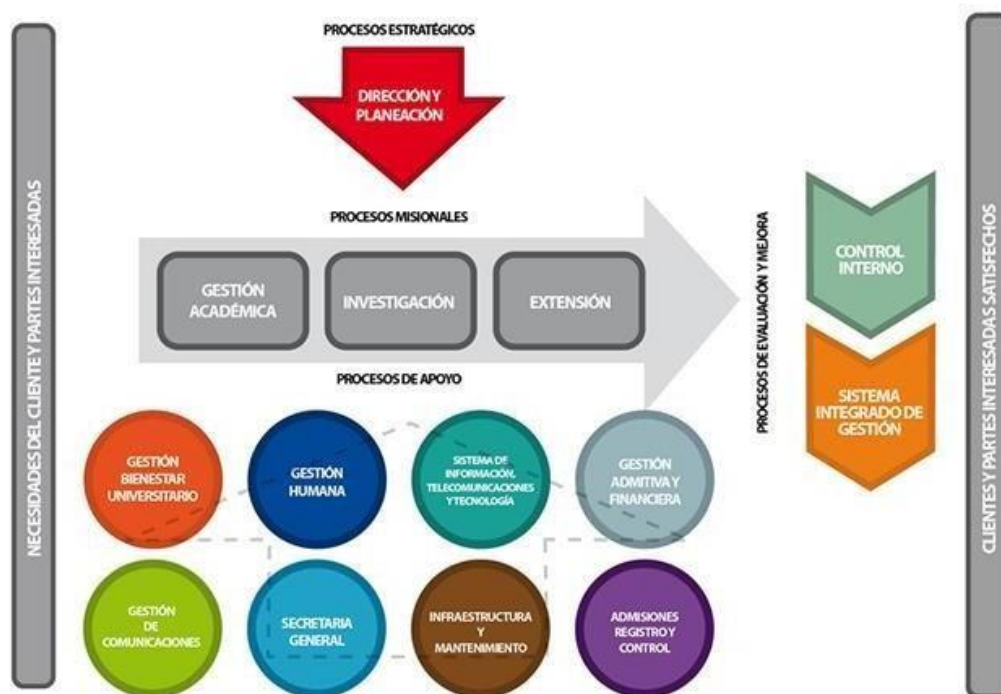


Figura 13. Mapa de Procesos Universidad Francisco de Paula Santander Ocaña.
Fuente. Universidad Francisco de Paula Santander Ocaña.

Desarrollo Organizacional BDO AUDIT. Objetivos de Calidad

- Prestar los servicios cumpliendo con los requerimientos contractuales, actuando dentro del marco normativo que los rige.
- Mantener el sistema de gestión de la calidad funcionando eficazmente.
- Crecer con eficacia y eficiencia.
- Aumentar la competencia del personal.
- Utilizar las herramientas metodológicas de acuerdo con los lineamientos internos de la empresa.
- Administrar física y lógicamente el sistema de información y los recursos tecnológicos brindando soporte y asesoría a la prestación del servicio.

Desarrollo Organizacional MINISTERIO TIC. Mapa de Macroprocesos



Figura 14 Mapa de Macroprocesos Ministerio TIC.
Fuente. Ministerio TIC.

Objetivos y funciones. Los objetivos del Ministerio de Tecnologías de la Información y las Comunicaciones, conforme lo dispuesto por el artículo 17 de la Ley 1341 de 2009 son:

- Diseñar, formular, adoptar y promover las políticas, planes, programas y proyectos del Sector de Tecnologías de la Información y las Comunicaciones, en correspondencia con la Constitución Política y la ley, con el fin de contribuir al desarrollo económico, social y político de la Nación y elevar el bienestar de los colombianos.
- Promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación.
- Impulsar el desarrollo y fortalecimiento del Sector de Tecnologías de la Información y las Comunicaciones, promover la investigación e innovación, buscando su competitividad y avance tecnológico conforme al entorno nacional e internacional.

Valores

- Honestidad.
- Respeto.
- Compromiso.
- Diligencia.
- Justicia.
- Responsabilidad.

Estructura empresarial. Estructura Empresarial COLOMBIA MAYOR

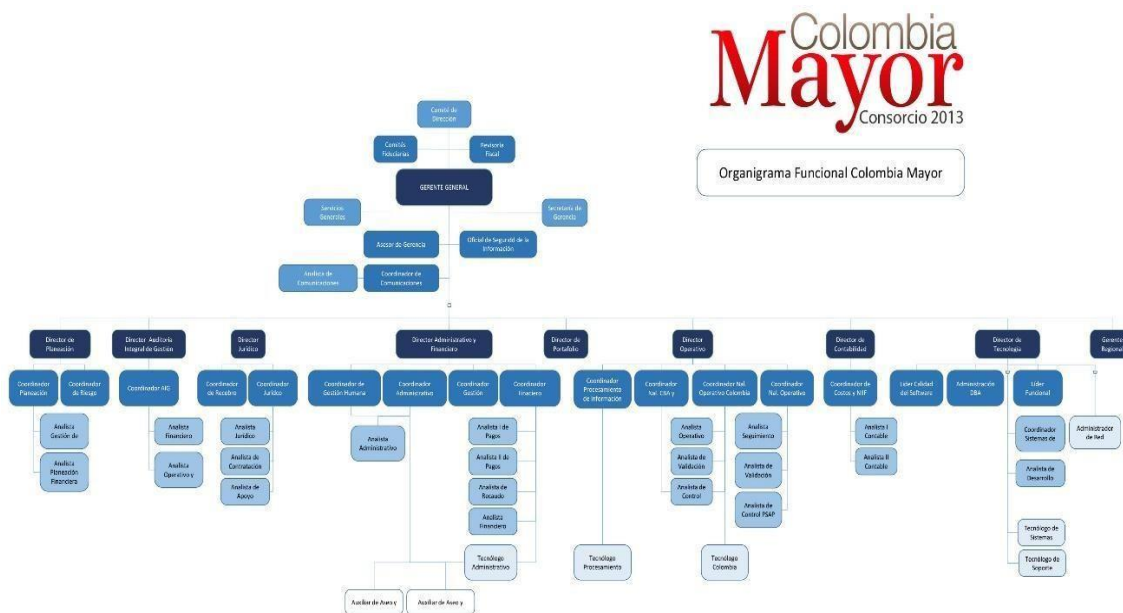


Figura 15. Organigrama General Colombia Mayor.
Fuente. Colombia Mayor.

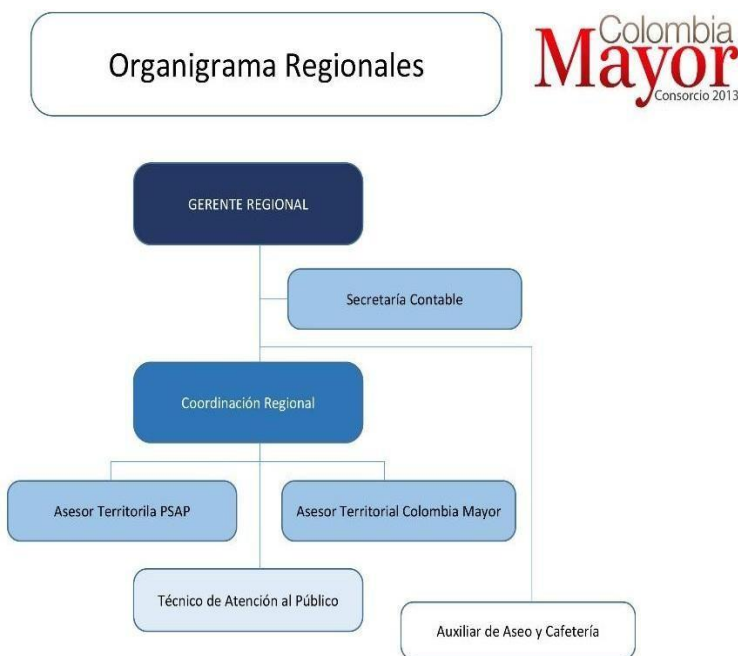


Figura 16. Organigrama Regional Colombia Mayor.
Fuente. Colombia Mayor.

Estructura Empresarial SEGUROS MUNDIAL

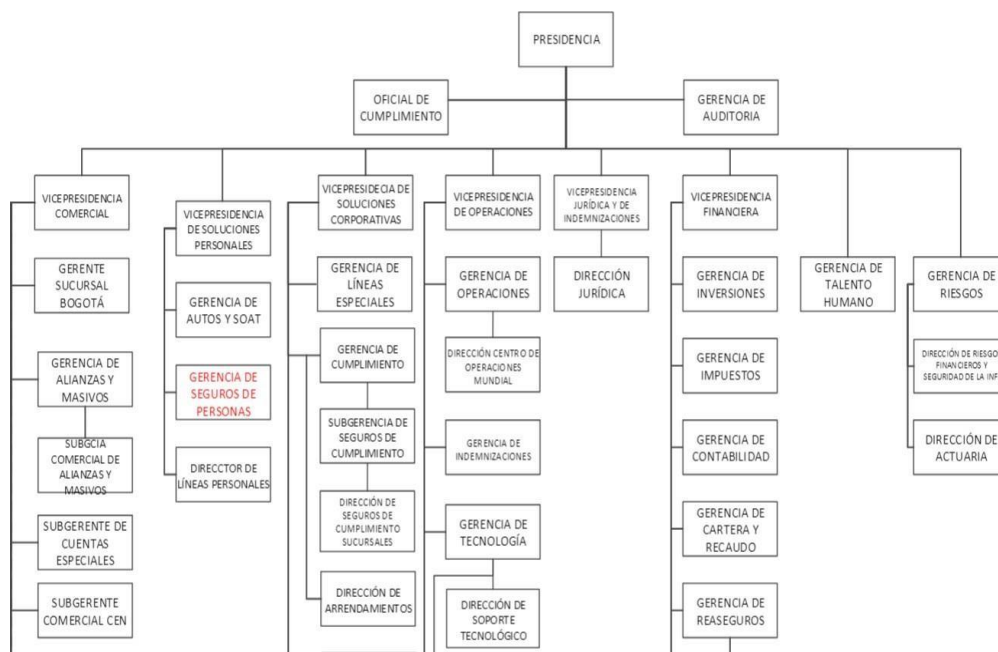


Figura 17. Estructura Empresarial Seguros Mundial.
Fuente. Seguros Mundial.

Estructura Empresarial Universidad Francisco de Paula Santander Ocaña

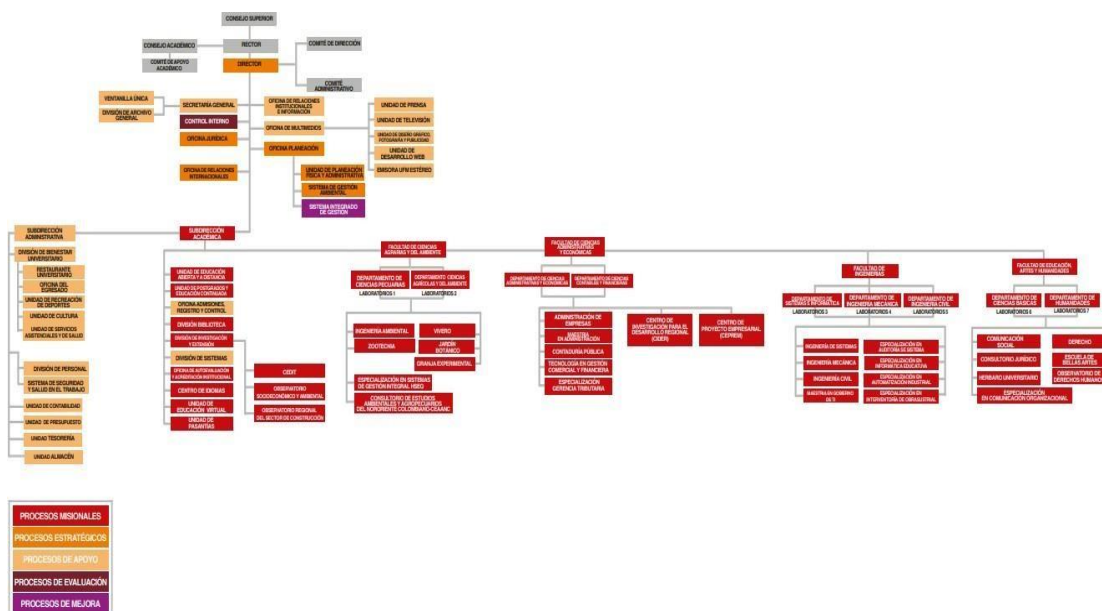


Figura 18. Estructura Organizacional Universidad Francisco de Paula Santander Ocaña.
Fuente. Universidad Francisco de Paula Santander Ocaña.

Estructura Empresarial BDO AUDIT. BDO AUDIT en Colombia dispone la siguiente estructura:

Unidad de Negocio

- Auditoría y Aseguramiento.
- Consultoría.
- Impuestos y Legal.
- Outsourcing.

Área de Servicio

- Auditoría de Procesos de Negocios.
- Auditoría de Tecnologías de la Información.
- Auditoría Externa de Gestión y Resultados.
- Auditoría Externa.
- Auditoría Interna.
- Compilación de Estados Financieros.
- Debida Diligencia - Due Diligence.
- Interventorías.
- Trabajos con procedimientos convenidos.
- Asesoría NIIF e IPSAS.
- Avalúos.

- Consultoría en la Evaluación de los Impactos Tributarios de las NIIF.
- Consultoría Tributaria.
- Contratación Civil y Comercial.
- Contratación Estatal.
- Derecho Laboral Individual.
- Derecho Migratorio.
- Derecho Societario.
- Implementación de Factura Electrónica.
- Outsourcing Tributario.
- Personas Naturales (Expatriados).
- Precios de Transferencia.
- Servicios de Debida Diligencia (Due Diligence) en Aspectos Fiscales.
- Administrativo y Financiero.
- Asesoría en Selección y Reclutamiento.
- Contabilidad.
- Impuestos.
- Legal y Corporativo.
- Nómina.
- Sector Público.

Servicio

- Administrativos.

- Seguimiento y Control.

Categoría de Industria

- Bienes de Consumo, Comercio y Retail.
- Energía y Recursos Naturales.
- Hotelería, Turismo y Entretenimiento.
- Ingeniería, Construcción y Finca Raíz.
- Manufactura.
- Organismos de Cooperación Multilateral.
- Salud, Química y Farmacéutica.
- Sector Financiero y Bursátil.
- Sector Público.
- Servicios.
- Tecnología, Medios y Telecomunicaciones.

Industria

- Agroindustria.
- Transporte y Logística.
- Servicios Públicos.

Estructura Empresarial MINISTERIO TIC

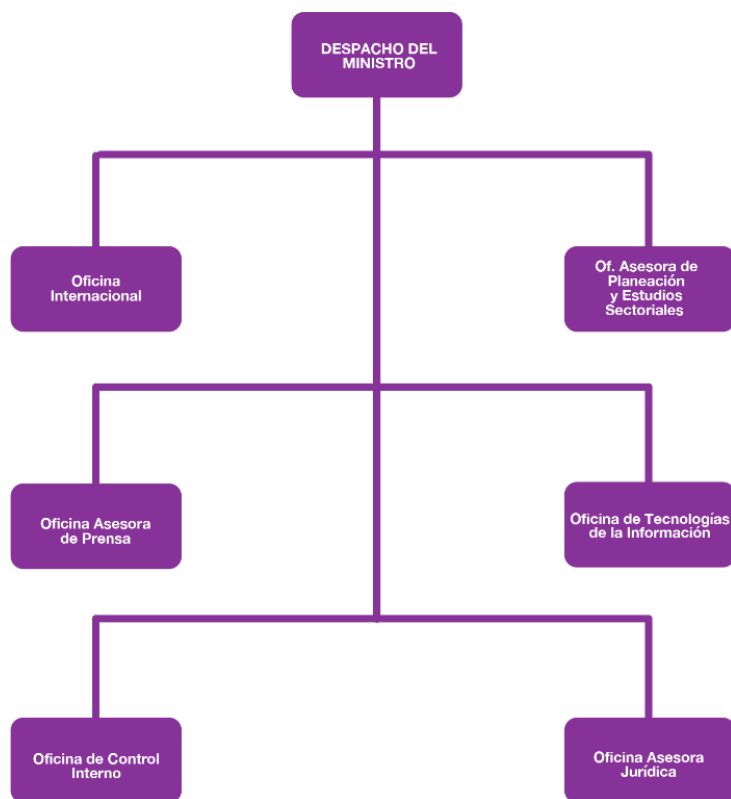


Figura 19. Organigrama Despacho del Ministro Ministerio TIC.
Fuente. Ministerio TIC.

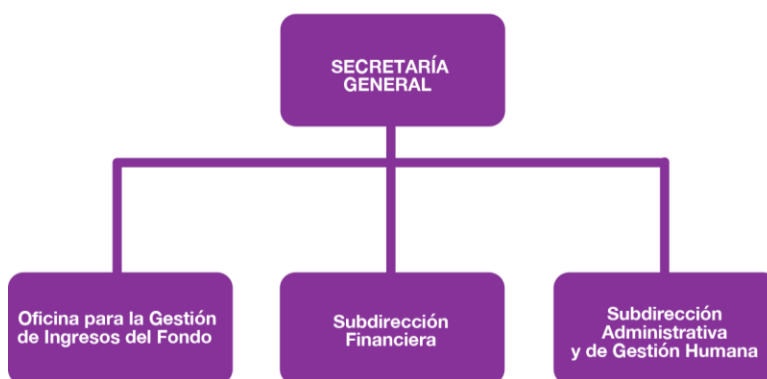


Figura 20. Organigrama Secretaría General Ministerio TIC.
Fuente. Ministerio TIC.

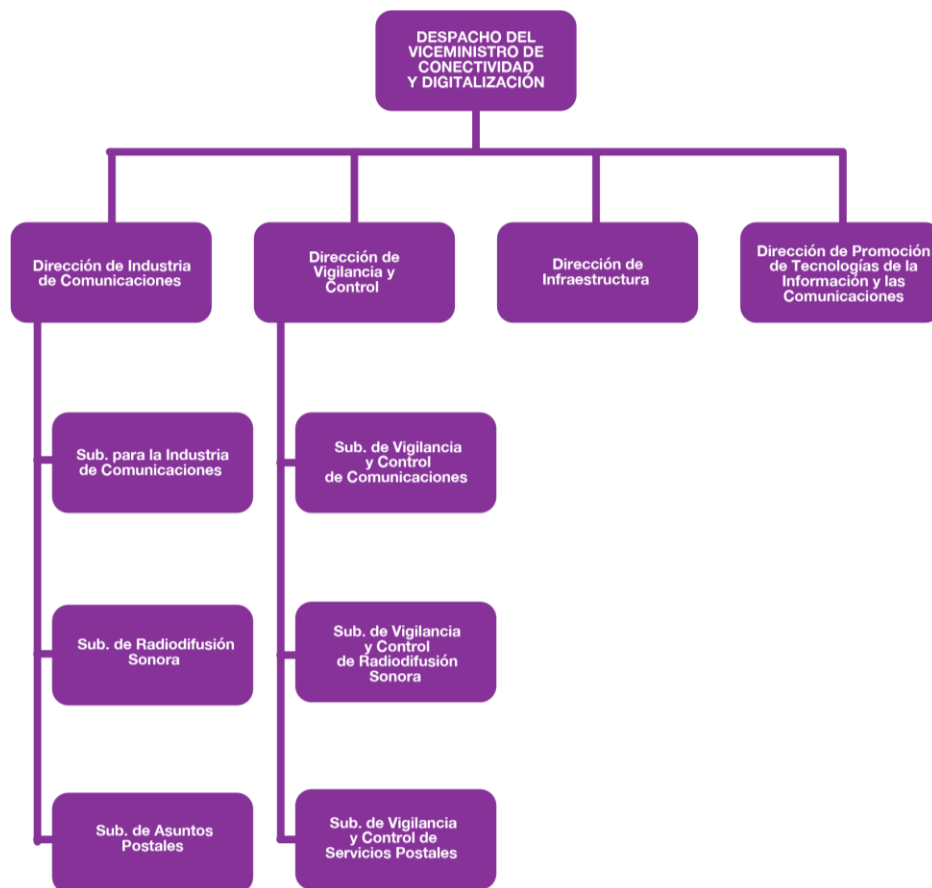


Figura 21. Organigrama Despacho del Viceministro Ministerio TIC.
Fuente. Ministerio TIC.



Figura 22. Organigrama Órganos de Asesoría y Coordinación Ministerio TIC.
Fuente. Ministerio TIC.

Globalización en la empresa. Globalización en la Empresa COLOMBIA MAYOR

La empresa Colombia Mayor actualmente reside en Colombia y su operación tiene un alcance –Nacionall. Sin embargo, en el contexto de las tecnologías de la información adquiere

servicios en la nube –Internetl que conllevan al análisis de la protección de sus datos cuando son manejados por empresas que proveen el servicio en línea con asentamiento en otros países. Esto implica una razón fundamental para validar que la empresa Colombia Mayor al adquirir estos servicios externos le aseguren que sus informaciones tratadas en servidores puestos en otros países cumplan con la normatividad legal vigente en término de protección de datos personales y de seguridad de la información de la empresa.

Globalización en la Empresa SEGUROS MUNDIAL. Respecto al contexto global, SEGUROS MUNDIAL mantiene un perfil de manejo nacional, por tanto, no se identificó una perspectiva de participación internacional a nivel propio de expansión del negocio al exterior. Sin embargo, al ser una empresa que actualmente utiliza la tecnología como medio para ofrecer servicios a sus clientes a través de internet, esto la hace una empresa visual a nivel mundial, y aunque no ofrezca un servicio internacional, si está sometida al manejo de unas buenas prácticas que le permitan controlar su tecnología y la protección de su información.

Globalización en la Empresa UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. La Universidad Francisco de Paula Santander Ocaña ha contemplado en su misión la incorporación de un componente importante de innovación y tecnología como apoyo para ser evolutiva, sostenible y adaptable a las nuevas necesidades empresariales a nivel académico y al ser complementada con su visión el cual establece el desarrollo de una estratégica que conlleva a la internacionalización de la institución la proyecta como una entidad enfocada en términos de la globalización. Para lograrlo ha establecido las siguientes estrategias:

- Desarrollo institucional de la internacionalización.
- Internacionalización de la academia.
- Internacionalización de la investigación.

Globalización en la Empresa BDO AUDIT. BDO manifiesta en términos de globalización manifiesta:

Desde la fundación en 1963, la historia BDO ha sido una continua respuesta a las necesidades cambiantes de nuestros clientes y nuestra gente. Nuestra historia es relevante hoy porque nuestros clientes valoran la continuidad y la estabilidad de una red que se ha desarrollado tan exitosamente durante más de cincuenta años turbulentos. Igualmente, nuestros socios y el personal saben que trabajan para una organización bien establecida que está construida en base a valores claros y un pasado exitoso.

La organización internacional inicial era conocida como el grupo Binder Seidman International, formado por firmas respetadas que ya estaban bien establecidas en Canadá, Alemania, los Países Bajos, el Reino Unido y los Estados Unidos y deseaban compartir y ampliar sus conocimientos con el fin de servir de mejor manera a sus clientes. En 1973, la red adoptó el nombre BDO, compuesto de las iniciales de las tres firmas miembro fundadoras: Binder (Reino Unido), Dijker (Países Bajos) y Otte (Alemania).

Estamos orgullosos de que en los siguientes 50 años más, BDO ha crecido en US\$8.1 mil millones más en negocios, operando en más de 162 países. Hemos logrado esto mediante la

adaptación a los cambios provocados por fuerzas externas tales como la regulación y globalización, así como las cambiantes necesidades y expectativas de nuestros clientes.

Pero para BDO, no se detiene allí. Vivimos y trabajamos en un entorno desafiante caracterizado por una economía mundial imprevisible, continua agitación política y la amenaza omnipresente del terrorismo. Al igual que en todos los negocios, debemos tomar decisiones estratégicas para asegurar que podemos seguir atrayendo clientes globales, entrar en nuevos mercados, mejorar el rendimiento y gestionar el riesgo.

Hemos invertido en infraestructura global, tecnología y estamos listos: esto es lo que nos distingue de nuestros competidores.

Sobre todo, seguiremos entregando servicio excepcional al cliente para quienes nos conocen, porque esto es lo que nos diferencia en nuestro mercado. La excelencia técnica es un hecho, pero nuestro programa de servicio excepcional al cliente está incorporado en nuestra estrategia y se lleva a cabo a un nivel verdaderamente global.

Globalización en la Empresa MINISTERIO TIC. Como parte de la internacionalización el Ministerio TIC ha establecido las siguientes estrategias:

- Posicionamiento internacional Marca Colombia TI.
- Participación en ruedas de negocio y eventos especializados.
- Mipymes formales con presencia WEB y/o Móvil.

- Mipymes que hacen transacciones mediante comercio electrónico.
- Teletrabajo.
- Implementar un hub de tecnología que será el referente a nivel regional (Alianza Pacífico y Latinoamérica).

Legislación vinculante. Legislación Vinculante COLOMBIA MAYOR

- Constitución Política de Colombia. Por el cual, se definen las normas, derechos y deberes de los colombianos y el estado.
- Ley 1581 OCT 17, 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 MAR 6, 2014. Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones".
Publicada en el Diario Oficial No. 49.084 del 6 de marzo de 2014.

Legislación Vinculante SEGUROS MUNDIAL

- Ley 1266 DIC 31, 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. (Habeas Data).
- Ley 1581 OCT 17, 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

Legislación Vinculante UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
OCAÑA

- Constitución Política de Colombia. Por el cual, se definen las normas, derechos y deberes de los colombianos y el estado.
- Ley 1581 OCT 17, 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 MAR 6, 2014. Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones".
Publicada en el Diario Oficial No. 49.084 del 6 de marzo de 2014.

Legislación Vinculante BDO AUDIT

- Constitución Política de Colombia. Por el cual, se definen las normas, derechos y deberes de los colombianos y el estado.
- Ley 1581 OCT 17, 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

Legislación Vinculante MINISTERIO TIC

- Constitución Política de Colombia. Por el cual, se definen las normas, derechos y deberes de los colombianos y el estado.

- Ley 1581 OCT 17, 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 MAR 6, 2014. Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones". Publicada en el Diario Oficial No. 49.084 del 6 de marzo de 2014.

Normas prácticas. Normas y Buenas Prácticas Aplicadas en COLOMBIA MAYOR

Buenas Prácticas de Seguridad de la Información

- NTC ISO/IEC 27001:2013. Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI).
- NTC ISO/IEC 27002:2015. Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información.
- NTC ISO/IEC 27003:2007. Implementación de un Sistema de Gestión de la Seguridad de la Información.

Buenas Prácticas de Riesgos

- NTC ISO/IEC 27005:2009. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.
- NTC ISO 31000:2011. Gestión del Riesgo – Principios y Directrices.

Buenas Prácticas de Gobierno de TI

- COBIT 4.1. Marco de Referencia de Gobierno de Tecnologías de la Información y Control.

4.2.1.1.1 Normas y Buenas Prácticas Aplicadas en SEGUROS MUNDIAL

Buenas Prácticas de Seguridad de la Información

- NTC ISO/IEC 27001:2013. Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI).
- NTC ISO/IEC 27002:2015. Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información.

Buenas Prácticas de Riesgos

- NTC ISO 31000:2011. Gestión del Riesgo – Principios y Directrices.

Buenas Prácticas de Gobierno de TI

- N/A.

Normas y Buenas Prácticas Aplicadas en UNIVERSIDAD FRANCISCO DE PAULA
SANTANDER OCAÑA

Buenas Prácticas de Seguridad de la Información

- NTC ISO/IEC 27001:2005. Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI).
- NTC ISO/IEC 27002. Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información.

Buenas Prácticas de Riesgos

- NTC ISO 31000:2009. Gestión del Riesgo – Principios y Directrices.

Buenas Prácticas de Gobierno de TI

- NTC ISO 38500:2009. Gobierno Corporativo de la Tecnología de la Información.
- COBIT 4.0. Marco de Referencia de Gobierno de Tecnologías de la Información.

Normas y Buenas Prácticas Aplicadas en BDO AUDIT

Normas y Buenas Prácticas Aplicadas en MINISTERIO TIC

Buenas Prácticas de Seguridad de la Información

- NTC ISO/IEC 27001:2013. Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI).
- NTC ISO/IEC 27002:2015. Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información.
- NTC ISO/IEC 27003:2007. Implementación de un Sistema de Gestión de la Seguridad de la Información.

Buenas Prácticas de Riesgos

- NTC ISO/IEC 27005:2009. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.
- NTC ISO 31000:2011. Gestión del Riesgo – Principios y Directrices.

Buenas Prácticas de Gobierno de TI

- NTC ISO 38500:2009. Gobierno Corporativo de la Tecnología de la Información.
- COBIT 5. Marco de Referencia de Gobierno y Gestión para las Tecnologías de la Información.

4.3 Sistematización de la información

Como parte de esta investigación se hace un análisis de la información recolectada con relación a cada uno de los objetivos previstos (objetivos específicos) y a la vez se hace un

contraste con elementos teóricos dando solidez a cada uno de los elementos planteados. Es significativo fundamentar y apoyar algunos elementos dentro de lo que es lo cuantitativo; razón por la cual se incluyen datos numéricos como base para una sistematización teórica que surge de las categorías encontradas y analizadas y para tal fin es pertinente señalar que mencionado análisis se refleja en las redes sistémicas que surgen del Atlas Ti; razón que permite dar mayor rigurosidad científica a los postulados que sean planteados. Aspectos que se migraron a la data para ser analizados por contraste con respecto a la teoría y a los que los informantes señalan.

4.3.1. Análisis de aplicación de las categorías en las empresas. Al analizar la información recolectada de las diferentes empresas se estimó la aplicabilidad de cada una de las categorías en las mismas, obteniendo como resultado lo siguiente:

Tabla 2 *Aplicación de las Categorías en las Empresas*

Empresa	Categoría						
	Gobierno de TI	Tratamiento de la Información	Desarrollo organizacional	Estructura empresarial	Globalización en la empresa	Legislación vinculante	Normas prácticas
COLOMBIA MAYOR 2013	NO	SI	SI	SI	NO	SI	SI
SEGUROS MUNDIAL	NO	SI	SI	SI	NO	SI	SI
UNIVERSIDAD FRANCISCO DE PAULA	NO	SI	SI	SI	SI	SI	SI
SANTANDER OCAÑA	NO	SI	SI	SI	SI	SI	SI
BDO AUDIT	NO	SI	SI	SI	SI	SI	SI
MINISTERIO TIC	SI	SI	SI	SI	SI	SI	SI

Fuente: Autor del proyecto

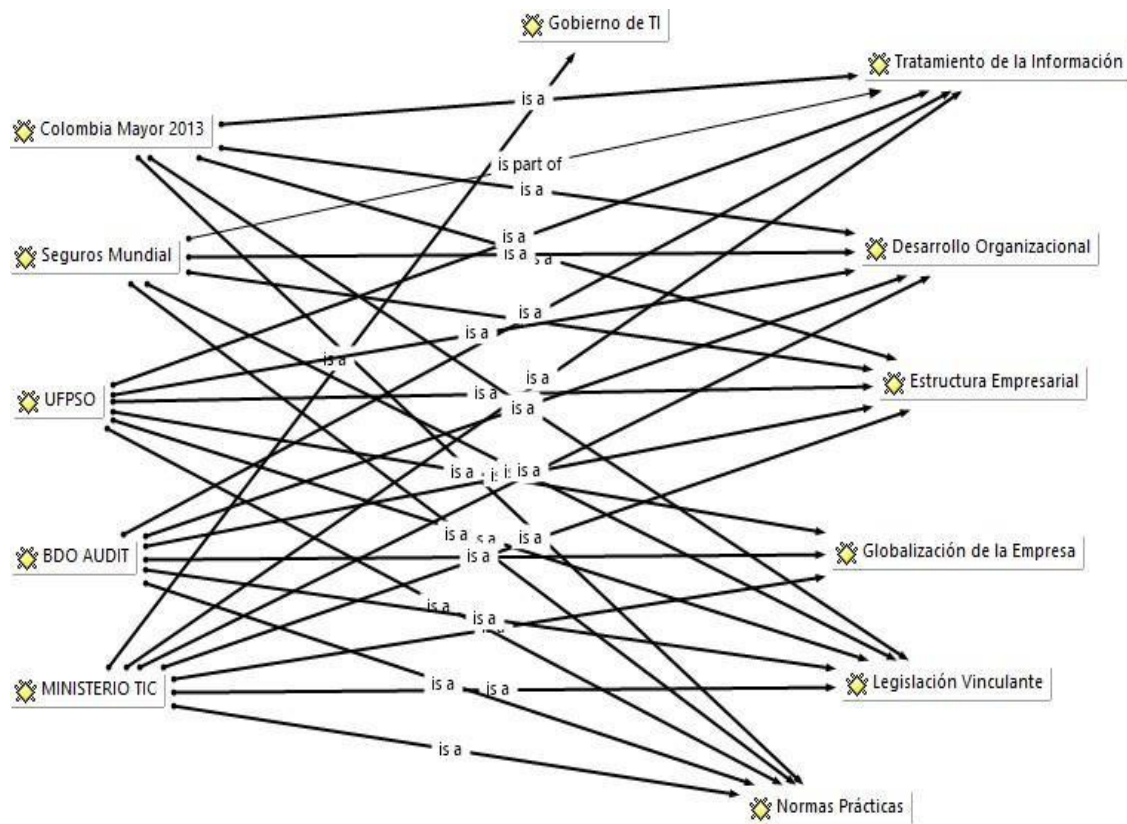


Figura 23. Concreción de categorías en la Empresas

Fuente. Autor del proyecto

Análisis de Aplicación de las Categorías en las Empresas

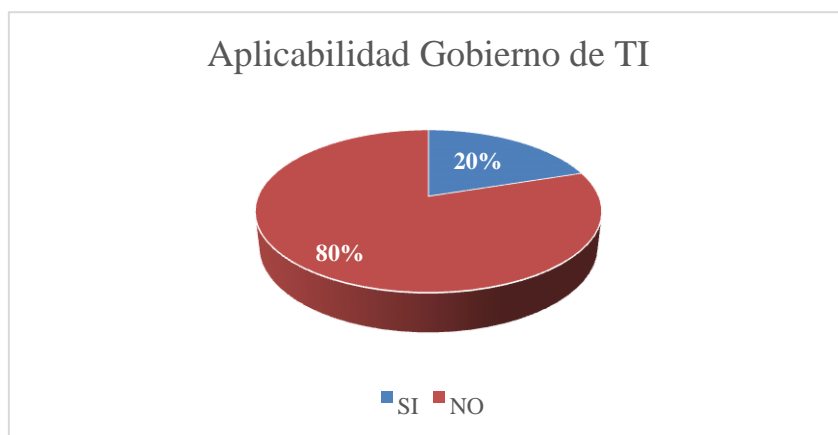


Figura 24. Aplicabilidad Gobierno de TI

Fuente. Autor del proyecto

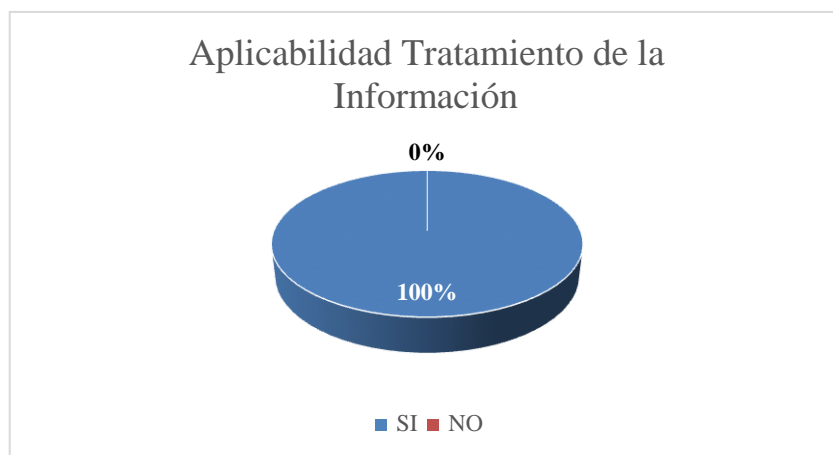


Figura 25. Aplicabilidad Tratamiento de la Información.

Fuente. Autor del proyecto



Figura 26. Aplicabilidad Desarrollo Organizacional.

Fuente. Autor del proyecto

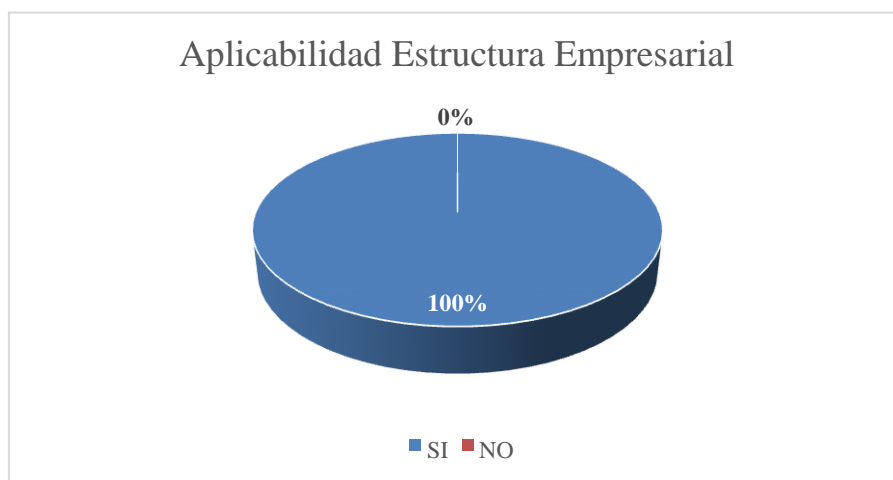


Figura 27. Aplicabilidad Estructura Empresarial.

Fuente. Autor del proyecto

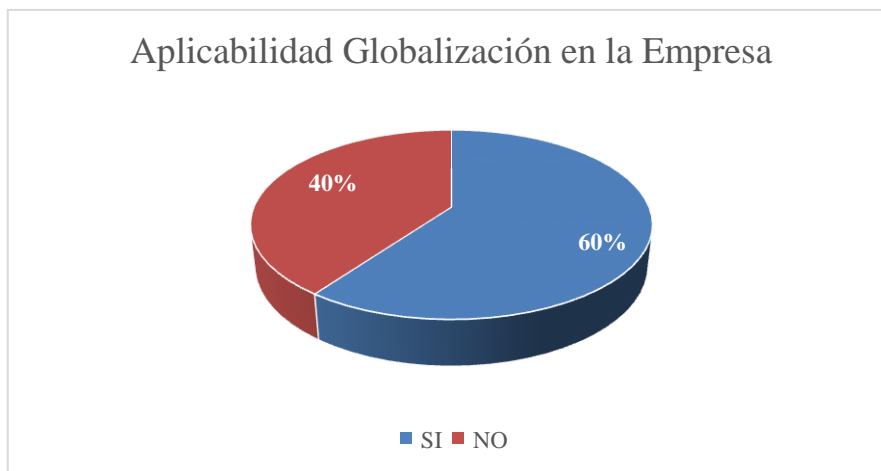


Figura 28. Aplicabilidad Globalización en la Empresa.

Fuente. Autor del proyecto

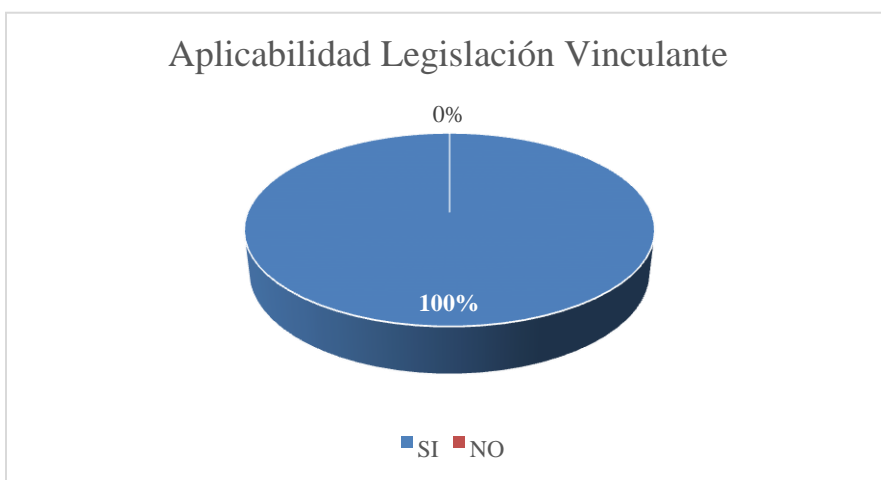


Figura 29. Aplicabilidad Legislación Vinculante.

Fuente. Autor del proyecto

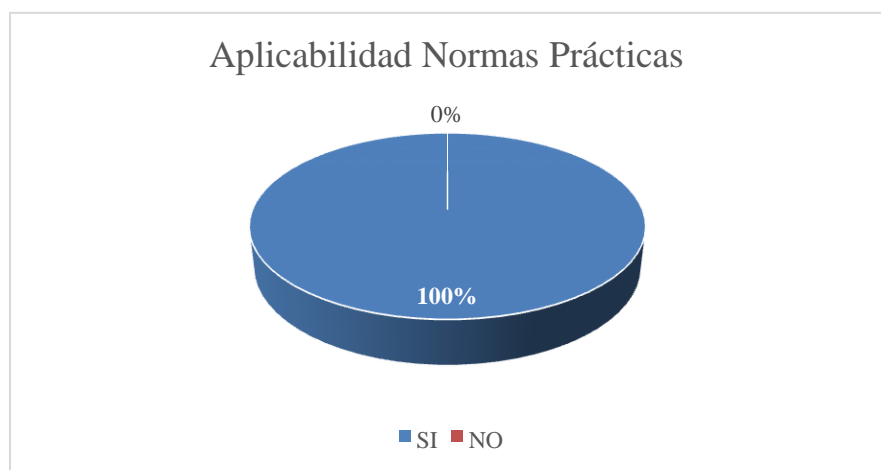


Figura 30. Aplicabilidad Normas Prácticas.

Fuente. Autor del proyecto

4.3.2. Nivel de madurez de aplicación de categorías en las empresas. Complementario a lo anterior, conforme a las buenas prácticas de COBIT 5 se aplicó el nivel de madurez de aplicabilidad de cada una de las categorías en las empresas:

Niveles de Madurez de COBIT 5 (ISACA, 2012)

- **Proceso Incompleto.** El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.
- **Proceso Ejecutado.** El proceso implementado alcanza su propósito.
- **Proceso Gestionado.** El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
- **Proceso Establecido** (dos atributos) – El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.
- **Proceso Predecible.** (dos atributos) – El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.
- **Proceso Optimizado.** (dos atributos) – El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas empresariales presentes y futuros.

Resultados de aplicación de los niveles de madurez

Tabla 3 Niveles de Madurez por Categoría

Empresa	Niveles de Madurez por Categoría						
	Gobierno de TI	Tratamiento de la Información	Desarrollo organizacional	Estructura empresarial	Globalización en la empresa	Legislación vinculante	Normas prácticas
COLOMBIA MAYOR 2013	Incompleto	Ejecutado	Optimizado	Optimizado	Incompleto	Optimizado	Predecible
SEGUROS MUNDIAL	Incompleto	Ejecutado	Optimizado	Optimizado	Incompleto	Optimizado	Predecible
UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA	Incompleto	Ejecutado	Optimizado	Optimizado	Optimizado	Optimizado	Predecible
BDO AUDIT	Incompleto	Ejecutado	Optimizado	Establecido	Predecible	Optimizado	Establecido
MINISTERIO TIC	Optimizado	Ejecutado	Optimizado	Optimizado	Optimizado	Optimizado	Optimizado

Fuente. Autor del proyecto

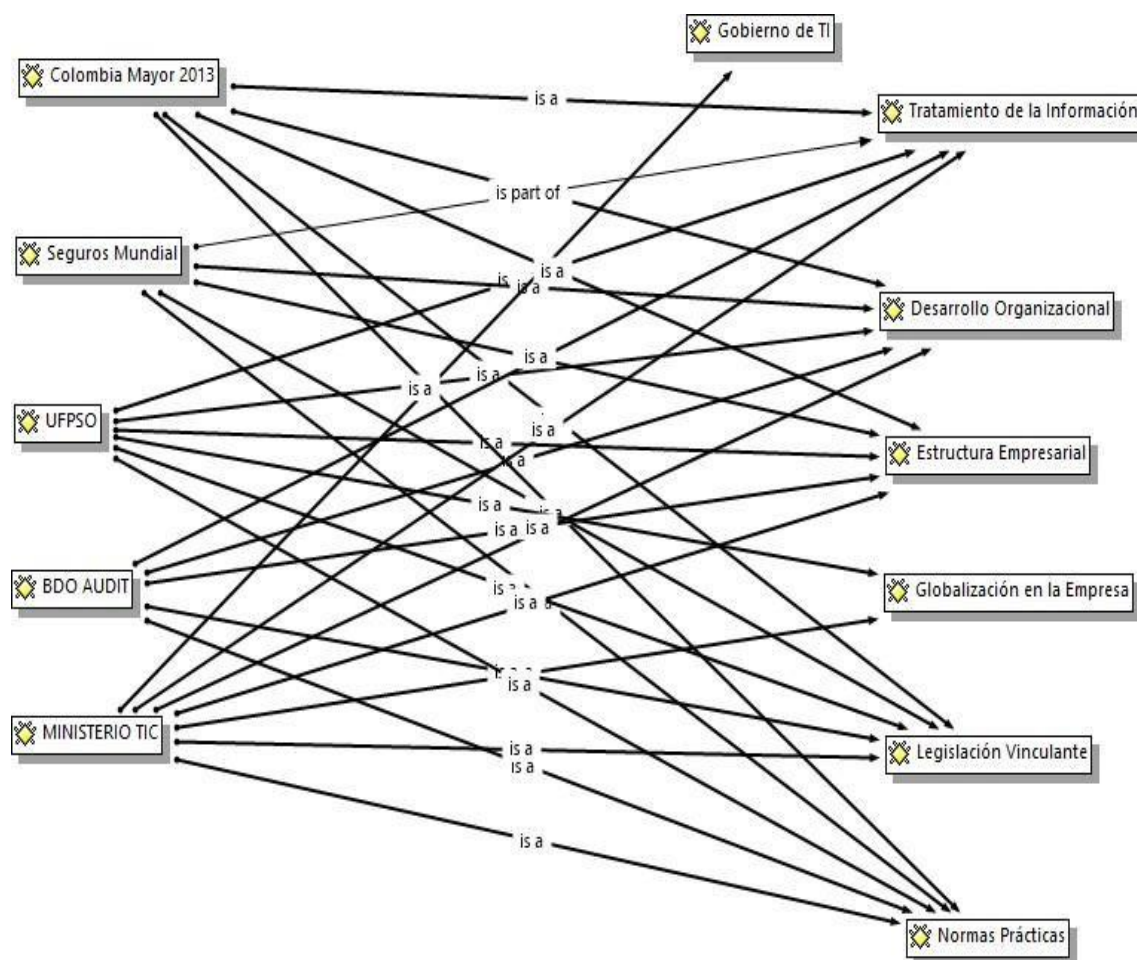


Figura 31. Concreción de las Categorías por Niveles de Madurez.

Fuente. Autor del proyecto

Análisis de los Niveles de Madurez por Categorías en las Empresas

Aplicación Nivel de Madurez Categoría Gobierno de TI

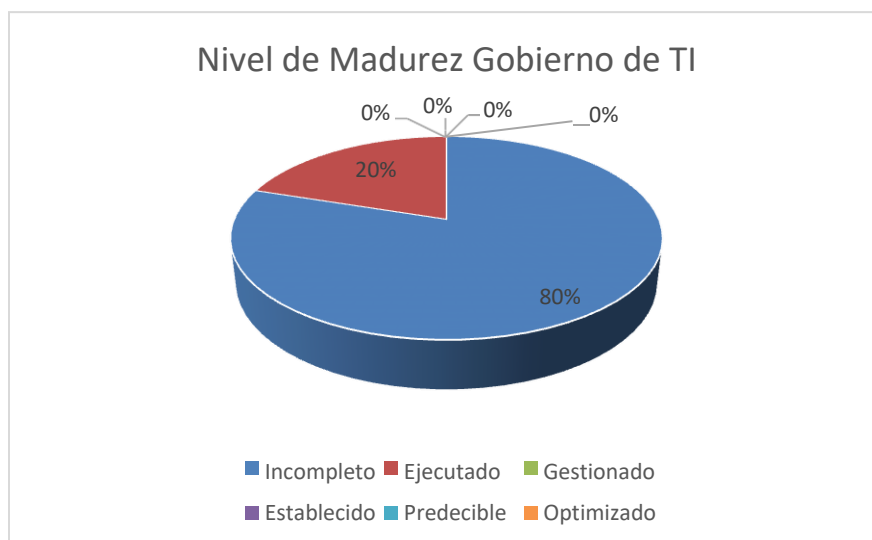


Figura 32. Nivel de Madurez Gobierno de TI.

Fuente. Autor del proyecto

Aplicación Nivel de Madurez Categoría Tratamiento de Información

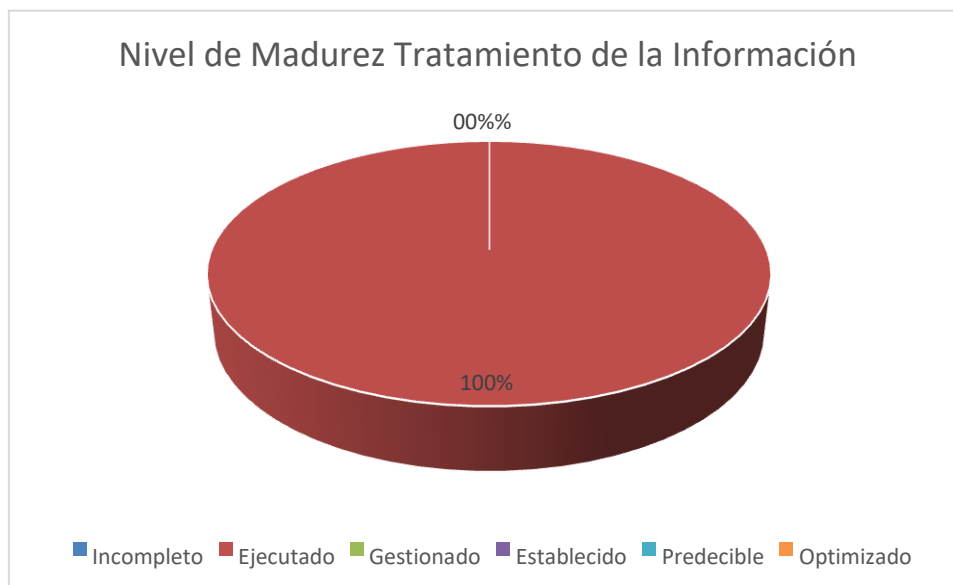


Figura 33. Nivel de Madurez Tratamiento de la Información.

Fuente. Autor del proyecto

Aplicación Nivel de Madurez Categoría Desarrollo Organizacional

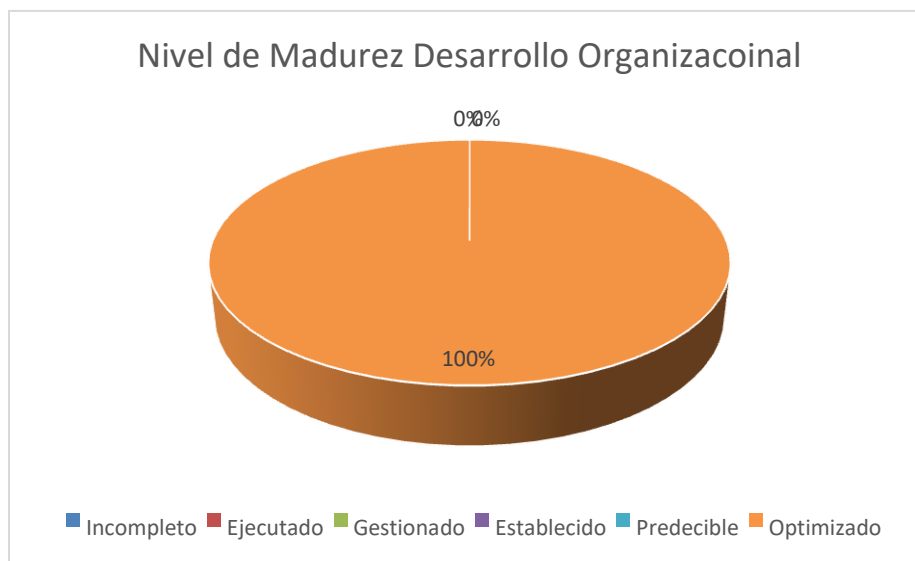


Figura 34. Nivel de Madurez Desarrollo Organizacional

Fuente. Autor del proyecto

Aplicación Nivel de Madurez Categoría Estructura Empresarial

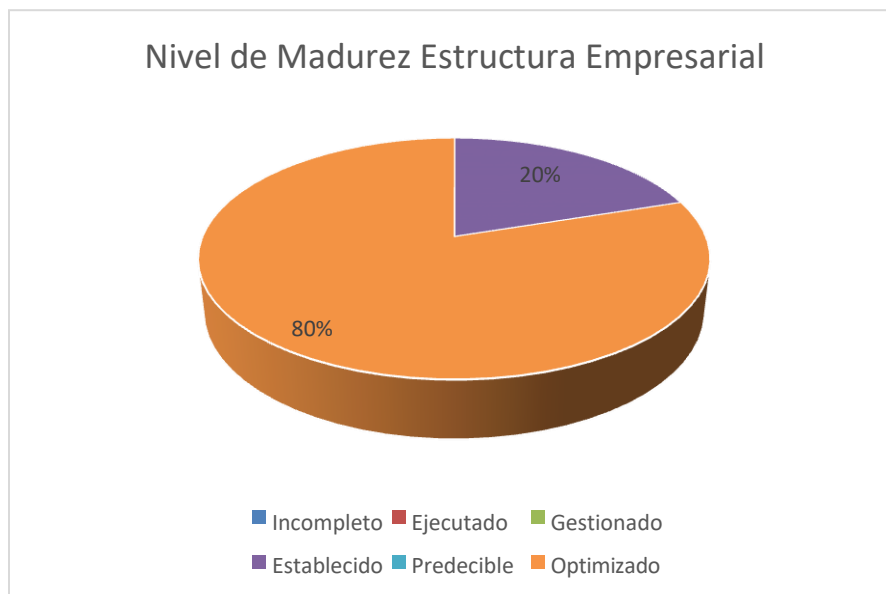


Figura 35. Nivel de Madurez Estructura Empresarial.

Fuente. Autor del proyecto

Aplicación Nivel de Madurez Categoría Globalización en la Empresa

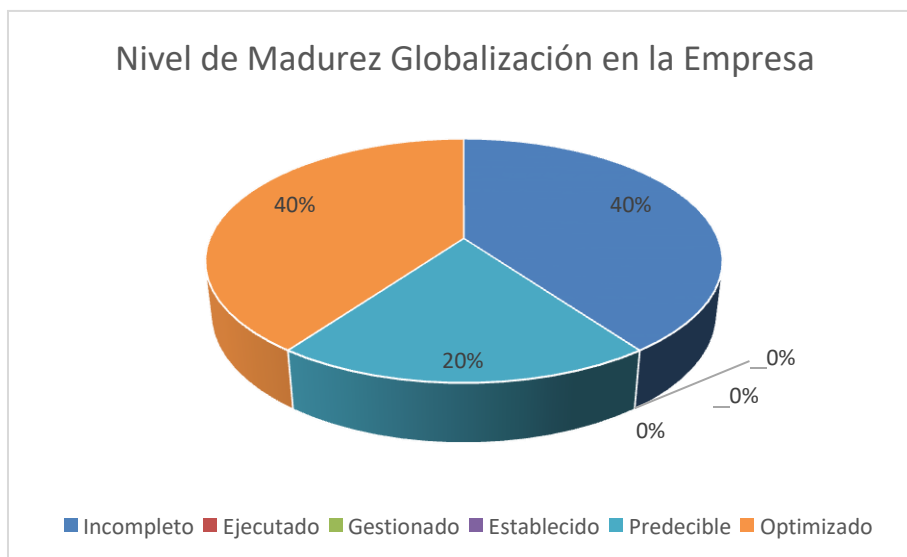


Figura 36. Nivel de Madurez Globalización en la Empresa.

Fuente. Autor del proyecto

Aplicación Nivel de Madurez Categoría Legislación Vinculante

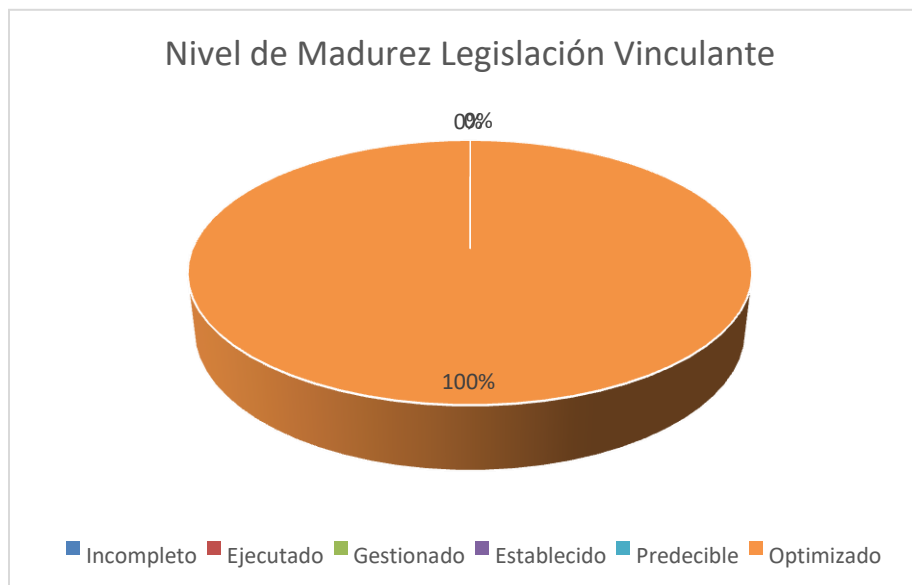


Figura 37. Nivel de Madurez Legislación Vinculante.

Fuente. Autor del proyecto

Aplicación Categoría Normas y Buenas Prácticas

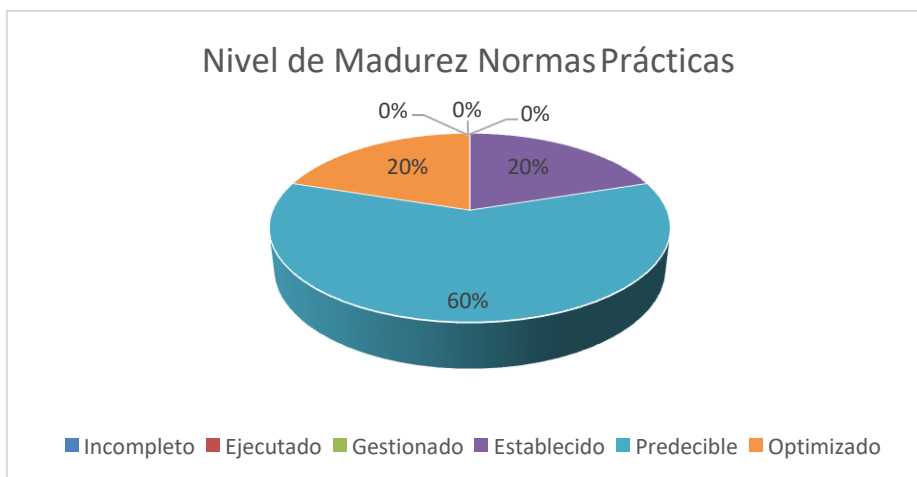


Figura 38. Ni Nivel de Madurez Buenas Prácticas.
Fuente. Autor del proyecto

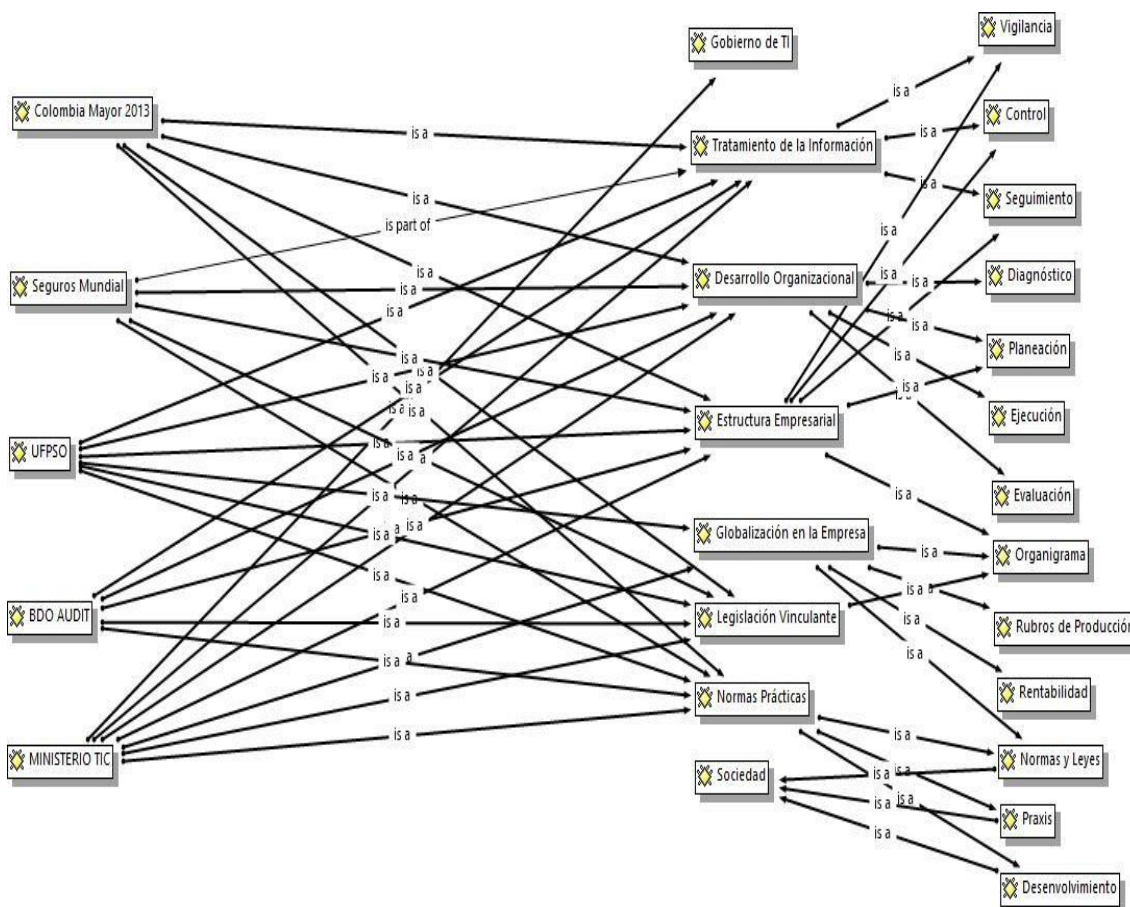


Figura 39. Concreción de categorías surgidas del apoyo estadístico.
Fuente. Autor del proyecto

Atendiendo a la información recolectada se logró inferir que el desarrollo de la investigación conduce a establecer un modelo de gobierno de tratamiento de la información para la empresa colombiana en la globalización como prospectiva de desarrollo organizacional; entendiéndose que se convierte en un aporte de marcada relevancia para el desarrollo y progreso empresarial generando nuevos escenarios y visión que confluyen en innovación e intercambio para las transformaciones sociales a fin de concretar esfuerzos para que los procesos se conviertan en un camino para el tratamiento de la información y por ende generando una política del gobierno de TI para ser implementado en diversas instituciones de cualquier tipo.

4.4 Modelo de gobierno de tratamiento de la información para la empresa colombiana en la globalización como prospectiva de desarrollo organizacional

Desarrollo. Esta investigación se desarrolló contemplando como objetivo principal la estructuración de un Modelo de Gobierno de Tratamiento de la Información para la Empresa Colombiana, a partir de la protección de los derechos fundamentales a nivel tecnológico, ambiental, cultural y político o gobierno corporativo de TI, identificando la realidad actual que enfrenta la empresa colombiana en el tratamiento de datos personales en la Globalización.

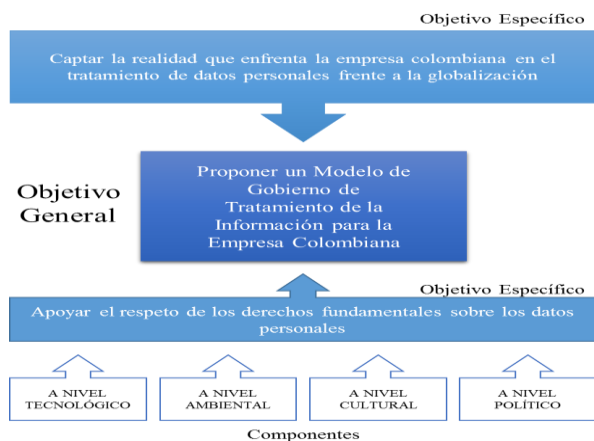


Figura 40. Objetivos del Modelo de Gobierno de Tratamiento de la Información
Fuente. Autor del proyecto

El desarrollo de un modelo de tratamiento de la información de datos personales desde el contexto del gobierno de TI es considerado como una herramienta de apoyo a nivel corporativo para la empresa colombiana en razón de ser competitiva, sostenible y adaptable a las nuevas necesidades que exige la globalización y como parte de su prospectiva de su desarrollo organizacional en el cumplimiento de su misión, visión y metas establecidas. El dato y la Información. La Real Academia de la española, define dato como –información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho. En el campo tecnológico define dato como información disponible adecuadamente para su tratamiento por un ordenador. En un contexto semántico define la información como hechos o circunstancias que otros desconocen, y que puede generar ventajas a quien dispone de ella. Datos personales. La información nos identifica y representa ante la sociedad. Es decisión de cualquier nación darle un valor jurídico en el que ampare la protección de los datos personales en términos de los derechos fundamentales que sean establecidos. Considerando lo anterior, se describen algunas definiciones de dato personal: De acuerdo a lo establecido en los estándares de protección de datos personales para los estados americanos, los Datos Personales son cualquier información referente a una persona física identificada, esta puede mostrarse en diferentes formas tal como gráfica, texto, numérica, etc. Se puede identificar a una persona cuando es determinada de forma directa o indirectamente, en unos plazos razonables.

En España se define datos de carácter personal por la ley orgánica de protección de datos a la información correspondiente a personas físicas que puedan ser identificadas [14]. La OEA en su modelo interamericano de acceso a la Información define información personal como aquella que se encuentra asociada a una persona identificada como viva [15], del mismo modo se define

por el Reglamento General de Protección de Datos de Europa. En Colombia según la ley 1581 se asocia a personas naturales determinadas o determinables de 2012 [5].

Conforme a lo anterior, se propone diseñar un Modelo de Gobierno de Tratamiento de la Información para la Empresa Colombiana, como un elemento fundamental en la organización permitiendo la protección de datos personales, en cumplimiento de los derechos fundamentales de sus titulares.

4.4.1 Impacto de la legislación aplicable al tratamiento de la información de datos personales y prácticas relacionadas. Esta investigación se fundamenta en una metodología cualitativa basada en la teoría fundamentada [16], manteniendo un enfoque descriptivo, en el cual a partir del análisis documental se captará la realidad que enfrenta actualmente la empresa colombiana en el tratamiento de datos personales frente a la globalización. La Teoría Fundamentada es considerada un método de investigación basada en los datos con el fin de identificar procesos sociales [17]. Así mismo, a partir de un enfoque cualitativo conduce a obtener respuestas sobre lo ocurrido y la razón de los fenómenos sociales, se fundamenta en un muestreo teórico e información proporcionada sobre el tratamiento de datos personales en las empresas colombianas y las tendencias que hoy en día se encuentran establecidas a nivel nacional e internacional. Este estudio se contextualiza sobre la legislación aplicable al tratamiento de la información de datos personales y prácticas relacionadas, a partir de este se proyecta la estructura del modelo de gobierno de tratamiento de la información para la empresa colombiana en la globalización como prospectiva de desarrollo organizacional. Se realizó una matriz de operacionalización de variables donde se identificaron como dimensiones la legal,

tecnológica y política y como indicadores la normatividad nacional e internacional, la legislación de TI, los estándares de TI, la seguridad de la información y los tratados internacionales.

Metodología. Gráficamente la metodología utilizada para el desarrollo del modelo de tratamiento de datos personales para la empresa colombiana se visualiza de la siguiente manera:



Figura 41. Metodología del Modelo de Gobierno de Tratamiento de la Información
Fuente. Autor del proyecto

Desarrollo de la Metodología

Objetivo. Contextualizar la legislación aplicable al tratamiento de la información de datos personales y prácticas relacionadas.

Actividad 1. Análisis Documental para: Identificar la legislación nacional sobre el tratamiento de la información. Se tomó como fuente la normatividad de protección de datos personales de la Superintendencia de Industria y Comercio (SIC, 2018).

*Indicador 1. Matriz de legislación tratamiento de datos personales.***Tabla 4. Matriz de Legislación Nacional Tratamiento de Datos Personales.**

Documento Jurídico	Descripción
Constitución Política de Colombia	Por el cual se definen las normas, derechos y deberes de los colombianos y el estado.
Ley 1266 DIC 31, 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. (Habeas Data).
Decreto 1727 MAYO 15, 2009	"Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la informaciónl.
Decreto 2952 AGO 6, 2010	Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008
Ley 1581 OCT 17, 2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Resolución 76434 DIC 4, 2012	Por la cual se deroga el contenido del título V de la Circular Única de la Superintendencia de Industria y Comercio, sobre acreditación, y se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la Ley 1266 de 2008, sobre reporte de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, las cuales se incorporan en el citado título Diario Oficial: 48.635 del 5 de diciembre de 2012
Resolución 20752 ABR 23, 2013	Por la cual se fijan las tasas por servicios de instrucción, formación, enseñanza o divulgación que preste la Entidad en temas relacionados con protección de datos personales. Diario Oficial: 48.771 del 24 de abril de 2013
Decreto 1377 JUN 27, 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 1712 MAR 6, 2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones". Publicada en el Diario Oficial No. 49.084 del 6 de marzo de 2014
Decreto 886 MAYO 13, 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos Diario oficial No. 49150 del 13 de mayo de 2014

Tabla 4. Continuación

Circular 02 NOV 4, 2015	Fecha de expedición: 3 de noviembre de 2015 Diario Oficial: 49686 del 4 de noviembre de 2015 Adicionar el Capítulo Segundo en el Título V de la Circular Única de la Superintendencia de Industria y Comercio.
Circular 01 MAR 24, 2017	Modifica el Capítulo Segundo del Título V de la Circular Única de la Superintendencia de Industria y Comercio Diario Oficial 50051 del 8 de noviembre de 2016.
Sentencia C-748/11 MAR 24, 2017	Control constitucional al Proyecto de Ley Estatutaria No. 184 de 2010 Senado; 046 de 2010 Cámara, –por la cual se dictan disposiciones generales para la protección de datos personales
Sentencia C-1011/08 MAR 24, 2017	Revisión de constitucionalidad del Proyecto de Ley Estatutaria No. 27/06 Senado – 221/07 Cámara (Acum. 05/06 Senado) –por la cual Expediente PE-029 28 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.
Circular 05 AGO 11, 2017	"Adicionar un Capítulo Tercero al Título V de la Circular Única" Publicada en el Diario Oficial N° 50.321 del jueves 10 de agosto de 2017.
Circular 08 DIC 18, 2017	Modifica el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única. Publicada en el Diario Oficial No. 50448 del 15 de diciembre de 2017.
Decreto 90 de 2018 ENE 19, 2018	Por el cual se modifican los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto 1074 de 2015 -Decreto Único Reglamentario del Sector Comercio, Industria y Turismo Diario Oficial 50480 del 18 enero de 2018.
TÍTULO V MAR 28, 2018	Protección de datos personales.

Fuente. Autor del proyecto

Actividad 2. Análisis documental para: Identificar la legislación internacional sobre el tratamiento de la información. Se tomó como referencia la normatividad establecida por la OEA sobre diversos países que muestran legislación en la protección de datos personales (OEA, 2018).

Indicador 2. Matriz de legislación tratamiento de datos personales.

Tabla 5 Matriz de Legislación Internacional Tratamiento de Datos Personales.

País	Documento Jurídico	Descripción
Antigua y Barbuda	The Freedom of Information Act, 2004	UN ACTO para promover la máxima divulgación de información en el interés público, para garantizar y facilitar el derecho de acceso a la información y para proporcionar mecanismos efectivos para Asegúrate ese derecho.
	The Integrity In Public Life Act, 2004	Para prohibir para proveer para el establecimiento de una Integridad Comisión a los efectos de recibir las declaraciones de los asuntos de personas que ocupan puestos específicos en la vida pública, por el propósito de establecer probidad, integridad y rendición de cuentas en la vida pública y para asuntos relacionados.
	The Prevention of Corruption Act, 2004 The Computer Misuse Act, 2006	Para prever la prevención de la corrupción. Para prohibir el acceso no autorizado, el uso o la interferencia a cualquier programa o datos almacenados en una computadora y en una computadora en sí misma y para facilitar la recopilación y el uso de evidencia electrónica
Argentina	Constitución de la Nación Argentina	Derechos y deberes de los ciudadanos y gobierno de la Argentina.
	Ley 25.326 Octubre 4 de 2000	Ley de Protección de Datos Personales
	Decreto 1172/2003 Ley 25.831 Noviembre 26 de 2003	Acceso a la información pública Régimen de libre acceso a la información pública ambiental
Bahamas	The Bahamas Constitution, 1973 (Ver artículo 23) <i>Data Protection Act, 2003</i>	Derechos y deberes de los ciudadanos y gobierno de las Bhamas. Protección de datos
Barbados	The Constitution of Barbados (Ver artículo 20)	Derechos y deberes de los ciudadanos y del gobierno de Barbados.
Belize	Constitution of Belize, 1981 (Ver artículo 12)	Derechos y deberes de los ciudadanos y del gobierno de Belize.
	Freedom of Information Act, Chapter 13	Libertad de la información.
Bolivia	Constitución de la República de Bolivia (Ver artículos 20 y 127 hasta 131)	Derechos y deberes de los ciudadanos y del gobierno de Bolivia.
	Ley N° 1818. Ley del Defensor del Pueblo	Disposiciones generales naturaleza, gratuidad, sede y ámbito de competencia de la institución
Brasil	Constitución Política de la República Federativa del Brasil, 1988 (Ver artículos 10 y 33)	Derechos y deberes de los ciudadanos y del gobierno de Brasil.
	LEI N° 12.527, DE 18 DE NOVENBRO DE 2011	Regula el acceso a la información prevista en el de conformidad con lo dispuesto en el artículo. 5 en el inciso II del § 3o del arte. 37 y en el artículo 2 del artículo. 216 de la Constitución Federal; modifica la Ley no 8.112, de 11 de diciembre de 1990; revoca la Ley no 11.111, de 5 de mayo de 2005, y los dispositivos de la Ley 8159, de 8 de enero de

Tabla 5. Continuación

	Proyecto de Ley: Anteproyeto de Lei sobre a Protecao de Dados Pessoais	1991; y da otras disposiciones. Dispone sobre la protección de datos personales, la privacidad y da otras disposiciones.
Canadá	Proyecto de Ley: Brazilian Draft Bill on Data Protection Access to Information Act Personal Information Protection and Electronic Documents Act	Esta Ley regula el procesamiento de datos personales, a fin de proteger los derechos fundamentales de la libertad y la privacidad de las personas físicas. Acceso a la Información Protección de la información personal y documentos electrónicos
Chile	Constitución Política de la República de Chile de 1980 (Ver artículo 19) Ley 20285 20-08-2008	Derechos y deberes de los ciudadanos y del gobierno de Chile. Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado
	Ley 19628 28-08-1999 Proyecto de Ley: Proyecto de Ley que Modifica la ley N° 19.628, sobre Protección de la Vida Privada y Protección de Datos de Carácter Personal	Ley de Protección de datos de carácter personal Modificación de la ley de protección de la vida privada y protección de carácter personal.
Colombia	Constitución Política de Colombia (Ver artículo 15) Ley Estatutaria 1581 de 2012	Derechos y deberes de los ciudadanos y del gobierno de Colombia. Por la cual se dictan disposiciones generales para la protección de datos personales
	Ley Estatutaria 1266 de 2008. Habeas Data	Ley de habeas data. 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.
	Código Contencioso Administrativo Ley 58 de 1982 Ley 57 de 1985	Código contencioso administrativo Por el cual se reforma el Código Contencioso Administrativo. Por la cual se ordena la publicidad de los actos y documentos oficiales.
	Ley 80 de 1993	por la cual se expide el Estatuto General de Contratación de la Administración Pública
	Ley 136 de 1994	Por la cual se dictan normas tendientes a modernizar la organización y el funcionamiento de los municipios.
	Ley 962 de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos
	Ley 594 de 2000	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
	Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos
	Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
	Decreto 4886 de 2011	Por medio de! cual se modifica la estmctura de la Superintendencia de Industria y Comercio, se determinan las funciones 'de sus dependencias y se dictan otras disposiciones
	Decreto 1151 de 2008	Por el cual se establecen los lineamientos generales de la

Tabla 5. Continuación

		Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
Costa Rica	<p>Proyecto de Ley: Proyecto de Ley Estatutaria 156 de 2011. SENADO</p> <p>Constitución Política de la República de Costa Rica (Ver artículo 28)</p> <p>Compendio Legislación Costarricense y el Derecho de Acceso a la Información Pública</p> <p>EXPEDIENTE No. 16.198</p>	<p>Por medio de la cual, se crea información pública s disposiciones. la Ley de transparencia y del derecho de acceso a la nacional.</p> <p>Derechos y deberes de los ciudadanos y del gobierno de Costa Rica.</p> <p>La Legislación Costarricense y el Derecho de Acceso a la Información Pública</p>
Dominica	<p>Ley n.º 8968 septiembre de 2011</p> <p>Decreto Ejecutivo n.º 37554-JP marzo de 2013.</p> <p>Constitution of the Commonwealth of Dominica of 1978, updated through Act 22 of 1984 (Ver artículo 9)</p>	<p>LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA</p> <p>LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES</p> <p>Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales</p> <p>Derechos y deberes de los ciudadanos y del gobierno de Dominica.</p>
Ecuador	<p>Constitución de la República del Ecuador (Ver artículos 11 y 19)</p> <p>Ley 24, Registro Oficial Suplemento 337 de 18 de Mayo del 2004.</p>	<p>Derechos y deberes de los ciudadanos y del gobierno de Ecuador.</p> <p>Ley Orgánica de Transparencia y Acceso a la Información</p>
El Salvador	<p>Constitución de la República de El Salvador (Ver artículo 6)</p> <p>DECRETO No. 534</p>	<p>Derechos y deberes de los ciudadanos y del gobierno del Salvador.</p> <p>Ley de Acceso a la Información Pública</p>
Estados Unidos de América	<p>The Freedom of Information Act, 5 U.S.C. § 552.</p> <p>Electronic Communications Privacy Act</p>	<p>The Freedom of Information Act. Ley de la libertad de la información.</p> <p>LEY DE PRIVACIDAD DE COMUNICACIONES ELECTRÓNICAS</p> <p>CÓDIGO DE LOS ESTADOS UNIDOS</p> <p>Orden ejecutiva</p>
Guatemala	<p>Executive Order 13392 of December 14, 2005</p> <p>Executive Order 13526 of December 29, 2009</p> <p>The Privacy Act of 1974</p> <p>Constitución Política de la República de Guatemala (Ver artículo 35)</p> <p>Código Penal de Guatemala Decreto No. 17-73 Arts. 274 "D" y 274 -FII</p> <p>DECRETO NÚMERO 57-2008</p> <p>Iniciativa 4090-2009</p> <p>Proyecto de Ley:</p>	<p>Orden ejecutiva</p> <p>LEY DE LA PRIVACIDAD.</p> <p>Derechos y deberes de los ciudadanos y del gobierno de Guatemala.</p> <p>DE LOS DELITOS CONTRA EL DERECHO DE AUTOR, LA PROPIEDAD INDUSTRIAL Y DELITOS INFORMATICOS</p> <p>Ley de Acceso a la Información Pública</p> <p>Ley de Protección de Datos Personales</p> <p>Proyecto de reforma a la Ley de Acceso a la Información Pública</p>
Guyana	<p>Iniciativa 4328</p> <p>Constitution of the</p>	<p>Derechos y deberes de los ciudadanos y del gobierno de</p>

Tabla 5. Continuación

	Cooperative Republic of Guyana (Ver artículo 146) GUYANA BILL No. 10 of 2011	Guyana. Acceso a la información.
Haití	1987 Constitution of Haiti (Ver artículo 40)	Derechos y deberes de los ciudadanos y del gobierno de Haití.
Honduras	Constitución Política De La Republica De Honduras de 1982 (Ver artículos 68 y 182) DECRETO No. 170-2006	Derechos y deberes de los ciudadanos y del gobierno de Honduras.
Jamaica	The Constitution of Jamaica (Ver artículo 22) JAMAICA No. 21— 2002	Ley de Transparencia y Acceso a la Información Pública Derechos y deberes de los ciudadanos y del gobierno de Jamaica.
México	Constitución Política de los Estados Unidos Mexicanos (Ver artículos 6 y 73 apartado XXIX) Diario Oficial de la Federación el 11 de junio de 2002 (Última reforma publicada DOF 06-06-2006) DOF: 05/07/2010	The Access to Information Act. El acceso a la información. Derechos y deberes de los ciudadanos y del gobierno de México. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental Ley Federal de Protección de Datos Personales en Posesión de los Particulares. DECRETO por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
Nicaragua	Constitución Política de la República de Nicaragua (Ver artículo 26) LEY No. 621, Aprobada el 16 de Mayo del 2007 LEY No. 787, Aprobada el 29 de Marzo de 2012	Derechos y deberes de los ciudadanos y del gobierno de Nicaragua. Ley de Acceso a la Información Pública Ley de Protección de Datos Personales
Panamá	Constitución Política de la República de Panamá (Ver artículos 42 y 43) Ley N° 6 de 22 de enero de 2002 Ley No. 13 de 1957 Ley No. 24 del 22 de mayo de 2002 Ley No. 3 del 5 de enero de 2000	Derechos y deberes de los ciudadanos y del gobierno de Panamá Ley de transparencia en la gestión pública Ley orgánica de los Archivos Nacionales de la República de Panamá Por la cual se regula el servicio de información sobre el historial de crédito (...) (Artículos 23 y 30) Ley General sobre las Infecciones de Transmisión Sexual, el Virus de la Inmunodeficiencia Humana y el Sida (Artículos 34 y 37)
Paraguay	Constitución de la República de Paraguay, 1992 (Ver artículos 28, 33 y 135) Ley N° 632 Ley N° 4381	Derechos y deberes de los ciudadanos y del gobierno de Paraguay Orgánica de la Defensoría del Pueblo Modifica el art. 1° y 3° de la Ley N° 838/96. Por la cual se indemniza a víctimas de violaciones de derechos humanos durante la dictadura de 1954 a 1989.

Tabla 5. Continuación

	Ley N° 3075	Modifica el art. 1° de la Ley N° 2494/04. Por la cual se indemniza a víctimas de violaciones de derechos humanos durante la dictadura de 1954 a 1989.
	Ley N° 1682, de 16 de enero de 2001	Que reglamenta la información de carácter privado
	Ley N° 1969, de 3 de septiembre de 2002	Que modifica, amplía y deroga varios artículos de la Ley N° 1682. Poder legislativo ley n° 1969 que modifica, amplía y deroga varios artículos de la ley n° 1682/2001 "que reglamenta la información de carácter privado"
Perú	Constitución Política del Perú (Ver artículos 2, 11, 161 y 162)	Derechos y deberes de los ciudadanos y del gobierno de Perú
	DECRETO SUPREMO N° 072-2003-PCM 07/08/2003	Ley de Transparencia y Acceso a la Información Pública
	LEY N° 29733 03 de julio de 2011	Ley de Protección de datos personales
	Ley N° 27309, de 17 de julio de 2000	Ley que incorpora los delitos informáticos al Código Penal
	LEY N° 28237 31-05-2004	Código Procesal Constitucional
	Decreto Supremo N° 003-2013-JUS, de 21 de marzo de 2013,	Por el que se aprueba el Reglamento de la Ley de Protección de Datos Personales
	Decreto Supremo N° 072-2003-PCM, de 7 de agosto de 2003,	por el que se aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública
	Resolución Ministerial 111-2009 MTC/03, de 6 de febrero de 2009	Salvaguarda derecho a la inviolabilidad y secreto de las telecomunicaciones y Protección Datos Personales y regula las acciones de supervisión y control a cargo del Ministerio de Transportes y Comunicaciones
	Proyecto de Ley: Proyecto de Ley N° 1269/2011	Gestión de Intereses en la Administración Pública
	Proyecto de Ley N° 1260/2011	Modifica el art. 5° de la Ley 27806. Ley de transparencia y acceso a la información pública.
República Dominicana	Constitución de la República Dominicana (Ver artículos 44, 191 y 192)	Derechos y deberes de los ciudadanos y del gobierno de la República Dominicana
	Ley No. 200-04	Ley General de Libre Acceso a la Información Pública
	Ley No. 481-08	Ley General de Archivos de la República Dominicana
	Ley No. 288-05 del 18 de agosto de 2005	Por la cual se regula las Sociedades de Intermediación Crediticia y de Protección al Titular de la Información
	Ley 172-13 del 26 de noviembre de 2013	Ley Orgánica sobre la Protección de Datos de Carácter Personal
San Vicente y las Granadinas	Constitution of Saint Vincent and the Grenadines, 1979 (Ver artículo 10)	Derechos y deberes de los ciudadanos y del gobierno de San Vicente y las Granadinas
	Freedom of Information Act, 2003	Ley de libertad de información
Santa Lucía	Constitution of Saint Lucia, 1979 (Ver artículos 9 y 10)	Derechos y deberes de los ciudadanos y del gobierno de Santa Lucía
Suriname	1987 Constitution of	Derechos y deberes de los ciudadanos y del gobierno de

Tabla 5. Continuación

	Suriname with Reforms of 1992 (Ver artículo 17)	Suriname
Trinidad y Tobago	Constitution of the Republic of Trinidad and Tobago (Ver artículo 4)	Derechos y deberes de los ciudadanos y del gobierno de Trinidad y Tobago
	LAWS OF TRINIDAD AND TOBAGO CHAPTER 22:02 Act No. 13 of 2011	Freedom of Information Act. Ley de libertad de la información Data Protection Act 2011. Proporcionar protección personal Privacidad e información
Uruguay	Constitución de la República Oriental del Uruguay (Ver artículo 10) Ley 18.381. Ley N° 18.220. Ley N° 18.331.	Derechos y deberes de los ciudadanos y del gobierno de Uruguay Derecho de Acceso a la Información Pública Sistema Nacional de Archivos Protección de datos personales y acción de "Habeas Data"
	Ley N° 17.823, de 7 de septiembre de 2004. Ley 19.030 Aprueba el Convenio N° 108	Código de la Niñez y la Adolescencia. (Arts. 218, 219, 221 y 222) Del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y el Protocolo Adicional al Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos transfronterizos de Datos
	Decreto N° 664/008, de 22 de diciembre de 2008	Por el que se crea el Registro de Bases de Datos Personales, adscrito la Unidad Reguladora y de Control de Datos Personales (URCDP)
Venezuela	Constitución de la República Bolivariana de Venezuela (Ver artículos 28 y 58) Normas Venezolanas de 2002	Derechos y deberes de los ciudadanos y del gobierno de Venezuela Normas Venezolanas sobre Acceso a la Información en poder del Sector Público al 2002
	Proyecto de Ley: Ley Orgánica de Transparencia y Acceso a la Información	Proyecto de Ley Orgánica de Transparencia y Acceso a la Información
Sudáfrica	Protection of Personal Information Bill	Protección de la información personal
España	Guía para clientes Prestadores de servicios de Cloud Computing – AGPD	Guía para clientes que contraten servicios de Cloud Computing – AGPD Orientaciones para prestadores de servicios de Cloud Computing – AGPD
Reino Unido	<i>Ley Orgánica</i> 15/1999 Information Commissioner's Office	Ley orgánica de protección de datos personales Guía para la protección de datos

Fuente. Autor del proyecto

Actividad 3. Análisis documental para: Identificar buenas prácticas de tratamiento de la información.

Indicador 3. Matriz de buenas prácticas de tratamiento de la información.

Tabla 6. Matriz de Buenas Prácticas de Tratamiento de la Información

Buena Práctica	Descripción
NTC ISO/IEC 27001:2013	Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI).
NTC ISO/IEC 27002:2015	Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información.
NTC ISO/IEC 27003:2007	Implementación de un Sistema de Gestión de la Seguridad de la Información
NTC ISO/IEC 27005:2009	Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.
NTC ISO 31000:2011	Gestión del Riesgo – Principios y Directrices.
NTC ISO 38500:2009	Gobierno Corporativo de la Tecnología de la Información.
COBIT 5	Marco de Referencia de Gobierno y Gestión para las Tecnologías de la Información.

Fuente. Autor del proyecto

Análisis y resultados. Los resultados obtenidos partieron del diseño y aplicación de un modelo de estudio y análisis de los diferentes contextos aplicables sobre el tratamiento de datos personales requeridos para la empresa. Considerando lo anterior, este modelo se ha fundamentado en el estudio del:

Contexto de la Legislación, el cual se relaciona a las disposiciones normativas legales sobre tratamiento de la información, tratamiento de los datos personales, la globalización del tratamiento de los datos personales y en el tratamiento de la información en la empresa.

Contexto de Gobierno de Tecnología de la Información, haciendo referencia a las diferentes buenas prácticas y modelos de manejo de la información relacionados que aportan al desarrollo de la presente investigación.

Así mismo, considerando el análisis de la información recolectada de los contextos mencionados se llega a un resultado final del alcance de este trabajo logrando dar una contextualización en la empresa colombiana como parte de su visión, adaptabilidad, sostenibilidad y evolución frente a la globalización del tratamiento de la información de los datos personales. A continuación, se muestra el modelo de resultados obtenido:



Figura 42. Modelo de Resultados del Modelo de Gobierno de Tratamiento de la Información.
Fuente. Autor del proyecto

Aplicación del Modelo de Análisis. Para la contextualización de la legislación aplicable se presenta:

El tratamiento de la información. Se fundamenta en aprender a transformar la información en conocimiento, es un término que los últimos años ha conllevado a las organizaciones y a los países a tomar medidas pertinentes en razón de dar especial cumplimiento de los derechos que les conciernen a las personas sobre el habeas data; su ciclo comprende la generación, el almacenaje, el procesamiento y la transmisión. En el Modelo Gavilán de competencia se maneja la información en cuatro etapas: La definición, la búsqueda y evaluación, el análisis, y por último la síntesis y utiliza la información. En el contexto normativo se define el tratamiento de información. En España en el artículo 3 de Ley Orgánica de Protección de Datos (LOPD) es definido como procedimientos y operaciones ya sea automatizado o no, que posibiliten su tratamiento o gestión, de igual manera, se incluyen las cesiones de datos resultantes de consultas, comunicaciones, transferencias e interconexiones. En Colombia la Ley 1581 de 2012 (Ley de Protección de Datos) lo define como cualquier operación o conjunto de operaciones sobre datos personales.

Legislación del tratamiento de la información de datos personales. En términos normativos la protección de los datos personales ha tomado un impulso significativo finalizando la década de los 90, pero a inicios del año 2000 es donde ha tenido más desarrollo. En Europa a partir del año 1999 España emite la Ley Orgánica de Protección de Datos de Carácter Personal. En Colombia la regulación en materia de tratamiento de datos personales trasciende a partir de la Constitución Política del 91 en su Artículo 15, el cual menciona el derecho que tiene cualquier persona a su intimidad, su buen nombre; el artículo 20 señala la libertad que tienen las personas para expresarse y de recibir información, de fundar medios, el derecho a la rectificación y a la no censura. Pero es solo, después del año 2000 donde comienza a tener más auge. De esta manera,

en el 2008 el hábeas data se establece en la ley 1266, con múltiples usos sobre todo en el sector financiero y la ley de delitos informáticos (1273) en el 2009. Es así, como en el año 2012 se define la Ley 1581 por el cual se reglamenta la protección de datos personales en Colombia. Y en el año 2014 el gobierno colombiano emite la Ley 1712 referente a la transparencia y del Derecho de Acceso a la Información Pública Nacional. En Colombia, la transferencia de datos a nivel internacional exige el cumplimiento de requisitos mínimos establecidos en determinada ley, como es el caso descrito por la Ley 1581 de 2012.

Sin embargo, la normatividad colombiana se ha proyectado el tratamiento de la información con otros países, el cual sea considerada óptima para llegar a acuerdos que faciliten esta actividad interempresarial. En cumplimiento de lo anterior, el Gobierno Nacional a través de la Superintendencia de Industria y Comercio como complemento a la Ley 1581 de 2012 ha definido la circular 05 del 10 (agosto de 2017) en el cual manifiesta a los Responsables del Tratamiento de Datos Personales en el cual considera los países presentados por la Comisión Europea que disponen de una regulación adecuada para la protección de los datos personales.

La globalización en el tratamiento de los datos personales. Comunidades como la Comisión Europea hablan de un enfoque global de la protección de los datos personales y ha establecido el Reglamento General de Protección de Datos (RGPD), por el cual define los lineamientos de protección de datos para los países de la Unión Europea. Así mismo, con la participación de naciones se ha manifestado el interés frente al tratamiento de datos o de la información, razón por la cual, también organismos internacionales como la OEA (Organización de los Estados Americanos), el cual establece a través de la Ley Modelo Interamericana sobre

Protección de Datos Personales (en elaboración), trabajan en dar lineamientos que permitan estandarizar la adopción de una normatividad común a nivel internacional que incentive la integración de las naciones asociadas con la finalidad de dar un tratamiento de la información en condiciones óptimas de seguridad y calidad de la misma para las organizaciones y en especial para los titulares o dueños de los datos. En este contexto la OEA manifiesta que es una ley modelo establece parámetros generales o una hoja de ruta. En la OEA, -una ley modelo es el resultado de un proceso inclusivo abierto a la participación de todos los sectores, tantos gobiernos como la sociedad civil, el sector académico, la industria, etc. En el seno de la Organización se han aprobado ya varias leyes modelo, como la Ley Modelo Interamericana sobre Acceso a la Información Pública y la Ley Modelo sobre Garantías Mobiliarias. Así mismo, la Red Iberoamericana de Protección de Datos ha emprendido sus esfuerzos por establecer los lineamientos necesarios con el mismo objetivo de dar un tratamiento adecuado a la información por parte de las naciones suscritas constituyendo una directriz para iniciativas de los países para sus regulaciones.

Tratamiento de la información en la empresa. Es necesario que la empresa de hoy en día tenga una transformación frente al manejo de la información y a la protección de los datos personales que maneja, asegurando los derechos de sus titulares o propietarios conforme a la legislación nacional y la internacional, especialmente con los países donde tiene proyectado o mantiene cualquier tipo de procesamiento, almacenamiento o de manejo de la información. Adicionalmente, la legislación relacionada al tratamiento de la información en un contexto empresarial, hace visible la necesidad en la empresa de dar cumplimiento en términos legales. En Colombia existen acuerdos como el TLC, NAFTA, CARICOM, MERCOSUR, entre otros. Estos

son convenios internacionales que de alguna manera obligan a cumplir con ciertos requisitos comerciales y económicos, y que, a su vez, se ven reflejados en el adecuado manejo de la información para su óptimo desarrollo.

Contexto de Gobierno de Tecnología de la Información. Frente al tratamiento de la información en el contexto de gobierno de TI, Priebe y Markus, han desarrollado un Modelo de Información Comercial a nivel metodológico que hace relación a los proyectos, datos científicos y gobernanza de Big Data Castillo, en su tesis menciona la gestión de datos como una mejora soporte para tomar decisiones en los negocios. Así mismo, en Perú presenta una propuesta para empresas prestadoras de salud con un enfoque de seguridad de la información bajo el enfoque de COBIT 5.0. A nivel de gobierno en Colombia el Ministerio de Tecnologías de la Información y las Comunicaciones en el 2016, ha diseñado un modelo de seguridad y privacidad de la información. En la universidad Nacional ha desarrollado un framework para el gobierno de la información con base en COBIT. Desde el contexto de datos personales, Gacitúa presenta en su tesis doctoral manifiesta la importancia que tiene la protección de datos para la prevención y la represión penal en Europa.

Así mismo desde el contexto de las tecnologías, la importancia que tienen la información, el gobierno de datos en la organización y de ciberseguridad, hoy en día manifiesta la necesidad que debe tener la empresa en el manejo de su información como parte del gobierno corporativo y de la seguridad que debe ser aplicada sobre el tratamiento de la misma

Con esta contextualización se pueden ir identificando los siguientes elementos:

Visión, adaptabilidad, sostenibilidad y evolución. El mercado cada día exige más y mejores productos y servicios, que soportan en la calidad el poder adquisitivo. Sin embargo, la adquisición de un bien, producto o servicio es determinado por medio de procesos precontractuales o contractuales donde existe un intercambio de información, donde el usuario generalmente debe dar sus datos personales para que sean procesados por la empresa que en su buen hacer los requiere para iniciar, consolidar o finiquitar un negocio entre las partes, en razón de cumplir un objetivo en particular generando un beneficio mutuo.

Visión Global: Toda empresa que requiera incursionar actualmente en el mercado nacional o internacional es necesario que a nivel estratégico se proyecte en términos de cumplir de los requisitos legales que le aplican, y uno de estos es la protección de los datos personales que maneja. El gobierno de información en la organización y de ciberseguridad, hoy en día manifiesta la necesidad que debe tener la empresa en el manejo de su información como parte del gobierno corporativo y de la seguridad que debe ser aplicada sobre el tratamiento de la misma

Adaptabilidad: Actualmente, no existe una estandarización en el tratamiento de la información de datos personales a nivel mundial que le permita a la empresa determinar como parte de su gobierno corporativo alinearse a la globalización, el cual contribuya a un desarrollo organizacional, y que dicho tratamiento sea adaptable a lo establecido en las leyes nacionales e internacionales que determinan directrices o lineamientos que son fundamentados al cumplimiento de los mismos, dando libre decisión a la empresa de adopción de medidas y buenas prácticas en el manejo de su información a nivel interno.

Sostenibilidad: La sostenibilidad de la empresa en el mercado hoy no radica solamente en el control financiero, la demanda, la oferta o demás características productivas o económicas, es necesario darle cabida a –la información, en especial, a la información personal de ese actor importante en el sector comercial –los clientes.

Es así que los datos personales de los clientes y de todos los actores que interactúan con la empresa son parte fundamental hoy en día para que la organización aparte de cumplir una legislación requiera protegerla para preservar sus derechos fundamentales y para dar esa confianza y credibilidad del mismo frente a los productos y servicios que adquiere con cualquier compañía o entidad.

Evolución: Leyes que ya se encuentran establecidas en otros países sobre el tratamiento de la información y la suma de más naciones que adoptan directrices sobre el manejo de los datos, hace pensar que se ha iniciado un periodo en el que la Globalización del Tratamiento de la Información Personal en el campo Empresarial debe hacer parte fundamental en todas las organizaciones que mantienen una visión competitiva y sostenible en el mercado a nivel nacional e internacional, en el cual la estandarización sean la base fundamental para dar una solución viable a las empresas.

Por tal motivo, el desarrollo evolutivo empresarial debe concebirse como parte de la estrategia de una empresa y en especial del compromiso de la alta dirección, quien a su vez debe fomentar esta cultura organizacional en todas sus áreas y empleados, a través de la sensibilización de un adecuado tratamiento de los datos personales que maneja la empresa.

4.5 Estructuración del modelo de gobierno de tratamiento de la información para la empresa colombiana en la globalización como prospectiva de desarrollo organizacional.

4.5.1 Establecimiento del modelo de gobierno de tratamiento de la información para la empresa colombiana. Al haber aplicado el modelo de análisis sobre la contextualización de la empresa colombiana frente al tratamiento de los datos personales a nivel legislativo y gobierno de TI se enfrenta al cumplimiento de los derechos fundamentales de sobre la intimidad y privacidad de la información que maneja de sus titulares. Considerando lo anterior, en la empresa colombiana debe nacer el objetivo de mantener un cambio dinámico con una visión empresarial el cual le permita ser adaptable, sostenible y evolutiva cumpliendo con la normatividad establecida sobre el tratamiento de los datos personales en un contexto nacional y/o internacional contemplando su permanencia en la globalización. Por tal motivo, como parte de esta investigación se propone mostrar parte de la fundamentación y estructura para establecer un Modelo de Gobierno de Tratamiento de la Información como una herramienta de apoyo fundamental para lograr el objetivo mencionado.

4.5.2 Contexto general del modelo. El modelo se fundamenta en el desarrollo de tres (3) contextos generales que a su vez incorporan los elementos que hacen parte del mismo. De esta manera, a continuación se presenta la contextualización general del modelo:

- Contexto Transversal.
- Contexto Externo.
- Contexto Interno.

Contexto Transversal. Este contexto se encuentra establecido por los siguientes elementos:

- Ejes Organizacionales.
- Ciclo PHVA.
- Gestión de Riesgo.

Contexto Externo. El contexto externo está determinado por las partes interesadas sobre el proceso de tratamiento de la información de los datos personales, el cual está comprendido por:

Partes Interesadas:

- Titulares de datos personales.
- Gobierno Nacional.
- Entes de Control.
- Mercado Internacional.

Contexto Interno. El contexto interno está trazado por la parte organizacional de la empresa colombiana con base a su operatividad a nivel estratégico, táctico y operativo, mediante la cual se aplica el cumplimiento de requisitos legales, buenas de gobierno y gestión de TI, buenas prácticas de tratamiento de la información y buenas prácticas de seguridad de la información, como responsable del tratamiento de los datos personales de las partes interesadas y

como cumplimiento a las necesidades del mercado nacional o internacional. Así, el contexto interno se encuentra constituido por:

- Nivel Estratégico.
- Nivel Táctico.
- Nivel Operativo.

4.5.3 Elementos del contexto del modelo. Los elementos que hacen parte de este modelo se encuentran distribuidos en los tres (3) contextos establecidos. De esta manera, se establecen los contextos para el tratamiento de los datos personales en la empresa colombiana:

- Contexto Transversal.
- Contexto Externo.
- Contexto Interno.

Elementos del Contexto Transversal. En el contexto transversal se encuentran los siguientes elementos:

Ejes Transversales Organizacionales. El modelo como elementos importantes dispone de cuatro (4) ejes transversales asociados a un ciclo PHVA, y que direccionan la empresa a mantener un desarrollo organizacional en la globalización que enfrenta en el tratamiento de los datos personales. Estos ejes son los siguientes:

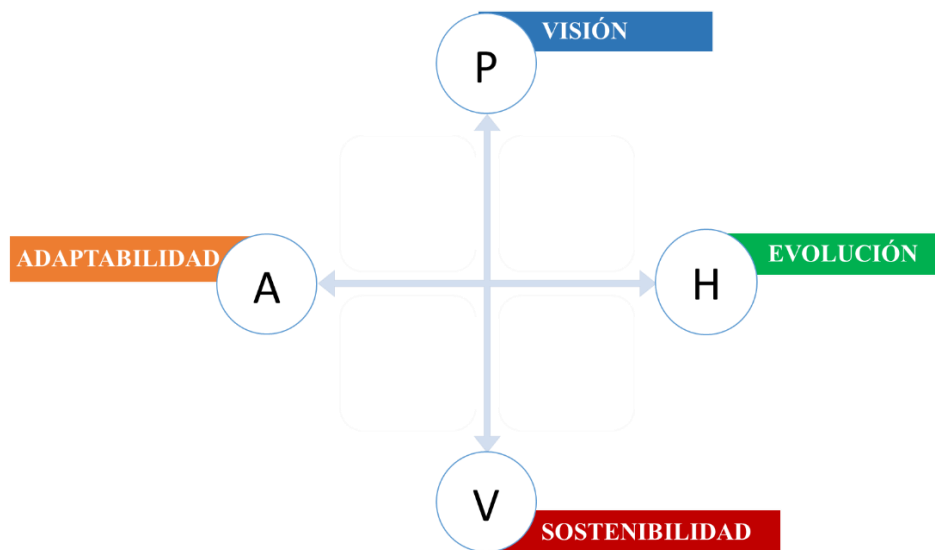


Figura 43. Ejes Organizacionales del Modelo de Gobierno de Tratamiento de la Información.

Fuente. Autor del proyecto

Ciclo PHVA. El ciclo PHVA (Planear, Hacer, Verificar y Actuar), hace parte fundamental de toda la operación del tratamiento de la información de datos personales en la organización. Este se establece como ejes cardinales de todo el proceso enfocado a una mejora continua del mismo en razón de mantener una visión, evolución, sostenibilidad y adaptabilidad de la organización frente al cumplimiento de los requisitos de las partes interesadas a nivel local y global. De esta manera, este ciclo se aplicará en todas los niveles organizacionales conforme a la actividad o proyecto que se desarrolle dentro del mismo para cumplir con el objetivo de proteger los datos personales en las operaciones del negocio.

Gestión de Riesgos. La Gestión de Riesgos en un elemento que tiene un comportamiento transversal en este modelo, debido a que actúa sobre toda la operación de la organización en sus diferentes niveles (Estratégico, Táctico y Operativo), con el fin de mantener una revisión clara en

toda la organización frente a la protección de los datos personales que se enfrentan a posibles amenazas que puedan afectar su correcto tratamiento.

Metodología de gestión de riesgos. Para la gestión de riesgos se define la siguiente metodología basada en la ISO 27005:

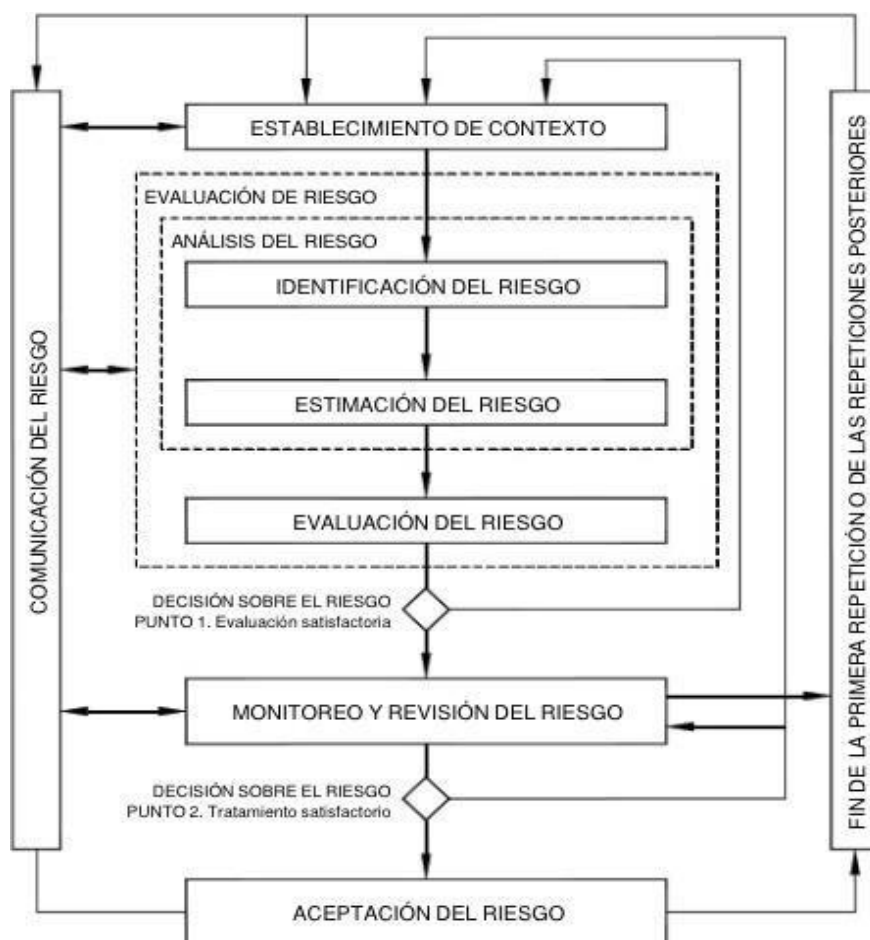


Figura 44. Ejes Proceso de Gestión de Riesgos.
Fuente. ISO 27005.

Este proceso de gestión de riesgos estará enfocado en un ciclo PHVA para ser operado. De esta manera se contemplan las siguientes actividades en cada fase:

Planeación de la Gestión de Riesgos. Actividades

- Establecer el contexto.
- Valorar el riesgo.
- Planificar el tratamiento de los riesgos.
- Aceptación de los riesgos.
- Establecimiento del contexto del riesgo.

El contexto se establece conforme a los riesgos que presentan el tratamiento de los datos personales y a las amenazas a las que se enfrenta. Así mismo, al cumplimiento de la protección de los datos personales conforme a la legislación, normatividad, acuerdos comerciales y contractuales asumidos por la organización. De esta manera, como parte del contexto se establece el propósito:

Propósitos de la Gestión de Riesgos:

- Proteger los datos personales de todos los Titulares que proveen su información a la empresa colombiana.
- Cumplir con la legislación nacional e internacional, acuerdos comerciales y contratos que aplican a la empresa en términos de la protección de datos personales.
- Dar soporte o insumo al sistema de gestión de seguridad de la información de la empresa.
- Preparación para el plan de tratamiento de datos personales para la empresa colombiana.

Criterios de Evaluación de Riesgo

VARIABLES DE EVALUACIÓN DEL RIESGO. La evaluación del riesgo contemplará las siguientes variables o categorías:

Tabla 7 Variables de Evaluación del Riesgo.

Categoría	Causa	Riesgo
Gobierno de TI	Deficiencia en la optimización de la Tecnología en la empresa conforme con la misión y visión establecida (Evolución)	Pérdida de evolución empresarial.
Tratamiento de la Información	Incumplimiento al derecho a la intimidad de las personas (Conformidad)	Pérdida de la conformidad.
Desarrollo Organizacional	Deficiencia en la adaptación de la empresa para el cumplimiento de los requisitos de las partes interesadas y necesidades del mercado. (Adaptabilidad)	Pérdida de adaptabilidad.
Estructura Empresarial	Deficiencia en las operaciones para cumplir con los objetivos empresariales. (Sostenibilidad)	Pérdida de sostenibilidad.
Globalización en la Empresa	Pérdida de oportunidades de expansión del negocio (Visión).	Pérdida de expansión del negocio (Visión).
Cumplimiento de la Legislación Vinculante	Sanciones legales por incumplimiento de la legislación, normatividad, acuerdos comerciales o contractuales. (Conformidad)	Pérdida de la conformidad.
Normas y Buenas Prácticas	Pérdida de competitividad empresarial (Evolución).	Pérdida de evolución empresarial.

Fuente. Autor del proyecto

Criterio de Evaluación del Riesgo

Tabla 8 Criterios Evaluación del Riesgo.

Valor	Nivel de Riesgo	Descripción
9	Crítico	Pérdida Total de la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.
2-6	Moderado	Pérdida parcial de la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.
1	Aceptable	Pérdida leve (no significativa) de la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.

Fuente. Autor del proyecto

Criterios de Impacto

Variables de impacto. Las variables o categorías de impacto se establecen a continuación:

Tabla 9 Variables de impacto.

Categoría	Criterio de Riesgo	Riesgo	Componentes que impacta
Gobierno de TI	Deficiencia en la optimización de la Tecnología en la empresa conforme con la misión y visión establecida (Evolución)	Pérdida de evolución empresarial.	Evolución Estrategia
Tratamiento de la Información	Incumplimiento al derecho a la intimidad de las personas. (Conformidad)	Pérdida de la conformidad.	Conformidad
Desarrollo Organizacional	Deficiencia en la adaptación de la empresa para el cumplimiento de los requisitos de las partes interesadas y necesidades del mercado. (Adaptabilidad)	Pérdida de adaptabilidad.	Adaptabilidad
Estructura Empresarial	Deficiencia en las operaciones para cumplir con los objetivos empresariales. (Sostenibilidad)	Pérdida de sostenibilidad.	Sostenibilidad
Globalización en la Empresa	Pérdida de oportunidades de expansión del negocio (Visión).	Pérdida de expansión del negocio (Visión).	Visión
Cumplimiento de	Sanciones legales por	Pérdida de la	Conformidad

Tabla 9. Continuación

la Legislación Vinculante	incumplimiento de la legislación, normatividad, acuerdos comerciales o contractuales.	conformidad.	
Normas y Buenas Prácticas	Pérdida de competitividad empresarial (Evolución).	Pérdida de evolución empresarial.	Evolución

Nota. Fuente: Elaboración Propia, 2018.

Tabla 10 Criterios de Impacto.

Valor	Nivel de Impacto	Descripción
3	Alto	Afecta la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.
2	Medio	Puede afectar la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.
1	Bajo	Afecta la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.

Fuente. Autor del proyecto

Criterios de Aceptación de Riesgo. La aceptación del riesgo conforme a los criterios de evaluación de riesgo en su parte cuantitativa será en un valor -1||. Complementando lo anterior se da el criterio cualitativo de aceptación del riesgo por variable categoría:

Tabla 11 Criterios de Aceptación de Riesgo.

Categoría	Criterio de Riesgo	Riesgo	Criterio de Aceptación
Gobierno de TI	Deficiencia en la optimización de la Tecnología en la empresa conforme con la misión y visión establecida (Evolución)	Pérdida de evolución empresarial.	Puede ser aceptado.
Tratamiento de la Información	Incumplimiento al derecho a la intimidad de las personas. (Conformidad)	Pérdida de la conformidad.	No puede ser aceptado.

Tabla 11. Continuación

Desarrollo Organizacional	Deficiencia en la adaptación de la empresa para el cumplimiento de los requisitos de las partes interesadas y necesidades del mercado. (Adaptabilidad)	Pérdida de adaptabilidad.	Puede ser aceptado.
Estructura Empresarial	Deficiencia en las operaciones para cumplir con los objetivos empresariales. (Sostenibilidad)	Pérdida de sostenibilidad.	Puede ser aceptado.
Globalización en la Empresa	Pérdida de oportunidades de expansión del negocio (Visión).	Pérdida de expansión del negocio (Visión).	Puede ser aceptado.
Cumplimiento de la Legislación Vinculante	Sanciones legales por incumplimiento de la legislación, normatividad, acuerdos comerciales o contractuales.	Pérdida de la conformidad.	No puede ser aceptado.
Normas y Buenas Prácticas	Pérdida de competitividad empresarial (Evolución).	Pérdida de evolución empresarial.	Puede ser aceptado.

Fuente. Autor del proyecto

Organización de la Gestión de Riesgos de Protección de Datos Personales

Responsables y Funciones de la Gestión de Riesgos:

Tabla 12 Responsables y Funciones de la Gestión de Riesgos.

Ref.	Responsable	Funciones
	Alta Dirección	Asumir el compromiso con la gestión de riesgos en la empresa. Liderar el proceso de gestión de riesgos. Apoyar estrategias en la gestión de riesgos. Comunicar en la organización la gestión de riesgos.
	Jefe de Gestión de Riesgos	Dirigir, coordinar y supervisar el proceso de gestión de riesgos.

Tabla 12. Continuación

	Definir estrategias para la gestión de riesgos en la organización y llevarlas a la Alta Dirección.
	Gestionar con la Alta Dirección los recursos para la gestión de riesgos.
	Fomentar la cultura organizacional en la gestión del riesgo en la organización.
	Comunicar a los interesados y a la Alta Dirección la gestión de riesgos.
Analista riesgos	Apoyar con la recepción, análisis y gestión de tratamiento de riesgos.
	Hacer seguimiento al tratamiento de riesgos.
	Documentar los riesgos.
	Comunicar al Jefe de Riesgos la recepción, análisis y gestión de riesgos.
Jefes de Área	Comunicar los riesgos de su área al responsable de los riesgos en la empresa.
	Ejecutar las actividades de los planes de tratamiento establecidos sobre los riesgos.
	Comunicar al Jefe de Riesgos la gestión y tratamiento de los riesgos de su área.
Empleados	Identificar y reportar eventos de riesgos en la empresa.
	Comunicar los riesgos a su Jefe Inmediato.
Partes Interesadas Externas	Recibir comunicación de la empresa sobre la gestión de los riesgos. Especialmente, en el tratamiento de sus datos personales.

Fuente. Autor del proyecto

Valoración del Riesgo. Análisis del Riesgo.

Identificar los riesgos. La identificación de los riesgos parten de:

Identificar los Activos: Los activos se identificarán y se registrarán en el inventario de activos:

Tabla 13 Inventario de Activos.

Ref.	Nombre Activo	Tipo Activo	Área que pertenece	Responsable
-------------	----------------------	--------------------	---------------------------	--------------------

Fuente. Autor del proyecto

Identificar las Amenazas: Se identificarán las amenazas conforme a lo siguiente:

Tabla 14 Inventario de Amenazas.

Ref.	Nombre Amenaza	Tipo Activo (Interna/Externa)
-------------	-----------------------	--

Fuente. Elaboración Propia, 2018.

Identificar los controles existentes: Se identificarán los controles existentes en la organización:

Tabla 15 Inventario de Controles.

Ref.	Nombre Control	Tipo Control
-------------	-----------------------	---------------------

Preventivo

Detectivo

Fuente. Autor del proyecto

Identificar las vulnerabilidades existentes: Se identificarán las vulnerabilidades existentes en la organización:

Tabla 16 *Inventario de Vulnerabilidades.*

Ref.	Nombre Vulnerabilidad
-------------	------------------------------

Fuente. Autor del proyecto

Identificar las consecuencias: Se identificarán las vulnerabilidades que presenta la organización:

Tabla 17 *Inventario de Consecuencias.*

Ref.	Nombre Consecuencia
	Pérdida de Confidencialidad
	Pérdida de Integridad
	Pérdida de Disponibilidad
	Sanciones legales
	Pérdida de imagen
	Pérdida económica
	Pérdida de oportunidades de mercado

Fuente. Autor del proyecto

Estimación del riesgo. La estimación del riesgo se realizará conforme a la siguiente metodología:

Priorización de los Activos de Información. Criterios de Priorización de los Activos de Información:

Tabla 18 *Priorización de los Activos de Información.*

Escala	Prioridad del Activo	Prioridad
3	Indispensable	El activo es vital y la afectación o pérdida del mismo compromete la operación del negocio.
2	Importante	El activo es importante y la afectación o pérdida del mismo puede comprometer la operación del negocio con la posibilidad de recuperarse.
1	Irrelevante	El activo es importante y la afectación o pérdida del mismo no compromete la operación del negocio y es fácilmente reemplazable.

Fuente. Autor del proyecto

Evaluación de las Consecuencias. Se evaluarán las consecuencias conforme a ciertos escenarios que se pueden presentar sobre las amenazas y vulnerabilidades sobre los activos de información:

Tabla 19 *Escenario de las Consecuencias.*

<u>Activo</u>	<u>Amenaza</u>	<u>Vulnerabilidad</u>	<u>Consecuencia</u>
---------------	----------------	-----------------------	---------------------

Fuente. Autor del proyecto

Tabla 20 *Evaluación Probabilidad de Ocurrencia.*

Ref.	Escenario			Evaluación Probabilidad de Ocurrencia			
	Activo	Amenaza	Vulnerabilidad	Consecuencia	Escala	Prob.	Descripción
E1					3	Recurrente	El escenario se puede presentar recurrentemente, más de 3 veces al año.
E2					2	Ocasional	El escenario se puede presentar ocasionalmente, máximo 2 veces al año.
...					1	Poco probable	El escenario difícilmente se puede presentar, máximo una vez al año.

Fuente. Autor del proyecto

Tabla 21 Evaluación Probabilidad de Impacto.

Ref.	Escenario				Evaluación Probabilidad de Impacto		
	Activo	Amenaza	Vulnerabilidad	Consecuencia	Escala	Prob.	Descripción
E1					3	Alta	El escenario afecta las operaciones del negocio y su recuperación es compleja. Afecta la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.
E2					2	Media	El escenario puede afectar las operaciones del negocio y puede ser recuperada. Puede afectar la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.
...					1	Baja	El escenario afectaría muy poco o no las operaciones del negocio. Afecta poco o nada la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.

Fuente. Autor del proyecto

Evaluación del Riesgo. La evaluación de riesgos se realizará conforme a la siguiente operación:

NIVEL DE RIESGOS = Probabilidad de Ocurrencia X Probabilidad de Impacto.

$$NR = PO \times PI$$

NR: Nivel de Riesgo.

PO: Probabilidad de Ocurrencia.

PI: Probabilidad de Impacto.

Tabla 22 *Evaluación del Riesgo.*

Escenario					Evaluación de Riesgos				
Ref.	Activo	Amenaza	Vulnerabilidad	Consecuencia	PO	PI	Valor	Nivel Riesgo	Descripción
E1							9	Crítico	Afecta la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.
E2							4	Moderado	Puede afectar la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.
...							1	Aceptable	Afecta la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.

Fuente. Autor del proyecto

Mapa de Riesgos

Impacto	3	3	6	9
	2	2	4	6
	1	1	2	3
		1	2	3
		Probabilidad		

Figura 45 . Mapa de Riesgos.
Fuente. Autor del proyecto

Tratamiento del Riesgo. Una vez establecidos los niveles de riesgos, amenazas, vulnerabilidades y controles se define el tratamiento de los riesgos. Para lo cual, se definen los siguientes criterios:

Tabla 23 *Criterios del tratamiento de riesgos.*

Ref	Tratamiento del Riesgo	Descripción
	Reducirlo	Aplicar los controles necesarios de manera interna en la organización con el fin de llevarlo al nivel de riesgo residual aceptable.
	Retenerlo	Aceptar los riesgos conforme a los criterios de aceptación de los mismos determinados.
	Evitarlo	Evitar las actividades que conllevan al origen del riesgo.
	Transferirlo	Delegar o asignar el riesgo a otro responsable interno o externo con el fin de mitigarlo o actuar sobre el mismo.

Fuente. Autor del proyecto

Para lo cual, se determina el siguiente elemento a aplicar:

Tabla 24 *Criterios del tratamiento de riesgos.*

Ref.	Requisito	Actividad	Responsable	Fecha inicial	Fecha Final
-------------	------------------	------------------	--------------------	----------------------	--------------------

Fuente. Autor del proyecto

Ejecución de la Gestión de Riesgos.

Actividades. Implementar el plan de tratamiento de riesgo.

Verificación de la Gestión de Riesgos.

Actividades. Monitoreo y revisión de los riesgos.

Actuación. Actividades Realizar mejora continua a la gestión de riesgos.

- Evaluación del riesgo.
- Monitoreo y revisión del riesgo.
- Aceptación del riesgo.
- Comunicación del riesgo.

A nivel del contexto externo

Partes Interesadas. Las partes interesadas determinan la regulación, requisitos normativos, cumplimientos de ley y/o necesidades que deben ser suplidas en el mercado empresarial como parte la protección de la información en las operaciones de las organizaciones.

A nivel del contexto interno. *En contexto interno se encuentra consolidado por los siguientes elementos:*

- Tres niveles organizacionales (Estratégico, Táctico y Operativo).
- Gestión de Riesgos.

Niveles organizacionales. El modelo como parte de su estructura incorpora tres (3) niveles organizacionales (Estratégico, Táctico y Operativo), de tal manera que se consolide el tratamiento de la información de datos personales en toda la empresa, sus áreas, cargos, roles y funcionarios. De esta manera se definen en los tres niveles organizacionales la operación del modelo:

Nivel Estratégico. En el nivel estratégico se encuentran los siguientes elementos fundamentales:

Tabla 25 Elementos del Nivel Estratégico.

Nivel Estratégico	Elementos
Contexto Jurídico.	<ul style="list-style-type: none"> • Legislación Nacional. • Legislación Internacional. • Acuerdos Internacionales. • Tratados de Libre Comercio.
Contexto Organizacional.	<ul style="list-style-type: none"> • Estrategia. • Comité Directivo. • Metas y métricas. • Responsables de Tratamiento de Datos Personales. • Encargados de Tratamiento de Datos Personales. • Transferencia de Datos a Otros Países.
Contexto Gobierno de TI	Direccionamiento Política de Gobierno de TI. Política de Protección de Datos Personales. Política de Seguridad de la Información. Evaluar, Orientar y Supervisar <ul style="list-style-type: none"> • EDM01. Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.

Tabla 25. Continuación

- EDM02. Asegurar la Entrega de Beneficios.
- EDM03. Asegurar la Optimización del Riesgo.
- EDM04. Asegurar la Optimización de los Recursos.
- EDM05. Asegurar la Transferencia hacia las Partes Interesadas.

Fuente. Autor del proyecto

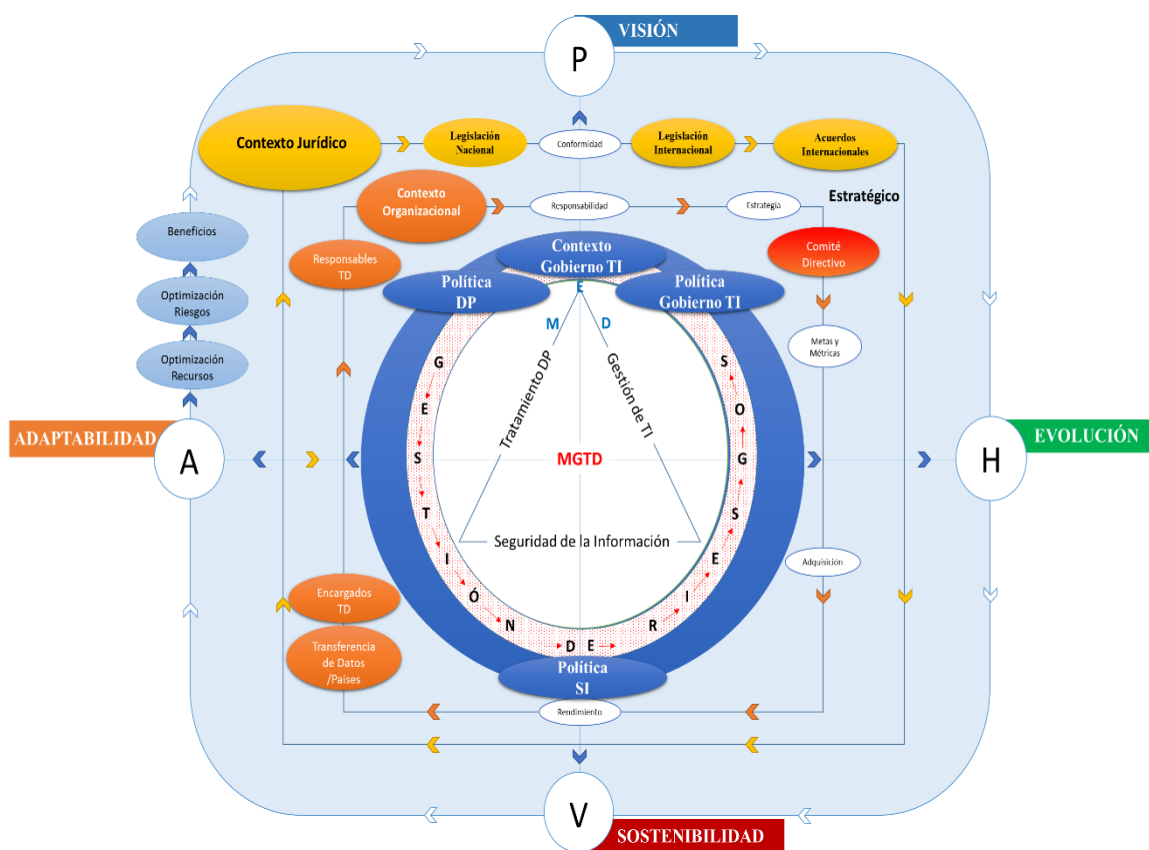


Figura 46. Elementos del Nivel Estratégico.

Fuente. Autor del proyecto

Desarrollo del Contexto Jurídico

Legislación Nacional. Actualmente, en Colombia la legislación de tratamiento de la información de datos personales para las empresas colombianas radica en el cumplimiento de lo siguiente:

Constitución Política de Colombia de 1991. Conforme a la Constitución Política de Colombia de 1991 en su Artículo 15 se da el derecho fundamental a las personas sobre su intimidad. –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. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los 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 interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley. Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar. Para efectos tributarios 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.

Así mismo, en la Constitución en su –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 censural.

Ley 1266 de 2008 por la cual se regula el habeas data en Colombia. En esta Ley –se dictan las disposiciones generales del habeas 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 disposicionesl.

De manera importante, se manifiesta que esta Ley está realmente enfocada especialmente a la empresa Colombiana del sector comercial y financiero o que de alguna manera requiera manejar y proteger la información de sus clientes relacionados con sus datos crediticios. Así mismo, esta ley nace con el fin de proteger los datos crediticios y comerciales de las personas o clientes que manejan las empresas colombianas.

Ley 1581 de 2012 por el cual se regula la protección de los datos personales en Colombia. Esta ley tiene como objeto —desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma (Artículo 1)l. Así mismo, esta ley aplica a cualquier base de datos que contenga información personal que sea manejada por cualquier empresa en Colombia como lo cita en su –Artículo 2°. Ámbito de aplicación. Los principios y disposiciones

contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La Ley 1581 de 2012 realmente maneja con contexto jurídico, otro organizacional y otro que trasciende al manejo tecnológico sobre la información. De esta manera, a continuación se describen de manera general algunos de sus elementos fundamentales:

Principios Rectores de la Ley 1581 de 2012:

- Principio de legalidad en materia de Tratamiento de datos
- Principio de finalidad
- Principio de libertad
- Principio de veracidad o calidad:
- Principio de transparencia
- Principio de acceso y circulación restringida
- Principio de seguridad
- Principio de confidencialidad

Categorías de Datos según la Ley 1581 de 2012

- Datos Sensibles.

Derechos sobre el Tratamiento de los Datos según la Ley 1581 de 2012. *Derechos de los Titulares de los Datos:*

- Conocer, actualizar y rectificar sus datos personales.
- Solicitar prueba de la autorización otorgada.
- Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones.
- Revocar la autorización y/o solicitar la supresión del dato.
- Acceder en forma gratuita a sus datos personales.

Derechos de los niños, niñas y adolescentes. “Se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes”.

- Tratamiento de datos sensibles.
- Autorización del Titular.
- Suministro de la información.
- Deber de informar al Titular.
- Procedimientos
 - Consultas.
 - Reclamos.
 - Requisito de procedibilidad.

- Deberes de los responsables del tratamiento y encargados del tratamiento
 - Deberes de los Responsables del Tratamiento.
 - Deberes de los Encargados del Tratamiento.
- Autoridad de protección de datos.
- Procedimiento y sanciones.
- Del Registro Nacional de Bases de Datos.
- Transferencia de datos a terceros países

Legislación Internacional. En el contexto internacional se encuentra una gran variedad de regulación como se evidencia en la **Tabla 2.** Matriz de Legislación Internacional Tratamiento de Datos Personales. Esta legislación es un insumo para la empresa colombiana siendo autónoma de elegir cualquier contratación con cualquiera de estas naciones en el cual requiera intercambiar datos personales (ej. Datos en la –Nubell o –icloutll). Sin embargo, es importante aclarar que es deber de la empresa colombiana garantizar la seguridad de los datos personales de sus Titulares que haya recolectado y comparta en otras naciones. Por tal motivo, es necesario que previamente a una contratación o asumir cualquier servicio de información se cerciore sobre la normatividad de protección de datos personales que tiene el país y a su vez del cumplimiento de la misma respecto a los requisitos legales en Colombia.

Acuerdos Internacionales / Tratados de Libre Comercio:

- TLC Colombia – México.
- El Salvador, Guatemala y Honduras.

- CAN.
- CARICOM.
- MERCOSUR.
- Chile.
- EFTA.
- Canadá.
- Estados Unidos.
- Acuerdo de alcance Parcial con Venezuela.
- Cuba.
- Unión Europea.
- Alianza del Pacífico.
- Corea.
- Costa Rica.

Desarrollo del Contexto Organizacional

Estrategia. La empresa colombiana para el tratamiento de los datos personales debe definir, implementar y mantener estrategias a nivel corporativo, el cual sean asumidas con el compromiso de la Alta Dirección, posesionadas en la organización y comunicadas a todos sus funcionarios o empleados en razón de lograr conseguir el objetivo de las mismas.

Las estrategias deben ser definidas conforme a las necesidades legales y empresariales de la organización.

Considerando la propuesta de este proyecto se propone que la empresa colombiana desarrolle sus estrategias de tratamiento de la información de datos personales conforme a sus cuatro ejes fundamentales (visión, evolución, sostenibilidad y adaptabilidad) soportadas por el desarrollo de las categorías enfocadas con:

- Gobierno de TI.
- Tratamiento de la Información.
- Desarrollo organizacional.
- Estructura empresarial.
- Globalización en la empresa.
- Legislación vinculante.
- Normas prácticas.

Propuesta estrategias de tratamiento de información de datos personales. Se proponen las siguientes estrategias de tratamiento de la información de datos personales para la empresa colombiana:

Tabla 26 *Estrategias de Tratamiento de Información de Datos Personales*

Ref.	Categoría	Estrategia	Eje que Impulsa
E1	Gobierno de TI.	Establecer, implementar y comunicar una Política de Gobierno de TI enfocada al tratamiento adecuado de los datos personales en la organización.	Evolución
E2	Tratamiento de la Información.	Establecer, implementar y comunicar una Política de <u>Protección de Datos Personales</u>	Adaptabilidad

Tabla 26. Continuación

		en la organización.	
E3	Desarrollo organizacional.	Fomentar la cultura organizacional sobre el tratamiento de los datos personales en la empresa. Establecer una misión que involucre la calidad y seguridad de la información que maneja la empresa.	Adaptabilidad
E4	Estructura empresarial.	Desarrollar una estructura organizacional que incluya un área o rol específico con el tratamiento de los datos personales en la empresa. Segregar las funciones de seguridad informática del tratamiento de los datos personales. Constituir un Comité de Tratamiento de Datos o en su defecto que se incluyan sus responsabilidades en el Comité de Seguridad de la Información.	Sostenibilidad
E5	Globalización en la empresa.	Ampliar la visión de la empresa a un entorno internacional conforme a la comercialización de sus productos y servicios, y en especial al tratamiento de los datos para el caso de adquirir servicios de información en otras naciones, o en su defecto prestarlos desde nuestro país al exterior.	Visión
E6	Legislación vinculante.	Validar y dar oportuno constantemente la legislación nacional en términos de protección de datos personales. A nivel internacional validar la legislación de otras naciones frente a la nuestra con el fin de identificar el cumplimiento de los requisitos mínimos de la nuestra.	Adaptabilidad
E7	Normas prácticas	Establecer, implementar y	Evolución

Tabla 26. Continuación

comunicar una Política de Seguridad de la Información enfocada al tratamiento adecuado de los datos personales en la organización.

Aplicar estándares de seguridad de la información como la norma ISO 27001 o el Marco de Seguridad de COBIT.

Fuente. Autor del proyecto

Comité Directivo. En la empresa debe existir el Comité Directivo, que en razón de responsable o encargado del tratamiento de los datos personales de la empresa debe asumir responsabilidades sobre esta temática.

Conformación del Comité Directivo (Tratamiento de Datos Personales). El Comité Directivo para el desarrollar el tema de tratamiento de datos personales debe estar conformado como mínimo por:

- Presidente o Gerente de la Empresa.
- Jefes de Área de la Empresa.
- Responsable de la Seguridad de la Información.
- Responsable de la Gestión de Riesgos.
- Responsable del Tratamiento de la Información de Datos Personales.
- Responsable de Auditoría.
- Responsable Jurídico.
- Responsable de Tecnología.

Responsabilidades y Funciones del Comité Directivo en el Tratamiento de Datos

Personales. El Comité Directivo frente al tema del tratamiento de datos personales en la organización debe:

- Asumir compromiso con el tratamiento de datos personales en la empresa.
- Definir el responsable y encargados de tratamiento de datos personales en la empresa.
- Hacer seguimiento periódico a nivel estratégico del tratamiento de datos personales en la empresa.
- Tomar decisiones sobre el tratamiento de datos personales en la empresa.
- Apoyar con recursos el tratamiento de datos personales en la empresa.
- Responder a las partes interesadas por el adecuado tratamiento de datos personales en la empresa.
- Establecer estrategias que permitan a la empresa tener un direccionamiento en el gobierno de TI, tratamiento de la información, desarrollo organizacional, estructura empresarial organizada, proyección globalizada, cumplimiento de requisitos legales y buenas prácticas en el tratamiento de los datos personales manteniendo una visión, evolución, adaptación y sostenibilidad en el mercado.
- Mantener la cultura organizacional en el tratamiento de los datos personales en la empresa.

Metas y métricas. Para el control del tratamiento de los datos personales en la empresa se proponen las siguientes metas y métricas:

Metas. Para el tratamiento de datos personales se definen las siguientes metas:

- Cumplir con toda la legislación nacional e internacional, acuerdos comerciales y contractuales aplicables a la empresa sobre el tratamiento de los datos personales.
- Responder a los titulares de los datos personales sobre el adecuado tratamiento de su información respetando el derecho a la intimidad, derecho de acceso sobre su información y protección de la misma.
- Evitar sanciones relacionadas con el tratamiento de los datos personales.
- Dar seguridad y confianza a las partes interesadas (clientes y terceros) sobre el tratamiento de sus datos personales.

Métricas. Para el tratamiento de los datos personales en la organización se proponen métricas basadas en los siguientes indicadores:

Tabla 27 *Métricas de Tratamiento de Información de Datos Personales*

Ref.	Nombre Indicador	Objetivo	Métrica
M1	Cumplimiento de requisitos legales	Validar el estado de cumplimiento de la legislación, acuerdos comerciales y contractuales relacionados con el tratamiento de los datos personales.	$CRL = NRC / NRT$ CRL: Cumplimiento de requisitos legales. NRC: Número de requisitos cumplidos. NRT: Número de requisitos totales.
M2	Atención de consultas de datos personales	Validar el cumplimiento del derecho de consulta sobre los datos personales de los titulares.	$ACDP = NCA / NCR$ ACDP: Atención de consultas de datos personales. NCA: Número de consultas atendidas. NCR: Número de consultas recibidas.
M3	Atención de reclamos de datos personales	Validar el cumplimiento del derecho de reclamo sobre los datos personales de los titulares.	$ARDP = NRA / NRR$ ARDP: Atención de reclamo de datos personales. NRA: Número de reclamos atendidos.

Tabla 27 Continuación

M4	Atención de Quejas de tratamiento de datos a la Superintendencia de Industria y Comercio (SIC)	Validar el cumplimiento del derecho de queja de los titulares ante la SIC sobre los datos personales de los titulares.	<p>NRR: Número de reclamos recibidos. $AQDP = NQA / NQR$</p> <p>AQDP: Atención de quejas de datos personales. NQA: Número de atención de quejas atendidas. NQR: Número de atención quejas recibidas (SIC)</p>
M5	Bases de datos personales registradas en el Registro Nacional de Bases de Datos Personales (RNBD)	Validar el cumplimiento de datos personales registradas en el RNBD.	<p>$RBD = NBDR / NBDT$</p> <p>RBD: Registro de bases de datos personales en el RNBD. NBDR: Número de bases de datos personales registradas. NBDT: Número de bases de datos personales totales identificadas en la empresa. $PE = VPE / CS$</p>
M6	Pérdidas económicas por sanciones realizadas por tratamiento de datos personales	Validar la cantidad de pérdidas económicas de la empresa por sanciones o incumplimiento del tratamiento de datos personales.	<p>PE: Pérdida económica. VPE: Valor pérdida económica. CS: Cantidad de sanciones.</p>
M7	Incidencias de seguridad de tratamiento de datos personales	Validar el número de atención de incidencias de seguridad de los datos personales.	<p>$IA = NIA / NIR$</p> <p>IA: Incidencias de seguridad atendidas. NIA: Número de incidencias atendidas. NIR: Número de incidencias recibidas.</p>
M8	Cumplimiento de los principios de tratamiento de datos personales	Validar el cumplimiento de los principios de tratamiento de datos personales en la empresa.	<p>$CPTD = CPC / CTP$</p> <p>CPTD: Cumplimiento de principios de tratamiento de datos. CPC: Cantidad principios cumplidos. CTP: Cantidad de total de principios.</p>
M9	Autorización de datos	Validar el cumplimiento de autorización de datos recibidos por los titulares.	<p>$ADP = NADR / NRDP$</p> <p>ADP: Autorización de datos personales. NADR: Número de autorización de datos recibidas. NRDP: Número de registros de datos personales en las bases de datos.</p>

Tabla 27. Continuación

M10	Revocación de autorización de datos	Validar las revocaciones de autorización de datos.	$RAD = NRAD / NRDP$ <p>RAD: Revocación de autorización de datos. NRAD: Número de revocación de autorización de datos. NRDP: Número de registros de datos personales en las bases de datos.</p>
------------	-------------------------------------	--	--

Fuente. Autor del proyecto

Responsables de Tratamiento de Datos Personales. El tratamiento de datos personales debe tener un o unos responsables de los mismos, el cual como función principal es la potestad de tomar decisiones sobre los mismos. Por tanto, en la empresa colombiana como responsables de los datos personales puede ser:

- Presidente de la empresa.
- Gerente General de la empresa.
- Representante legal de la empresa.

O al que oficialmente sea designado por el Comité Directivo de la empresa.

Como parte del responsable del tratamiento de los datos personales se propone realizar un acta de compromiso donde se oficialice esta responsabilidad en la empresa. A continuación se propone el siguiente modelo de acta de compromiso:

LOGO DE LA EMPRESA
ACTA DE COMPROMISO RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES
<p>El COMITÉ DIRECTIVO de la empresa _____, en su facultad de definir el tratamiento de datos personales en la organización asigna de manera unánime al Sr (a) _____, identificado con C.C. No. _____, de la ciudad de _____, quien actúa en calidad de GERENTE GENERAL, como RESPONSABLE DEL TRATAMIENTO DE LOS DATOS PERSONALES.</p> <p>Conforme a lo anterior, se firma a los ____ días del mes de ____ del año ____.</p> <p>Acepta,</p> <p>_____</p> <p>NOMBRE Y APELLIDOS RESPONSABLE Responsable Tratamiento de Datos Personales.</p> <p>_____</p> <p>NOMBRES REPRESENTANTES COMITÉ Cargo</p>

Figura 47. Modelo Acta Compromiso del Tratamiento de Datos Personales.
 Fuente. Autor del proyecto

Encargados de Tratamiento de Datos Personales. Los encargados de tratamiento de datos personales en la empresa son aquellos a los que se les delega una acción sobre la misma. Estos encargados son designados por el responsable del tratamiento de la empresa conforme a las funciones y responsabilidades en la organización que involucran el tratamiento de datos personales.

Dentro de los encargados de tratamiento de los datos personales en la empresa se pueden determinar los siguientes:

Tabla 28 Encargados de Tratamiento de Datos Personales.

Ref	Encargado	Activo Encargado
	Responsable de Tecnología	Bases de Datos de Personales en formato electrónico.
	Responsable de Recursos Humanos	Bases de Datos de Empleados y Familiares.
	Responsable Administrativo	Bases de Datos de Visitantes. Bases de Datos de Contratistas. Bases de Datos de Proveedores.
	Responsable de Mercadeo	Bases de Datos de los Clientes.
	Responsable de Gestión Documental	Bases de Datos de Personales en formato físico.

Fuente. Autor del proyecto

Transferencia de Datos a Otros Países. La empresa en caso que requiera transferir datos a otros países es necesario que se tenga presente las siguientes indicaciones:

- Identificación y análisis de la legislación de tratamiento de datos personales del país al cual se pretende transferir datos personales.
- Validar la legislación de tratamiento de datos personales de los otros países frente al cumplimiento de los requisitos mínimos de protección de datos personales exigidos en nuestro país.
- Solicitar autorización de los datos personales a sus titulares para transferencia de datos a otros países.

Transferencia de Datos a Terceros. La transferencia de datos personales puede darse de manera local con empresas actuantes en Colombia o con empresas que ofrecen servicios de tratamiento de la información en otros países. Conforme a lo anterior, la empresa colombiana a la hora de transferir datos a terceros a nivel nacional o internacional debe cumplir lo siguiente:

Para transferencia de datos a terceros nacionales:

- Validar la autorización de los datos personales por parte del Titular para transferir datos a terceros nacionales. De lo contrario, solicitar dicha autorización al Titular.
- Validar el cumplimiento de la legislación de protección de datos personales por parte del terceros.
- Establecer un convenio o contrato formal con el tercero donde se evidencie la delegación de encargado del tratamiento de los datos personales.
- Incluir en los convenios con terceros todos los requisitos de seguridad necesarios requeridos por la empresa responsable para el tratamiento de los datos personales. Por ejemplo, cláusulas de confidencialidad, propiedad de la información, tratamiento de los datos personales y demás requisitos de seguridad y privacidad de la información.
- Validar la seguridad de la información del tratamiento de los datos personales del tercero.
- Transferir los datos personales de forma segura, enviando la información cifrada y entregada directamente a los encargados.
- Mantener una comunicación permanente sobre la gestión del tratamiento de los datos personales encargados al tercero.

Para transferencia de datos a terceros internacionales:

- Validar legislación de protección de datos personales en el país donde se encuentra el tercero al cual se le delegará el encargo de tratamiento de la información.

- Verificar el cumplimiento de la legislación de protección datos personales por parte de la empresa del otro país
- Solicitar la autorización de datos personales por parte de los Titulares para la transferencia de datos personales a terceros de otros países.
- Establecer un convenio o contrato formal con el tercero donde se evidencie la delegación de encargado del tratamiento de los datos personales.
- Incluir en los convenios con terceros todos los requisitos de seguridad necesarios requeridos por la empresa responsable para el tratamiento de los datos personales. Por ejemplo, cláusulas de confidencialidad, propiedad de la información, tratamiento de los datos personales y demás requisitos de seguridad y privacidad de la información.
- Validar la seguridad de la información del tratamiento de los datos personales del tercero.
- Transferir los datos personales de forma segura, enviando la información cifrada y entregada directamente a los encargados.
- Mantener una comunicación permanente sobre la gestión del tratamiento de los datos personales encargados al tercero.

Desarrollo del Contexto Gobierno de TI

Direccionamiento. La empresa debe definir unas políticas como parte del direccionamiento que se le da al tratamiento de los datos personales. Por tal motivo, debe definir una política de gobierno de TI el cual fortalezca el direccionamiento del tratamiento de la información de los datos a través de las tecnologías de la información en la organización. Una política de protección de datos en cumplimiento a la legislación vigente en Colombia y una

política de seguridad de la información el cual establezca el compromiso en la empresa para mantener segura y de manera privada la información. Conforme a lo anterior se proponen unos modelos de las políticas mencionadas:

Modelo: Política De Gobierno De Ti

La empresa_____de Colombia establece la política de gobierno de TI como compromiso de direccionamiento de las tecnologías de la información como un marco estratégico y apoyo en toda la organización frente al cumplimiento de sus metas corporativas, misión, VISIÓN y EVOLUCIÓN empresarial.

Modelo: Política De Protección De Datos Personales

La empresa_____de Colombia asume el compromiso con el tratamiento y protección de los datos personales almacenadas en sus bases de datos que contienen información de sus Titulares conforme a la finalidad establecida, asegurando los derechos que le asisten sobre la misma y dando CONFORMIDAD a la legislación vigente en Colombia.

Modelo: política de seguridad de la información.

La empresa_____de Colombia establece la política de seguridad la información como compromiso de la Alta Dirección y toda la organización con sus clientes y partes interesadas sobre manejo seguro de la información, gestionando los riesgos sobre la misma

dando cumplimiento a los principios de integridad, disponibilidad y confidencialidad, y así mismo, a los requisitos legales y contractuales vigentes relacionados, haciéndola ADAPTABLE y SOSTENIBLE en el campo empresarial.

Evaluar, Orientar y Supervisar. El Direccionamiento del gobierno de TI según COBIT 5 se desarrolla dando cumplimiento a tres fases: Evaluar, Orientar y Supervisar que a su vez se relaciona con la definición de las siguientes temáticas:

- EDM01. Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.
- EDM02. Asegurar la Entrega de Beneficios.
- EDM03. Asegurar la Optimización del Riesgo.
- EDM04. Asegurar la Optimización de los Recursos.
- EDM05. Asegurar la Transferencia hacia las Partes Interesadas.

Nivel Táctico. En el nivel táctico se cumple con las directrices y lineamientos establecidos en el nivel estratégico. Para esto, es necesario aplicar buenas prácticas para el tratamiento de datos personales, gestión de TI y seguridad de la información el cual consideran los siguientes elementos fundamentales:

Tabla 29 Elementos del Nivel Táctico.

Nivel Táctico	Definición de Elementos
Buenas prácticas de Tratamiento de Datos Personales.	<ul style="list-style-type: none"> • PDP. Procedimientos de Datos Personales. • FDP. Formatos de Tratamiento de Datos Personales. • APDP. Avisos de Privacidad de Datos Personales. • HDP. Herramientas de Tecnologías de la Información para el Tratamiento de Datos Personales. • CDP. Clasificación de la Información de Datos

Tabla 29. Continuación

Buenas prácticas de Gestión de TI.

- Personales.
 - BDP. Bases de Datos Personales.
 - Alinear, Planificar y Organizar.
 - APO01. Gestionar el Marco de Gestión de TI.
 - APO02. Gestionar la Estrategia.
 - APO03. Gestionar la Arquitectura Empresarial.
 - APO04. Gestionar la Innovación.
 - APO05. Gestionar el Portafolio.
 - APO06. Gestionar el Presupuesto y los Costes.
 - APO07. Gestionar los Recursos Humanos.
 - APO08. Gestionar las Relaciones.
 - APO09. Gestionar los Acuerdos de Servicio.
 - APO10. Gestionar los Proveedores.
 - APO11. Gestionar la Calidad.
 - APO12. Gestionar el Riesgo.
 - APO13. Gestionar la Seguridad.
 - Construir, Adquirir e Implementar.
 - BAI01. Gestionar los Programas y Proyectos.
 - BAI02. Gestionar la Definición de Requisitos.
 - BAI03. Gestionar la Identificación y la Construcción de Soluciones.
 - BAI04. Gestionar la Disponibilidad y la Capacidad.
 - BAI05. Gestionar la Introducción de Cambios Organizados.
 - BAI06. Gestionar los Cambios.
 - BAI07. Gestionar la Aceptación del Cambio y de la Transición.
 - BAI08. Gestionar el Conocimiento.
 - BAI09. Gestionar los Activos.
 - BAI10. Gestionar la Configuración.
 - Entregar, dar Servicio y Soporte.
 - DSS01. Gestionar las Operaciones.
 - DSS02. Gestionar las Peticiones y los Incidentes del Servicio.
 - DSS03. Gestionar los Problemas.
 - DSS04. Gestionar la Continuidad.
 - DSS05. Gestionar los Servicios de Seguridad.
 - DSS06. Gestionar los Controles de los Procesos del Negocio.
 - Supervisar, Evaluar y Valorar
 - MEA01. Supervisar, Evaluar y Valorar Rendimiento y Conformidad.
 - MEA02. Supervisar, Evaluar el Sistema de Control Interno.
 - MEA03. Supervisar y Valorar la Conformidad con los Requerimientos Externos.
-

Tabla 30. Continuación

Buenas prácticas de Seguridad de la Información.

- A5. Política de Seguridad de la Información.
- A6. Organización de Seguridad de la Información.
- A7. Seguridad de los Recursos Humanos.
- A8. Gestión de Activos.
- A9. Control de Accesos.
- A10. Cifrado de la Información.
- A11. Seguridad Física y Ambiental.
- A12. Seguridad de las Operaciones.
- A13. Seguridad de las Comunicaciones.
- A14. Adquisición, Desarrollo y Mantenimiento de Sistemas.
- A15. Relación con los Proveedores.
- A16. Gestión de Incidentes.
- A17. Seguridad en la Continuidad del Negocio.
- A18. Cumplimiento.

Fuente. Autor del proyecto

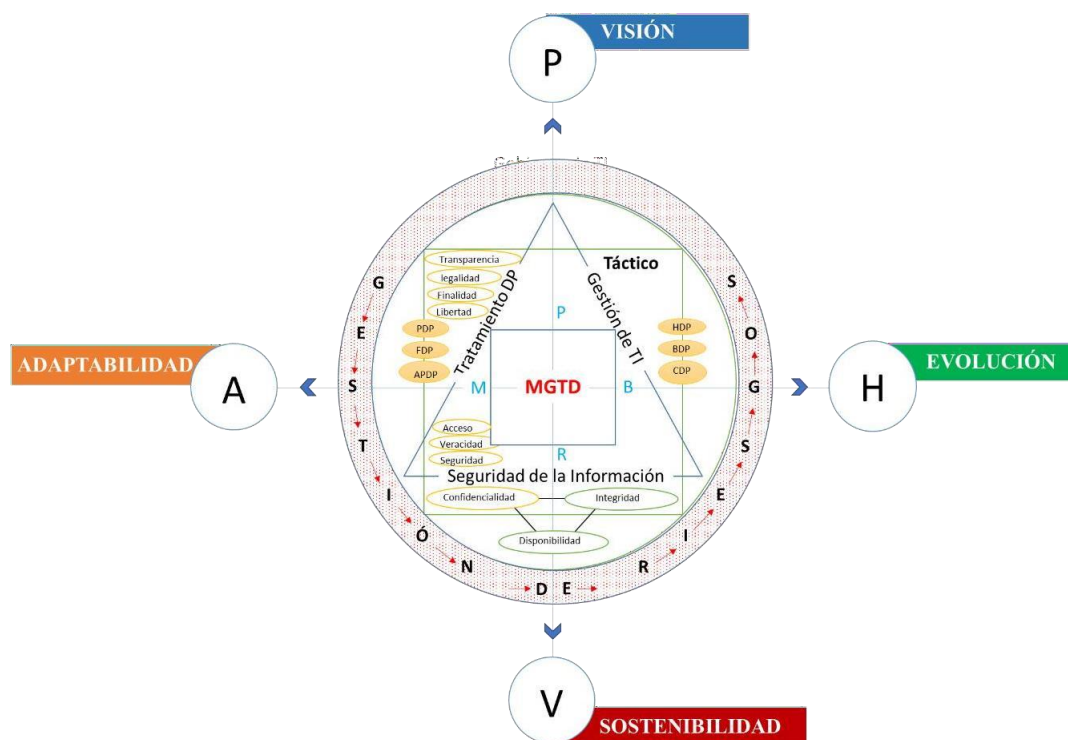
Elementos del Nivel Táctico

Figura 48. Elementos del Nivel Táctico.

Fuente. Autor del proyecto

Nivel Operativo. En el nivel operativo se aplica las buenas prácticas de TI establecidas en el nivel táctico. De esta manera, en este nivel se encuentran los siguientes elementos fundamentales:

Tabla 30 Elementos del Nivel Operativo.

Nivel Operativo	Aplicar Elementos
Buenas prácticas de Tratamiento de Datos Personales.	<ul style="list-style-type: none"> • Aplicar PDP. Procedimientos de Datos Personales: <ul style="list-style-type: none"> ○ Procedimiento de Consulta, Reclamos y Procedibilidad. • Aplicar el FDP. Formatos de Autorización de Datos Personales. • Aplicar APDP. Avisos de Privacidad de Datos Personales. • Aplicar HDP. Herramientas de Tecnologías de la Información para el Tratamiento de Datos Personales. • CDP. Clasificación de la Información de Datos Personales. • Registrar BDP. Bases de Datos Personales en el Registro Nacional de Base de Datos.
Buenas prácticas de Gestión de TI.	<p>Aplicar las siguientes buenas prácticas:</p> <p>Alinear, Planificar y Organizar.</p> <ul style="list-style-type: none"> • APO01. Gestionar el Marco de Gestión de TI. • APO02. Gestionar la Estrategia. • APO03. Gestionar la Arquitectura Empresarial. • APO04. Gestionar la Innovación. • APO05. Gestionar el Portafolio. • APO06. Gestionar el Presupuesto y los Costes. • APO07. Gestionar los Recursos Humanos. • APO08. Gestionar las Relaciones. • APO09. Gestionar los Acuerdos de Servicio. • APO10. Gestionar los Proveedores. • APO11. Gestionar la Calidad. • APO12. Gestionar el Riesgo. • APO13. Gestionar la Seguridad. <p>Construir, Adquirir e Implementar.</p> <ul style="list-style-type: none"> • BAI01. Gestionar los Programas y Proyectos. • BAI02. Gestionar la Definición de Requisitos. • BAI03. Gestionar la Identificación y la Construcción de Soluciones. • BAI04. Gestionar la Disponibilidad y la Capacidad. • BAI05. Gestionar la Introducción de Cambios

Tabla 30. Continuación

<p>Buenas prácticas de Seguridad de la Información.</p>	<p>Organizados.</p> <ul style="list-style-type: none"> • BAI06. Gestionar los Cambios. • BAI07. Gestionar la Aceptación del Cambio y de la Transición. • BAI08. Gestionar el Conocimiento. • BAI09. Gestionar los Activos. • BAI10. Gestionar la Configuración.
	<p>Entregar, dar Servicio y Soporte.</p> <ul style="list-style-type: none"> • DSS01. Gestionar las Operaciones. • DSS02. Gestionar las Peticiones y los Incidentes del Servicio. • DSS03. Gestionar los Problemas. • DSS04. Gestionar la Continuidad. • DSS05. Gestionar los Servicios de Seguridad. • DSS06. Gestionar los Controles de los Procesos del Negocio. <p>Supervisar, Evaluar y Valorar</p> <ul style="list-style-type: none"> • MEA01. Supervisar, Evaluar y Valorar Rendimiento y Conformidad. • MEA02. Supervisar, Evaluar el Sistema de Control Interno. • MEA03. Supervisar y Valorar la Conformidad con los Requerimientos Externos. • Aplicar A5. Política de Seguridad de la Información. • Aplicar A6. Organización de Seguridad de la Información. • Aplicar A7. Seguridad de los Recursos Humanos. • Aplicar A8. Gestión de Activos. • Aplicar A9. Control de Accesos. • Aplicar A10. Cifrado de la Información. • Aplicar A11. Seguridad Física y Ambiental. • Aplicar A12. Seguridad de las Operaciones. • Aplicar A13. Seguridad de las Comunicaciones. • Aplicar A14. Adquisición, Desarrollo y Mantenimiento de Sistemas. • Aplicar A15. Relación con los Proveedores. • Aplicar A16. Gestión de Incidentes. • Aplicar A17. Seguridad en la Continuidad del Negocio. • Aplicar A18. Cumplimiento.

Fuente. Autor del proyecto

Elementos del Nivel Operativo

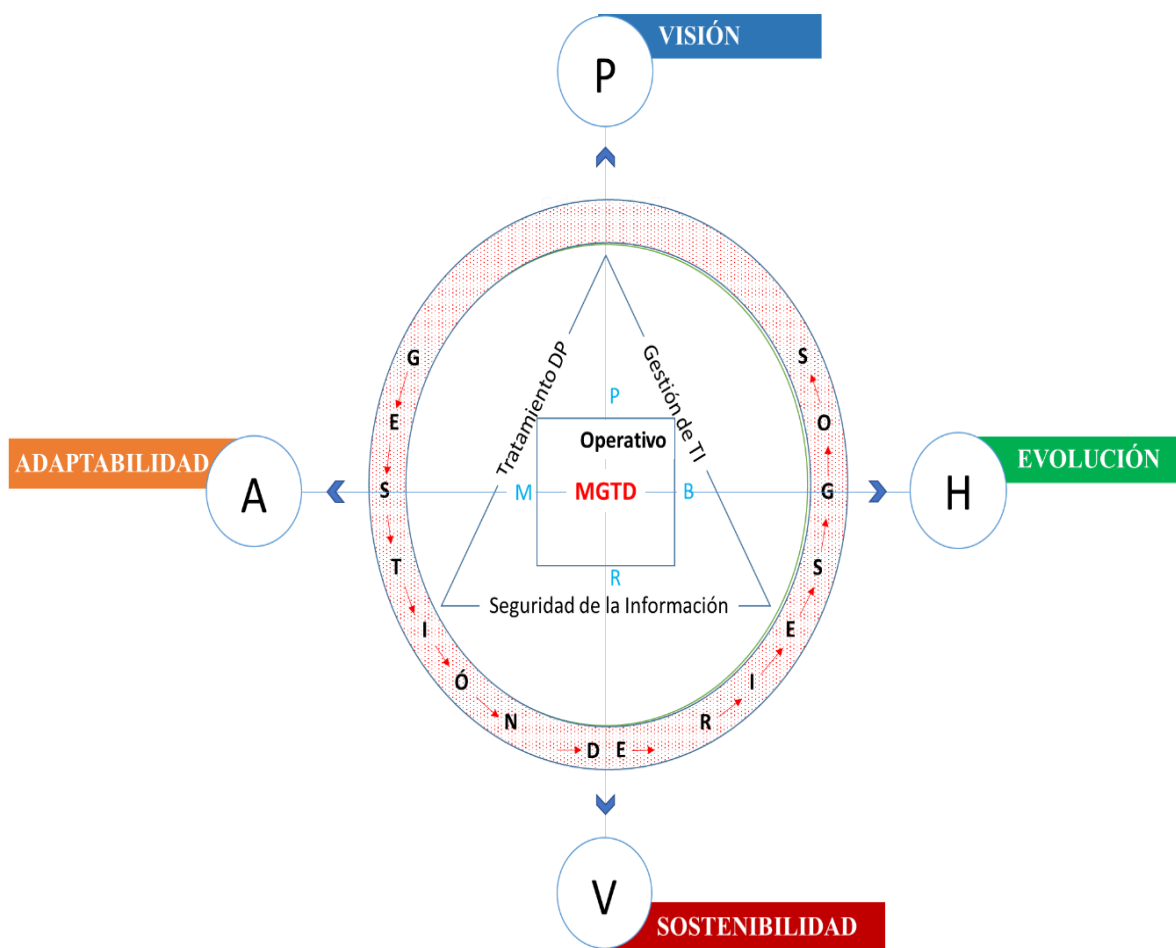


Figura 49. Elementos del Nivel Operativo.
Fuente. Autor del proyecto

MODELO DE GOBIERNO DE TRATAMIENTO DE LA INFORMACIÓN PARA LA EMPRESA COLOMBIANA

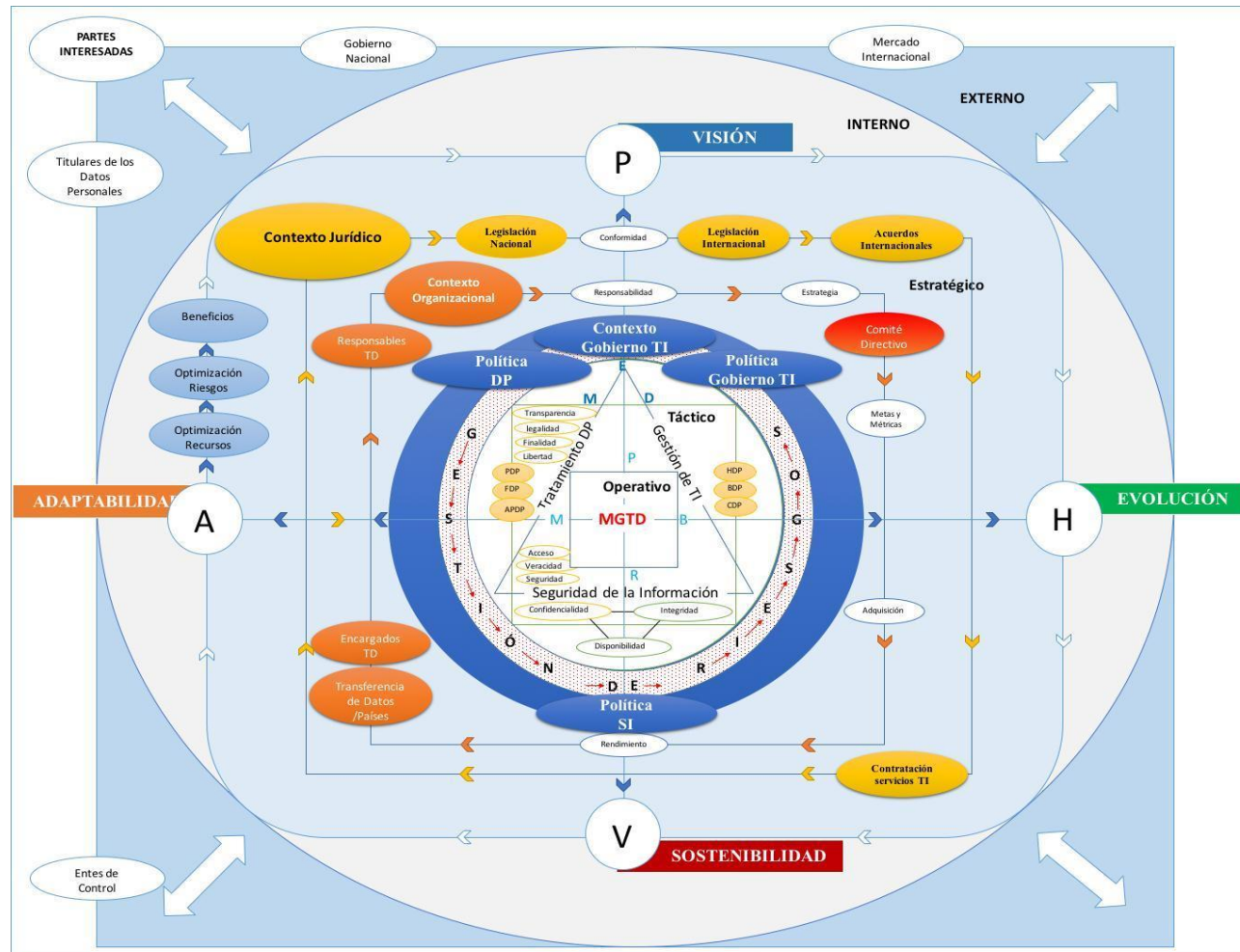


Figura 50. Modelo de gobierno de tratamiento de la información para la empresa colombiana.
 Fuente. Autor del proyecto

4.6 Analizar la factibilidad de aplicación del modelo de gobierno de tratamiento de la información para la empresa colombiana.

Operación del Modelo. El Modelo de Gobierno de Tratamiento de la Información para la Empresa Colombiana que se ha definido como una propuesta para enfrentar la globalización y como prospectiva de desarrollo organizacional establece su operación de la siguiente manera:

Entradas del modelo. Las entradas del modelo se encuentran establecidas por las partes interesadas.

Información de las partes interesadas. Las Partes Interesadas emiten información que ingresa al modelo para ser tratada conforme a los requisitos legales, normativos o propios del Titular de los Datos. Por tal motivo, dependiendo de cada parte interesada se establecen los elementos que determinan el ingreso de información al modelo:

Tabla 31 Partes Interesadas.

Parte Interesada	Requisito de Entrada al Modelo	Ley o Normativa que aplica
El Gobierno Nacional	Define el derecho a la intimidad como derecho fundamental de las personas en Colombia.	Constitución Política de Colombia (Artículo. 15).
	Habeas Data	Ley 1266 de 2008.
	Emite la Ley de Protección de Datos Personales en Colombia.	Ley 1581 de 2012.
Los Titulares de los Datos	Requiere de toda empresa	Constitución Política de

Tabla 31. Continuación

	colombiana a la cual maneje sus datos personales que se respete el derecho a la intimidad sobre su información personal.	Colombia (Artículo. 15). Ley 1581 de 2012.
El Mercado Internacional	Se definen acuerdos internacionales o tratados de libre comercio que exigen el cumplimiento de lineamientos políticos, legales, económicos, comerciales, entre otros, que requieren un adecuado tratamiento de los datos.	Acuerdos Internacionales. Tratados de Libre Comercio.
Proveedores de Servicios de TI	Define los requisitos legales a nivel contractual para demanda de servicios de TI a nivel nacional o en otros países, por el cual se realiza Transferencia de Datos.	Convenios. Contratos Empresariales.

Fuente. Autor del proyecto

Definición del inventario de la legislación colombiana de protección de datos

personales. Como elemento de apoyo a la entrada de información se define un inventario con la Legislación Colombiana relacionada con la protección de datos personales:

Tabla 32 Inventario de la Legislación Colombiana de Protección de Datos Personales.

Ref.	Fuente	Nombre Legislación	Descripción
1	Presidencia de la República de Colombia	Constitución Política de Colombia de 1991.	Artículo 15 por la cual se otorga el derecho de la intimidad de los ciudadanos.
2	Presidencia de la República de Colombia	Ley 1266 de 2008.	Ley de Habeas Data.
3	Presidencia de la República de Colombia	Ley 1581 de 2012	Ley de Protección de Datos Personales.

Fuente. Autor del proyecto

Definición del inventario de acuerdos internacionales y tratados de libre comercio. Se deben identificar todos los acuerdos internacionales y tratados de libre comercio que le aplican a la empresa colombiana con el fin de validar la aplicabilidad del tratamiento de los datos personales en caso de sostener negocios o intercambio de información a otras naciones:

Tabla 32 *Inventario de Acuerdos Internacionales y Tratados de Libre Comercio.*

Ref.	Fuente	Nombre Acuerdo / Tratado Libre Comercio	Descripción
-------------	---------------	--	--------------------

Fuente. Autor del proyecto

Definición del Inventario de contratación o outsourcing de TI. Se deben identificar todos los contratos que tiene o requiera realizar la empresa en materia de outsourcing relacionado con TI o cualquier modalidad que requiera intercambio de información a nivel nacional o internacional

Tabla 33 *Inventario de Contratación o Outsourcing de TI.*

Ref.	Contratista	Contrato No.	Descripción	Contratación Nacional o Internacional
-------------	--------------------	---------------------	--------------------	--

Fuente. Autor del proyecto

Procesamiento de la información. Una vez determinada la información de entrada relacionada con la legislación, acuerdos comerciales y contratación outsourcing de TI se procede con el procesamiento de la misma conforme a las siguientes etapas:

Etapas Preliminares:

- Recolección y análisis de la información de entrada.
- Evaluación del contexto jurídico.
- Análisis de riesgos del contexto jurídico.

Etapas de Operación (ciclo operativo):

- Planeación de tratamiento de información de datos personales en la empresa en cumplimiento de los requisitos de entrada.
- Ejecución del plan.
- Verificación del plan.
- Actuación sobre el plan.

Etapas Preliminares:

- Recolección y análisis de la información de entrada.

En esta fase se recolectan los inventarios de la diferente información o documentación de entrada. De esta manera se recolecta:

- Inventario de la Legislación Colombiana de Protección de Datos Personales.
- Definición del Inventario de Acuerdos Internacionales y Tratados de Libre Comercio.
- Definición del Inventario de Contratación o Outsourcing de TI.

Evaluación del contexto jurídico. Una vez recolectada la información de entrada se procede a realizar un análisis y evaluación exhaustiva de todo el contexto jurídico, con el fin de identificar el cumplimiento de la empresa frente a la legislación, normatividad, acuerdos comerciales o contractuales.

La evaluación se realizará utilizando la siguiente lista de chequeo:

Tabla 34 Evaluación del Contexto Jurídico.

Ref.	Legislación/ Acuerdo/ Contrato TI	Requisito	Aplica SI/NO
-------------	--	------------------	-------------------------

Fuente. Autor del proyecto

Análisis de Cumplimiento del Contexto Jurídico. El análisis del contexto jurídico se realizará conforme a la aplicación de una lista de chequeo que incorpora todos los lineamientos

jurídicos, legales, normativos, acuerdos comerciales y requisitos contractuales relacionados con el tratamiento de la información de los datos personales.

Para esto se propone la siguiente herramienta:

Tabla 35 Nivel de Cumplimiento del Contexto Jurídico.

Ref.	Legislación/Acuerdo/ Contrato TI	Requisito	Nivel de Cumplimiento 0%-100%
-------------	---	------------------	--

Fuente. Autor del proyecto

Análisis de riesgos del contexto jurídico. El análisis de riesgos sobre el contexto jurídico se realiza conforme a la metodología establecida para este modelo citada en el numeral 5.2.3.1.3 Gestión de Riesgos. Y así mismo, tomando como insumo la evaluación de cumplimiento del contexto jurídico establecida con la lista de chequeo del punto anterior. Así, de esta manera debe registrarse los niveles de riesgos que presenta la organización frente al contexto jurídico. Por tal razón, como parte de esta evaluación se propone el siguiente registro:

Tabla 36 Análisis de Riesgos del Contexto Jurídico.

Ref.	Activo	Escenario				Evaluación de Riesgos			
		Amenaza	Vulnerabilidad	Consecuencia	PO	PI	Nivel de Riesgos	Descripción	Descripción
E1	Requisito Legal						9	Crítico	Afecta la conformidad, visión, evolución, adaptabilidad y sostenibilidad

Tabla 36. Continuación

E2	Requisito Acuerdo Comercial, TLC	2-6	Moderado	de la empresa. Puede afectar la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.
...	Requisito Contractual	1	Aceptable	Afecta la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.

Fuente. Autor del proyecto

Etapa de Operación (ciclo operativo): Planeación de tratamiento de información de datos personales en la empresa en cumplimiento de los requisitos de entrada.

Tabla 37 Plan de tratamiento de la información de datos personales.

Ref.	Legislación/ Acuerdo/ <u>Contrato TI</u>	Requisito	Actividad	Responsable	Fecha inicial	Fecha Final
------	--	-----------	-----------	-------------	---------------	-------------

Fuente. Autor del proyecto

Ejecución del plan. En esta fase se debe llevar a cabo la realización de todas las actividades establecidas en la planeación del tratamiento de la información de datos personales, conforme a los riesgos identificados y al análisis de cumplimiento de toda la legislación, normatividad, acuerdos comerciales y contractuales que se establezcan en la organización. Se propone una ficha de control de actividades de ejecución:

Tabla 38 Ficha de Control de Actividades de Ejecución.

Ref.	Actividad	Responsable	Recursos Asignados	Tiempo de Ejecución	Fecha inicial	Fecha Final
-------------	------------------	--------------------	-------------------------------	------------------------------------	--------------------------	------------------------

Fuente. Autor del proyecto

Verificación del plan. En esta etapa se realizará un seguimiento periódico de la ejecución de las actividades del plan en los tiempos establecidos, con el fin de validar el cumplimiento de las mismas y determinar las estrategias oportunas para su adecuado control y realización del mismo. Para esto la empresa debe definir lo siguiente:

- Responsable del seguimiento del plan.
- Tiempo de seguimiento del plan.
- Actividades de seguimiento del plan.
- Informe de seguimiento del plan.

Se propone la siguiente herramienta de control de seguimiento y verificación:

Tabla 39 Ficha de Control de Seguimiento del Plan.

Empresa					Plan #			
Ref.	Nombre Activo	Evaluador Actividad	Responsable	Recursos Asignados	Fecha Seguimiento: Tiempo de Ejecución	Fecha inicial	Fecha Final	Estado Avance

Fuente. Autor del proyecto

Actuación sobre el plan. En esta fase se debe realizar el plan de mejora el cual permita mantener la correcta ejecución y optimización del mismo conforme al cumplimiento de los objetivos. Para esto se establecerá lo siguiente:

- Acciones de Mejora.
- Acciones Correctivas.
- Acciones Preventivas.

Se propone el siguiente formato de plan de mejora:

Tabla 40 Plan de Mejora.

Ref.	Acción	Tipo Acción	Estado	Fecha inicial	Fecha Final
A1	Acción 1	Preventiva	Reducirlo		
A2	Acción 2	Correctiva	Retenerlo		
A3	Acción 3	Mejora	Evitarlo		
...	Transferirlo		

Fuente. Autor del proyecto

4.6.1 Aplicación del modelo de gobierno de tratamiento de la información para la empresa colombiana. Para analizar la factibilidad de aplicación del modelo se eligió una empresa mixta (sector público y privado), el cual se encontró en fase de implementación de la ley 1581 de 2012 por la cual se rige la protección de datos personales en Colombia.

Operación del Modelo. La operación del Modelo para la empresa Colombia Mayor se definió considerando lo siguiente:

Entradas del Modelo. Como parte de las entradas para la empresa Colombia Mayor se definieron las partes interesadas.

Información de las Partes Interesadas. A continuación se determina la información que emiten las partes interesadas de Colombia Mayor:

Tabla 41 Partes Interesadas de Colombia Mayor.

Parte Interesada	Requisito de Entrada al Modelo	Ley o Normativa que aplica
El Gobierno Nacional <ul style="list-style-type: none"> • Presidencia de la República de Colombia. • Superintendencia de Industria y Comercio. 	Define el derecho a la intimidad como derecho fundamental de las personas en Colombia.	Constitución Política de Colombia (Artículo. 15).
	Habeas Data	Ley 1266 de 2008.
	Emite la Ley de Protección de Datos Personales en Colombia.	Ley 1581 de 2012.
Los Titulares de los Datos <ul style="list-style-type: none"> • Beneficiarios del programa de subsidio Colombia Mayor. • Beneficiarios del programa 	Derecho a la intimidad sobre su información personal.	Constitución Política de Colombia (Artículo. 15).
		Ley 1581 de 2012.

Tabla 41. Continuación

de subsidio del aporte en pensión.		
<ul style="list-style-type: none"> • Alcaldías municipales. • Centros de Atención del Adulto Mayor. • Ministerio del trabajo. • Entes de control. 		
El Mercado Internacional	Se definen acuerdos internacionales o tratados de libre comercio que exigen el cumplimiento de lineamientos políticos, legales, económicos, comerciales, entre otros, que requieren un adecuado tratamiento de los datos.	Acuerdos Internacionales. Tratados de Libre Comercio.
Proveedores de Servicios de TI	Cláusulas contractuales y ANS de seguridad y privacidad de la información.	Convenios. Contratos Empresariales.
<ul style="list-style-type: none"> • Proveedor de procesamiento de información. 	Cláusulas contractuales y ANS de servicios y productos tecnológicos.	
<ul style="list-style-type: none"> • Proveedor de servicios de redes de comunicaciones. 	Cláusulas contractuales y ANS de servicios y productos tecnológicos.	
<ul style="list-style-type: none"> • Proveedor de gestión documental. 	Convenios y ANS de servicios y productos tecnológicos.	
<ul style="list-style-type: none"> • Proveedor de pagos de subsidios. 	Convenios y ANS de servicios y productos tecnológicos.	
<ul style="list-style-type: none"> • Proveedor de bases de datos para cruces. 	Convenios y ANS de servicios y productos tecnológicos.	
<ul style="list-style-type: none"> • Proveedor de servicios de callcenter. 	Convenios y ANS de servicios y productos tecnológicos.	
<ul style="list-style-type: none"> • Proveedor de servicios de hosting. 	Convenios y ANS de servicios y productos tecnológicos.	

Fuente. Autor del proyecto

Definición del Inventario de la legislación colombiana de protección de datos

personales que aplica a Colombia mayor. A continuación se estableció la Legislación

Colombiana relacionada con la protección de datos personales que aplica a Colombia Mayor:

Tabla 42 Inventario de la Legislación Colombiana de Protección de Datos Personales para Colombia Mayor

Ref.	Fuente	Nombre Legislación	Descripción
1	Presidencia de la República de Colombia	Constitución Política de Colombia de 1991.	Artículo 15 por la cual se otorga el derecho de la intimidad de los ciudadanos.
2	Presidencia de la República de Colombia	Ley 1266 de 2008.	Ley de Habeas Data.
3	Presidencia de la República de Colombia	Ley 1581 de 2012	Ley de Protección de Datos Personales.

Fuente. Autor del proyecto

Inventario de acuerdos internacionales y tratados de libre comercio. Se definió el inventario de acuerdos internacionales y tratados de libre comercio que aplican a Colombia Mayor conforme a su contexto organizacional:

Tabla 43 Inventario de Acuerdos Internacionales y Tratados de Libre Comercio.

Ref.	Fuente	Nombre Acuerdo / Tratado Libre Comercio	Descripción
-------------	---------------	--	--------------------

Fuente. Autor del proyecto

Definición del inventario de contratación o outsourcing de TI. Se definió el inventario de contratación y outsourcing que prestan servicios a Colombia Mayor, especialmente, los enfocados a los críticos:

Tabla 44 Inventario de Contratación o Outsourcing de TI.

Ref.	Contratista	Contrato No.	Descripción	Contratación Nacional o Internacional
	Claro	XXX	Servicios de centro de cómputo principal	Nacional
	Level3	XXX	Servicios de centro de cómputo alternativo	Nacional
	Carvajal S.A.	XXX	Servicios de procesamiento de información	Nacional
	Sistemcobro	XXX	Servicios de atención al cliente.	Nacional
	Icloud	XXX	Servicios de hosting	Nacional (con impacto internacional)

Fuente. Autor del proyecto

Procesamiento de la información. El procesamiento de la información para Colombia

Mayor se determinó así:

Etapas Preliminares:

- Recolección y análisis de la información de entrada.
- Evaluación del contexto jurídico.
- Análisis de riesgos del contexto jurídico.

Etapas de Operación (ciclo operativo):

- Planeación de tratamiento de información de datos personales en la empresa en cumplimiento de los requisitos de entrada.
- Ejecución del plan.
- Verificación del plan.
- Actuación sobre el plan.

Etapas Preliminares:

Recolección y análisis de la información de entrada. Se recolectaron los inventarios de la diferente información o documentación de entrada. De esta manera se recolectó:

- Inventario de las partes interesadas.
- Inventario de la Legislación Colombiana de Protección de Datos Personales.
- Definición del Inventario de Acuerdos Internacionales y Tratados de Libre Comercio.
- Definición del Inventario de Contratación o Outsourcing de TI.

Evaluación del contexto jurídico Colombia Mayor. La evaluación se realizó utilizando la siguiente lista de chequeo:

Tabla 45 Evaluación del Contexto Jurídico.

Ref.	Legislación/ Acuerdo/ Contrato TI	Requisito	Aplica SI/NO
	Constitución Política de Colombia de 1991.	Artículo 15.	SI
	Ley 1266 de 2008.		SI
	Ley 1581 de 2012	Todos los contemplados en la ley.	SI

Tabla 45. Continuación

Contrato de servicios de centro de cómputo principal	Cláusulas contractuales, convenios y ANS de seguridad y privacidad de la información y servicios tecnológicos.	SI
Contrato de servicios de centro de cómputo alterno	Cláusulas contractuales, convenios y ANS de seguridad y privacidad de la información y servicios tecnológicos.	SI
Contrato de servicios de procesamiento de información	Cláusulas contractuales, convenios y ANS de seguridad y privacidad de la información y servicios tecnológicos.	SI
Contrato de servicios de atención al cliente.	Cláusulas contractuales, convenios y ANS de seguridad y privacidad de la información y servicios tecnológicos.	SI
Contrato de servicios de hosting	Cláusulas contractuales, convenios y ANS de seguridad y privacidad de la información y servicios tecnológicos.	SI

Fuente. Autor del proyecto

Análisis de Cumplimiento del Contexto Jurídico Colombia Mayor. El análisis del contexto jurídico para Colombia Mayor se estableció de la siguiente manera:

Para esto se propone la siguiente herramienta:

Tabla 46 Nivel de Cumplimiento del Contexto Jurídico.

Ref.	Legislación/Acuerdo/ Contrato TI	Requisito	Nivel de Cumplimiento 0%-100%
	Constitución Política de Colombia de 1991.	Artículo 15.	100%
	Ley 1581 de 2012	Todos los contemplados en la ley.	80%

Tabla 46. Continuación

Contrato de servicios de centro de cómputo principal	Cláusulas contractuales, convenios y ANS de seguridad y privacidad de la información y servicios tecnológicos.	
Contrato de servicios de centro de cómputo alterno	Cláusulas contractuales, convenios y ANS de seguridad y privacidad de la información y servicios tecnológicos.	100%
Contrato de servicios de procesamiento de información	Cláusulas contractuales, convenios y ANS de seguridad y privacidad de la información y servicios tecnológicos.	100%
Contrato de servicios de atención al cliente.	Cláusulas contractuales, convenios y ANS de seguridad y privacidad de la información y servicios tecnológicos.	80%
Contrato de servicios de hosting	Cláusulas contractuales, convenios y ANS de seguridad y privacidad de la información y servicios tecnológicos.	100%

Fuente. Autor del proyecto

Análisis de riesgos del contexto jurídico. Se realizó el análisis de riesgos del contexto

jurídico, obteniendo lo siguiente:

Tabla 47 Análisis de Riesgos del Contexto Jurídico.

Re f.	Escenario				Evaluación de Riesgos				
	Activo	Amenaza	Vulnerabilidad	Consecuencia	P O	P I	Nivel de Riesgos	Descripción	Descripción
E1	Registro de bases de datos personales en la Superintendencia de Industria y Comercio.	Incumplimiento de la ley 1581 de 2012	Deficiencia de personal para labores de tratamiento de datos	Sanción económica	3	3	Moderado	Afecta la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.	
E2	Autorización de datos personales	Incumplimiento de la ley 1581 de 2012	No aprovisionamiento de recursos para gestionar la autorización de datos de titulares antiguos.		2	3	Moderado	Puede afectar la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.	

Tabla 47. Continuación

...	Transferencia de datos a terceros en otros países	Incumplimiento de la ley 1581 de 2012	Falla o falta de validación del cumplimiento de la ley 1581 de 2012 por parte del país donde se transfieren los datos	1	3	Moderado	Puede afectar la conformidad, visión, evolución, adaptabilidad y sostenibilidad de la empresa.
-----	---	---------------------------------------	---	---	---	-----------------	--

Fuente. Autor del proyecto

Etapas de Operación (ciclo operativo): Planeación de tratamiento de información de datos personales en la empresa en cumplimiento de los requisitos de entrada.

Tabla 48 Plan de tratamiento de la información de datos personales.

Ref.	Legislación/ Acuerdo/ Contrato TI	Requisito	Actividad	Responsable	Fecha inicial	Fecha Final
Ley 1581 de 2012	Registro de las bases de datos personales en la SIC		1. Realizar inventario de las bases de datos personales de Colombia Mayor.	Oficial de Seguridad de la Información.	01/01/2019	20/01/2019
			2. Determinar nombres y cantidad de registros de cada base de datos identificada.	Oficial de Seguridad de la Información.	21/01/2019	25/01/2019
			3. Registrar las bases de datos personales en la SIC.	Oficial de Seguridad de la Información.	26/01/2019	31/01/2019
Ley 1581 de 2012	Solicitar autorización de datos personales a titulares pendientes.		4. Realizar inventario de titulares pendientes de autorización.	Oficial de Seguridad de la Información.	01/01/2019	15/01/2019
			5. Solicitar autorización	Oficial de Seguridad de la	16/01/2019	15/02/2019

Tabla 48. Continuación

	de datos a Información. titulares pendientes.				
6.	Almacenar evidencias de autorización de datos pendientes.	Oficial de Seguridad de la Información.	15/02/2019	28/02/2019	

Fuente. Autor del proyecto

Ejecución del plan. En esta fase se debe llevar a cabo la realización de todas las actividades establecidas en la planeación del tratamiento de la información de datos personales, conforme a los riesgos identificados y al análisis de cumplimiento de toda la legislación, normatividad, acuerdos comerciales y contractuales que se establezcan en la organización. Se propone una ficha de control de actividades de ejecución:

Tabla 49 Ficha de Control de Actividades de Ejecución.

Ref.	Actividad	Responsable	Recursos Asignados	Tiempo de Ejecución	Fecha inicial	Fecha Final
1.	Realizar inventario de las bases de datos personales de Colombia Mayor.	Oficial de seguridad de la información.	Humanos: Oficial de seguridad de la información.	21 días	01/01/2019	20/01/2019
2.	Determinar nombres y cantidad de registros de cada base de datos identificada.	Oficial de seguridad de la información	Analista de apoyo de seguridad de la información. Económicos: \$ 20.000.000	5 días	21/01/2019	25/01/2019
3.	Registrar las bases de datos personales en la SIC.	Oficial de seguridad de la información	Tecnológicos: 2 PC. Licencias de Sw. Redes de comunicaciones. Administrativos:	7 días	26/01/2019	31/01/2019

Tabla 49. Continuación

			Registros en papel. Registros electrónicos.			
4.	Realizar inventario de titulares pendientes de autorización.	Oficial de seguridad de la información		16 días	01/01/2019	15/01/2019
5.	Solicitar autorización de datos a titulares pendientes.	Oficial de seguridad de la información		15 días	16/01/2019	15/02/2019
6.	Almacenar evidencias de autorización de datos pendientes.	Oficial de seguridad de la información		14 días	15/02/2019	28/02/2019

Fuente. Autor del proyecto

Verificación del plan. Para la verificación del plan se estableció:

- Responsable del seguimiento del plan:

Oficial de Seguridad de la Información.

- Tiempo de seguimiento del plan:

2 meses

- Actividades de seguimiento del plan:

Revisión del registro de bases de datos personales.

Revisión de avance de autorización de datos personales pendientes.

- Informe de seguimiento del plan:

Informe parcial de seguimiento mes de enero.

Informe final de seguimiento total del proyecto.

Seguimiento y verificación:

Tabla 50 Ficha de Control de Seguimiento del Plan.

Empresa					Plan #			
Ref.	Nombre Activo	Actividad	Responsable	Recursos Asignados	Fecha Seguimiento: Tiempo de Ejecución	Fecha inicial	Fecha Final	Estado Avance
	Registro de bases de datos personales en la Superintendencia de Industria y Comercio.	1. Realizar inventario de las bases de datos personales de Colombia Mayor.	Oficial de Seguridad de la Información	Humanos: Oficial de seguridad de la información. Analista de apoyo de seguridad de la información. Económicos: \$ 20.000.000 Tecnológicos: 2 PC. Licencias de Sw. Redes de comunicaciones. Administrativos: Registros en papel. Registros electrónicos	21 días	01/01/2019	20/01/2019	0%
		2. Determinar nombres y cantidad de registros de cada base de datos identificada.						
		3. Registrar las bases de datos personales en la SIC.						

Fuente. Autor del proyecto

Actuación sobre el plan. En esta fase se debe realizar el plan de mejora el cual permita mantener la correcta ejecución y optimización del mismo conforme al cumplimiento de los objetivos. Para esto se establecerá lo siguiente:

- Acciones de Mejora.
- Acciones Correctivas.
- Acciones Preventivas.

Se propone el siguiente formato de plan de mejora:

Tabla 51 Plan de Mejora.

Ref.	Acción	Tipo Acción	Estado	Fecha inicial	Fecha Final
A1	Realizar registro de bases de datos personales en la SIC	Preventiva	Reducirlo	26/01/2019	31/01/2019
A2	Solicitar autorización de datos a titulares pendientes.	Correctiva	Reducirlo	16/01/2019	15/02/2019

Fuente. Autor del proyecto

5. Remembranzas de la investigación

El inadecuado tratamiento de la información en la empresa a nivel interno y externo puede conllevar a la pérdida de la imagen frente a sus clientes, ser menos adaptables, competitivas y sostenibles en el mercado, afectando la productividad y utilidades, y en efecto, el cumplimiento de sus objetivos y metas estratégicas. Por tal motivo, es indispensable establecer estrategias adecuadas de tratamiento de la información en la organización como base fundamental en cumplimiento de su misión y visión empresarial en términos empresariales y legales actuales. La empresa en razón de su existencia y prevalencia en el mercado sea local o internacional debe mantenerse vigente a toda legislación o normatividad en términos de protección de datos personales, validar su cumplimiento y establecer acuerdos claros que le permitan mantener su actividad conforme a los cambios y nuevas necesidades del mercado y en especial de la sociedad que interactúa con ella.

Es necesario que la empresa de hoy tome conciencia de la importancia que tiene el adecuado tratamiento de la información personal en cumplimiento de su misión, visión y todo el marco estratégico corporativo, de tal manera que se estructure a nivel organizacional un gobierno sobre la misma, con el fin de cumplir los requisitos legales y generar un valor agregado a su negocio, haciéndola más sólida, sostenible y competitiva en las nuevas tendencias empresariales. A nivel internacional la empresa realmente se enfrenta a nuevas normativas y tendencias, en el cual la estandarización en el tratamiento de la información entre países pretende ser el objetivo común para poder compartir, intercambiar o transferir datos, dando la responsabilidad al manejo de los mismos y haciéndolos encargados y partícipes de una responsabilidad compartida que

trasciende al cumplimiento de requisitos legales, acuerdos y buenas prácticas que deben ser adoptadas para preservar la seguridad y calidad de la información de las organizaciones.

Referencias

Agencia Española de Protección de Datos. (2005). Estándares Internacionales sobre Protección de Datos y Privacidad. Madrid.

Agencia Española de Protección de Datos. (2012). Resolución De Autorización de Transferencias Internacionales de Datos a Perú. España.

Almanza, Ricardo. (2016). Tendencias 2016 Encuesta Nacional de Seguridad Informática. *Revista Sistemas de la Asociación Colombia de Ingenieros*. Recuperado de: <http://acis.org.co/archivos/Revista/Sistemasedicion139.pdf>

Asamblea Nacional Constituyente. (1991). Constitución Política de Colombia. Colombia.

Beck, Ulrich. (1998). ¿Qué es la globalización ?. Recuperado de: https://ocw.uca.es/pluginfile.php/1496/mod_resource/content/1/beckulrichqueeslaglobalizacion.pdf

Beck, Ulrich. (1998). ¿Qué es la globalización ?. Recuperado de: https://ocw.uca.es/pluginfile.php/1496/mod_resource/content/1/beckulrichqueeslaglobalizacion.pdf

Belloch, Consuelo. (2014). Las Tecnologías de la Información y Comunicación (T.I.C.).

Recuperado de: <https://www.uv.es/~bellochc/pdf/pwtic1.pdf>

Belloch, Consuelo. (2014). Las Tecnologías de la Información y Comunicación (T.I.C.).

Recuperado de: <https://www.uv.es/~bellochc/pdf/pwtic1.pdf>

Castillo Alvarado, César Alejandro. (2015). *Una Gestión de Datos para Mejorar y Dar Soporte a la Toma De Decisiones en los Negocios* (Tesis Maestría). México.

Centro Cibernético Policial. (2017). Estadística Centro Cibernético Policial. Plataforma de atención a incidentes 24/7. Recuperado de: <https://caivirtual.policia.gov.co/>

Comisión Europea. (2010). Un enfoque global de la protección de los datos personales en la Unión Europea. Bruselas.

Congreso de la República de Colombia, (1999). Ley 527 de 1999 del Acceso y Uso de los Mensajes de Datos, del Comercio Electrónico y de las Firmas Digitales. Recuperado de: <http://es.presidencia.gov.co/normativa/leyes>

Congreso de la República de Colombia, (1999). Ley 527 de 1999 del Acceso y Uso de los Mensajes de Datos, del Comercio Electrónico y de las Firmas Digitales. Recuperado de: <http://es.presidencia.gov.co/normativa/leyes>

Congreso de la República de Colombia, (2009), Ley 1273 de 2009 Protección de la Información y de los Datos - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Recuperado de: <http://es.presidencia.gov.co/normativa/leyes>

Congreso de la República de Colombia, (2009), Ley 1273 de 2009 Protección de la Información y de los Datos - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Recuperado de: <http://es.presidencia.gov.co/normativa/leyes>

Congreso de la República de Colombia, (2017), Ley 1266 (2008) Ley del Hábeas Data y se Regula el Manejo de la Información Contendida en Bases de Datos Personales, en Especial la Financiera, Crediticia, Comercial, de Servicios y la Proveniente de Terceros Países y se dictan otras disposiciones. Recuperado de: <http://es.presidencia.gov.co/normativa/leyes>

Congreso de la República de Colombia, (2017), Ley 23 de 1982 Ley Derechos de Autor.
Recuperado de: <http://es.presidencia.gov.co/normativa/leyes>

Congreso de la República de Colombia, (2017), Ley 594 de 2000 Ley General de Archivos.
Recuperado de: <http://es.presidencia.gov.co/normativa/leyes>

Congreso de la República de Colombia. (2012). Ley 1581 de 2012 Protección de Datos Personales. Recuperado de: <http://es.presidencia.gov.co/normativa/leyes>

Congreso de la República de Colombia. (2012). Ley 1581 de 2012 Protección de Datos Personales. Recuperado de: <http://es.presidencia.gov.co/normativa/leyes>

Congreso de la República de Colombia. (2014). Ley 1712 de 2014 Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Recuperado de: <http://es.presidencia.gov.co/normativa/leyes>

Congreso de la República de Colombia. (2014). Ley 1712 de 2014 Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Recuperado de: <http://es.presidencia.gov.co/normativa/leyes>

Congreso de la República de Colombia. (2017). Leyes. Colombia. Recuperado de: <http://es.presidencia.gov.co/normativa/leyes>

Consejo Nacional de Política Económica y Social. (2009). CONPES 3582 política nacional de ciencia, tecnología e innovación. Recuperado de: <http://www.colombiacompetitiva.gov.co/sneci/Documents/conpes-3582-de-2009.pdf>

Consejo Nacional de Política Económica y Social. (2009). CONPES 3582 política nacional de ciencia, tecnología e innovación. Recuperado de: <http://www.colombiacompetitiva.gov.co/sneci/Documents/conpes-3582-de-2009.pdf>

Consejo Nacional de Política Económica y Social. (2015). CONPES 3834 Política para Estimular la Inversión Privada en Ciencia, Tecnología e Innovación a través de Deducciones Tributarias. Recuperado de: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3834.pdf>

Consejo Nacional de Política Económica y Social. (2015). CONPES 3834 Política para Estimular la Inversión Privada en Ciencia, Tecnología e Innovación a través de Deducciones Tributarias. Recuperado de: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3834.pdf>

Consejo Nacional de Política Económica y Social. (2016). CONPES 3854 política nacional de seguridad digital. Recuperado de: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

Consejo Nacional de Política Económica y Social. (2016). CONPES 3854 política nacional de seguridad digital. Recuperado de: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

EduTEKA. (2007). Tratamiento de la Información y Competencia Digital. Recuperado de: <http://eduteka.icesi.edu.co/pdfdir/GuiaGavilan.pdf>

EduTEKA. (2007). Tratamiento de la Información y Competencia Digital. Recuperado de: <http://eduteka.icesi.edu.co/pdfdir/GuiaGavilan.pdf>

Expansión. (2017). ¿Necesitamos una ley mundial que proteja la privacidad en la Red?. Madrid.

Recuperado de: <http://www.expansion.com/juridico/actualidad-tendencias/2017/02/01/58922b5f46163f63308b4597.html>

Gacitúa Espósito, Alejandro Luis. El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea (En busca del equilibrio entre la libertad y la seguridad). 2014.

Glaser, B. G., & Strauss, A. L. (2017). *Discovery of grounded theory: Strategies for qualitative research*. Routledge.

Gobierno de España. (1999). Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Gobierno de España. (1999). Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Infométrika. (2014). Estudio de Cultura de la seguridad de la información, garantía de protección en el Estado. Recuperado de <http://www.mintic.gov.co/portal/604/w3-article-7368.html>

Institute of Electrical and Electronics Engineers (IEEE). (2014). La Ciberseguridad en la Unión Europea. Artículo. Recuperado de:

http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO77bis-2014_CiberseguridadProteccionInformacion_H.Wegener.pdf

Institute of Electrical and Electronics Engineers (IEEE). (2014). La Ciberseguridad en la Unión Europea. Artículo. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO77bis-2014_CiberseguridadProteccionInformacion_H.Wegener.pdf

Instituto Colombiano de Normas Técnicas y Certificación. (2007). Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información. Bogotá D.C.: ICONTEC. NTC ISO/IEC 27002.

Instituto Colombiano de Normas Técnicas y Certificación. (2007). Tecnología de la Información. Implementación de un Sistema de Gestión de la Seguridad de la Información Bogotá D.C.: ICONTEC, 2007. NTC ISO/IEC 27003.

Instituto Colombiano de Normas Técnicas y Certificación. (2009). Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información. Bogotá D.C.: ICONTEC. NTC ISO/IEC 27005.

Instituto Colombiano de Normas Técnicas y Certificación. (2009). Gobierno Corporativo de la Tecnología de la Información. Bogotá D.C.: ICONTEC. NTC ISO 38500.

Instituto Colombiano de Normas Técnicas y Certificación. (2011). Gestión del Riesgo – Principios y Directrices. Bogotá D.C.: ICONTEC. NTC ISO 31000.

Instituto Colombiano de Normas Técnicas y Certificación. (2013). Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI). Bogotá D.C.: ICONTEC. NTC ISO/IEC 27001.

LA CIBERSEGURIDAD EN LA UNIÓN EUROPEA. Artículo. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEE077bis-2014_CiberseguridadProteccionInformacion_H.Wegener.pdf IEEE. 2014.

Lepage Hoces, Diana Estefanía. Diseño de un modelo de gobierno de TI con enfoque de seguridad de información para empresas prestadoras de servicios de salud bajo la óptica de Cobit 5.0. 2014.

Ministerio de Comercio de Industria y Turismo. (2017). Publicación Inversiones en ciencia y tecnología son insuficientes para competir en el TLC: Colciencias. Recuperado de: http://www.tlc.gov.co/publicaciones/12698/inversiones_en_ciencia_y_tecnologia_son_insuficientes_para_competir_en_el_tlc_colciencias

Ministerio de Comercio de Industria y Turismo. (2017). Publicación Inversiones en ciencia y tecnología son insuficientes para competir en el TLC: Colciencias. Recuperado de: http://www.tlc.gov.co/publicaciones/12698/inversiones_en_ciencia_y_tecnologia_son_insuficientes_para_competir_en_el_tlc_colciencias

OEA. Protección de datos Personales. Desarrollos normativos por país. Recuperado de:

http://www.oas.org/es/sla/ddi/proteccion_datos_personales_dn.asp

Organización de los Estados Americanos (OEA). (2013). Asamblea General Acceso a la Información Pública y Protección de Datos Personales. Guatemala.

Organización de los Estados Americanos (OEA). (2017). Comentarios y Guía de Implementación para la Ley Modelo Interamericana sobre Acceso a la Información. Recuperado de: http://www.oas.org/es/sla/ddi/docs/AG-RES_2841_XL-O-10_esp.pdf

Organización de los Estados Americanos (OEA). (2017). Comentarios y Guía de Implementación para la Ley Modelo Interamericana sobre Acceso a la Información. Disponible en: http://www.oas.org/es/sla/ddi/docs/AG-RES_2841_XL-O-10_esp.pdf

Organización de los Estados Americanos (OEA). (2017). Ley Modelo Interamericana sobre Protección de Datos Personales (en elaboración). Estados Unidos.

Organización de los Estados Americanos (OEA). (2017). Ley Modelo Interamericana sobre Acceso a la Información Pública. Recuperado de: http://www.oas.org/es/sla/ddi/docs/AG-RES_2607_XL-O-10_esp.pdf

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA). (2017). Ley Modelo Interamericana sobre Protección de Datos Personales (en elaboración). Estados Unidos.

Policía Nacional. Informe: Amenazas del Cibercrimen en Colombia 2016-2017. Recuperado de:

https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Real Academia Española (RAE) (2017). Diccionario de la Lengua Española. Disponible en:

<http://dle.rae.es/?id=LXrOqrN>

Recuperado de: <http://www.sic.gov.co/noticias/por-violaciones-de-datos-personales-superindustria-ha-impuesto-sanciones-por-mas-de-21-mil-millones-de-pesos>

Red Iberoamericana de Protección de Datos. (2017). Estándares de Protección de Datos Personales para los Estados Iberoamericanos. Recuperado de: http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf

Red iberoamericana de protección de datos. (2017). Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

Remolina Angarita, Nelson. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 *International Law*, *Revista Colombiana de Derecho Internacional*, 489-52.

Remolina, Nelson. (2012). Aproximación Constitucional de la Protección de Datos en Latinoamérica. Red Académica Internacional de Protección de Datos Personales - *Revista Internacional de Protección de Datos Personales*. Bogotá.

Rincón Flórez, Carolina. (2016). *Diseño de un framework para el gobierno de información con base en COBIT* (Tesis Maestría). Universidad Nacional de Colombia. Medellín.

Rincón Flórez, Carolina. (2016). *Diseño de un framework para el gobierno de información con base en COBIT* (Tesis Maestría). Universidad Nacional de Colombia. Medellín.

Rincón Flórez, Carolina. (2016). *Diseño de un framework para el gobierno de información con base en COBIT* (Tesis Maestría). Universidad Nacional de Colombia. Medellín.

Ruiz, José Ignacio. (2012). Metodología de la Investigación Cualitativa. Recuperado de <https://books.google.es/books?hl=es&lr=&id=WdaAt6ogAykC&oi=fnd&pg=PA9&dq=investigacion+positivista&ots=sGp6aCzdLT&sig=9J8mSeBV82mz4zssT3keATwXEyo#v=onepage&q=metodo%20cualitativo%20positivista&f=false>

Silva, Alicia. (2008). La Globalización Cultural y las Tecnologías de Información Comunicación en la Cibersociedad. *Revista Razón y Palabra*. Recuperado de: <http://www.redalyc.org/pdf/1995/199520727016.pdf>

Silva, Alicia. (2008). La Globalización Cultural y las Tecnologías de Información Comunicación en la Cibersociedad. *Revista Razón y Palabra*. Recuperado de: <http://www.redalyc.org/pdf/1995/199520727016.pdf>

Strauss y Corbin. (1998). Bases de la investigación cualitativa. Técnicas y procedimientos para desarrollar la teoría fundamentada. Recuperado de: https://s3.amazonaws.com/academia.edu.documents/38537364/Teoria_Fundamentada.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1525729014&Signature=UqLKI2c3hwr5LXOBSoxRiJQrUHI%3D&response-content-disposition=inline%3B%20filename%3DTeoria_Fundamentada.pdf

Strauss y Corbin. (1998). Bases de la investigación cualitativa. Técnicas y procedimientos para desarrollar la teoría fundamentada. Recuperado de: https://s3.amazonaws.com/academia.edu.documents/38537364/Teoria_Fundamentada.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1525729014&Signature=UqLKI2c3hwr5LXOBSoxRiJQrUHI%3D&response-content-disposition=inline%3B%20filename%3DTeoria_Fundamentada.pdf

Superintendencia de Industria y Comercio. (2017). Circular Externa No. 05 del 10 de agosto de 2017 -Adicionar un Capítulo Tercero [Transferencia de datos personales a terceros países] al Título V de la Circular Únicall. Colombia.

Superintendencia de Industria y Comercio. (2017). Por violaciones de datos personales, Superindustria ha impuesto sanciones por más de \$21 mil millones de pesos.

Superintendencia de Industria y Comercio. (2017). Tratados de Libre Comercio Colombia.

Superintendencia de industria y comercio. (2017). Tratados de Libre Comercio Colombia.

Superintendencia de Industria y Comercio. (2018). Protección de Datos Personales. Normativa.

Recuperado de: <http://www.sic.gov.co/>

Systems Audit and Control Association (ISACA). (2015). Presentación Gobierno de Datos.

Montevideo.

Recuperado

de:

<https://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2015/CIGRAS-2015.09.09-03-Gobierno%20de%20datos-Gustavo%20Mesa-Hector%20Cotelo.pdf>

Torsten Priebe , Stefan Markus, Business information modeling: A methodology for data-intensive projects, data science and big data governance, Proceedings of the 2015 IEEE International Conference on Big Data (Big Data), p.2056-2065, October 29-November 01, 2015

Valbuena Abogados. Estudio sobre la Aplicación en Colombia de las Normas sobre la Transferencia Internacional de Datos Personales. Bogotá.

Vivancos, Jordi. (2014). Tratamiento de la información y competencia digital. De la base de datos e-libro.

Vivancos, Jordi. (2014). Tratamiento de la información y competencia digital. De la base de datos e-libro.

Apéndices

Apéndice A. Matriz de Operacionalización Documental

Propósito	Conceptualización	Dimensiones	Subdimensiones
Contextualizar la legislación aplicable al tratamiento de la información de datos personales y prácticas relacionadas.	La legislación de tratamiento de datos personales es la regulación o normativa que emiten los países para protegerlos y tratarlos adecuadamente con el fin de dar garantías a sus titulares de la preservación de sus derechos fundamentales sobre sus datos.	Legal	Nacional
			Internacional
		Tecnológico	Normativo de Tecnologías de Información.
		Política	Relaciones internacionales
		Organizacional	Gobierno de Tratamiento de la Información Cumplimiento
		Social	Vulneración de los derechos fundamentales
Económico	Sanciones económicas		

Fuente. Adaptación de la Universidad Francisco de Paula Santander Ocaña.