RESUMEN – TRABAJO DE GRADO

AUTORES	JESÚS ANDRÉS OVALLOS OVALLOS
FACULTAD	DE INGENIERÍAS
PLAN DE ESTUDIOS	MAESTRIA EN GOBIERNO DE TI
DIRECTOR	VIVIANA ANDREA LÓPEZ BALLESTEROS
TÍTULO DE LA TESIS	METODOLOGÍA DE GESTIÓN DE CONTROLES PARA LA PRIVACIDAD DE LA INFORMACIÓN, BASADA EN LA NORMATIVA LEGAL COLOMBIANA

RESUMEN
(70 palabras aproximadamente)

LA FINALIDAD DEL PRESENTE TRABAJO DE INVESTIGACIÓN ES DISEÑAR UNA METODOLOGÍA QUE FACILITE A LAS ENTIDADES PÚBLICO-PRIVADAS CUMPLIR CON LA LEGISLACIÓN COLOMBIANA EXISTENTE REFERENTE A LA PROTECCIÓN DE DATOS PERSONALES Y A LA SEGURIDAD DE LA INFORMACIÓN, MEDIANTE LA IMPLEMENTACIÓN DE CONTROLES. SE INICIA CON LA VALIDACIÓN DE LOS REFERENTES TEÓRICOS, ENTENDIDOS CÓMO ESTÁNDARES O BUENAS PRÁCTICAS, SE ANALIZA EL COMPENDIO LEGAL COLOMBIANO RELACIONADO CON LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN,

CARACTERÍSTICAS

PÁGINAS: 127	PLANOS: 0	ILUSTRACIONES: 127	CD-ROM:1

METODOLOGÍA DE GESTIÓN DE CONTROLES PARA LA PRIVACIDAD DE LA INFORMACIÓN, BASADA EN LA NORMATIVA LEGAL COLOMBIANA

AUTOR

JESÚS ANDRÉS OVALLOS OVALLOS

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

Director

VIVIANA ANDREA LÓPEZ BALLESTEROS

Magister

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

MAESTRIA EN GOBIERNO DE TECNOLOGÍA DE LA INFORMACIÓN

Ocaña, Colombia **Febrero, 2020**

Índice

Lista de tablas

Lista de figuras

Introducción

La finalidad del presente trabajo de investigación es diseñar una metodología que facilite a las entidades público-privadas cumplir con la legislación colombiana existente referente a la protección de datos personales y a la seguridad de la información, mediante la implementación de controles. Se inicia con la validación de los referentes teóricos, entendidos cómo estándares o buenas prácticas, se analiza el compendio legal colombiano relacionado con la seguridad y privacidad de la información, obteniendo el esquema temático a cumplir posteriormente con la definición y aplicación del compendio de controles de seguridad.

En el primer capítulo se presenta el problema, los objetivos, la justificación y las delimitaciones. En el segundo capítulo se muestra el marco referencial que incluye el marco histórico con sus antecedentes, el marco conceptual, el marco contextual, el marco teórico y legal. En el tercer capítulo se describe la metodología empleada, las técnicas de recolección de información, de validación y análisis de datos. En el último capítulo se incluye la información referente a la administración del proyecto con los recursos humanos, financieros, institucionales y el cronograma de actividades.

Capítulo 1. Metodología de gestión de controles para la privacidad de la información, basada en la normativa legal colombiana

1.1 Planteamiento del problema

Las organizaciones se interesan cada vez más por su información, salvaguardarla se ha vuelto un objetivo de negocio, "La seguridad de la información está relacionada con la información en sí misma, como activo estratégico de la organización" posee elementos característicos, estos son; la integridad, la confidencialidad y la disponibilidad, "La tríada de la CIA nos da un modelo por el cual podemos pensar y discutir los conceptos de seguridad, y tiende a estar muy centrado en la seguridad, en lo que se refiere a los datos." (Andress, 2011). La gestión de la Seguridad de la Información (SI) se realiza por medio de controles, su fin es evitar que se concreten riesgos asociados al contexto de la información de negocio de las organizaciones. "Los controles de seguridad de la información tienen un impacto en los procesos organizacionales, la tecnología y la manera en que los empleados procesan la información."(Da Veiga & Martins, 2015).

La Ley 1581 de 2012 (Congreso de la República de Colombia, 2012), desarrolla el derecho constitucional que tienen sus ciudadanos para, conocer, actualizar y rectificar las informaciones que se hayan recolectado sobre ellas en bases de datos o archivos, además delega el control a la superintendencia de industria y comercio como ente de vigilancia. "La Superintendencia de Industria y Comercio ha impuesto desde el año 2010, un total de 619 multas por un valor

superior a los $21.000 millones de pesos, en ejercicio de sus funciones de inspección, vigilancia y control del régimen de protección de datos personales". (SIC, 2017).

A lo largo de los últimos años, las organizaciones han venido experimentado numerosas pérdidas que han impactado negativamente en su información y en la privacidad de los datos. La OEA y Symantec manifiestan que el número de vulnerabilidades a 2013 fue de 6787, en comparación con las 5291 vulnerabilidades detectadas en el año 2012 (OEA & Symantec, 2014). Con respecto a la adopción de controles y estándares en seguridad informática y cibernética por parte de las organizaciones, la encuesta realizada por la OEA y Trend Micro en el año 2015, expresa que solo el 37% manifestó tener adoptado algún estándar de seguridad (Trend Micro & OEA, 2015).

El estándar ISO/IEC 27001 es un referente para conocer que organizaciones gestionan su seguridad por medio de un sistema de gestión de seguridad de la información- SGSI, esta vincula a la ISO/IEC 27002 que es un compendio de controles de seguridad; según información publicada por la Organización Internacional de Estandarización desde el año 2012 al 2016, 1448 organizaciones se han certificado en el continente americano (ISO, 2016)

Los controles de seguridad de la información son diversos y abundantes, existen variedad de frameworks y estándares que los sugieren. "A pesar de la gran cantidad de opciones para herramientas, metodologías y estándares disponibles, cuando se usa independientemente, estos no son lo suficientemente amplios para satisfacer todas las necesidades de la administración de TI" (Gehrmann, 2012). Es necesario una metodología de gestión de controles que reúna las

principales características de las normativas referentes a nivel mundial, creando un portafolio de controles de seguridad que permita en el contexto colombiano facilitar la tarea de selección para cumplir con requerimientos legales asociados al tratamiento seguro de la información.

1.2 Formulación del problema

¿Cuál metodología de selección e implementación de controles de Seguridad de la información, facilitará a las organizaciones colombianas gestionar la seguridad y privacidad de la información de manera exitosa?

1.3 Objetivos

1.3.1 Objetivo general. Diseñar una metodología de gestión de controles para la privacidad de la información, alineada en la normativa legal colombiana.

1.3.2 Objetivos específicos. Determinar los estándares y metodologías referentes a la privacidad de la información.

Analizar el esquema legal referente a las exigencias de la ley colombiana para la protección de la privacidad de la información.

Definir el compendio de controles de privacidad de la información a aplicar como línea base de protección, basados en las estructuras temáticas analizadas.

Elaborar la metodología que facilite la gestión de la privacidad de la información, alineada en la normatividad legal colombiana y validar en un caso práctico.

1.4 Justificación

La explotación de una vulnerabilidad puede ocasionar daños irreparables para las organizaciones, pérdida de credibilidad y disminución de ingresos.(Cavusoglu, Mishra, & Raghunathan, 2004). La inversión en tecnología para seguridad informática es la que presenta mayor gasto e inversión en las organizaciones, en comparación con otro tipo de tecnologías como virtualización o cloud computing (Computerworld, 2014) , por tanto y para mitigar los riegos asociados a la seguridad y privacidad de la información, es necesario desarrollar e implementar estrategias de seguridad de manera eficiente y efectiva (Ernest Chang & Lin, 2007)

El decreto 1078 de 2015 “Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones” (Ministerio de Tecnologías de la Información y Comunicación, 2015), establece el cumplimiento de actividades de seguridad y privacidad de la información, estas incluidas en el modelo de gobierno en línea, a partir del año 2015 al 2020, involucrando al sector de TI en Colombia. “El desarrollo de una economía digital sólida y segura es primordial para el país, ya que esta contribuye positivamente a la prosperidad económica y social del mismo” (Departamento Nacional de Planeación, 2016).

Esta metodología pretende abordar componentes pedagógicos, que faciliten el entendimiento y la implementación de controles para fortalecer la seguridad y privacidad de la

información de organizaciones públicas y privadas regidas por la normatividad colombiana a través leyes y decretos.

1.5 Delimitaciones

1.5.1 Delimitación geográfica. Al ser el diseño de una metodología con fines de implementación y teniendo en cuenta que la temática está basada en la normativa legal colombiana el proyecto se delimita al sector público y privado de Colombia.

1.5.2 Delimitación temporal. La ejecución de las actividades necesarias para el desarrollo de la presente propuesta tendrá una duración estimada de 12 meses.

1.5.3 Delimitación conceptual. Para la realización del proyecto de investigación se tendrá en cuenta la Familia ISO/IEC 27000 (en especial ISO 27002:2015) descripción de controles de seguridad, la publicación NIST 800-53 Rev4 (actualización), el Marco para la mejora de la ciberseguridad de la infraestructura crítica del NIST (framework-for-improving-critical-infrastructure-cybersecurity-core), ITIL V3, la normativa PCI-DSS, estándar de seguridad de datos de la industria de tarjetas de pago en su versión 3.2, legislación colombiana asociada a la seguridad y privacidad de la información (Ley 1581 de 2012 para la protección de datos personales, su decreto reglamentario 1377 de 2013, el Conpes 3854 de 2016 que establece la política nacional de seguridad digital, el decreto 1078 de 2017 decreto único reglamentario de las tecnologías de la información y las comunicaciones).

1.5.4 Delimitación operativa. Para realizar una metodología de selección de controles que permita tener una línea de ruta de la implementación de contramedidas informáticas en las organizaciones, se hace necesario estudiar los referentes en este tema a nivel nacional e internacional para ello se hace referencia a la delimitación conceptual antes comentada.

Posteriormente se seleccionarán estándares que sirvan como referente principal, esto con el fin de buscar alinear la nueva metodología a estándares reconocidos y aceptados nacional e internacionalmente, se seleccionaran los objetivos estratégicos comunes a las organizaciones colombianas del sector público privado basado en la legislación referente al tema y se propondrá una línea base de controles para cumplir con los objetivos trazados y así pasar a diseñar una metodología para la gestión de estos.

Capítulo 2. Marco referencial

2.1 Marco histórico

Antecedentes. Mucho se habla en seguridad de la información sobre el rol positivo o negativo que juega el aspecto humano, en un entorno organizacional los empleados actuales y anteriores siguen siendo considerados como una de las causas principales de incidentes de seguridad de la información (Da Veiga & Martins, 2015). Estos autores propusieron una investigación de tipo cuantitativa, donde a través de la aplicación de un cuestionario ISCA "evaluación de cultura de seguridad de la información" a empleados de una organización, obtenían deficiencias o fortalezas en ocho dimensiones de seguridad de la información definidas previamente.

La investigación se desarrolló durante ocho años, evaluándose la cultura de seguridad de la información en cuatro periodos, esto permitió fortalecer las dimensiones donde había deficiencias cada vez que se obtenían los resultados, puesto que se realizaban jornadas de formación, la concepción de este mecanismo era que la seguridad de la información para los empleados se convirtiera en algo habitual, articulando todo el esquema organizacional entorno a ello.

(Otero, 2015) Desarrolló una metodología para la evaluación de controles de seguridad de la información, basado en la convergencia de conceptos y teorías como la lógica difusa, conjuntos borrosos, técnica de razonamiento borroso, estas teorías permiten una evaluación más

precisa de los criterios que utilizan las metodologías tradicionales, esto con el fin de hacer una selección de controles más efectiva y exhaustiva en las organizaciones financieras.

La metodología de evaluación de controles tuvo un impacto positivo en la seguridad de la información de la organización, la implementación de un nuevo conjunto de controles resolvió con éxito los riesgos adiciones de seguridad de la información de las áreas evaluadas. El autor de igual manera concluye que en un futuro a la metodología se le pueden agregar otros factores de criterios como: regulaciones, objetivos de la organización, entre otros.

En Colombia, el ministerio de las tecnologías de la información y las comunicaciones - MinTIC, desarrolló el modelo de seguridad y privacidad de la información MSPI, este busca preservar la confidencialidad, integridad, disponibilidad y privacidad de la información, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos (MinTIC, 2015). Este modelo esta diseñado en 5 fases (Diagnóstico, implementación, evaluación de desempeño, mejora continua).

2.2 Marco conceptual

En esta sección se elabora una revisión bibliográfica de los conceptos y teorías a partir de los cuales se sustenta el proyecto.

Confidencialidad. Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. (ISO, 2017)

Disponibilidad. Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. (ISO, 2017)

Integridad. Propiedad de salvaguardar la exactitud y estado completo de los activos. (ISO, 2017)

Control. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (ISO, 2017)

Dato personal. Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Encargado del tratamiento. Persona natural o jurídica, pública o privada, que por sí mima o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Integridad. Propiedad de exactitud y completitud de la información. (ISO, 2017)

Privacidad de la información. Preservación de la información de identificación personal según disposiciones legales y normativas vigentes. AUTOR

Responsable del tratamiento. Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o tratamiento de los datos. LEY 1581

Gestión de riesgos. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y tratamiento de riesgos. (ISO, 2017)

Tratamiento. Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Seguridad de la información. Preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO, 2017)

2.3 Marco contextual

Este proyecto está dirigido a las organizaciones públicas de orden nacional y territorial u organizaciones privadas que funjan como proveedor de servicios y que estén cobijadas bajo la normatividad legal colombiana, para el cumplimiento de requerimientos relacionados con la seguridad y privacidad de la información, a través de la implementación de una metodología de gestión de controles de seguridad.

El estado colombiano a través de leyes y decretos establece lineamientos de obligatorio cumplimiento para la conservación de la seguridad y privacidad de la información, estos

componentes legales se implementan y regulan en programas, estrategias y/o consejos de política económica y social. Una estrategia en particular es la llamada “estrategia de gobierno en línea” donde uno de sus cuatro componentes es precisamente la gestión de la seguridad y privacidad de la información.

2.4 Marco teórico

Este trabajo de investigación tiene como fundamento teórico principal la seguridad de la información, esta se puede definir como “Preservación de la confidencialidad, integridad y disponibilidad de la información” (ISO/IEC, 2017) o “la protección de la información y sus elementos críticos, incluidos los sistemas y el hardware que use, almacene y transmita esa información”(Whitman & Mattord, 2012, p. 8). Estos autores (2012) también manifiestan que hay tres características críticas de la información que le dan valor a las organizaciones, hablan de que estas características críticas no se limitan solamente a la confidencialidad, integridad y disponibilidad, por lo tanto, se deben complementar con precisión, autenticidad y utilidad.

Leyes colombianas como la ley 1581 tratamiento de datos personales (Congreso de la república de Colombia, 2012) y la ley de la protección de la información y los datos (Congreso de la república de Colombia, 2009), crean un escenario que obliga a las instituciones públicas y privadas a cumplir con ciertos lineamientos con respecto a la seguridad y privacidad de la información, ya cada vez hay más interés por parte de las personas y las organizaciones en este tema, según Martin & Rice (2011) las “personas y las organizaciones tienen serias preocupaciones sobre la aparición del cibercrimen en nuestras comunidades.” (p. 9).

Mencionado el referente teórico, y los sustentos legales del proyecto, se hace necesario el acompañamiento de un conjunto de estándares y buenas prácticas que son base fundamental de la presente investigación. Es de gran importancia el grupo de normas de la familia ISO/IEC 27000, según ISO/IEC (2015) en su versión 27002 esta manifiesta que esta es "un documento guía para organizaciones que implementan controles de seguridad de la información comúnmente aceptados" (p. 9), por lo cual se adapta a las necesidades del proyecto para la formulación de una línea base de controles de seguridad.

Existe la necesidad de evaluar la efectividad de los controles que se implementan, "La selección de controles de seguridad y privacidad apropiados para un sistema de información es una tarea importante que puede tener implicaciones significativas en las operaciones y activos de una organización, así como en el bienestar de las personas." (Ross, 2014), lo anterior hace mención a la publicación del NIST SP 800-53 rA4.

Los estándares tienen como finalidad el facilitar el trabajo de las organizaciones y de las personas a la hora de manejar y procesar su información de forma segura, es por lo anterior que cada vez se crean más estándares con una enfoque más específico, dependiendo del tipo de industria o de información en particular, este es el caso de las organizaciones que manejan tarjetas de crédito, "Las Normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial" (Industria de Tarjetas de Credito PCI, 2016), además PCI (2016) "proporciona una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de cuentas." (p. 5)

2.5 Marco legal

A continuación, se referencia la normatividad que sustenta legalmente el desarrollo del presente proyecto.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios.

Decreto 1377 de 2013. Se reglamenta parcialmente la Ley 1581 de 2012, facilitando la implementación y el cumplimiento de la Ley 1581 de 2012, reglamentando aspectos particulares relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, además consagra políticas de tratamiento de los responsables y encargados.

Decreto 1074 de 2015. Por medio del cual se expide el Decreto único reglamentario del sector de comercio, industria y turismo, el cual tiene por objeto compilar las normas reglamentarias preexistentes que rigen el sector. Compilación de los Decretos 2364 de 2012, 333 de 2014, entre otros.

Conpes 3854 de 2016. Consejo nacional de política económica y social – Política nacional de seguridad digital.

Decreto 1078 de 2015. Por medio del cual se expide el Decreto único reglamentario del sector TIC, el cual tiene por objeto compilar las normas reglamentarias preexistentes que rigen el sector.

Ley 1712 de 2012. Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente.

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. Se reglamenta la información mínima que debe contener dicho registro, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los responsables del tratamiento.

Ley 1032 de 2006. Por la cual se modifican los artículos 257, 271, 272 y 306 del código penal (artículo 271. violación a los derechos patrimoniales de autor y derechos conexos).

Circular Externa SFC 052 de 2007. Por la cual la Superintendencia Financiera de Colombia incrementa los estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios que ofrecen a sus clientes y usuarios las entidades vigiladas por esta Entidad.

Ley 1266 de 2008. Contempla las disposiciones generales en relación al derecho de 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 disposiciones.

Decreto 1727 de 2009. 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 información.

Capítulo 3. Diseño metodológico

3.1 Tipo de investigación

Teniendo en cuenta el objeto de la presente investigación, esta se desarrolla bajo un enfoque cuantitativo, especialmente porque esta técnica se caracteriza por la búsqueda y la acumulación de datos. Las hipótesis previamente formuladas son probadas en las conclusiones despendidas del análisis de los datos acumulados, el elemento principal de este enfoque es el número, que es procesado por construcciones estadísticas. Los datos recabados deben poseer dos principios centrales: la validez y la confiabilidad, esto busca garantizarse por medio de la aplicación de técnicas, por ejemplo: las encuestas. (Ackerman & Com, 2013). “La investigación cuantitativa se ha caracterizado por recoger y analizar datos cuantitativos sobre variables.” (Guerrero, 2014).

Además de desarrollarse bajo un enfoque cuantitativo, esta investigación estará basada en un estudio descriptivo, según Ackerman & Com (2013) “los trabajos descriptivos realizan diagnósticos respecto algún tema particular”. Los estudios descriptivos buscan especificar las propiedades, los perfiles de las personas, las características, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Lo que pretenden es recolectar información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, su objetivo no es indicar cómo se relacionan éstas. (Hernández, Fernández, & Baptista, 2014)

3.2 Seguimiento metodológico del proyecto

Para el cumplimiento del objetivo general del proyecto, se detallan las actividades e indicadores en el siguiente cuadro metodológico.

Tabla 1
Modelo Metodológico

OBJETIVOS DE LA INVESTIGACIÓN	ACTIVIDADES POR OBJETIVO	INDICADOR POR ACTIVIDAD
Determinar los estándares y metodologías referentes a la privacidad de la información.	Identificar estándares referentes a seguridad y privacidad de la información.	Listado de estándares de seguridad de la información.
	Diseñar instrumento para la selección de estándares	Guion de preguntas (encuesta)
	Seleccionar los estándares con los que se va a desarrollar el proyecto.	Características principales de los estándares seleccionados.
Analizar el esquema legal referente a las exigencias de la ley colombiana para la protección de la privacidad de la información.	Analizar el contexo normativo internacional de la protección de datos.	Análisis documental y listado de regulaciones a nivel internacional.
	Identificar normas, decretos, y leyes que sean referentes para la gestión de la seguridad y privacidad de la información.	Listado de normas, decretos y leyes.
Definir el compendio de controles privacidad de la información a aplicar como línea base de protección, basados en las estructuras temáticas analizadas.	Identificar elementos que conforman el compendio.	Elementos identificados
	Diseñar el compendio de controles.	Estructura del compendio
	Documentar el compendio de controles base	Documento del compendio de controles de seguridad de la información

Tabla 1. Continuación

Elaborar la metodología que facilite la gestión de la privacidad de la información, basada en la normatividad legal colombiana y validar en un caso práctico.	Diseñar una metodología para la aplicación de los controles base	Documento que contiene la metodología diseñada
	Seleccionar la entidad donde se validará la metodología	Nombre de la entidad seleccionada
	Implementar la metodología a la entidad para la aplicación de los controles base	Informe de implementación de la metodología

Fuente. Autor del proyecto

3.3 Población

La población es el conjunto o la totalidad de unidades que se van a estudiar, es decir, por todos aquellos elementos cómo: personas, animales, objetos, sucesos, fenómenos, entre otros, que pueden conformar el ámbito de una investigación, ejemplo de poblaciones pueden ser los docentes, los alumnos, los mamíferos, los seres invertebrados, las instituciones educativas. Se hace necesario también que una población se delimite en tres componentes base; contenido, tiempo y lugar. (Niño, 2011).

El proyecto tendrá como población objeto, todas las entidades públicas o privadas que se encuentren cobijadas bajo la normativa legal colombiana para la protección de la seguridad y privacidad de la información, la metodología a desarrollar busca facilitar el cumplimiento por parte de cualquier tipo de organización el cumplimiento regulatorio establecido.

3.4 Muestra

La muestra es la porción del universo total de elementos o unidades que se van a utilizar para llevar a cabo la investigación, En otras palabras, es una parte del total de unidades potenciales de análisis que se encuentran dentro del universo, elegida de acuerdo con un criterio de selección. Según los objetivos de la investigación se puede optar por uno de los distintos tipos de muestra; muestra homogénea, muestra heterogénea, muestra representativa y muestra no representativas. (Ackerman & Com, 2013)

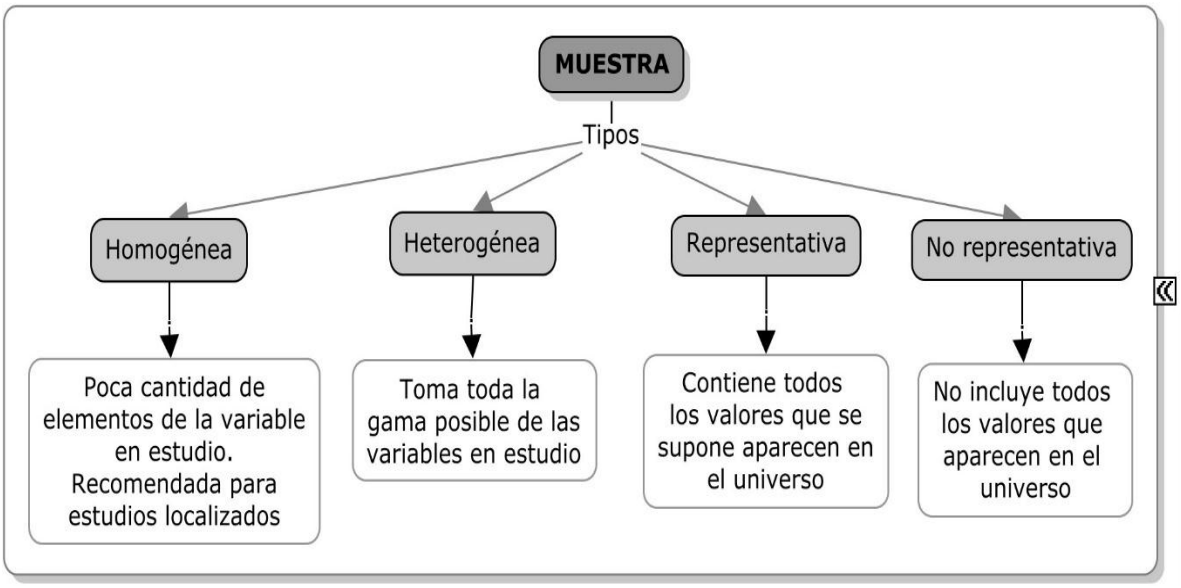


Figura 1. Tipos de muestra
Fuente. Autor del proyecto

Según lo manifiestan (Hernández et al., 2014), "La muestra es, en esencia, un subgrupo de la población. Digamos que es un subconjunto de elementos que pertenecen a ese conjunto definido en sus características al que llamamos población." Las muestras suelen clasificarse en dos grandes ramas: las muestras probabilísticas y las muestras no probabilísticas.

3.5 Técnicas de recolección de la información.

Según Lerma (2009), “Para obtener la información sobre las variables se utilizan instrumentos tales como la observación, los documentos existentes, los cuestionarios y las entrevistas, entre otros” (p. 94). Diseñada la variable, los indicadores se tienen en cuenta, y con base a ellos se formulan o diseñan preguntas, y por medio de los instrumentos mencionados anteriormente, conseguir la información correspondiente. (Lerma, 2009).

Dependiendo de los enfoques y el tipo de investigación que se desarrolle, los datos se entenderán de distinta manera. Para algunos, los datos son operadores empíricos y para otros son las propiedades de los objetos investigados. (Niño, 2011). Durante el desarrollo del proyecto se emplearán técnicas de recolección de información, para el caso del primer objetivo específico referente a determinar los estándares de seguridad de la información se aplicará una encuesta que apoyará la selección de los estándares más socializados y usados, y para el objetivo final se empleará un guion de preguntas para aplicar a un panel de expertos con el fin de validar la metodología propuesta antes de su implementación.

3.6 Análisis de la información

El análisis de la información o para otros análisis de contenido o de los datos, consiste en descomponer y examinar las partes de un todo, buscando con esto reconocer varios aspectos como: su naturaleza, las relaciones y las características, esto concluye con el regreso al todo, en otras palabras, con la síntesis, lo cual permite la obtención del conocimiento. Concluyendo, al

análisis lleva a la síntesis y la síntesis al análisis, es un proceso de ir y venir. (Niño, 2011). Alguno autores proponen que el análisis de la información debe estructurarse en un plan, así lo menciona (Lerma, 2009), el investigador en esta etapa planifica y expone las principales expresiones matemáticas con el fin de verificar las hipótesis. Estas expresiones se pueden plantear en tablas, o figuras (gráficas, croquis, esquemas y todo tipo de contenido que permita ilustrar o aclarar parte del contenido), la elaboración del plan implica hacer una revisión detallada de la relación entre las variables y los posibles resultados.

El proyecto en su primer objetivo desarrollará una lista de preguntas, orientadas en tipo encuesta, que permitirá obtener un diagnóstico de los estándares de seguridad, el análisis de estos datos estará enfocado a conocer los modelos más usados por las organizaciones, esto será aplicado a profesionales que trabajan actualmente en el área de seguridad y privacidad de la información

Capítulo 4. Resultados

4.1 Determinar los estándares y metodologías de seguridad y privacidad de la información.

Según (Whitman & Mattord, 2012) uno de los primeros documentos en hablar y dimensionar de otra forma la seguridad informática fue el Rand Report R-609, a finales de los 60's. Este amplió el concepto de la seguridad informática más allá del control de acceso físico y del hardware, abonando controles en nuevos campos como: asegurar los datos y restringir el acceso a ellos, además de involucrar a todos los actores y áreas de las organizaciones en la seguridad de la información.

En su libro, los anteriores autores también mencionan que poco tiempo después del Rand R-609 surge el proyecto MULTICS (servicio de información y computación multiplexado), quien fue el primer sistema operativo en considerar aspectos de seguridad informática en su diseño y funcionamiento.

Según comentan a mediados del año 1969, tiempo después de la reestructuración de MULTICS varios de sus desarrolladores crean el popular sistema operativo UNIX, que a diferencia de su antecesor no consideró ningún componente de seguridad, solo 10 años después el componente de seguridad más simple, la contraseña, fue agregado a su funcionamiento.

4.1.1 Identificar estándares referentes a seguridad y privacidad de la información

Tabla 2
Estándares de seguridad y privacidad de la información

NORMATIVA / ESTÁNDAR	FABRICANTE	VERSIÓN	OBSERVACIONES
ISO/IEC 27000:2018	International Organitation Standartdization (Organización internacional de estandarización	:2018	Tecnologías de la Información. Técnicas de seguridad. Sistemas de Gestión de seguridad de la información. Visión general y vocabulario.
ISO/IEC 27001:2013		:2013	Tecnologías de la Información. Técnicas de seguridad. Sistemas de Gestión de seguridad de la información. Requisitos
ISO/IEC 27002:2013		:2013	Tecnologías de la Información. Técnicas de seguridad. Sistemas de Gestión de seguridad de la información. Código de práctica para controles de seguridad de la información
ISO/IEC 38500		:2015	Gobierno corporativo de la tecnología de la información
ISO/IEC 27701		:2019	Tecnologías de la Información. Técnicas de seguridad. Código de prácticas para la protección de la información de identificación personal.
ISO/IEC 29100		:2011	Tecnologías de la información. Técnicas de seguridad. Marco de Privacidad
PCI-DSS	Pay Card Industry (Industria de tarjetas de pago)	Version 3.2.1	Estándar de Seguridad de los datos de la industria de tarjeta de pagos
ENISA Good practice for guide for incident management	European Union Agency for Cybersecurity	2010	Guía de buenas prácticas para la gestión de incidentes
ENISA Strategies for incident response and cyber crisis cooperations	European Union Agency for Cybersecurity	2016	Estrategia para la respuesta a incidentes y la cooperación en crisis cibernéticas
CREST cyber security incident response guide	CREST International	Version 1	Guía de adquisición de respuesta a incidentes de seguridad cibernética
Cyber Security body of knowledge	Cybok	Versión 2.1	Guía para el conjunto de conocimientos de ciberseguridad. Establece la estructura temática que se debe manejar a la hora sde enseñar ciberseguridad
FFIEC Information security	Federal Financial Institutions Examination	2016	Folleto de seguridad de la información. Aborda factores

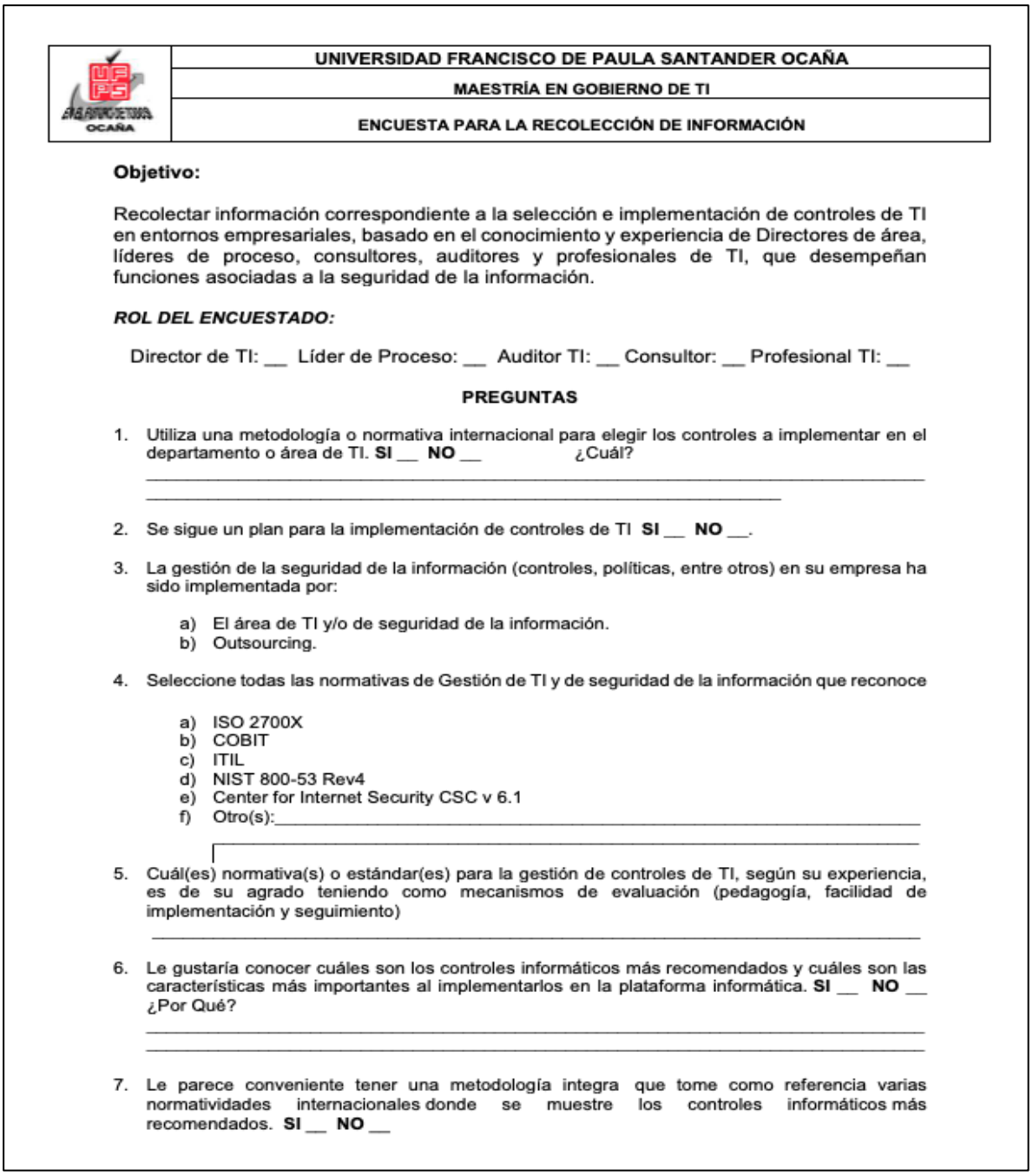
Tabla 2. Continuación

	Council's (Consejo Federal de Examen de Instituciones Financiera)		necesarios para evaluar el nivel de seguridad de sistemas de información de entidades financieras
FFIEC Cat		2017	Cibersecurity Assessment Tool (Herramienta de evaluación de la seguridad cibernética)
Cis Controls	Center for internet security (Centro de seguridad de Internet)	Version 7.1	Son un conjunto de acciones priorizadas, que constituyen mejores prácticas para mitigar ataques comunes contra sistemas y redes.
Cobit	Isaca - Systems Audit and Control Association (Asociación de Auditoría y control de Sistemas de Información)	Version 5.0	Es un marco de trabajo, para mejorar la comprensión y gestión de las tecnologiás de la información.
NIST SP 800-53	National Institute of Standars and Technology (Instituto nacional de estándares y tecnología)	A r4-2014	Evaluación de controles de seguridad y privacidad en sistemas de información y organizaciones federales
NIST Framework		Version 1.1	Marco para la mejora de la seguridad cibernética de las infraestructuras críticas.
Modelo de Seguridad y privacidad de la información (MSPI)	Ministerio de las TIC, República de Colombia	Versión 3.0.2 2016	Documento de buenas prácticas en seguridad y privacidad de la información para las entidades del estado
Modelo de tratamiento de la información para la empresa Colombiana	Maestría de Gobierno de TI Jorge Alberto Camargo	2018	Herramienta de apoyo a nivel corporativo para la empresa colombiana, diseñada como una buena práctica para el tratamiento de la información

Fuente. Autor del proyecto

4.1.2 Diseñar instrumento para la selección de estándares. El proceso de identificación de estándares o metodologías referentes al tratamiento de la seguridad y privacidad de la información, permitió seleccionar un compendio de normas o buenas prácticas internacionales, algunas bajo enfoque de formulación de controles para la seguridad de la información, otras diseñadas como marco de trabajo (framework). Esta búsqueda será correlacionada con los datos que arrojó la encuesta hecha a profesionales de seguridad de la información en Colombia, que al momento del diligenciamiento de la misma ostentaban cargos en el sector en mención tales como: Director de TI, líder de proceso, auditor, consultor o profesional de TI. Se pretende

encontrar puntos en común entre la búsqueda realizada por el autor y sus preferencias, con los resultados que arrojó la encuesta, delimitando de esta manera los conceptos y buenas prácticas a utilizar en el proyecto. El modelo de encuesta aplicado se encuentra a continuación en la imagen.



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

MAESTRÍA EN GOBIERNO DE TI

ENCUESTA PARA LA RECOLECCIÓN DE INFORMACIÓN

Objetivo:

Recolectar información correspondiente a la selección e implementación de controles de TI en entornos empresariales, basado en el conocimiento y experiencia de Directores de área, líderes de proceso, consultores, auditores y profesionales de TI, que desempeñan funciones asociadas a la seguridad de la información.

ROL DEL ENCUESTADO:

Director de TI: __ Líder de Proceso: __ Auditor TI: __ Consultor: __ Profesional TI: __

PREGUNTAS

1. Utiliza una metodología o normativa internacional para elegir los controles a implementar en el departamento o área de TI. **SI** __ **NO** __ ¿Cuál?
   _____
   _____
2. Se sigue un plan para la implementación de controles de TI **SI** __ **NO** __.
3. La gestión de la seguridad de la información (controles, políticas, entre otros) en su empresa ha sido implementada por:
   a) El área de TI y/o de seguridad de la información.
   b) Outsourcing.
4. Seleccione todas las normativas de Gestión de TI y de seguridad de la información que reconoce
   a) ISO 2700X
   b) COBIT
   c) ITIL
   d) NIST 800-53 Rev4
   e) Center for Internet Security CSC v 6.1
   f) Otro(s):_____
   _____
5. Cuál(es) normativa(s) o estándar(es) para la gestión de controles de TI, según su experiencia, es de su agrado teniendo como mecanismos de evaluación (pedagogía, facilidad de implementación y seguimiento)
   _____
6. Le gustaría conocer cuáles son los controles informáticos más recomendados y cuáles son las características más importantes al implementarlos en la plataforma informática. **SI** __ **NO** __ ¿Por Qué?
   _____
   _____
7. Le parece conveniente tener una metodología integra que tome como referencia varias normatividades internacionales donde se muestre los controles informáticos más recomendados. **SI** __ **NO** __

Figura 2. Encuesta
Fuente. Autor del proyecto

Encuestados por Rol. El siguiente gráfico presenta la relación de los encuestados según el rol que tenían asignado al momento de la encuesta.

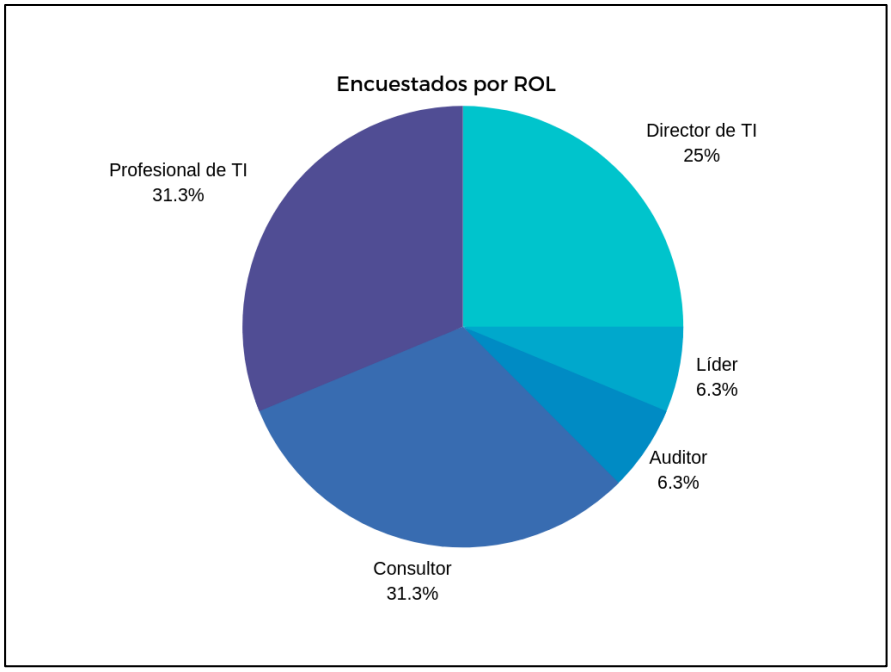


Figura 3. Encuestados según el rol
Fuente. Autor del proyecto

Interpretación. El gráfico anterior nos muestra la población muestra encuestada, estos roles corresponden a profesionales dedicados a temas de tecnología y seguridad de la información.

Primera pregunta. ¿Utiliza una metodología o normativa internacional para elegir los controles a implementar en el departamento o área de TI?, Si o no ¿Cuál?

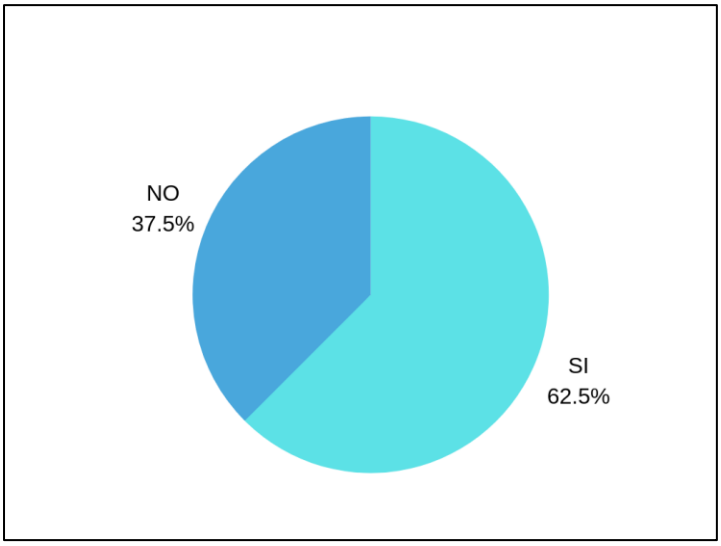


Figura 4. Metodología o normativa internacional
Fuente. Autor del proyecto

Interpretación. Más de 6 de cada 10 profesionales, reconocieron que en sus áreas de tecnología utilizan alguna normativa para elegir controles de seguridad.

Segunda pregunta. ¿Se sigue un plan para la implementación de controles de TI? Si, No

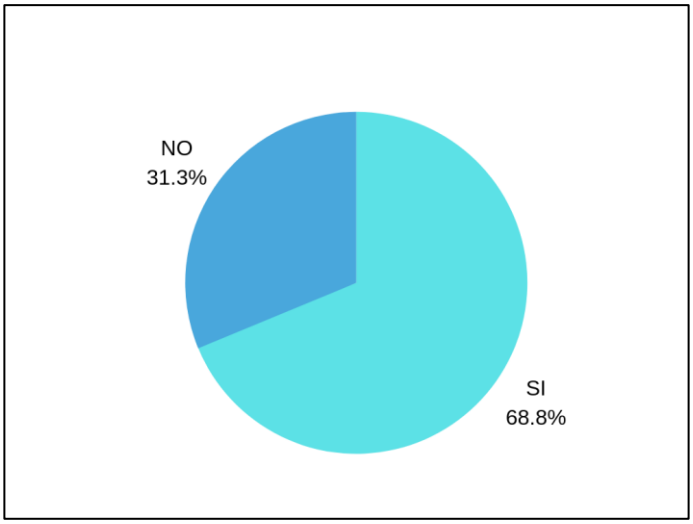


Figura 5. $implementación de controles
Fuente. Autor del proyecto

Interpretación. Tres de cada diez encuestados, manifiesta que no sigue algún plan para la implementación de controles de TI.

Tercera pregunta. La gestión de la seguridad de la información (controles, políticas, entre otros) en su empresa ha sido implementada por:

El área de TI y/o seguridad de la información.

Outsourcing

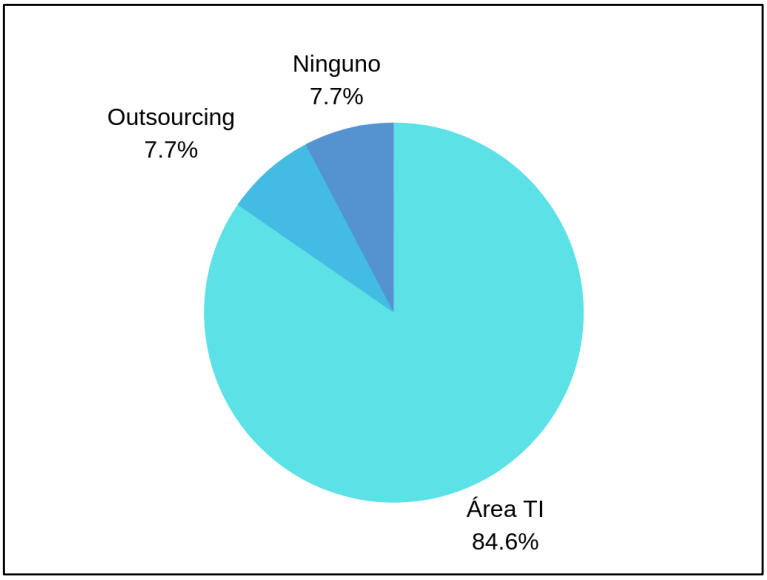


Figura 6. Gestión de la seguridad de la información
Fuente. Autor del proyecto

Interpretación. La anterior pregunta, arroja que solo el 7.7% de los encuestados gestiona su seguridad de la información a través de la contratación de un tercero, un 88.6% gestiona su propia seguridad y un 7.7% no gestiona su información bajo estándares de seguridad.

Cuarta pregunta. Seleccione todas las normativas de Gestión de TI y de seguridad de la información que reconoce

ISO 2700X

COBIT

ITIL

NIST 800-53 Rev4

Center for Internet Security CSC v 6.1

Otra

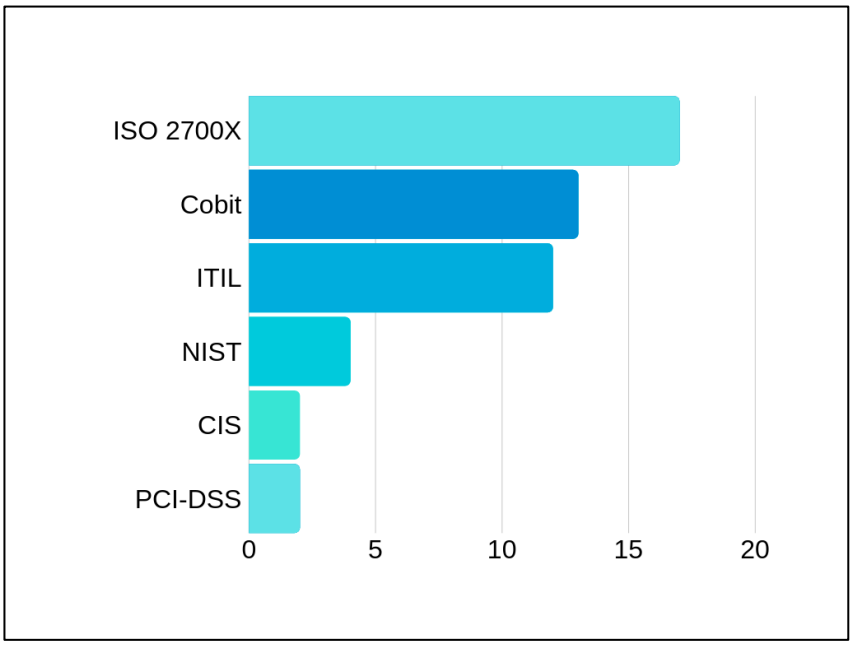


Figura 7. Normativas de Gestión de TI
Fuente. Autor del proyecto

Interpretación. La anterior pregunta, permite concluir que el estándar para la gestión de seguridad de la información más conocido, es la ISO/IEC 27000, a demás permitió incluir en el listado una norma no formulada de manera expresa en la pregunta, esta fue PCI-DSS, que es el estándar de seguridad de los datos, creado por la industria de tarjetas de pago.

Quinta pregunta. ¿Cuál(es) normativa(s) o estándar(es) para la gestión de controles de TI, según su experiencia, es de su agrado teniendo como mecanismos de evaluación (pedagogía, facilidad de implementación y seguimiento)

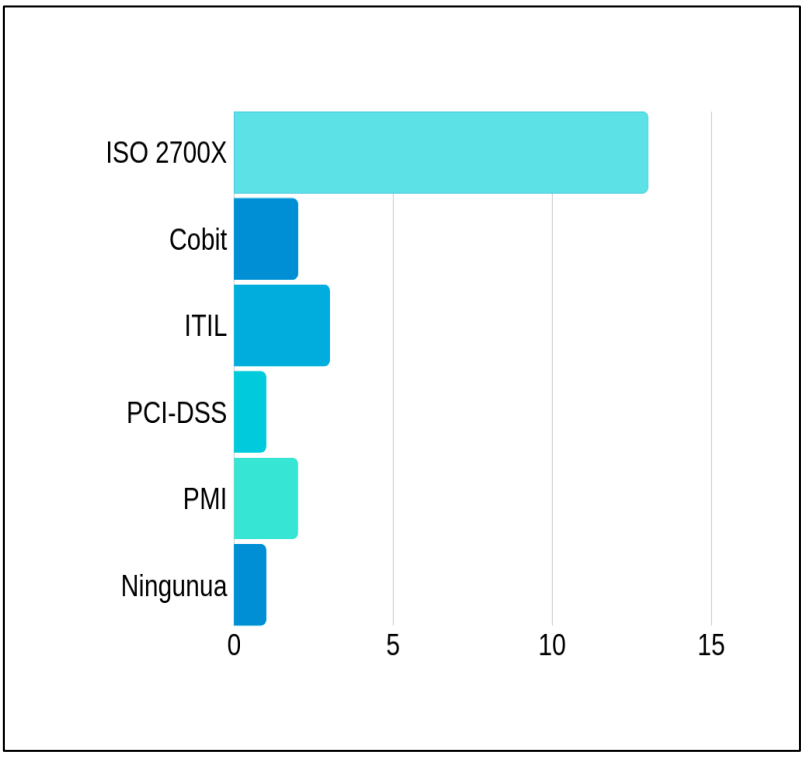


Figura 8. Normativa para la gestión de controles de TI
Fuente. Autor del proyecto

Interpretación. La pregunta anterior busca identificar cuál de los estándares o buenas prácticas es de más fácil manejo e interpretación; obteniendo el mejor resultado la norma ISO/IEC 27000, seguido de la biblioteca de infraestructura de tecnologías de la información, más conocido como ITIL.

Sexta pregunta. ¿Le gustaría conocer cuáles son los controles informáticos más recomendados y cuáles son las características más importantes al implementarlos en la plataforma informática? SI __ NO __ ¿Por Qué?

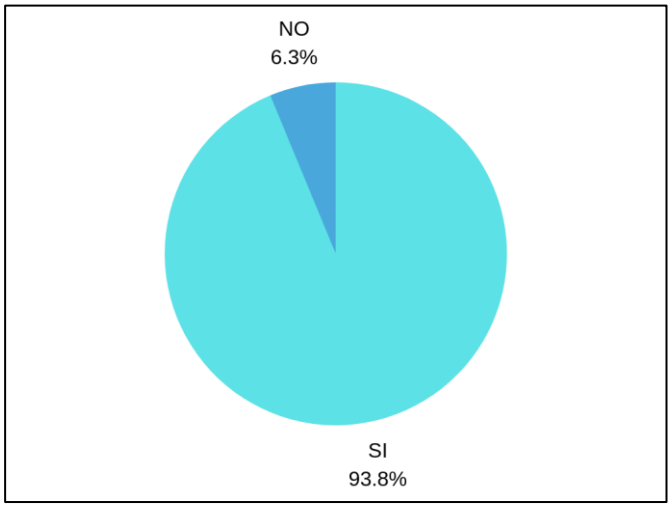


Figura 9. Controles informáticos
Fuente. Autor del proyecto

Interpretación. Aproximadamente un 94% de los encuestados, en esta pregunta manifiesta temer intención de conocer cuáles son los controles más utilizados en la gestión de la seguridad de la información.

Séptima pregunta. ¿Le parece conveniente tener una metodología integra que tome como referencia varias normatividades internacionales donde se muestre los controles informáticos más recomendados? SI __ NO __

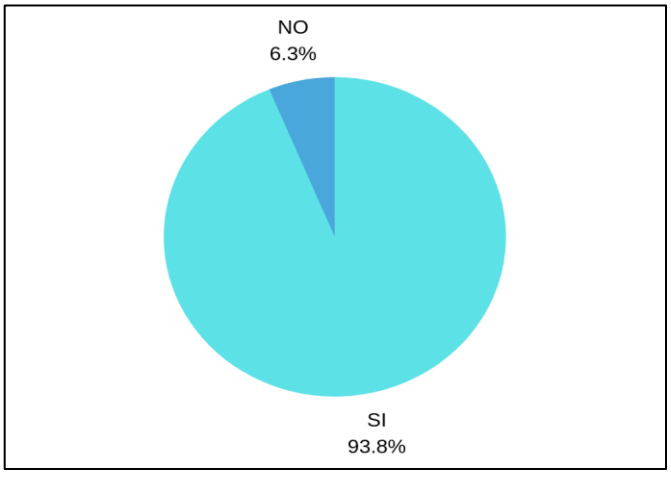


Figura 10. Metodología integra
Fuente. Autor del proyecto

Interpretación. Solo un 6.3% de los encuestados manifiesta que no le interesa una metodología que tome los estándares o normativas más importantes y formule un compendio de controles recomendados.

4.1.3 Seleccionar los estándares con los que se va a desarrollar el proyecto.

Familia ISO/IEC 27000. La familia ISO/IEC 27001 es un marco de buenas prácticas para la implementación de sistemas de gestión de seguridad de la información SGSI, desarrollado por el organismo internacional de estandarización, por sus siglas en inglés ISO. La familia 27000 divide su estructura en 4 secciones para facilitar su entendimiento y aplicación de la siguiente manera: a.) descripción general del estándar y terminología, b.) normas que especifican requisitos, c.) normas que especifican pautas o guías generales y d.) normas que describen pautas o guías para sectores específicos.

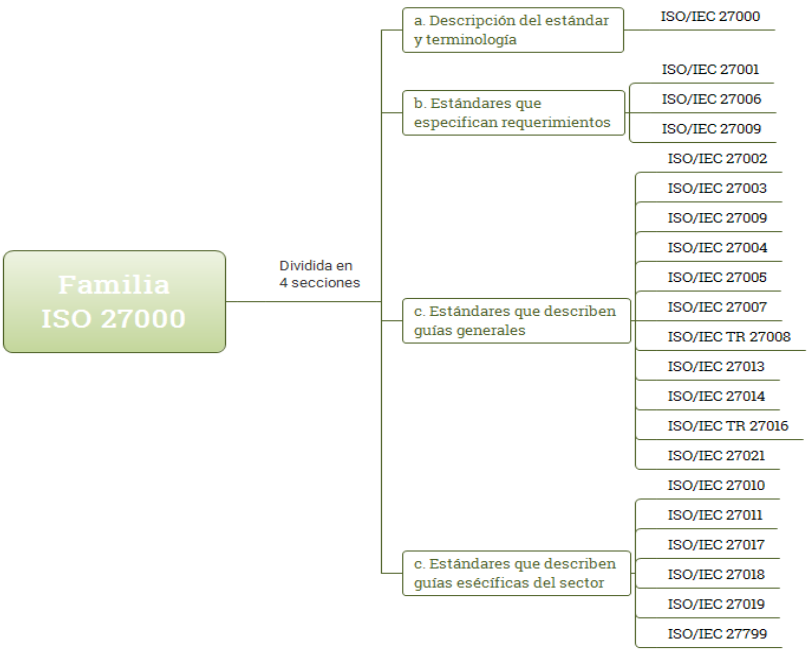


Figura 11. Estructura de la familia de norma ISO 27000
Fuente. Autor del proyecto

Origen. Su inicio se remonta al año 1995, cuando la empresa normalizadora británica BSI (British standard institution) lanza la norma BS 7799-1, con el objetivo de brindar a las empresas un entorno de buenas prácticas para el manejo de la seguridad de la información, sin embargo, no tenía un enfoque de certificación. En el año 2000, ISO como organismo internacional de estandarización toma la BS 7799-1 y la convierte en la ISO 17799, solo es hasta el año 2005 que se publica la primera versión de la norma ISO 27001:2005.

Descripción. Como se observa en el gráfico anterior, el estándar ISO 27000 está conformado por una familia de normas que se enlazan y se complementan entre sí, sin embargo, las que son de relevancia para el proyecto de investigación es la norma ISO/IEC 27001:2013 y la ISO/IEC 27002. La primer norma es orientada a la certificación de cumplimiento, las organizaciones interesadas en cumplir con los lineamientos establecidos, pueden someterse a un proceso de verificación de requerimientos mínimos y recibir por parte de un ente certificador la credencial que los acredita como certificados en la norma, y la segunda nos brinda un código o conjunto de prácticas o controles de seguridad de la información de manera detallada, ya que estos se encuentran mencionados en el anexo A de la ISO/IEC 27001 pero sin mayor desglose.

Estructura. La norma ISO/IEC 27001, actualmente se encuentra en su versión 2013, sucesora de la versión 2005. En esta última versión, la norma se apaga a la estructura y lineamientos establecidos por ISO en sus directivas en 2014, conocida como estructura de alto nivel o “Anexo SL”.

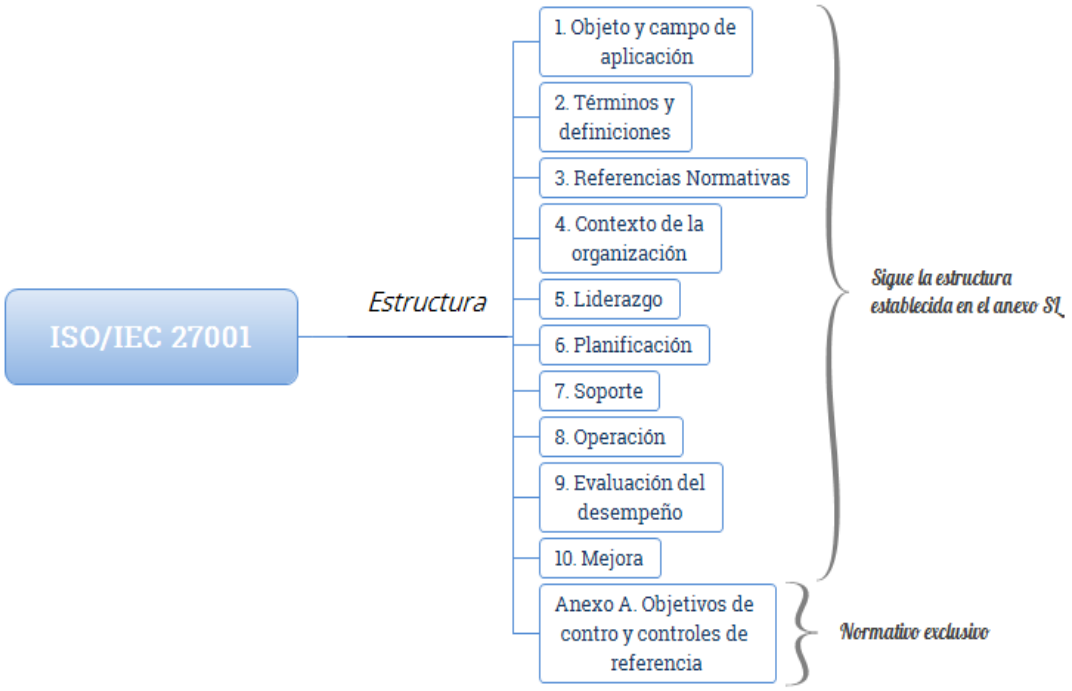


Figura 12. Estructura norma ISO/IEC 27001:2013
Fuente. Autor del proyecto

La norma ISO/IEC 27002:2013 "Código de práctica de controles de la seguridad de la información"(Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, 2013) es un complemento a la gestión de requisitos planteados en la norma ISO/IEC 27001:2013, y menciona en detalle los objetivos de control planteados en el Anexo A, de mencionada norma. Estos objetivos de control, también conocidos como "dominios" son catorce (14), los cuales albergan trerinta y cinco (35) categorías de seguridad principales que a su vez desglosan 114 controles de referencia. El orden de los objetivos de control de la norma no tiene ninguna relevancia a la hora de su implementación, además pueden ser usados como mecanismo de iniciación en el momento en que la organización decida comenzar a gestionar controles de seguridad; dejando en claro que muchos de los objetivos planteados en la norma no puedan ser aplicados en la organización, lo más seguro es que se puedan requerir más controles y

directrices que no estén en la guía, ya que cada organización posee características que la hacen única frente a otras.

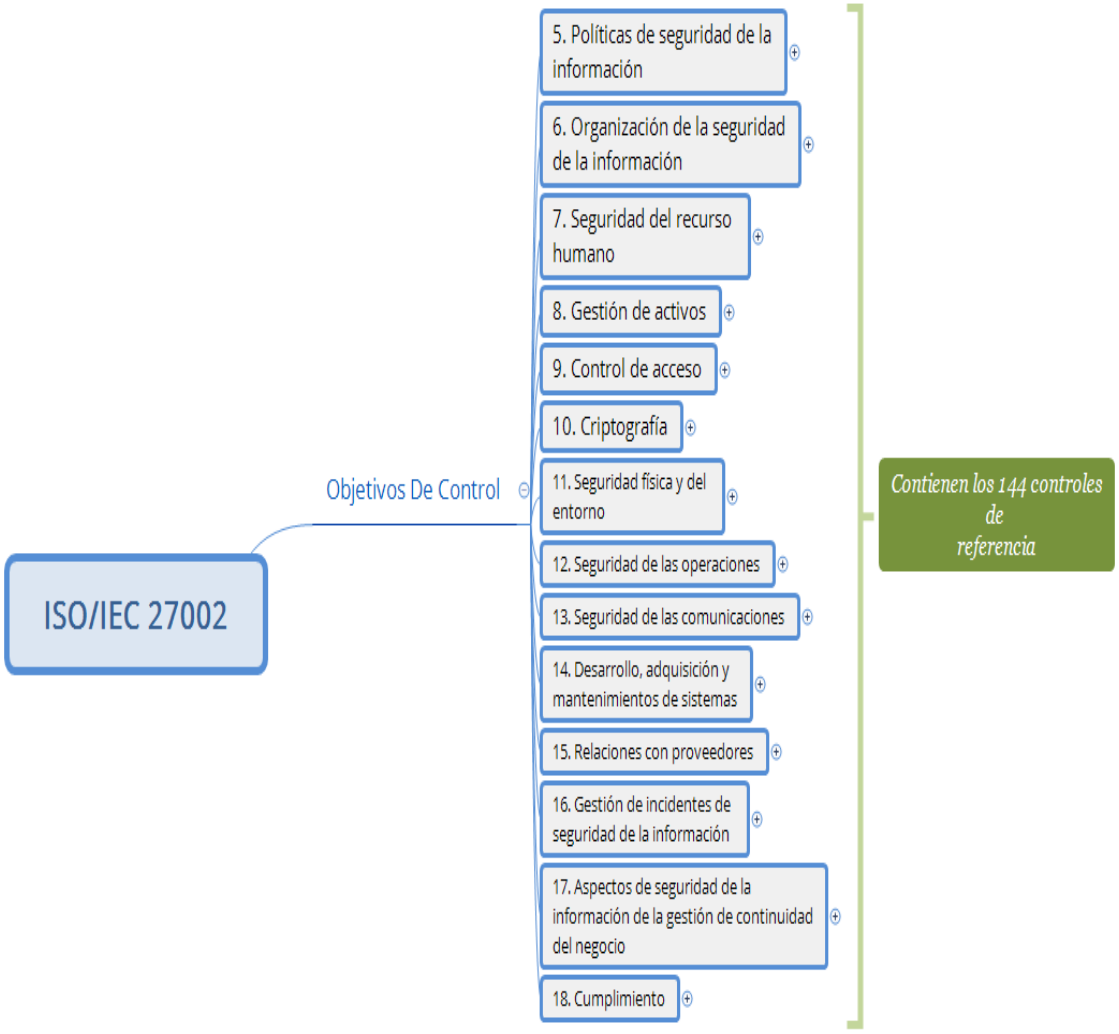


Figura 13. Objetivos de control ISO/IEC 27002:2015
Fuente. Autor del proyecto

La siguiente tabla nos detalla las treinta y cinco (35) categorías de seguridad, organizadas según al objetivo de control o dominio al que pertenezcan, numerados como lo establece la norma desde el inciso cinco (5) hasta el dieciocho (18).

Tabla 3
Estructura de controles ISO/IEC 27002:2013

OBJETIVO DE CONTROL	CATEGORÍAS DE SEGURIDAD
5. Políticas de seguridad de la información	5.1 Directrices establecidas por la organización para la seguridad de la información
6. Organización de la seguridad de la información	6.1 Organización interna 6.2 Dispositivos móviles y teletrabajo
7. Seguridad del recurso humano	7.1 Antes de asumir el empleo 7.2 Durante la ejecución del empleo 7.3 Terminación y cambio de empleo
8. Gestión de activos	8.1 Responsabilidad por los activos 8.2 Clasificación de la información 8.3 Manejo de medios
9. Control de acceso	9.1 Requisitos del negocio para el control de acceso 9.2 Gestión de acceso de usuarios 9.3 Responsabilidad de los usuarios 9.4 Control de acceso a sistemas y aplicaciones
10. Criptografía	10.1 Controles criptográficos
11. Seguridad física y del entorno	11.1 Áreas seguras 11.2 Equipos
12. Seguridad de las operaciones	12.1 Procedimientos operaciones y responsabilidades 12.2 Protección contra códigos maliciosos 12.3 Control de respaldo 12.4 Registro (Looging) y seguimiento 12.5 Control de software operacional 12.6 Gestión de la vulnerabilidad técnica 12.7 Consideraciones sobre auditorías de sistemas de información
13. Seguridad de las comunicaciones	13.1 Gestión de la seguridad de las redes 13.2 Transferencia de información
14. Desarrollo, adquisición y mantenimientos de sistemas	14.1 Requisitos de seguridad de los sistemas de información 14.2 Seguridad en los procesos de desarrollo y de soporte 14.3 Datos de prueba
15. Relaciones con proveedores	15.1 Seguridad de la información en las relaciones con los proveedores 15.2 Gestión de la prestación de servicios de proveedores
16. Gestión de incidentes de seguridad de la información	16.1 Gestión de incidentes y mejoras en la seguridad de la información
17. Aspectos de seguridad de la información de la gestión de continuidad del negocio	17.1 Continuidad de seguridad de la información 17.2 Redundancias
18. Cumplimiento	18.1 Cumplimientos de requisitos legales y contractuales 18.2 Revisiones de seguridad de la información

Fuente. Adaptación del autor

PCI-DSS. Las normas de seguridad de datos de la industria de tarjetas de pago, agrupa un conjunto de requerimientos técnicos y operativos que buscan facilitar la adopción de medidas de seguridad de los datos a nivel global. Su aplicación va orientada a organizaciones que participen en el procesamiento y tratamiento de información de las tarjetas de pago, esto incluye a los involucrados de manera directa e indirecta, como lo son: comerciantes, proveedores de servicio, adquirientes y a las entidades emisoras de las tarjetas. La norma PCI-DSS es de cumplimiento obligatorio para aquellas entidades que almacenen, procesen o transmitan datos del titular de la tarjeta (CHD) y/o datos confidenciales de autenticación (SAD).

Origen. En 2006 surge el PCI Security Standards Council, un foro mundial encargado de la formualción, gestión, educación y conocimiento orientado a las normas de seguridad en la industria de tarjetas de pago (PCI). Se destacan la norma de seguridad de datos (DSS) y las norma de seguridad de datos para las aplicaciones de pago (PA-DSS) y los requisitos de seguridad de transacciones con PIN (PTS).

El PCI Security Standards Council fue fundado por 5 miembros: American Express, Discover Financial Services, JCB International, MasterCard y Visa Inc. Las franquicias comparten de manera equitativa el control del consejo y de la misma manera comparten la responsabilidad de la adminisración de la organización. Las marcas acordaron incoporar la PCI DSS como referente para el cumplimiento de requisitos técnicos en materia de seguridad de los datos.

Descripción. La norma de seguridad de los datos PCI DSS de la industria de tarjetas de pago, busca fomentar y mejorar la seguridad de los datos del titular de la tarjeta y generar medidas de seguridad uniformes a nivel global. Todas las entidades que participen en el manejo de las tarjetas de pago; comerciantes, procesadores, adquirientes, entidades emisoras y proveedores de servicios y aquellas que almacenen, procesen o transmitan datos del titular de la tarjeta (CHD) y/o datos confidenciales de autenticación (SAD).

Estructura. PCI DSS se encuentra actualmente en su versión 3.2.1, revisión lanzada en mayo de 2018. Su estructura se centra en 12 requisitos para la gestión y evaluación de la seguridad de los datos, agrupados en 6 componentes; 1) Desarrolle y mantenga redes y sistemas seguros, 2) Proteger los datos del titular de la tarjeta, 3) Mantener un programa de administración de vulnerabilidad, 4) Implementar medidas sólidas de control de acceso, 5) Supervisar y evaluar las redes con regularidad y 6) Mantener una política de seguridad de la información.

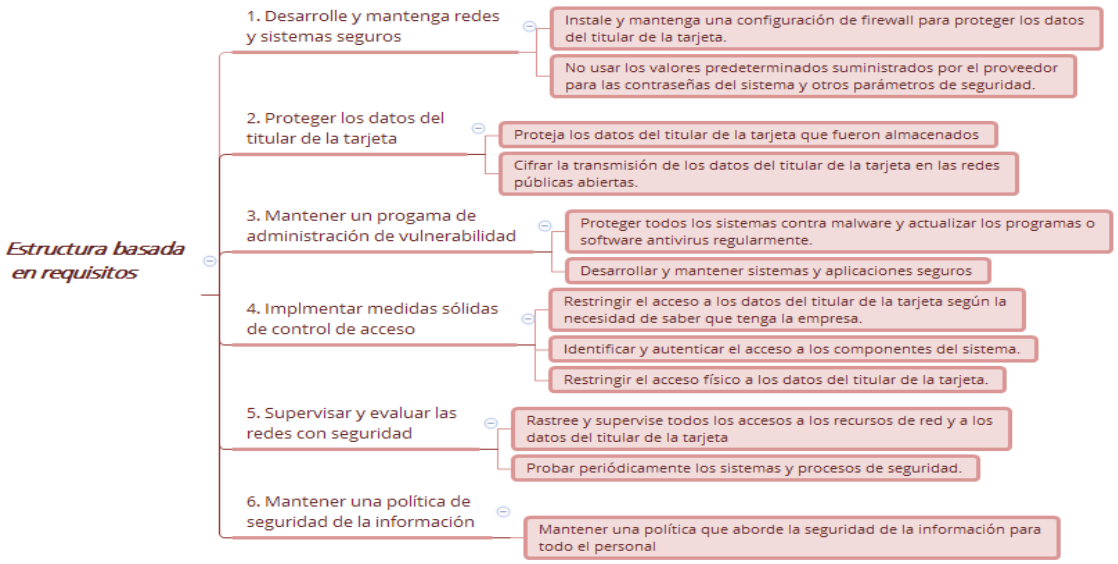


Figura 14. Estructura de requisitos PCI DSS
Fuente. Adaptación del autor

Cis Controls. Los controles CIS, son diseñados por el centro para la seguridad de internet, una entidad sin ánimo de lucro, fundada e integrada por un conglomerado de expertos y voluntarios en seguridad cuya preocupación unánime es la defensa cibernética. La pérdida de grandes volúmenes de datos, la violación de la intimidad y de los datos personales, los constantes ataques de denegación de servicios, y otro sin fin de eventos han ocasionado que la gestión de la seguridad de la información sea una exigencia en todas las organizaciones, incluso creando roles y dependencias con participación en las decisiones de gobierno empresarial.

Origen. El centro de seguridad de internet, inició labores en el mes de octubre del año 2000 y uno de sus trabajos destacados es la lista de controles (CIS Controls), aunque posee otro tipo de iniciativas destacadas como lo son: CIS Benchmarks, quién junto al CIS Controls constituyen un conjunto de buenas prácticas para proteger sistemas y datos de TI, de los ataques más generalizados. Además, cuenta con la iniciativa llamada CIS Hardened Images, que son entornos virtualizados preconfigurados de manera segura para ser escalados en la nube.

Descripción. "CIS Controls es un conjunto de acciones priorizadas que colectivamente forman un conjunto de mejores prácticas de defensa que mitigan los ataques más comunes contra sistemas y redes"(Secure & Secure, 2019).

Estructura. CIS Controls está diseñado y estructurado bajo tres tipos de controles generales, 1) Básicos, 2) Fundamentales y 3) Organizativos, que en conjunto suman un total de 20, además, cada control está conformado por subcontroles, esto con el fin de dar un nivel de detalle a la implementación de cada uno de ellos, en total esta buena práctica formula 171

controles (subcontroles) para mitigar el impacto de los ataques más comunes que se pueden presentar.

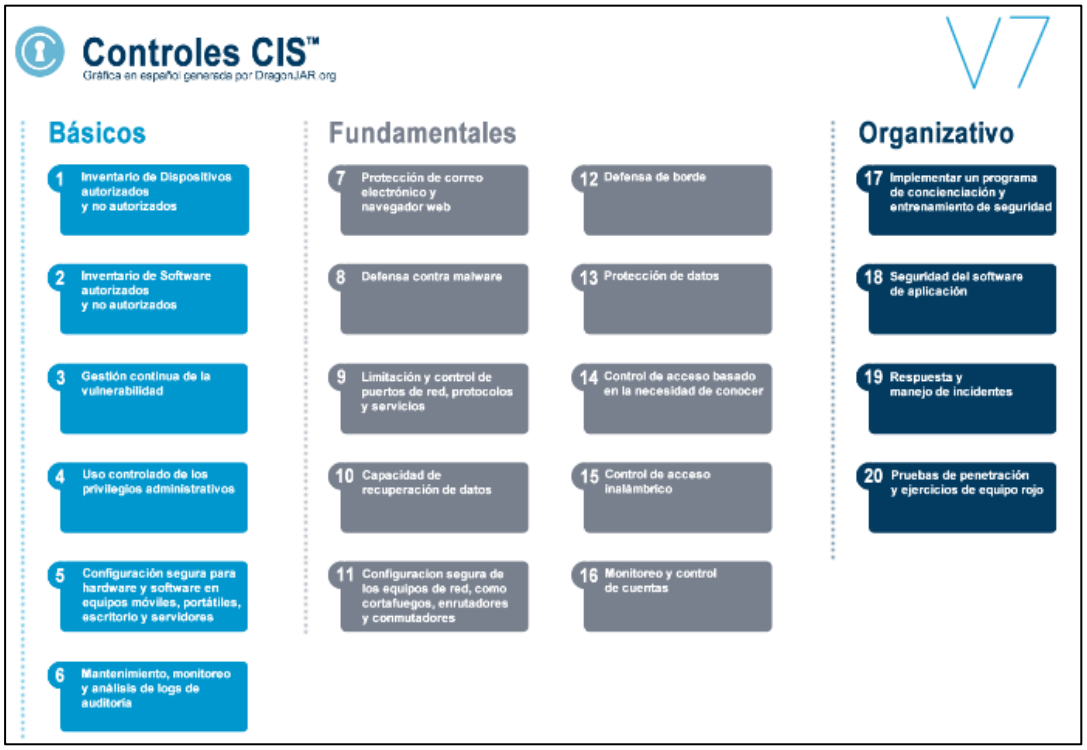


Figura 15. Controles CIS en español
Fuente. https://comunidad.dragonjar.info/discussion/9869/grafica-de-los-cis-controls-7-en-espanol

CIS Controls dentro de su estructura, establece un conjunto de principios sobre los cuales esta buena práctica justifica su sistema de defensa cibernética. Estos principios se detallan a continuación:

- La ofensa informa a la defensa,
- Priorización,
- Mediciones y métricas,
- Diagnóstico y mitigación continuos,
- Automatización.

Por otra parte, este conjunto de acciones priorizadas (controles), establece en su esquema de clasificación y estandarización un conjunto de “tipos de activos” y un listado de “funciones de seguridad”, según el ámbito de aplicación de los controles, por ejemplo, de tipos de activos encontramos como uno de ellos el “dato” y como una función de seguridad tenemos el criterio de “identificar”, entre otros

	Aplicaciones
	Datos
TIPOS DE ACTIVOS	*Dispositivos*
	Red
	Usuarios

Los criterios que hacen parte de las funciones de seguridad, establecen el tipo de acción que tendrá el control o la medida que se va a implantar, estas van desde identificar hasta responder, en detalle son las siguientes:

- Identificar
- Detectar
- Proteger
- Responder

Modelo de tratamiento de la información para la empresa Colombiana. El Modelo de tratamiento de la información para la empresa colombiana, fue desarrollado en el año 2018 por el estudiante de maestría en Gobierno de Tecnologías de la información JORGE ALBERTO

CAMARGO, de la Universidad Francisco de Paula Santander Ocaña. Este modelo es un compendio articulado entre normatividad, legislación colombiana y buenas prácticas de TI, en busca de la competitividad y adaptabilidad de las organizaciones a las nuevas necesidades que exige la globalización entorno al tratamiento de los datos y la información.

Estructura. El desarrollo de este modelo se basa en una estructura basada en tres aspectos primordiales, de los cuales posteriormente se van derivando subcomponentes y elementos que articulan un todo un modelo de tratamiento de datos. Los tres aspectos primordiales, o mejor conocidos como contextos son:

Contexto transversal. El contexto transversal se fundamenta en cuatro pilares, estos son: Visión, evolución, sostenibilidad y adaptabilidad, en sincronía con el ciclo PHVA. El objetivo del contexto transversal es direccionar y mantener a la organización en un enfoque actualizado y globalizado con respecto al tratamiento de datos personales.

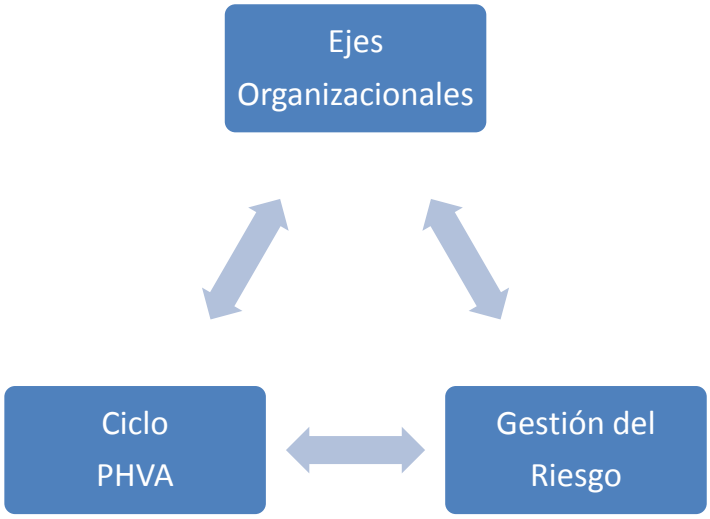


Figura 16. Componentes del eje transversal, adaptación Autor
Fuente. Autor del proyecto

Contexto interno. Este contexto hace referencia a las habilidades propias de la organización a nivel estratégico, operativo y táctico que se deberán implementar para el cumplimiento de requisitos legales y de las buenas prácticas de TI para el tratamiento de la información, está siempre de la mano con las mejores prácticas en seguridad de la información.

Contexto externo. El contexto externo hace referencia a aquellas partes interesadas que tengan incidencia o relación con el tratamiento de datos personales, afectando de manera directa cualquier toma de decisiones en los que se vean involucrados los datos que sean de responsabilidad de la organización. Esta fase contempla cuatro pilares que se muestran en la siguiente figura.

Figura 17. Componentes o pilares del Contexto externo
Fuente. Autor del proyecto

En resumen, el modelo de tratamiento de la información para la empresa colombiana, se convierte en una especie de framework entorno a como las organizaciones deberían gestionar sus datos. En la siguiente figura se muestra el modelo en su totalidad.

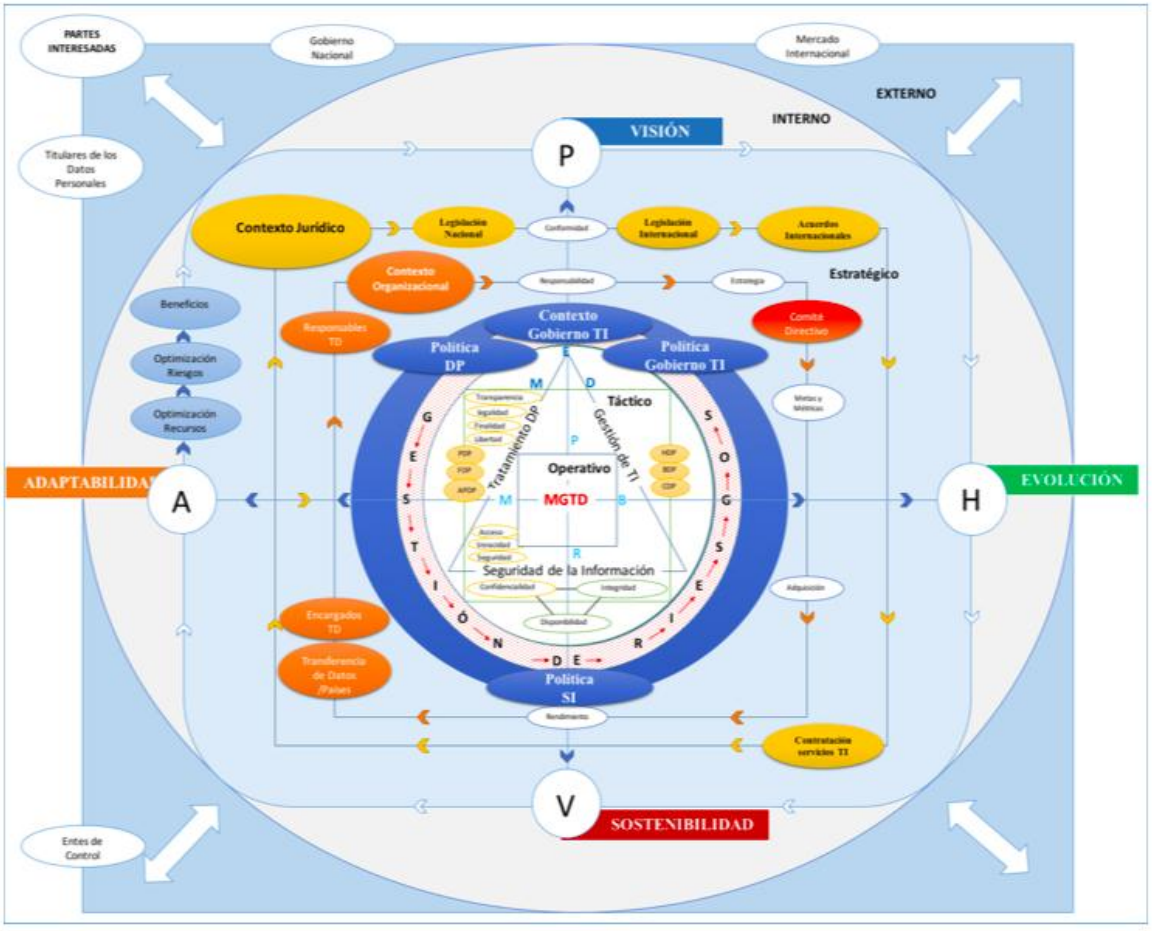


Figura 18. Esquema de Modelo de tratamiento de la información para la empresa colombiana
Fuente. Modelo de tratamiento de la información para la empresa colombiana, 2018.

4.2 Análisis del esquema legal referente a las exigencias de la ley colombiana para la protección de la seguridad y privacidad de la información.

El análisis documental que será ejecutado en este objetivo, da muestras de que Colombia ha tomado en serio y de manera particular el tema de protección y tratamiento de datos desde el año 2008, con la implementación de la ley 1266 de dicho año, "Por la cual se dictan 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 disposiciones" (Congreso de la república de Colombia, 2008), conocida como le de habeas data, la cual, posterior a la creación de la ley de protección de datos 1581 de 2012, pasó a conocerse como ley de habeas data financiero, es decir que Colombia cuenta con dos tipos de regulaciones en el ámbito de la protección de datos, una hacia el sector financiero (ley 1266) y la otra con enfoque hacia la información y su tratamiento en personas naturales (ley 1581), sin importar la naturaleza pública o privada de la organización que recopile los datos personales.

4.2.1 Análisis del contexto normativo internacional de la protección de datos. El 28 de enero de 1981, surge el convenio Nº108 del Consejo de Europa, denominado "Para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", quizás uno de los primeros documentos en abordar de forma expresa el tratamiento de datos personales en el mundo. A pesar de que en esos momentos el contexto y la dimensión del dato no supusiera las repercusiones que la tecnología traería para este, el convenio Nº108 es actualmente un referente en legislación y estructura para normativas relativas al tratamiento de los datos en diferentes países.

El convenio 108 está estructurado en siete (7) capítulos y veintisiete (27) artículos, su objeto es "garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ".(Europa, 1981)

La revisión documental en cuanto a normativas y legislación internacional referente a la privacidad de la información o protección de datos personales, permitió observar que el continente europeo, a través de la Unión Europea es quien mayores avances registra en legislación, normativa o regulación para esta actividad. La siguiente tabla enlista los principales acuerdos legislatorios en materia de privacidad, protección y tratamiento de datos de carácter personal.

Tabla 4
Normativa europea referente a la protección de datos

NORMATIVA	FECHA	DESCRIPCIÓN
Convenio 108 del Consejo de europa	28 de enero de 1981	Garantizar a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona
Directiva 95/46/CE del parlamento europeo y del consejo	24 de octubre de 1995	Que los Estados miembros garanticen la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.
Carta de los derecho fundamentales de la	7 de diciembre de 2000	Reforzar la protección de los derechos fundamentales a tenor

Tabla 4. Continuación

Unión Europea		de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos
Reglamento CE Nº 45/2001	18 de diciembre de 2000	Proporcionar a las personas unos derechos protegidos jurídicamente, que especifique las obligaciones de los responsables del tratamiento dentro de las instituciones y los organismos comunitarios en materia de tratamiento de datos y por el que se cree una autoridad de control independiente responsable de vigilancia de los tratamientos de los datos personales efectuados por las instituciones y los organismos comunitarios.
Convenio 108 (Protocolo adicional)	8 de noviembre de 2001	Con la intensificación de los intercambios de datos de carácter personal a través de las fronteras nacionales, es necesario garantizar la protección efectiva de los derechos humanos y de las libertades fundamentales y, en particular, del derecho al respeto de la vida privada, en relación con tales intercambios
Directiva 2002/58/CE del parlamento europeo y del consejo	12 de julio de 2002	Garantizar el respeto de los derechos fundamentales y observa los principios consagrados, en particular, en la Carta de los Derechos Fundamentales de la Unión Europea. Señaladamente, la presente Directiva pretende garantizar el pleno respeto de los derechos enunciados en los artículos 7 y 8 de dicha Carta.
Tratado de Lisboa	13 de diciembre de 2007	Reformar la estructura y el modo de funcionamiento de la Unión Europea. Fomentar la participación y protección de los

		ciudadanos, crear un nuevo orden institucional y modificar los procesos de toma de decisiones en aras de una mayor eficacia y transparencia. Organiza y clarifica por primera vez las competencias de la Unión.
Directiva sobre retención de datos	8 de abril de 2015	Armonizar las disposiciones de los Estados miembros sobre la conservación de determinados datos generados o tratados por los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Garantizar la disponibilidad de esos datos con fines de prevención, investigación, detección y enjuiciamiento de delitos graves, como la delincuencia organizada y el terrorismo.
Reglamento del parlamento europeo y del consejo, relativo a la protección de datos personales	6 de abril de 2016	Sustituir a la Directiva 95/46/CE y reforzar los derechos a la protección de datos de las personas físicas y mejorar las oportunidades para las empresas facilitando el libre flujo de los datos personales en el mercado único digital.
Ley orgánica 3/2018, de protección de Datos Personales y garantía de los derechos digitales - LOPD	5 de diciembre de 2018	Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.

Fuente. Cronología de normas, IAITG 2018

4.2.2 Identificación de normas, decretos y leyes referentes a la gestión de la seguridad y privacidad de la información.

A continuación, se listan las normas, decretos y leyes colombianas, referentes a la gestión de la seguridad y privacidad de la información.

Tabla 5
Normativa colombiana referente a la protección de datos

NORMATIVA	FECHA	DESCRIPCIÓN
Constitución Política de Colombia	20 de julio de 1991	Por el cual se definen las normas, derechos y deberes de los colombianos y el estado.
Ley 1266	31 de diciembre de 2008	Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. (Habeas Data).
Decreto 1727	15 de mayo de 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 información".
Decreto 2952	6 de agosto de 2010	Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008
Ley 1581	17 de octubre de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Resolución 76434	4 de diciembre de 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

Tabla 5. Continuación

		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	23 de abril de 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	27 de junio de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 1712	6 de marzo de 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	13 de mayo de 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
Sentencia C-748/11	24 de marzo de 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

Tabla 5. Continuación

		datos personales”
Sentencia C-1011/08	24 de marzo de 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	11 de agosto de 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	18 de diciembre de 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	19 de enero de 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	28 de marzo de 2018	Protección de datos personales.
Circular 03	3 de agosto de 2018	Modifica los numerales 2.1 al 2.4 y elimina los numerales 2.5 al 2.7 del Capítulo Segundo del Título V de la Circular Única de la Superintendencia de Industria y Comercio, en relación con el Registro

Tabla 5. Continuación

		Nacional de Bases de Datos - RNBD. Publicada en el Diario Oficial No. 50672 del 1 de agosto de 2018.
Ley 1928	22 de agosto de 2018	Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. Publicado en el Diario Oficial No. 50664 del 3 de agosto de 2018
Circular 01	16 de enero de 2019	Obligación de registro de bases de datos
Circular 02	7 de noviembre de 2019	Circular externa no 2 de 07 de noviembre de 2019, relacionada con "incorporar el numeral 2.19 del capítulo segundo en el título ii de la circular única de la superintendencia de industria y comercio"

Fuente. Adaptación del autor, matriz de legislación tratamiento de datos personales, Modelo de tratamiento de información para la empresa colombiana 2018.

La tabla anterior identifica y lista la normativa que regula el tratamiento de datos en Colombia, sin embargo, es necesario que se ejerza una supervisión sobre las exigencias que estas plantean, esta supervisión se orienta al monitoreo de cumplimiento y las maniobras sancionatorias para aquellas figuras que no cumplan con lo establecido, estas actividades en Colombia son asignadas para su competencia a la superintendencia de industria y comercio.

Superintendencia de Industria y comercio SIC. La superintendencia de industria y comercio nace en el año de 1960, por medio del decreto 1653 del 15 de julio del año en mención, bajo el nombre de superintendencia de regulación económica. Adscrita a la rama ejecutiva del

poder y con la función especial de estudiar y aprobar las tarifas de servicios públicos como energía, acueducto, alcantarillado, además de las tarifas relacionadas a los espectáculos públicos, de los cines y de los hoteles.

La ley 1581 de 2012, en su artículo 19 "Autoridad de protección de datos", designa a la superintendencia de industria y comercio, funciones para garantizar que en el tratamiento de datos personales se respeten los principios, derechos y garantías provistos en la ley. También incorpora en el organigrama de la misma, la figura del superintendente delegado, quién será el que ejerza las funciones de autoridad de protección de datos. Dentro de las funciones se destacan las siguientes:

- Velar por el cumplimiento de la legislación en materia de datos personales.
- Ejercer como ente investigador del caso, de oficio o a petición de parte y, según los resultados, ordenar las acciones necesarias para hacer efectivo el cumplimiento del habeas data. Si se desconoce el derecho, podrá exigir que se conceda el acceso y suministro a los datos, la rectificación, actualización o supresión de los mismos.
- Disponer de bloqueos temporales de los datos, cuando según el aporte de pruebas, se pueda identificar un riesgo de la vulneración de derechos fundamentales.
- Promover los derechos de las personas en relación con el tratamiento de datos personales.
- Dar instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los responsables del tratamiento y encargados del tratamiento a las disposiciones previstas en la ley.

- Solicitar a los responsables del tratamiento y encargados del tratamiento la información necesaria para el ejercicio de sus funciones.
- Proferir declaraciones de conformidad sobre las transferencias internacionales de datos.
- Administrar el registro nacional público de bases de datos y emitir órdenes y los actos necesarios para su administración y funcionamiento.
- Sugerir o recomendar ajustes y adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional.
- Requerir colaboración internacional, cuando se afecten los derechos de los titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales.
- Las demás que le sean asignadas por ley.

La gestión de los datos, entorno al tratamiento y su privacidad tiene repercusiones legales y económicas en Colombia. Como se mencionaba en los párrafos anteriores, la autoridad en temas de protección de datos, es la superintendencia de industria y comercio. Es por eso que hoy en día toma relevancia el avanzar en mecanismos o buenas prácticas para cumplir con las exigencias normativas entorno a los datos, esta metodología es un apoyo para la implementación de controles que van contribuir a la correcta gestión y tratamiento de los datos en las organizaciones públicas y privadas, evitando posibles sanciones que en el ámbito económico según el artículo 22 de la ley 1581 “Sanciones”, podrían llegar hasta los dos mil (2000) salarios mínimos mensuales legales vigentes.

4.3 Definición del compendio de controles de privacidad de la información.

En este objetivo, en resumen, se definen los controles para gestionar la privacidad de la información, a través de la generación de un compendio basado en el análisis de los requisitos legales exigidos para el cumplimiento del tratamiento de la información y los datos.

4.3.1 Identificación de los elementos que conforman el compendio de controles. Los elementos que conforman el compendio, pretenden desglosar cada control identificado, y de esta manera facilitar su entendimiento, implementación y aplicación. Los elementos se tomaron teniendo como referencia los esquemas utilizados por el anexo A de la ISO/IEC 27001, del estándar de guía general ISO/IEC 27002, y del CIS Controls v7. Con esto se busca que el compendio de controles sea flexible y adaptable a los estándares o modelos más comunes de seguridad de la información.

El anexo A de la ISO/IEC 27001, plantea un modelo de presentación de controles similar a la tabla que se expone a continuación.

Tabla 6
Estructura Anexo A.

A.# OBJETIVO DE CONTROL		
A.#.# Categoría de Seguridad		
Objetivo: Se describe el objetivo de la categoría de seguridad		
A. #.#.#	Nombre del control de referencia.	Descripción del control de referencia.

Fuente. Adaptación del autor. ISO/IEC 27001

En el caso de CIS Controls (Controles del centro de seguridad del internet) establece un cuadro o tabla con mayores elementos que la descrita por el anexo A. Dentro de su

planteamiento para cada control crítico contiene: a) sub-control, b) tipo de activo, c) función de seguridad, d) control y una e) descripción.

Tabla 7
Subcontroles CIS.

Control Crítico #: Nombre del control				
Sub-control	Tipo de activo	Función de seguridad	Control	Descripción
#.#				

Fuente. Adaptación del autor. CIS Controls V7.

La tabla anterior de subcontroles de CIS, tiene inmersos elementos que serán útiles en el desarrollo de los controles de privacidad, se destacan el tipo de activo y la función de seguridad. Cómo tipo de activos CIS Controls establece los siguientes:

- Aplicaciones,
- Datos,
- Equipos,
- Redes,
- Usuarios.

Y cómo funciones de seguridad se especifican las siguientes:

- Identificar,
- Proteger,
- Detectar,

- Responder,
- Recuperar.

4.3.2 Diseño del compendio de controles. El compendio de controles para la privacidad de la información en su estructura, se desarrolla en sinergia con los modelos establecidos por ISO y el CIS, como se mencionó en el ítem anterior. La estructura general de un control contiene elementos básicos en cualquier modelo, tales como (nombre del control, objetivo, categoría, descripción del control, entre otros). En la siguiente tabla, el autor presenta una comparativa entre la estructura de control que presenta la ISO/IEC 27001 en su nexo A, frente a la estructura que plantea el CIS en su versión 7.

Tabla 8
Comparativa cuadros de control ISO 27001 Anexo A vs CIS controls.

ANEXO A	CIS Control v7
Objetivo de control	No existe
Categoría de seguridad	Control crítico
Objetivo	No existe
Nombre control de referencia	Control
Descripción del control de referencia	Control, Descripción
No existe	Tipo de activo
No existe	Función de seguridad

No coincidencias

Coincidencias

Fuente. Autor del proyecto

Según los elementos identificados anteriormente, además de revisada la regulación colombiana referente a privacidad de la información, el autor propone la siguiente estructura o esquema para la exposición del compendio base de controles de privacidad de la información.

Tabla 9

Esquema de cuadro de controles de privacidad.

# DOMINIO DE PRIVACIDAD			
Numeral-control	**Control**	**Descripción del control**	**Ciclo PHVA**
Ej. 1	Nombre del control de privacidad	Descripción del control planteado en detalle.	PHVA

Fuente. Autor del proyecto

El cuadro de controles base de privacidad, es un esquema práctico que busca facilitar la implementación y garantizar el cumplimiento normativo en temas de privacidad de la información o tratamiento de datos personales, lejos de un lenguaje ambiguo, por tal motivo se estructura con cinco elementos.

- Dominio de privacidad. Es el eje principal de un grupo de controles, generalmente un eje temático estará conformado por más de un control.
- Numeral control.Es una guía para numerar los controles que se proponen en un mismo dominio de privacidad.
- Nombre del control. Nombre concreto del control.
- Descripción del control: Menciona en detalle el control.
- Ciclo PHVA.: Especifica la fase del ciclo PHVA en donde se implementa el control.

4.3.3 Documentación del compendio de controles base. En este ítem se describen los controles identificados, que permiten tratar los requerimientos establecidos en la normatividad colombiana para el tratamiento de datos personales. Siguen la estructura planteada en el ítem 5.3.2, lo que busca un fácil entendimiento y aplicación de los controles.

Tabla 10

Documentación del compendio de controles

1. CONTEXTO DE LA ORGANIZACIÓN			
Numeral-control	Control	Descripción del control	Ciclo PHVA
1.1	Estructura organizacional	Se debe definir dentro de la estructura organizacional, los espacios necesarios para la toma de decisiones de alto nivel, referente al tratamiento de datos personales.	PLANEAR
1.2	Responsabilidades y roles para el tratamiento de datos personales	Se deben establecer y asignar todas las funciones para garantizar el adecuado tratamiento de los datos personales.	PLANEAR
1.3	Integración del tratamiento de datos al sistema de gestión.	Se debe integrar la documentación desarrollada para el proceso del tratamiento de datos, con el sistema de gestión de la organización.	HACER
2. POLÍTICAS DE TRATAMIENTO			
Numeral-control	Control	Descripción del control	Ciclo PHVA
2.1	Política de tratamiento de datos o privacidad.	Se debe definir la política de tratamientos de datos, acorde a los lineamientos normativos.	PLANEAR
2.2	Revisión de la política de tratamiento de datos.	La política de tratamiento de datos, debe ser revisada a intervalos de tiempo, o cuando se presenten cambios bruscos en la organización o a nivel normativo.	VERIFICAR ACTUAR
2.3	Difusión de la política de tratamiento de datos o privacidad.	El responsable del tratamiento de datos deberá garantizar la difusión de la política de tratamiento de datos personales, valiéndose de documentos, formatos electrónicos, medios verbales o cualquier tipo de tecnología.	HACER
3. AVISO DE PRIVACIDAD			
Numeral-control	Control	Descripción del control	Ciclo PHVA
3.1	Aviso de privacidad documentado.	Se debe establecer un aviso de privacidad, con el fin de que el titular se informe sobre la	PLANEAR

Tabla 10. Continuación

		existencia de políticas de tratamiento de datos.	
3.2	Almacenamiento del aviso de privacidad.	El responsable del tratamiento debe almacenar el modelo de aviso de privacidad, empleando documentos, medios informáticos o electrónicos.	HACER VERIFICAR
3.3	Difusión del aviso de privacidad.	El responsable del tratamiento de datos deberá garantizar la difusión del aviso de privacidad, valiéndose de documentos, formatos electrónicos, medios verbales o cualquier tipo de tecnología.	HACER
4. AUTORIZACIÓN DE TRATAMIENTO			
Numeral-control	Control	Descripción del control	Ciclo PHVA
4.1	Autorización de tratamiento de datos personales.	El responsable del tratamiento debe solicitar por medio físico o electrónico, la autorización del titular para el tratamiento de sus datos.	PLANEAR
4.2	Revocatoria de la autorización de tratamiento de datos.	Se debe facilitar los medios o mecanismos por parte del responsable, para que el titular solicite la revocatoria de autorización o la supresión de los datos otorgados.	PHVA
4.3	Prueba de la autorización de tratamiento de datos.	El responsable del tratamiento debe utilizar los medios necesarios para conservar la prueba de la autorización otorgada por los titulares.	HACER VERIFICAR
5. TRATAMIENTO DE DATOS			
Numeral-control	Control	Descripción del control	Ciclo PHVA
5.1	Procedimientos de cara al Responsable y/o Encargado.	La organización en función del responsable y/o el encargado del tratamiento de datos, debe establecer procedimientos para regular la recolección, uso, almacenamiento, circulación y supresión de los datos.	HACER
5.2	Procedimientos de cara al Titular.	La organización debe establecer procedimientos, guías o instructivos para facilitar al titular	HACER

Tabla 10. Continuación

		el acceso, actualización, supresión o rectificación de sus datos.	
5.3	Difusión de los procedimientos.	Se debe facilitar estrategias de comunicación internas y externas para informas a las partes interesadas sobre los procedimientos establecidos para el tratamiento de datos, de cara a la organización y a los titulares.	HACER
5.4	Ejercicio de los derechos del Titular.	La organización, bajo la potestad del responsable o encargado del tratamiento de datos, deberá asignar un área o persona, encargada de dar trámite a las solicitudes hechas por los titulares.	PLANEAR
6. REGISTRO NACIONAL DE BASE DE DATOS			
Numeral-control	Control	Descripción del control	Ciclo PHVA
6.1	Inscripción de la organización en el RNBD.	El responsable del tratamiento de datos, debe inscribir a la organización en el RNBD, con la información requerida.	PHVA
6.2	Inscripción de las bases de datos de la organización en el RNBD.	Se debe inscribir en el RNBD, de manera independiente, cada una de las bases de datos que contengan datos personales sujetos a tratamiento.	
6.3	Actualización de las bases de datos de la organización en el RNBD.	Se debe actualizar el registro de las bases de datos en el RNBD por parte del responsable, cuando se presenten cambios sustanciales o por orden de la SIC	
7. SEGURIDAD DE LOS DATOS			
Numeral-control	Control	Descripción del control	Ciclo PHVA
7.1	Buenas prácticas para la seguridad de la información	Implementar o gestionar la adopción de estándares o buenas prácticas para garantizar la seguridad de la información de la organización	PHVA

Fuente. Autor del proyecto

4.4 Elaboración de la metodología que facilite la gestión de la privacidad de la información, alineada con la normativa legal colombiana.

4.4.1 Diseño de una metodología para la aplicación de los controles base. La aplicación de controles en múltiples estrategias de tecnología, ya sea gestión de servicios TI, metodologías ágiles, o seguridad de la información, facilita el cumplimiento de lineamientos, indicadores o normativas exigidas. Para el presente trabajo, en Colombia se regula y vigila el tratamiento de datos personales (privacidad de la información), lo que genera un carácter de obligatoriedad en el cumplimiento de condiciones para todas aquellas empresas u organizaciones que realicen tratamiento de datos personales de nacionales, o empresas en el exterior que realicen tratamiento de datos de colombianos. Por tal motivo, como parte de esta investigación se propone mostrar una metodología que permita aplicar estos controles de tal forma que sea entendible y manejable por parte del personal encargado de su implementación. Como parte fundamental de esta metodología, se ejercerán acciones en tres ejes conceptuales que son:

- Condiciones internas.
- Guía de Implementación.
- Vigilancia normativa.

Condiciones Internas. Las organizaciones de enfoque público o privado, para cumplir con los requisitos normativos o legales impuestos para el tratamiento de los datos en Colombia, deben adoptar a parte de controles, un conjunto de buenas prácticas; según el nivel de madurez del manejo de la información en dichas organizaciones, si hay mayor robustez en el manejo de

procesos, pues es de entender que para esa empresa será más fácil establecer controles que en otra entidad que no cuente con sistemas de gestión o buenas prácticas para el manejo de sus procesos o procedimientos internos. Por tal motivo se establecen unas condiciones mínimas a nivel de funcionamiento interno para la implementación de controles.

- Liderazgo.
- Definición del alcance.
- Planeación y gestión (PHVA).

Liderazgo. La alta dirección de la entidad o de la organización, debe demostrar liderazgo, conocimiento y compromiso respecto al tratamiento de datos personales, reconociendo las directrices que se deben cumplir por mandato de la normativa o leyes vigentes. Este liderazgo debe cumplir con los siguientes postulados.

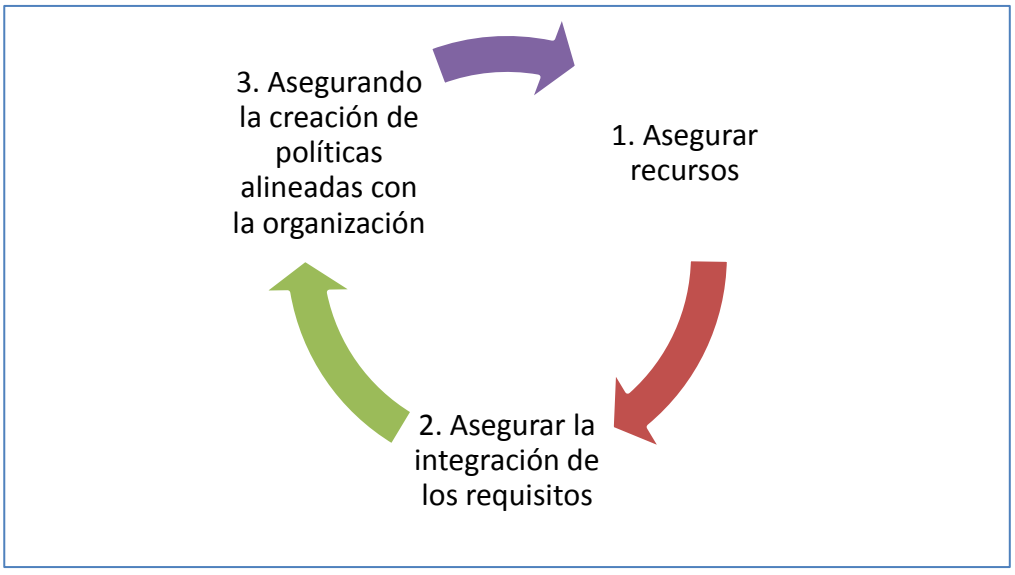


Figura 19. Compromisos de la alta dirección
Fuente. Autor del proyecto

La alta dirección debe separar los recursos necesarios para permitir una implementación adecuada de las políticas, procesos, procedimientos y controles asociados al tratamiento de datos personales. Debe propender por articular la documentación generada para la privacidad de los datos, en concordancia con el sistema de gestión de calidad y similares, además las políticas de tratamiento deben estar alienadas con los propósitos y las metas de la organización.

Definición del alcance. La organización debe determinar sus áreas y procesos involucrados y la aplicabilidad de las exigencias normativas o legales para calcular el alcance que tendrá el implementar controles para garantizar la privacidad de los datos de sus usuarios o titulares. Es importante a la hora de visualizar el alcance, el contexto interno y externo, es decir, aquellos factores que influirán de manera directa o indirecta en el tratamiento de datos personales.

Planeación y gestión (PHVA). La implementación y mantenimiento de los controles de privacidad, o controles para el tratamiento de datos personales, exige condiciones y esfuerzos internos en las organizaciones, por ende, la metodología sugiere tomar en cuenta el modelo de Deming o ciclo PHVA (planear, hacer, verificar y actuar), puesto que esto garantiza un constante monitoreo de la condiciones internas y externas asociadas al tratamiento de los datos. Cuando se habla de condiciones internas, se hace referencia a aspectos dentro de la organización que pueden ir variando en el tiempo, es decir, pueden ir surgiendo nuevos procesos, nuevas áreas, nuevos funcionarios que pueden afectar las condiciones de los controles, esto hace que los controles deban estar en un proceso de autoevaluación periódica, de la misma manera sucede con

las condiciones externas, ya que se pueden presentar cambios legales o normativos, que obliguen a realizarse ajustes inmediatos a los controles.

Los controles propuestos en el capítulo anterior, se articulan con el ciclo PHVA, facilitando la implementación y evaluación de los mismos.

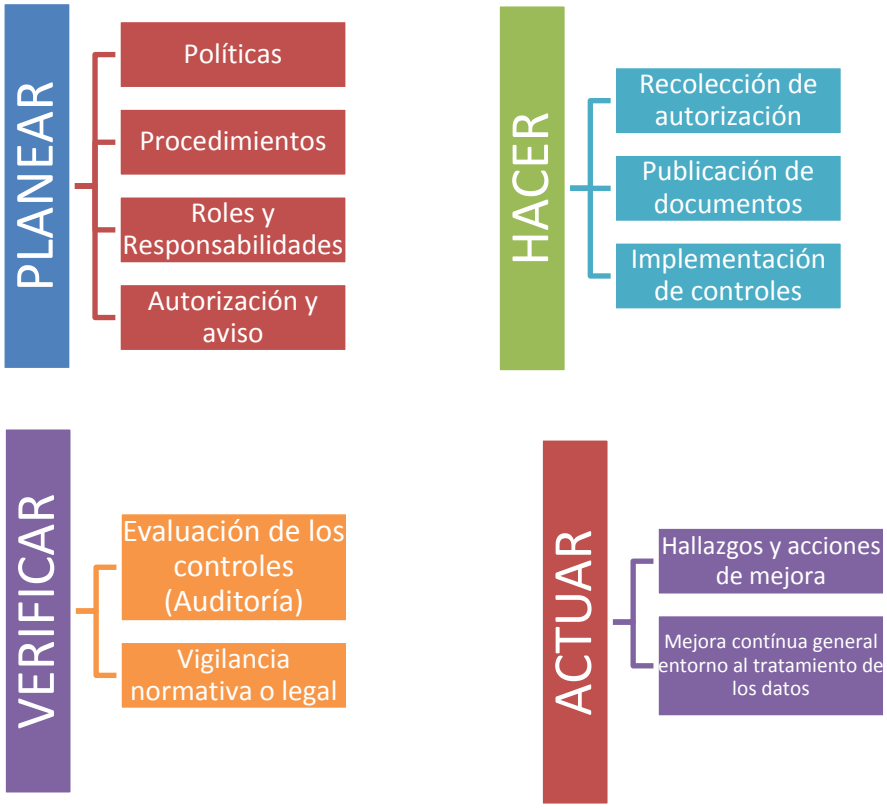


Figura 20. Ciclo PHVA entorno al tratamiento de datos.
Fuente. Autor del proyecto

Guía de implementación. A continuación, se esboza un conjunto de acciones que buscan detallar el compendio de controles de privacidad de la información o de tratamiento de datos personales. Es decir, se proponen estructuras documentales con el fin de facilitar la implementación de los controles, correspondiente a la fase “hacer” del ciclo PHVA.

Dominio #1. Contexto de la organización

Control 1.1 Estructura organizacional. Descripción. Se debe definir dentro de la estructura organizacional, los espacios necesarios para la toma de decisiones de alto nivel, referente al tratamiento de datos personales.

Aplicación. La organización debe implementar dentro de su estructura orgánica y funcional, el comité de privacidad de la información o comité de tratamiento de datos personales, cuya función será velar por el cumplimiento de la normativa colombiana al interior de la empresa, siendo ente de toma de decisiones de alto nivel. El comité dentro de sus funciones definirá al responsable y al encargado de tratamiento de datos, será actor de vigilancia a los posibles hallazgos entorno a la aplicación de controles, y demás actividades que propendan por la correcta aplicación de la norma.

Control 1.2 Responsabilidades y roles para el tratamiento de datos personales

Descripción. Se deben establecer y asignar todas las funciones para garantizar el adecuado tratamiento de los datos personales.

Aplicación. La organización, en cabeza del comité de privacidad de la información o comité de tratamiento de datos personales, deberá reglamentar las funciones y/o roles que tendrán el responsable y el encargado de tratamiento de datos personales, con el fin de garantizar las disposiciones dictadas por la normativa referente al tratamiento de datos.

Modelo. La siguiente plantilla es un referente para la aplicación del control dentro de las organizaciones.

ORGANIZACIÓN XXXXXXX
PROCESO DE TALENTO HUMANO
Manual de responsabilidades

Rol: Responsable del tratamiento de datos personales.
Objetivo: Asignar las respectivas funciones o responsabilidades para el "Responsable de tratamiento de datos personales en la organización xxxx"
Responsabilidades:
a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;
c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;
d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;
g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;
h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;
i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;
j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;
k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;
l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya
presentado la reclamación y no haya finalizado el trámite respectivo;
m) Informar a solicitud del Titular sobre el uso dado a sus datos;
n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la
administración de la información de los Titulares.
o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

_____
Firma funcionario asignado al rol

ORGANIZACIÓN XXXXXXX
PROCESO DE TALENTO HUMANO
Manual de responsabilidades

Rol: Responsable del tratamiento de datos personales.
Objetivo: Asignar las respectivas funciones o responsabilidades para el "Encargado de tratamiento de datos personales en la organización xxxx"
Responsabilidades:
a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;
d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;
e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;
f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares;
g) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley;
h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;
i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;
j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;
k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;
l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.
Parágrafo. En el evento en que concurran las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona,
le será exigible el cumplimiento de los deberes previstos para cada uno.

_____
Firma funcionario asignado al rol

Control 1.3 Integración del tratamiento de datos al sistema de gestión. Descripción. Se debe integrar la documentación desarrollada para el proceso del tratamiento de datos, con el sistema de gestión de la organización.

Aplicación. La gestión de tratamiento de datos dentro de la organización, debe ser integrada al sistema de gestión de calidad, con el fin de facilitar la adopción de la documentación generada, aprovechando el posible nivel de madurez con el que cuenta la entidad, esto permitirá integrar todo el componente de privacidad con el ciclo de los procesos internos que se llevan a cabo diariamente.

Dominio #2. Políticas de tratamiento

Control 2.1 Política de tratamiento de datos o privacidad. Descripción. Se debe definir la política de tratamientos de datos, acorde a los lineamientos normativos.

Aplicación. La política de tratamiento de datos o de privacidad de la información, es un documento que deberá constar en medio físico o electrónico, de fácil interpretación para los titulares y deberá contener mínimo la siguiente información: datos generales de la organización como; nombre, razón social domicilio, tratamiento y finalidad de los datos de los titulares, derechos que le asisten a titular, indicar el área encargada de atender las solicitudes de los titulares, los procedimientos para que el titular ejerza sus derechos, y la entrada en vigencia de la política.

Modelo. La siguiente plantilla es un referente para la aplicación del control dentro de las organizaciones.

ORGANIZACIÓN XXXXXXXXXX
Razón social

POLÍTICA DE PRIVACIDAD Y TRATAMIENTO DE DATOS PERSONALES

Que conforme al contenido de la Ley 1581 de 2012 por medio de la cual se dictan disposiciones generales para la protección de datos personales y el Decreto 1377 de 2013, por el cual se reglamenta de manera parcial la ley 1581 de 2012, las entidades deben adoptar dentro de sus procesos, políticas de protección de datos personales.
En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1° Adopción: La **ORGANIZACIÓN XXX**, en cumplimiento de la Ley 1581 de 2012, el Decreto reglamentario 1377 de 2013 y las demás disposiciones complementarias para la protección de datos personales, respecto a la recolección, uso, almacenamiento, circulación y supresión de todas aquellas actividades que contribuyan al tratamiento de datos personales, se permite informar a continuación los lineamientos generales en el presente documento.
ARTICULO 2°. DEFINICIONES: Para la ejecución de la presente política y de conformidad con la normatividad legal, serán aplicables las siguientes definiciones consagradas en la Ley 1581 de 2012 y el decreto 1377 de 2013.
Aviso de privacidad: XXXXXXXXXXXXXXXXXXX
Dato público: XXXXXXXXXXXXXXXXXXX
Datos sensibles: XXXXXXXXXXXXXXXXXXX
Datos biométricos: XXXXXXXXXXXXXXXXXXX
Transferencia: XXXXXXXXXXXXXXXXXXX
Transmisión: XXXXXXXXXXXXXXXXXXX
Tratamiento: XXXXXXXXXXXXXXXXXXX
Titular: XXXXXXXXXXXXXXXXXXX
Autorización: XXXXXXXXXXXXXXXXXXX
Responsable: XXXXXXXXXXXXXXXXXXX
Encargado: XXXXXXXXXXXXXXXXXXX
ARTÍCULO 3° PRINCIPIOS: La **ORGANIZACIÓN XXX**, estructura su Política de Protección de datos con base en los siguientes principios:
Principio de finalidad: XXXXXXXXXXXXXXXXXXX

Principio de libertad: XXXXXXXXXXXXXXXXXXX
Principio de veracidad o calidad: XXXXXXXXXXXXXXXXXXX
Principio de transparencia: XXXXXXXXXXXXXXXXXXX
Principio de seguridad: XXXXXXXXXXXXXXXXXXX
Principio de confidencialidad: XXXXXXXXXXXXXXXXXXX
ARTÍCULO 4°: DERECHOS DE LOS TITULARES: Los derechos de los Titulares de datos personales que reposen en las bases de datos de la **ORGANIZACIÓN XXX** son los siguientes:
Derecho a conocer, actualizar y rectificar sus datos personales: XXXXXXXXX
Derecho a solicitar prueba de la autorización: XXXXXXXXX
Derecho a ser informado frente al uso que se le ha dado a sus datos personales:

XXXXXXXXX
Derecho a revocar la autorización y/o a solicitar la supresión del dato: XXXXXXXXX
Derecho a acceder a sus datos personales: XXXXXXXXX
ARTÍCULO 5° FINALIDAD DE LA RECOLECCIÓN DE DATOS PERSONALES Y TRATAMIENTO DE LOS MISMOS: CORPONOR podrá hacer uso de los datos personales para:
Ejecutar la relación contractual existente con sus usuarios, proveedores y trabajadores, incluida el pago de obligaciones contractuales.
Proveer los servicios y/o los productos requeridos por sus usuarios.
Informar sobre nuevos productos o servicios y/o sobre cambios en los mismos.
Evaluar la calidad del servicio.
Entre otras…….
ARTÍCULO 6° AUTORIZACIÓN Y CLASES DE DATOS:
6.1 Autorización
Con antelación y/o al momento de efectuar la recolección del dato personal, la **ORGANIZACIÓN XXX** solicitará al titular del dato su autorización para efectuar su recolección y tratamiento, indicando la finalidad para la cual se solicita el dato, utilizando para esos efectos medios técnicos automatizados, escritos u orales, que permitan conservar prueba de la autorización y/o de la conducta inequívoca descrita en el artículo 7 del Decreto 1377 de 2013. Dicha autorización se solicitará por el tiempo que sea razonable y necesario para satisfacer las necesidades que dieron origen a la solicitud del dato y, en todo caso, con observancia de las leyes que rigen sobre la materia.
6.2 Casos en los que no se requiere autorización del titular de los datos
1. La autorización del titular no será necesaria cuando se trate de:
2. Datos de naturaleza Pública
3. Casos de urgencia médica o sanitaria
4. Tratamiento de información autorizado por la Ley para fines históricos, estadísticos o científicos.
5. Datos Relacionados con el Registro Civil de las personas.
ARTÍCULO 11. POLÍTICA
a) LA ORGANIZACIÓN XXX realiza el tratamiento de Datos Personales en ejercicio propio de sus funciones legales y para el efecto no requiere la autorización previa, expresa e informada del Titular. Sin embargo, cuando no corresponda a sus funciones deberá obtener la autorización por medio de un documento físico, correo electrónico, mensaje de datos, Internet, sitio web, o también de manera verbal o telefónica o en cualquier otro formato que permita su posterior consulta a fin de constatar de forma inequívoca que sin el consentimiento del titular los datos nunca hubieran sido capturados y almacenados en medios electrónicos. Así mismo se podrá obtener por medio de conductas claras e inequívocas del Titular que permitan concluir de una manera razonable que este otorgó su consentimiento para el manejo de sus Datos Personales.
b) LA ORGANIZACIÓN XXX solicitará la autorización a los Titulares de los datos personales y mantendrá las pruebas de ésta, cuando en virtud de las funciones de promoción, divulgación y capacitación, realice invitaciones a charlas, conferencias o eventos que impliquen el tratamiento de datos personales con una finalidad diferente para la cual fueron recolectados inicialmente.
c) En consecuencia, toda labor de tratamiento de Datos Personales realizada en LA ORGANIZACIÓN XXX deberá corresponder al ejercicio de sus funciones legales o a las finalidades mencionadas en la autorización otorgada por el Titular, cuando la situación

así lo amerite. De manera particular, las principales finalidades para el tratamiento de Datos Personales que corresponde a LA ORGANIZACIÓN XXX desarrollar en ejercicio de sus funciones.

d) El Dato Personal sometido a tratamiento deberá ser veraz, completo, exacto, actualizado, comprobable y comprensible. LA ORGANIZACIÓN XXX mantendrá la información bajo estas características siempre y cuando el titular informe oportunamente sus novedades.

e) Los Datos Personales solo serán tratados por aquellos funcionarios de LA ORGANIZACIÓN XXX que cuenten con el permiso para ello, o quienes dentro de sus funciones tengan a cargo la realización de tales actividades o por los Encargados.

f) LA ORGANIZACIÓN XXX autorizará expresamente al administrador de las bases de datos para realizar el tratamiento solicitado por el titular de la información.

g) LA ORGANIZACIÓN XXX no hará disponibles datos personales para su acceso a través de internet u otros medios masivos de comunicación, a menos que se trate de información pública o que se establezcan medidas técnicas que permitan controlar el acceso y restringirlo solo a las personas autorizadas por ley o por el titular.

h) Todo dato personal que no sea dato público se tratará por LA ORGANIZACIÓN XXX como confidencial, aun cuando la relación contractual o el vínculo entre el titular del dato personal y la ORGANIZACIÓN XXX haya finalizado.

i) Cada Subdirección, Jefatura, dependencia o área de LA ORGANIZACIÓN XXX debe evaluar la pertinencia de anonimizar los actos administrativos y/o documentos de carácter público que contengan datos personales, para su publicación.

j) El Titular, directamente o a través de las personas debidamente autorizadas, podrá consultar sus Datos Personales en todo momento y especialmente cada vez que existan modificaciones en las Políticas de Tratamiento de la información.

k) LA ORGANIZACIÓN XXX suministrará, actualizará, ratificará o suprimirá los Datos Personales a solicitud del Titular para corregir información parcial, inexacta, incompleta, fraccionada que induzca al error o aquella que haya sido tratada previa a la vigencia de la ley y que no tenga autorización o sea prohibida.

l) Cuando le sea solicitada información, ya sea mediante una petición, consulta o reclamo por parte del Titular, sobre la manera como son utilizados sus Datos Personales, LA ORGANIZACIÓN XXX deberá entregar dicha información.

m) A solicitud del Titular y cuando no tenga ningún deber legal o contractual de permanecer en las bases de datos de LA ORGANIZACIÓN XXX, los Datos Personales deberán ser eliminados. En caso de proceder una revocatoria de tipo parcial de la autorización para el Tratamiento de Datos personales para algunas de las finalidades de LA ORGANIZACIÓN XXX podrá seguir utilizando los datos para las demás finalidades respecto de las cuales no proceda dicha revocatoria.

n) Las políticas establecidas por la ORGANIZACIÓN XXX respecto al tratamiento de Datos Personales podrán ser modificadas en cualquier momento. Toda modificación se realizará con apego a la normatividad legal vigente, y las mismas entrarán en vigencia y tendrán efectos desde su publicación a través de los mecanismos dispuestos por LA ORGANIZACIÓN XXX para que los titulares conozcan la política de tratamiento de la información y los cambios que se produzcan en ella.

o) Los Datos Personales solo podrán ser tratados durante el tiempo y en la medida que la finalidad de su tratamiento lo justifique.

p) LA ORGANIZACIÓN XXX será más rigurosa en la aplicación de las políticas de tratamiento de la información cuando se trate del uso de datos personales de los niños,

niñas y adolescentes asegurando la protección de sus derechos fundamentales.

q) LA ORGANIZACIÓN XXX podrá intercambiar información de Datos Personales con autoridades gubernamentales o públicas tales como autoridades administrativas, de impuestos, organismos de investigación y autoridades judiciales, cuando la soliciten en ejercicio de sus funciones con previa autorización legal correspondiente.

r) Los Datos Personales sujetos a tratamiento deberán ser manejados proveyendo para ello todas las medidas tanto humanas como técnicas para su protección, brindando la seguridad de que ésta no pueda ser copiada, adulterada, eliminada, consultada o de alguna manera utilizada sin autorización o para uso fraudulento.

s) Cuando finalice alguna de las labores de tratamiento de Datos Personales por los trabajadores, contratistas o encargados del tratamiento, y aun después de finalizado su vínculo o relación contractual con LA ORGANIZACIÓN XXX, éstos están obligados a mantener la reserva de la información de acuerdo con la normatividad vigente en la materia.

t) LA ORGANIZACIÓN XXX divulgará en sus trabajadores, contratistas y terceros encargados del tratamiento las obligaciones que tienen en relación con el tratamiento de Datos Personales mediante campañas y actividades de orden pedagógico.

u) El Titular de los datos personales puede ejercer, principalmente, sus derechos mediante la presentación de consultas y reclamos ante LA ORGANIZACIÓN XXX, en su sede cuyo domicilio es la Calle XXXXXXXXXXXXXX y por el correo electrónico xxxxxxxx@organizacionxxx.com, indicando el tipo de trámite a llevarse a cabo con su información.

v) Cuando exista un Encargado del Tratamiento de Información de Datos Personales, LA ORGANIZACIÓN XXX deberá garantizar que la información que le suministra sea veraz, completa, exacta, actualizada, comprobable y comprensible. Adicionalmente le comunicará de manera oportuna todas las novedades a que haya lugar para que la información siempre se mantenga actualizada.

w) En el caso de existir un Encargado del Tratamiento de información de Datos Personales, la ORGANIZACIÓN XXX suministrará según el caso, información de Datos Personales únicamente cuyo Tratamiento realice en virtud de sus funciones legales y cuando excepcionalmente éstas no apliquen, con la autorización del Titular.

x) LA ORGANIZACIÓN XXX Informará al Encargado del Tratamiento de información de Datos Personales, de existir uno, cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

y) Cuando exista un Encargado del Tratamiento de información de Datos Personales, se exigirá que, en todo momento, se respeten las condiciones de seguridad y confidencialidad de la información del Titular establecidas por LA ORGANIZACIÓN XXX.

APROBADA el xx de xx del año xxxxx
COMUNÍQUESE Y CUMPLASE DE INMEDIATO

Control 2.2 Revisión de la política de tratamiento de datos.

Descripción. La política de tratamiento de datos, debe ser revisada a intervalos de tiempo, o cuando se presenten cambios bruscos en la organización o a nivel normativo.

Aplicación. Para cumplir a cabalidad con este control, la organización debe garantizar la revisión periódica de la política, ya que esta es propensa a cambios de fondo normativos o inclusos a actualizaciones internas por modificaciones en los procesos subyacentes al tratamiento de datos. Se puede generar un punto de control en el sistema de gestión, que exija la revisión periódica de la política de tratamiento de datos.

Control 2.3 Difusión de la Política de tratamiento de datos.

Descripción. El responsable del tratamiento de datos deberá garantizar la difusión de la política de tratamiento de datos personales, valiéndose de documentos, formatos electrónicos, medios verbales o cualquier tipo de tecnología.

Aplicación. La organización debe utilizar los mecanismos necesarios a su alcance, para comunicar y socializar su política de tratamiento de datos personales, a nivel interno por medio de las jornadas de inducción y reinducción, a través de los medios de difusión, como los son correos electrónicos y chats corporativos, en su sistema de gestión documental, y a nivel externo usando su página web, medios masivos de difusión, como la prensa, la radio, la televisión, redes sociales, entre otras estrategias.

Dominio #3. Aviso de privacidad

Control 3.1 Aviso de privacidad documentado.

Descripción. Se debe establecer un aviso de privacidad, con el fin de que el titular se informe sobre la existencia de políticas de tratamiento de datos.

Aplicación. En el caso de que no sea posible poner a disposición del Titular, las políticas de tratamiento de datos personales, la organización deberá informar por medio de un aviso de privacidad al titular sobre la existencia de políticas y la forma de acceder a ellas.

De manera explícita esto se puede hacer a través de ventanas emergentes en una página web, carteles ubicados en sitios estratégicos como: escaleras, ascensores, cerca de la ubicación de cámaras de video vigilancia, o en sitios donde de alguna forma se recolecten y traten datos personales.

Modelo. La siguiente plantilla es un referente para la aplicación del control dentro de las organizaciones.

ORGANIZACIÓN XXX

AVISO DE PRIVACIDAD

La ORGANIZACIÓN XXX, con domicilio en la ciudad XXXX, se presenta y actúa como el responsable del tratamiento de datos personales, con la siguiente información de contacto:

a) Dirección de atención XXXXXXXXXXX
b) Correo electrónico xxxxxxxx@organizacionxxx.com

c) Teléfono 111-1111111

Los datos recolectados, objeto de tratamiento, serán almacenados en nuestras bases de datos y serán utilizados de manera directa o indirecta a través de terceros aliados a la organización, teniendo como finalidad el cumplimiento del objeto y de los siguientes propósitos de la ORGANIZACIÓN XXX:

a) Ejecutar la relación contractual existente con sus usuarios, proveedores y trabajadores, incluida el pago de obligaciones contractuales.
b) Proveer los servicios y/o los productos requeridos por sus usuarios.
c) Informar sobre nuevos productos o servicios y/o sobre cambios en los mismos.
d) Evaluar la calidad del servicio.
e) Desarrollar el proceso de selección, evaluación, y vinculación laboral.
f) Soportar procesos de auditoría interna o externa.
g) Registrar la información de empleados y/o pensionados (activos e inactivos) en las bases de datos de la ORGANIZACIÓN XXX.
h) Los indicados en la autorización otorgada por el titular del dato o descritos en el aviso de privacidad respectivo, según sea el caso.
i) Suministrar, compartir, enviar o entregar sus datos personales a empresas filiales o vinculadas a la ORGANIZACIÓN XXX en el evento que dichas compañías requieran la información para los fines aquí indicados.

La organización XXX, les informa a los titulares de la información objeto de tratamiento, que pueden consultar la política de tratamiento de datos personales en su nivel de detalle, a través de la página web de la organización, así como los distintos procedimientos establecidos para el ejercicio de sus derechos de acceso, consulta, rectificación, actualización y supresión de los datos.

Control 3.2 Almacenamiento del Aviso de Privacidad.

Descripción. El responsable del tratamiento debe almacenar el modelo de aviso de privacidad, empleando documentos, medios informáticos o electrónicos.

Aplicación. Los responsables deben conservar el aviso de privacidad que utilicen para cumplir con el deber de dar a conocer a los titulares la existencia de políticas de tratamiento de datos del a información, y la forma de acceder a las mismas. Se debe almacenar el modelo de

aviso de privacidad se pueden emplear medios informáticos, electrónicos o de otra tecnología que garantice lo previsto en la ley 527 de 1999 y en el decreto 19 de 2012.

Control 3.3 Difusión del Aviso de privacidad.

Descripción. El responsable del tratamiento de datos deberá garantizar la difusión del aviso de privacidad, valiéndose de documentos, formatos electrónicos, medios verbales o cualquier tipo de tecnología.

Aplicación. La organización debe utilizar los mecanismos necesarios a su alcance, para comunicar y visualizar su aviso de privacidad, a nivel interno por medio de las jornadas de inducción y reinducción, a través de los medios de difusión, como los son correos electrónicos y chats corporativos, en su sistema de gestión documental, y a nivel externo usando su página web, medios masivos de difusión, como la prensa, la radio, redes sociales, entre otras estrategias.

Dominio #4. Autorización de tratamiento.

Control 4.1 Autorización de tratamiento de datos personales.

Descripción. El responsable del tratamiento debe solicitar por medio oral, físico o electrónico, la autorización del titular para el tratamiento de sus datos.

Aplicación. El tratamiento de datos personales es autorizado por parte del titular al responsable a través de la firma del documento de autorización de datos personales. Se busca

informar de manera explícita, previa al titular, que tipos de datos serán objeto de tratamiento y la finalidad de este. La autorización puede ser solicitada de forma oral, a través de medios electrónicos, usando vistas o formularios web, que en su defecto cumplirán la misma función que un documento en físico.

Modelo. La siguiente plantilla es un referente para la aplicación del control dentro de las organizaciones.

CARTA DE AUTORIZACIÓN PARA EL USO Y ALMACENAMIENTO DE DATOS PERSONALES

Asunto: autorización para el uso y almacenamiento de datos personales

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

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

2. Que me ha sido informada la (s) finalidad (es) de la recolección de los datos personales, la cual consiste en: Atención al ciudadano, Gestión de estadísticas internas, Gestión Administrativa, Gestión de clientes, Gestión de cobros y pagos, Gestión de facturación, Gestión tributaria y de recaudación, Procedimientos judiciales, Marketing, Publicidad propia, Comercio electrónico.

3. Es de carácter facultativo o voluntario responder preguntas que versen sobre datos sensibles o sobre menores de edad.

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

5. Los derechos pueden ser ejercidos a través de os canales dispuestos por LA ORGANIZACIÓN XXX y observando la Política de Tratamiento de Datos Personales.

6. Mediante la página web de la entidad www.La ORGANIZACIÓN XXX.com, a través del correo electrónico xxxxxxxx@organizacionxxx.com o al teléfono 111-1111 podre radicar cualquier tipo de requerimiento relacionado con el tratamiento de mis datos personales.

7. LA ORGANIZACIÓN XXX garantizara la confidencialidad, libertad, seguridad, veracidad, transparencia, acceso y circulación restringida de mis datos y se reservara el derecho de modificar su Política de Tratamiento de Datos Personales en cualquier momento. Cualquier cambio será informado y publicado oportunamente en la página web.

8. Teniendo en cuenta lo anterior, autorizo de manera voluntaria, previa, explicita, informada e inequívoca a LA ORGANIZACIÓN XXX para tratar mis datos personales de acuerdo con su Política de Tratamiento de Datos Personales para los fines relacionados con su objeto y en especial para fines legales, contractuales, misionales descritos en la Política de Tratamiento de Datos Personales de LA ORGANIZACIÓN XXX.

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

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

Control 4.2 Revocatoria de la autorización de tratamiento de datos.

Descripción. Se debe facilitar los medios o mecanismos por parte del responsable, para que el titular solicite la revocatoria de autorización o la supresión de los datos otorgados a través de un reclamo.

Aplicación. Para la revocatoria o supresión de la autorización de tratamiento de datos personales, el titular o el causahabiente tendrá la posibilidad de efectuar un reclamo dirigido al responsable o encargado del tratamiento, este será tramitado bajo las siguientes reglas:

- E l reclamo se formula o dirige hacia el responsable o al encargado del tratamiento, deberá contener la identificación del titular, el acontecimiento que da lugar al reclamo, dirección y la documentación anexa que quiera ofrecer. Si el titular formula un reclamo incompleto, se le

darán cinco (5) días para que subsane la falla, el reclamo se declarará desistido si pasado dos (2) meses el titular no presenta la información requerida.

- Cuando se reciba el reclamo, en la base de datos se deberá incluir una leyenda que diga "reclamo en trámite" durante dos (días hábiles mientras) este es atendido.
- La atención del reclamo tendrá por tiempo máximo quince (15) días hábiles, si este no es atendido en dichos términos, se deberá informar el motivo de la demora a los interesados, y se tendrán ocho (8) días hábiles siguientes al primer vencimiento para ser atendido.

Control 4.3 Prueba de la autorización de tratamiento de datos.

Descripción. El responsable del tratamiento debe utilizar los medios necesarios para conservar la prueba de la autorización otorgada por los titulares.

Aplicación. La autorización de tratamiento de datos personales se entenderá por aceptada cuando se realice de manera oral, escrita o mediante conductas inequívocas (tal es el caso de un check de aceptado en un formulario web). Sin importar la forma de manifestación de la aceptación se debe conservar prueba de la autorización.

- Si la autorización se manifiesta de manera oral, se deben implementar mecanismos de grabación de llamadas, y la disposición del archivo en un sitio de almacenamiento.
- Si la autorización se manifiesta por un medio escrito, el responsable debe vincular el documento dentro del sistema de archivos de la organización y gestionar su inclusión en las respectivas tablas de retención documental.

- Si la autorización se manifiesta por un medio electrónico, por ejemplo, un formulario colgado en la página web de la organización, se deberá garantizar su almacenamiento, e incluir este tipo de ficheros en el procedimiento de backup, para minimizar los riesgos de borrado, alteración o daño.

Dominio #5. Tratamiento de datos.

Control 5.1 Procedimientos de cara al responsable y/o encargado del tratamiento.

Descripción. La organización en función del responsable y/o el encargado del tratamiento de datos, debe establecer procedimientos para regular la recolección, uso, almacenamiento, circulación y supresión de los datos.

Aplicación. El tratamiento de datos personales de cara al responsable y/o encargado, implica el conjunto de acciones que estos pueden realizar con la información suministrada por los diversos titulares que aceptaron el tratamiento de sus datos, a través de la autorización de tratamiento. En ese orden de ideas la organización debe diseñar e implementar procedimientos para regular la recolección, el uso, almacenamiento, circulación y supresión de los datos.

Modelo. La siguiente plantilla es un referente para la aplicación del control dentro de las organizaciones.

ORGANIZACIÓN XXX
PROCESO DE TRATAMIENTO DE DATOS

Procedimiento: Recolección, uso, almacenamiento, circulación y supresión de datos.

Objetivo: Definir las actividades básicas para el tratamiento de la información desempeñadas por el responsable y el encargado del tratamiento en la organización, en cumplimiento de las disposiciones establecidas en la ley 1581 de 2012, el decreto 1377 de 2013, entre otras disposiciones.

Alcance: La información recolectada con fines de tratamiento, a través de la autorización del titular.

ACTIVIDADES.

1. Recolección de la Información.

Responsable 1	Responsable 2	Observaciones
Act 1.1 xxxxxxxxxxxxxxxxxx		
	Act 1.2 xxxxxxxxxxxxxxxxxx	

2. Uso de la Información.

Responsable 1	Responsable 2	Observaciones
Act 2.1 xxxxxxxxxxxxxxxxxx		
	Act 2.2 xxxxxxxxxxxxxxxxxx	

3. Almacenamiento de la Información.

Responsable 1	Responsable 2	Observaciones
Act 3.1 xxxxxxxxxxxxxxxxxx		
	Act 3.2 xxxxxxxxxxxxxxxxxx	

4. Circulación de la Información.

Responsable 1	Responsable 2	Observaciones
Act 4.1 xxxxxxxxxxxxxxxxxx		
	Act 4.2 xxxxxxxxxxxxxxxxxx	

5. Supresión de la Información

Responsable 1	Responsable 2	Observaciones
Act 5.1 xxxxxxxxxxxxxxxxxx		
	Act 5.2 xxxxxxxxxxxxxxxxxx	

NOTA:

Según las condiciones particulares de la entidad u organización donde se implementen los procedimientos, se deben tener en cuenta temas como: Riesgos, normogramas, control de versiones, entre otras.

Control 5.2 Procedimientos de cara al titular.

Descripción. La organización debe establecer procedimientos, guías o instructivos para facilitar al titular el acceso, actualización, supresión o rectificación de sus datos.

Aplicación. La normativa colombiana para el tratamiento de la privacidad de la información o tratamiento de datos personales, establece en la ley 1581 de 2012 los derechos que le asisten a los titulares de los datos; requerimiento imperativo de cumplir a través de manuales, guías o instructivos, implementados en el sistema de gestión o en la documentación de la organización, publicados en los medios de difusión institucionales (página web, sistema de gestión documental) y de fácil acceso para los interesados.

Modelo. La siguiente plantilla es un referente para la aplicación del control dentro de las organizaciones.

ORGANIZACIÓN XXX
PROCESO DE TRATAMIENTO DE DATOS
Manual, guía o instructivo, para el ejercicio de los derechos de los titulares en la organización.

Objetivo: Facilitar al titular, causahabiente o representante del titular, el ejercicio de sus derechos en el tratamiento de su información, orientados al acceso, actualización, supresión o rectificación de sus datos.

Disposiciones generales:

Para el ejercicio de los derechos de los titulares, el interesado (titular, causahabiente, o representante del titular) deberá demostrar o acreditar la identidad en forma suficiente por los medios que disponga el representante de tratamiento de la organización. El ejercicio de los derechos no tiene ningún costo para el titular, cómo lo dispone la ley 1581 de 2012 en su capítulo IV, artículos 20, 21, 22 y 23.

Declaratoria especial: Los derechos de niños y adolescentes en torno a la protección de datos, serán ejercidos por las personas que estén facultadas para representarlos.

1. Acceso a los datos personales.

Actividades o pasos para que el titular tenga acceso a sus datos personales.

a) Xxxxxxxxxxxxxxxxxxx
b) Xxxxxxxxxxxxxxxxxxx
c) Xxxxxxxxxxxxxxxxxxx

2. Actualización y/o rectificación de datos personales.

Actividades o pasos para que el titular solicite actualización o rectificación de sus datos personales.

a) Xxxxxxxxxxxxxxxxxxx
b) Xxxxxxxxxxxxxxxxxxx
c) Xxxxxxxxxxxxxxxxxxx

3. Supresión de datos personales.

Actividades o pasos para que el titular solicite la supresión de sus datos personales.

a) Xxxxxxxxxxxxxxxxxxx
b) Xxxxxxxxxxxxxxxxxxx
c) Xxxxxxxxxxxxxxxxxxx

Control 5.3 Difusión de los procedimientos.

Descripción. Se debe facilitar estrategias de comunicación internas y externas para informas a las partes interesadas sobre los procedimientos establecidos para el tratamiento de datos, de cara a la organización y a los titulares.

Aplicación. La organización debe utilizar los mecanismos necesarios a su alcance, para comunicar y visualizar los mecanismos para que los titulares ejerzan sus derechos, a nivel interno por medio de las jornadas de inducción y reinducción, a través de los medios de difusión, como los son correos electrónicos y chats corporativos, en su sistema de gestión documental, y a

nivel externo usando su página web, medios masivos de difusión, como la prensa, la radio, redes sociales, entre otras estrategias

Control 5.4 Ejercicio de los derechos del titular.

Descripción. La organización, bajo la potestad del responsable o encargado del tratamiento de datos, deberá asignar un área o persona, encargada de dar trámite a las solicitudes hechas por los titulares.

Aplicación. La organización a través de los medios legales e institucionales debe asignar al personal o área quiénes serán los responsables de coordinar y atender las solicitudes efectuadas por los interesados (titulares, causahabientes o representantes del titular).

Dominio #6. Registro nacional de bases de datos.

Control 6.1 Inscripción de la organización en el RNBD.

Descripción. El responsable del tratamiento de datos, debe inscribir a la organización en el RNBD, con la información requerida.

Aplicación. El responsable del tratamiento de datos de la organización, será el encargado de inscribir a la entidad en el registro nacional de bases de datos, portal dispuesto por la superintendencia de industria y comercio para el registro de las bases de datos sobre las que

reposen datos de titulares, este registro se deberá hace en la plataforma con dirección https://rnbd.sic.gov.co/sisi/publico/registrarSujetoObligado/, para posteriormente realizar el proceso de inscripción de bases de datos.

Control 6.2 Inscripción de las bases de datos de la organización en el RNBD.

Descripción. Se debe inscribir en el RNBD, de manera independiente, cada una de las bases de datos que contengan datos personales sujetos a tratamiento.

Aplicación. El responsable del tratamiento de datos de la organización, como primera medida deberá realizar el inventario de las bases de datos de la entidad que almacenen información de titulares potenciales, este inventario debe contener tanto las bases de datos en formato digital como en formato físico. Se deben identificar la cantidad de registros con los que cuenta cada base de datos, ya que esta es la información que se deberá subir al portal establecido por la superintendencia de industria y comercio para tal fin, en el siguiente enlace https://sic.gov.co/registro-nacional-de-bases-de-datos

Control 6.3 Actualización de las bases de datos de la organización en el RNBD.

Descripción. Se debe actualizar el registro de las bases de datos en el RNBD por parte del responsable, cuando se presenten cambios sustanciales o por orden de la SIC.

Aplicación. La organización a través del responsable y/o encargado del tratamiento de la información o los datos, debe establecer un procedimiento para la actualización de las bases de datos registradas en el registro nacional de bases de datos, evitando con esto cualquier omisión de la organización, ya que es probable que conforme se agreguen nuevos servicios se hará necesito recolectar información de agentes de tratamiento (clientes, proveedores, colaboradores).

Modelo. La siguiente plantilla es un referente para la aplicación del control dentro de las organizaciones.

ORGANIZACIÓN XXX
PROCESO DE TRATAMIENTO DE DATOS

Procedimiento: Actualización de bases de datos en el registro nacional de bases de datos.
Objetivo: Inscribir nuevas bases de datos en el RNBD o actualizar los registros de las bases e datos ya registradas en el portal.
Alcance: La información recolectada con fines de tratamiento, a través de la autorización del titular.

ACTIVIDADES.

a) Solicitud de aprobación para la recolección de datos personales

Funcionario/ Dependencia	Responsable Tratamiento	Observaciones
Act 1.1 Solicitud para la recolección de datos personales para XX fin		
	Act 1.2 Validación de la solicitud	
	Act 1.3 Verificación del tipo de datos a recolectar	
	Act 1.4 Aprobación y/o denegación de la solicitud y notificación al solicitante	

b) Revisión periódica de las bases de datos registradas

	Act 2.1 Revisión periódica de las bases de datos registradas	Punto de control (PC) El tiempo de revisión periódica es trimestral
	Act 2.2 De ser necesario realizar la	

respectiva
actualización en el
portal del RNBD

Dominio #7. Seguridad de los datos.

Control 7.1 Buenas prácticas para la seguridad de la información.

Descripción. Implementar o gestionar la adopción de estándares o buenas prácticas para garantizar la seguridad de la información de la organización.

Aplicación. La organización debe establecer medidas para la protección de su información, es decir, establecer procesos de seguridad de la información que permiten a su vez de un adecuado tratamiento de datos, garantizar la confidencialidad, integridad y disponibilidad de la misma, con el fin de mitigar los riesgos a los que se expone a diario la información de los titulares.

Se recomienda la apropiación de metodologías, guías o buenas prácticas nombradas en el proyecto de investigación, entre las de mayor aceptación e implementación se encuentran: la ISO/IEC 27002, la guía de la industria de tarjetas de pago PCI-DSS (Estándar de seguridad de datos), el informe NIST SP.800-53r4A, los controles del centro de seguridad de internet, versión 7 en español o 7.1 en inglés.

Vigilancia Normativa. El tercer y último elemento de la metodología de implementación del compendio de controles, consiste en la vigilancia permanente de los aspectos legales y normativos que rigen la privacidad de la información o el tratamiento de datos. En el aspecto

legal se analizan los cambios que se puedan presentar en Colombia, previstos en expedición de nuevas leyes o en la modificación o derogación de los artículos de las ya existentes, así como el seguimiento a las actuaciones de la superintendencia de industria y comercio y el superintendente delegado para la protección de datos personales. A demás de realizar vigilancia a las tendencias internacionales en buenas prácticas para la privacidad de la información y el tratamiento de datos; por ejemplo, las disposiciones que den organismos como la AEPD agencia española de protección de datos, y el SEPD supervisor europeo de protección de datos.

Figura 21. Ciclo de vigilancia en Protección de los Datos
Fuente. Autor del proyecto

4.4.2 Selección de la entidad donde se validará la metodología. El trabajo de investigación además de formular un compendio de controles para el cumplimiento de la normativa colombiana, referente a la privacidad de la información, o al tratamiento de datos personales, aplica los conceptos en una organización que cumpla con las características para la aplicación de los controles. Se toma para la aplicación de la metodología una entidad pública de Colombia, en particular la Corporación autónoma Regional de la Frontera Nororiental – CORPONOR.

Historia. Corponor es una entidad pública de orden territorial, creada mediante el decreto 3450 del 17 de diciembre de 1983 durante el gobierno de Belisario Betancourt, sus principales funciones en esa época eran "fomentar, coordinar, ejecutar y consolidar el desarrollo económico y social de la región comprendida dentro de su jurisdicción y con algunas funciones de administración de los recursos naturales y del Medio Ambiente". Posteriormente con la expedición de la ley 99 de 1993 la entidad transforma sus funciones, pasando a ser un Corporación autónoma, teniendo como jurisdicción el departamento de Norte de Santander, cuya función principal es ser la autoridad ambiental, de acuerdo con la normatividad establecida por el ministerio del medio ambiente y desarrollo sostenible.

Infraestructura. Su sede principal se encuentra ubicada en la ciudad de Cúcuta en la calle 13 Av. El bosque Nº 3E-278 Br Caobos, es conocida por su particular estructura, ya que al interior de sus instalaciones están divididas por una cuenca artificial, que asemeja a un caudal, además cuenta con variedad de peces y algunos ejemplares de iguanas y tortugas. Cuenta con locaciones en tres regiones del departamento, ubicadas en los municipios de Ocaña, Tibú y Pamplona.

Misión y Visión. La misión de la entidad es "Ejercer la autoridad ambiental propendiendo por el desarrollo humano sostenible, promoviendo la gestión ambiental colectiva y participativa en el departamento Norte de Santander." Y su visión "Ser en el 2019 la entidad reconocida, respetada y de referencia obligatoria para la toma de decisiones que orienten el desarrollo humano sostenible del departamento Norte de Santander."

Director general. El director general de la corporación es elegido para un período de cuatro (4) años, la elección de esta dignidad es efectuada por los miembros que integran en el consejo directivo, conformado por 12 miembros de diversos sectores; (1) representante de la presidencia de la república, (1) representante del ministerio del medio ambiente, (4) alcaldes representantes de la asamblea corporativa (2) representantes de los gremios, (2) representantes de ONG'S ambientalistas, (1) representante de las comunidades indígenas.

Organigrama. La estructura organizacional de la Corporación Autónoma Regional de la Frontera Nororiental es encabezada por la asamblea corporativa, posteriormente por el consejo directivo, seguido del director general. Cuenta con un secretario general, siete (7) subdirecciones, tres (3) oficinas y tres (7) direcciones territoriales.

Figura 22. Estructura organizacional Corponor.
Fuente. CORPONOR

Sistemas de gestión. Corponor se encuentra certificada en la adopción e implementación de varias normas de gestión, tales como ISO 9001:2015, ISO 14001:2015 y OSHAS 18001, esto

brinda un marco de madurez importante para la vinculación de los controles de privacidad o tratamiento de datos, facilitando su implementación. El sistema de gestión de corponor o SIGESCOR es un sistema integral que abarca principalmente las tres normas mencionadas anteriormente, establece los procesos estratégicos, misionales, de apoyo y de evaluación, a continuación la siguiente figura ilustra el mapa de procesos de la entidad.

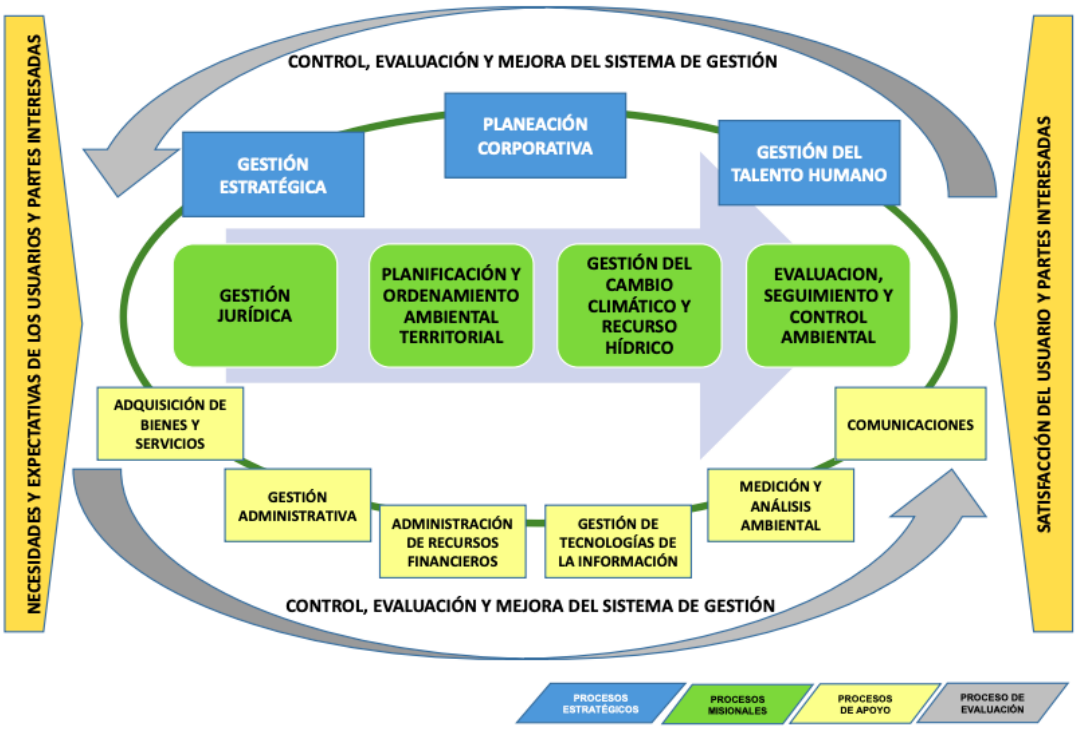


Figura 23. Mapa de procesos del sistema de gestión
Fuente. Sistema de gestión de Corponor, SIGESCOR.

4.4.3 Implementación de la metodología en la entidad seleccionada para la aplicación de los controles base. Como actividad final, el presente proyecto de investigación aplica la metodología diseñada, en la Corporación autónoma regional de la frontera nororiental, una entidad pública de orden regional, quién es la encargada de ejercer la autoridad ambiental en el departamento de Norte de Santander, comprendiendo todos sus municipios.

Condiciones internas.

Liderazgo. La Corporación autónoma regional de la frontera nororiental – CORPONOR, se encuentra en el proceso de diseño del nuevo plan de acción institucional para el cuatrienio 2020-2024, donde uno de los puntos fundamentales a establecer y formalizar es la gestión de la seguridad y privacidad de la información; donde el tratamiento de datos personales es parte esencial. Por ende, la organización a través del director general y la subdirectora de planeación y fronteras manifiestan el expreso compromiso de la alta dirección en la gestión de la privacidad de los datos.

Definición del alcance. La Corporación Autónoma Regional de la frontera nororiental en cumplimiento de la Ley 1581 de 2012, el Decreto reglamentario 1377 de 2013 y las demás disposiciones complementarias para la protección de datos personales, respecto a la recolección, uso, almacenamiento, circulación y supresión de todas aquellas actividades que contribuyan al tratamiento de datos personales, se permite adoptar las distintas buenas prácticas para la protección de datos personales en todos sus procesos de gestión y calidad.

Planeación y gestión (PHVA). La Corporación autónoma regional para la frontera nororiental – CORPONOR, incluirá la protección de los datos en sus procesos de control interno y de sistemas de gestión; de la misma manera como se viene haciendo con los procesos de calidad, de seguridad y salud en el trabajo y control ambiental, vinculando sus actividades con la designación de auditorías internas y de seguimiento de a los indicadores de gestión, asociados a la privacidad de los datos.

Guía de implementación (aplicación del compendio de controles). El proceso de implementación de la guía se encuentra en desarrollo, la Corporación Autónoma regional está en el proceso de construcción de su plan de acción institucional para el próximo cuatrienio, lo que genera un cronograma de implementación a mediano plazo, sin embargo, ya se encuentran diseñados y definidos los principales requerimientos.

CORPONOR

República de Colombia
Sistema Nacional Ambiental SINA
Ministerio de Ambiente y Desarrollo Sostenible
Corporación Autónoma Regional de la Frontera Nororiental

ISO 9001: 2015
ISO 14001: 2015
OHSAS 18001: 2007
NTC GP 1000: 2009
BUREAU VERITAS Certification

San José de Cúcuta, 07 de febrero de 2019

Señores
MAESTRÍA GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN
UFPSO
Ocaña

Asunto: Certificación de labores

Cordial Saludo.

La Corporación Autónoma Regional de la Frontera Nororiental – CORPONOR, se permite informar que el ingeniero de sistemas **JESÚS ANDRÉS OVALLOS OVALLOS,** se encuentra desarrollando actualmente las actividades relacionadas al proyecto de grado "METODOLOGÍA DE GESTIÓN DE CONTROLES DE PRIVACIDAD DE LA INFORMACIÓN, BASADA EN LA NORMATIVA LEGAL COLOMBIANA", contando con todo el apoyo institucional para lograr una exitosa implementación en la corporación.

Atentamente,

MELVA YANETH ÁLVAREZ VARGAS
Subdirectora de Planeación y Fronteras

Figura 24. Certificación de implementación de la metodología en CORPONOR.
Fuente. Autor del proyecto

Dominio #1. Contexto de la Organización. El primero dominio del compendio de controles establecido en la metodología propuesta; se cumple en CORPONOR implementando el comité de Privacidad y tratamiento de datos personales, asignando los roles del responsable y encargado del tratamiento de datos y vinculando los procesos del tratamiento de datos en el sistema de gestión en el mapa de procesos.

A través de un proyecto de acuerdo, la Corporación autónoma regional de la frontera nororiental, definirá el comité de privacidad de la información y tratamiento de datos personales, el cual estará conformado por los siguientes integrantes: El director general, el secretario general, un representante de cada subdirección, un responsable de cada oficina, y el responsable o encargado delegado para el tratamiento de datos personales. A continuación, se detalla el proyecto de acuerdo y el mapa de procesos actualizados con la vinculación del tratamiento de datos personales en el sistema de gestión de la entidad.

CORPONOR

REPÚBLICA DE COLOMBIA
SISTEMA NACIONAL AMBIENTAL SINA"
MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

CORPORACIÓN AUTÓNOMA REGIONAL DE LA FRONTERA NORORIENTAL – CORPONOR

Resolución No de

"Por la cual se reglamenta el comité de Protección y Tratamiento de Datos Personales"

EL DIRECTOR GENERAL

En uso de sus facultades constitucionales y legales, en especial, las concedidas en el artículo 29 de la Ley 99 de 1993, y

CONSIDERANDO

Que conforme al contenido de la Ley 1581 de 2012 por medio de la cual se dictan disposiciones generales para la protección de datos personales y el Decreto 1377 de 2013 por el cual se reglamenta de manera parcial la ley 1581 de 2012, las entidades deben adoptar dentro de sus procesos, políticas de protección de datos personales.

Que según la ley 1712 de 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", las entidades públicas deben crear procedimientos para la publicación, acceso a la información y creación de mecanismos de transparencia en el manejo de la misma.

Que de conformidad con el Decreto 103 de 2015, compilados en los decretos únicos reglamentarios 1080 y 1081 de 2015; por la cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones, la Corporación Autónoma Regional de la Frontera Nororiental – CORPONOR, debe identificar sus activos de información; de igual manera, debe establecer índices de información clasificada y reservada, esquemas de publicación de la información y políticas de gestión de la misma, entre otras obligaciones.

Que la LEY ESTATUTARIA 1581 DE 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", 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.

Que, en virtud de lo expuesto, se hace necesario implementar el comité de Protección y tratamiento de datos personales, con el objeto de reglamentar las actividades que este tema pueda generar para la corporación,

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1° Adopción: La Corporación Autónoma Regional para la Frontera Nororiental CORPONOR, en cumplimiento de la Ley 1581 de 2012, el Decreto reglamentario 1377 de 2013 y las demás disposiciones complementarias para la protección de datos personales, respecto a la recolección, uso, almacenamiento, circulación y supresión de todas aquellas actividades que contribuyan al tratamiento de datos personales, se permite informar a continuación los lineamientos generales en el presente documento.

ARTÍCULO 2°. CREACIÓN DEL COMITÉ DE PROTECCIÓN Y TRATAMIENTO DE DATOS: La Corporación Autónoma Regional de la frontera Noriental – CORPONOR, se permite crear y reglamentar el comité de Protección y Tratamiento de datos personales, quién será la máxima autoridad institucional en la toma de decisiones relacionadas a la privacidad y tratamiento de datos personales.

ARTÍCULO 3°. INTEGRANTES DEL COMITÉ: El comité de privacidad de la información y tratamiento de datos personales, estará conformado por los siguientes integrantes: El director general, el secretario general, un representante de cada subdirección, un responsable de cada oficina, y el responsable o encargado delegado para el tratamiento de datos personales.

ARTICULO 4°. DEFINICIONES: Para las actividades ejercidas por el comité de protección y tratamiento de datos personales, serán aplicables las siguientes definiciones consagradas en la Ley 1581 de 2012.

a) **Titular:** Persona Natural cuyos datos personales sean objeto de tratamiento.

b) **Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

c) **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

d) **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

ARTICULO 5°. FUNCIONES DEL COMITÉ: El comité de Protección y tratamiento de datos personales, tendrá a su cargo las siguientes funciones, con el fin de garantizar las disposiciones establecidas en la ley 1581 de 2012.

a) Fungir institucionalmente como el mecanismo delegado por la alta dirección, para garantizar la implementación de las disposiciones legales exigidas para el tratamiento de datos personales.

b) Vigilar la integración de los controles diseñados para el tratamiento de datos personales con el sistema integrado de gestión (SIGESCOR) de la entidad.

c) Delegar el área, proceso o funcionario que se desempeñará como RESPONSABLE del tratamiento de datos en la entidad.

d) Delegar el área, proceso o funcionario que se desempeñará como ENCARGADO del tratamiento de datos en la entidad.

e) Diseñar y establecer las funciones y actividades que desempeñarán tanto el RESPONSABLE como el ENCARGADO de tratamiento de datos personales.

f) Realizar el seguimiento a los hallazgos y no conformidades detectadas en los procesos de control interno y auditorías internas desarrolladas en la entidad.

g) Demás disposiciones que se puedan generar producto de la aplicación y cumplimientos de las exigencias normativas y legales

ARTÍCULO 4°. RESPONSABLES Y ENCARGADOS DE LA INFORMACIÓN EN LA CORPORACIÓN: La Corporación Autónoma Regional de la Frontera Nororiental - CORPONOR es la Responsable general del Tratamiento de la información que reposa en las bases de datos de cada una de las áreas que la conforman, liderado por la Subdirección de Planeación y Fronteras a través del proceso de apoyo de administración de sistemas de información quién fungirá como encargado del tratamiento, o a quien el comité de protección y tratamiento de datos delegue.

ARTÍCULO 5°. DEBERES DE LOS RESPONSABLES DE LA INFORMACIÓN: La Corporación Autónoma Regional de la Frontera Nororiental - CORPONOR como responsable de la información

presenta los siguientes deberes a su cargo:

a) Garantizar al titular, en todo tiempo, el pleno y efectivo derecho de Hábeas Data.

b) Solicitar y conservar, copia de la autorización otorgada por el Titular.

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

e) Rectificar la información cuando ésta sea incorrecta y comunicar lo pertinente a cada encargado del Tratamiento de información.

f) Tramitar las consultas y reclamos formulados en los términos señalados en la Ley 1581 de 2012.

g) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella

ARTÍCULO 6°. DEBERES DE LOS ENCARGADOS DE LA INFORMACIÓN

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo derecho del Habeas Data.

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos señalados en la Lay 1581 de 2012.

d) Actualizar las novedades sobre la información reportada por los Titulares de los datos dentro de los (5) días hábiles contados a partir de su recibo.

e) Tramitar las consultas y reclamos formulados por los Titulares en los términos señalados en la Ley 1581 de 2012.

f) Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la superintendencia de industria y comercio.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

RAFAEL NAVI GREGORIO ANGARITA LAMK

Nombres y Apellidos		*Cargo*	*Firma*
Revisó:	*Melva Yaneth Álvarez Vargas*	*Subdirectora de Planeación y Fronteras*	
Elaboró:	*Luis Omar Suescún Armesto*	*Asesor*	
Elaboró:	*Jesús Andrés Ovallos Ovallos*	*Profesional Contratista*	
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las disposiciones legales y/o técnicas vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma del Remitente.			

Figura 25. Mapa de procesos Corponor, con privacidad de la información
Fuente. Autor del proyecto

Dominio #2. Políticas de Tratamiento. El segundo dominio del compendio de controles establecido en la metodología de implementación, se cumple con la implementación de la política institucional de tratamiento de datos personales, la cual ya se encuentra vigente y publicada en la entidad, dando cumplimiento a los tres controles establecidos en este dominio. A continuación, se publican las evidencias que demuestran la implementación de dichos controles.

REPÚBLICA DE COLOMBIA
SISTEMA NACIONAL AMBIENTAL SINA"
MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

CORPORACIÓN AUTÓNOMA REGIONAL DE LA FRONTERA NORORIENTAL – CORPONOR

Resolución No de

"Por la cual se expide la Política de Protección y Tratamiento de Datos Personales"

EL DIRECTOR GENERAL

En uso de sus facultades constitucionales y legales, en especial, las concedidas en el artículo 29 de la Ley 99 de 1993, y

CONSIDERANDO

Que conforme al contenido de la Ley 1581 de 2012 por medio de la cual se dictan disposiciones generales para la protección de datos personales y el Decreto 1377 de 2013 por el cual se reglamenta de manera parcial la ley 1581 de 2012, las entidades deben adoptar dentro de sus procesos, políticas de protección de datos personales.

Que según la ley 1712 de 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", las entidades públicas deben crear procedimientos para la publicación, acceso a la información y creación de mecanismos de transparencia en el manejo de la misma.

Que de conformidad con el Decreto 103 de 2015, compilados en los decretos únicos reglamentarios 1080 y 1081 de 2015; por la cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones, la Corporación Autónoma Regional de la Frontera Nororiental – CORPONOR, debe identificar sus activos de información; de igual manera, debe establecer índices de información clasificada y reservada, esquemas de publicación de la información y políticas de gestión de la misma, entre otras obligaciones.

Que la LEY ESTATUTARIA 1581 DE 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", 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.

Que, en virtud de lo expuesto, se hace necesario implementar unas políticas de tratamiento de datos personales, con el objeto de ajustar el manejo de este tema al interior de la corporación, según el marco normativo anteriormente enunciado.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1° Adopción: La Corporación Autónoma Regional para la Frontera Nororiental CORPONOR, en cumplimiento de la Ley 1581 de 2012, el Decreto reglamentario 1377 de 2013 y las demás disposiciones complementarias para la protección de datos personales, respecto a la recolección, uso, almacenamiento, circulación y supresión de todas aquellas actividades que contribuyan al tratamiento de datos personales, se permite informar a continuación los lineamientos generales en el presente documento.

ARTICULO 2°. DEFINICIONES: Para la ejecución de la presente política y de conformidad con la normatividad legal, serán aplicables las siguientes definiciones consagradas en la Ley 1581 de 2012.

e) **Aviso de privacidad**: Comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

f) **Dato público**: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

g) **Datos sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, 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 biométricos.

h) **Datos biométricos** *Revista Seguridad Defensa Digital*. Por definición común, los datos biométricos son aquellos rasgos físicos, biológicos o de comportamiento de un individuo que lo identifican como único del resto de la población. Aquellos sistemas informáticos en los que se mide algún dato biométrico, como parte del proceso de identificación y/o autentificación de un sujeto, son conocidos como sistemas de seguridad biométrica o simplemente sistemas biométricos.

La siguiente lista son algunos ejemplos de datos biométricos:

- *Huellas dactilares*
- *Geometría de la mano*
- *Análisis del iris*
- *Análisis de retina*
- *Venas del dorso de la mano*
- *Rasgos faciales*
- *Patrón de voz*
- *Firma manuscrita*
- *Dinámica de tecleo*
- *Cadencia del paso al caminar*
- *Análisis gestual*
- *Análisis del ADN*

i) **Transferencia**: La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

j) **Transmisión**: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

k) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre los datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

l) **Dato personal**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

m) **Base de datos**: Conjunto organizado de datos personales que sea objeto de tratamiento.

n) **Titular:** Persona Natural cuyos datos personales sean objeto de tratamiento.

o) **Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

p) **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

q) **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

ARTÍCULO 3° PRINCIPIOS: La Corporación Autónoma Regional de la Frontera Nororiental - CORPONOR, estructura su Política de Protección de datos con base en los siguientes principios:

a) **Principio de legalidad:** El tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que se desarrollen.

b) **Principio de finalidad:** El Tratamiento de la información en la Corporación Autónoma Regional de la Frontera Nororiental - CORPONOR obedece a una finalidad legítima de acuerdo con la Constitución y la Ley, el cual se enmarcará en el manejo de la información para actividades relacionadas con su objeto social.

c) **Principio de libertad:** El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del titular. los datos personales no podrán ser obtenidos o divulgados sin previa autorización.

d) **Principio de veracidad o calidad:** La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.

e) **Principio de transparencia:** En el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, información sobre los datos que reposen en sus bases de datos que le conciernan.

f) **Principio de acceso y circulación restringida:** 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, en este sentido el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o

personas previstas en la 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 conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.

g) **Principio de seguridad:** La información sujeta a Tratamiento 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.

h) **Principio de confidencialidad:** Todas las personas que intervienen en el Tratamiento de datos están obligadas a garantizar la reserva de la información, inclusive una vez finalizada su relación con alguna de las labores que comprende el tratamiento.

ARTÍCULO 5°: DERECHOS DE LOS TITULARES: Los Titulares de datos personales que reposen en las bases de datos de la Corporación Autónoma Regional de la Frontera Nororiental - CORPONOR son los siguientes:

a) **Derecho a conocer, actualizar y rectificar sus datos personales**: Los Titulares de datos personales podrán ejercer este derecho frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error o aquellos cuyo tratamiento este expresamente prohibido o no ha sido autorizado.

b) **Derecho a solicitar prueba de la autorización**: Los Titulares de datos personales podrán solicitar prueba de la autorización otorgada para el Tratamiento de sus datos, de conformidad con lo previsto en el artículo 9 de la Ley 1581 de 2012. Se exceptúan de esta obligación los datos señalados en el artículo 10 de esta Ley.

c) **Derecho a ser informado frente al uso que se le ha dado a sus datos personales:** Los Titulares de datos personales tienen derecho a conocer en cualquier momento el uso que se les ha dado a sus datos personales previa solicitud dirigida al Responsable de la información.

d) **Derecho a revocar la autorización y/o a solicitar la supresión del dato:** Los Titulares de datos personales podrán revocar la autorización otorgada a la Corporación Autónoma Regional de la Frontera Nororiental - CORPONOR para el Tratamiento de sus datos personales, si evidencia que no han sido respetados los principios, derechos y garantías constitucionales y legales.

e) **Derecho a acceder a sus datos personales:** Los Titulares de datos personales podrán acceder de forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

ARTÍCULO 6° FINALIDAD DE LA RECOLECCIÓN DE DATOS PERSONALES Y TRATAMIENTO DE LOS MISMOS: CORPONOR podrá hacer uso de los datos personales para:

a) Ejecutar la relación contractual existente con sus usuarios, proveedores y trabajadores, incluida el pago de obligaciones contractuales.

b) Proveer los servicios y/o los productos requeridos por sus usuarios.

c) Informar sobre nuevos productos o servicios y/o sobre cambios en los mismos.

d) Evaluar la calidad del servicio.

e) Realizar estudios internos sobre hábitos de consumo.

f) Enviar al correo electrónico, celular o dispositivo móvil, vía mensajes de texto (SMS y/o MMS) o a través de cualquier otro medio análogo y/o digital de comunicación creado o por crearse, información comercial, publicitaria o promocional sobre los servicios, eventos y/o promociones, con el fin de impulsar, invitar, dirigir, ejecutar, informar y de manera general, llevar a cabo campañas, o concursos de carácter educativo, ambiental o publicitario, adelantados por CORPONOR y/o por terceras personas.

g) Desarrollar el proceso de selección, evaluación, y vinculación laboral.

h) Soportar procesos de auditoría interna o externa.

i) Registrar la información de empleados y/o pensionados (activos e inactivos) en las bases de datos de CORPONOR.

j) Los indicados en la autorización otorgada por el titular del dato o descritos en el aviso de privacidad respectivo, según sea el caso.

k) Suministrar, compartir, enviar o entregar sus datos personales a empresas filiales o vinculadas a CORPONOR en el evento que dichas compañías requieran la información para los fines aquí indicados.

Respecto de los datos (i) recolectados directamente en los puntos de seguridad, (ii) tomados de los documentos que suministran las personas al personal de seguridad y (iii) obtenidos de las videograbaciones que se realizan dentro o fuera de las instalaciones de CORPONOR, éstos se utilizarán para fines de seguridad de las personas, los bienes e instalaciones de CORPONOR y podrán ser utilizados como prueba en cualquier tipo de proceso.

Si un dato personal es proporcionado, dicha información será utilizada sólo para los propósitos aquí señalados, y por tanto, CORPONOR no procederá a vender, licenciar, transmitir, o divulgar la misma, salvo que: (i) exista autorización expresa para hacerlo; (ii) sea necesario para permitir a los contratistas o agentes prestar los servicios encomendados; (iii) sea necesario con el fin de proveer nuestros servicios y/o productos; (iv) sea necesario divulgarla a las entidades que prestan servicios de mercadeo en nombre de CORPONOR; (v) la información tenga relación con una fusión, consolidación, desinversión, u otro proceso de restructuración de la sociedad; (vi) que sea requerido o permitido por la ley.

CORPONOR podrá subcontratar a terceros para el procesamiento de determinadas funciones o información. Cuando efectivamente se subcontrate con terceros el procesamiento de información personal o se proporcione información personal a terceros prestadores de servicios, CORPONOR advierte a dichos terceros sobre la necesidad de proteger dicha información personal con medidas de seguridad apropiadas, se prohíbe el uso de la información para fines propios y se solicita que no se divulgue la información personal a otros.

ARTÍCULO 7° AUTORIZACIÓN Y CLASES DE DATOS:

1.1 Autorización

Con antelación y/o al momento de efectuar la recolección del dato personal, CORPONOR solicitará al titular del dato su autorización para efectuar su recolección y tratamiento, indicando la finalidad para la cual se solicita el dato, utilizando para esos efectos medios técnicos automatizados, escritos u orales, que permitan conservar prueba de la autorización y/o de la conducta inequívoca descrita en el artículo 7 del Decreto 1377 de 2013. Dicha autorización se solicitará por el tiempo que sea razonable y necesario para

satisfacer las necesidades que dieron origen a la solicitud del dato y, en todo caso, con observancia de las leyes que rigen sobre la materia.

1.2 Casos en los que no se requiere autorización del titular de los datos

La autorización del titular no será necesaria cuando se trate de:

- Datos de naturaleza Pública
- Casos de urgencia médica o sanitaria
- Tratamiento de información autorizado por la Ley para fines históricos, estadísticos o científicos.
- Datos Relacionados con el Registro Civil de las personas.

ARTÍCULO 8°. RESPONSABLES Y ENCARGADOS DE LA INFORMACIÓN EN LA CORPORACIÓN: La Corporación Autónoma Regional de la Frontera Nororiental - CORPONOR es la Responsable general del Tratamiento de la información que reposa en las bases de datos de cada una de las áreas que la conforman, liderado por la Subdirección de Planeación y Fronteras a través del proceso de apoyo de administración de sistemas de información, o a quien se delegue.

ARTÍCULO 9. POLÍTICA

a) CORPONOR realiza el tratamiento de Datos Personales en ejercicio propio de sus funciones legales y para el efecto no requiere la autorización previa, expresa e informada del Titular. Sin embargo, cuando no corresponda a sus funciones deberá obtener la autorización por medio de un documento físico, correo electrónico, mensaje de datos, Internet, sitio web, o también de manera verbal o telefónica o en cualquier otro formato que permita su posterior consulta a fin de constatar de forma inequívoca que sin el consentimiento del titular los datos nunca hubieran sido capturados y almacenados en medios electrónicos. Así mismo se podrá obtener por medio de conductas claras e inequívocas del Titular que permitan concluir de una manera razonable que este otorgó su consentimiento para el manejo de sus Datos Personales.

b) CORPONOR solicitará la autorización a los Titulares de los datos personales y mantendrá las pruebas de ésta, cuando en virtud de las funciones de promoción, divulgación y capacitación, realice invitaciones a charlas, conferencias o eventos que impliquen el tratamiento de datos personales con una finalidad diferente para la cual fueron recolectados inicialmente.

c) En consecuencia, toda labor de tratamiento de Datos Personales realizada en CORPONOR deberá corresponder al ejercicio de sus funciones legales o a las finalidades mencionadas en la autorización otorgada por el Titular, cuando la situación así lo amerite. De manera particular, las principales finalidades para el tratamiento de Datos Personales que corresponde a CORPONOR desarrollar en ejercicio de sus funciones.

d) El Dato Personal sometido a tratamiento deberá ser veraz, completo, exacto, actualizado, comprobable y comprensible. CORPONOR mantendrá la información bajo estas características siempre y cuando el titular informe oportunamente sus novedades.

e) Los Datos Personales solo serán tratados por aquellos funcionarios de CORPONOR que cuenten con el permiso para ello, o quienes dentro de sus funciones tengan a cargo la realización de tales actividades o por los Encargados.
f) CORPONOR autorizará expresamente al administrador de las bases de datos para realizar el tratamiento solicitado por el titular de la información.

g) CORPONOR no hará disponibles datos personales para su acceso a través de internet u otros medios masivos de comunicación, a menos que se trate de información pública o que se establezcan medidas técnicas que permitan controlar el acceso y restringirlo solo a las personas autorizadas por ley o por el titular.

h) Todo dato personal que no sea dato público se tratará por CORPONOR como confidencial, aun cuando la relación contractual o el vínculo entre el titular del dato personal y la CORPONOR haya finalizado.

i) Cada Subdirección, Jefatura, dependencia o área de CORPONOR debe evaluar la pertinencia de anonimizar los actos administrativos y/o documentos de carácter público que contengan datos personales, para su publicación.

j) El Titular, directamente o a través de las personas debidamente autorizadas, podrá consultar sus Datos Personales en todo momento y especialmente cada vez que existan modificaciones en las Políticas de Tratamiento de la información.

k) CORPONOR suministrará, actualizará, ratificará o suprimirá los Datos Personales a solicitud del Titular para corregir información parcial, inexacta, incompleta, fraccionada que induzca al error o aquella que haya sido tratada previa a la vigencia de la ley y que no tenga autorización o sea prohibida.

l) Cuando le sea solicitada información, ya sea mediante una petición, consulta o reclamo por parte del Titular, sobre la manera como son utilizados sus Datos Personales, CORPONOR deberá entregar dicha información.

m) A solicitud del Titular y cuando no tenga ningún deber legal o contractual de permanecer en las bases de datos de CORPONOR, los Datos Personales deberán ser eliminados. En caso de proceder una revocatoria de tipo parcial de la autorización para el Tratamiento de Datos personales para algunas de las finalidades de CORPONOR podrá seguir utilizando los datos para las demás finalidades respecto de las cuales no proceda dicha revocatoria.

n) Las políticas establecidas por la CORPONOR respecto al tratamiento de Datos Personales podrán ser modificadas en cualquier momento. Toda modificación se realizará con apego a la normatividad legal vigente, y las mismas entrarán en vigencia y tendrán efectos desde su publicación a través de los mecanismos dispuestos por CORPONOR para que los titulares conozcan la política de tratamiento de la información y los cambios que se produzcan en ella.

o) Los Datos Personales solo podrán ser tratados durante el tiempo y en la medida que la finalidad de su tratamiento lo justifique.

p) CORPONOR será más rigurosa en la aplicación de las políticas de tratamiento de la información cuando se trate del uso de datos personales de los niños, niñas y adolescentes asegurando la protección de sus derechos fundamentales.

q) CORPONOR podrá intercambiar información de Datos Personales con autoridades gubernamentales o públicas tales como autoridades administrativas, de impuestos, organismos de investigación y autoridades judiciales, cuando la soliciten en ejercicio de sus funciones con previa autorización legal correspondiente.

r) Los Datos Personales sujetos a tratamiento deberán ser manejados proveyendo para ello todas las medidas tanto humanas como técnicas para su protección, brindando la seguridad de que ésta no pueda ser copiada, adulterada, eliminada, consultada o de alguna manera utilizada sin autorización o para uso

fraudulento.

s) Cuando finalice alguna de las labores de tratamiento de Datos Personales por los trabajadores, contratistas o encargados del tratamiento, y aun después de finalizado su vínculo o relación contractual con CORPONOR, éstos están obligados a mantener la reserva de la información de acuerdo con la normatividad vigente en la materia.

t) CORPONOR divulgará en sus trabajadores, contratistas y terceros encargados del tratamiento las obligaciones que tienen en relación con el tratamiento de Datos Personales mediante campañas y actividades de orden pedagógico.

u) El Titular de los datos personales puede ejercer, principalmente, sus derechos mediante la presentación de consultas y reclamos ante CORPONOR, en su sede cuyo domicilio es la Calle 13 Av. El Bosque No. 3E-278 Barrio Caobos - Cúcuta - Norte de Santander y por el correo electrónico corponor@corponor.gov.co, indicando el tipo de trámite a llevarse a cabo con su información.

v) Cuando exista un Encargado del Tratamiento de Información de Datos Personales, CORPONOR deberá garantizar que la información que le suministra sea veraz, completa, exacta, actualizada, comprobable y comprensible. Adicionalmente le comunicará de manera oportuna todas las novedades a que haya lugar para que la información siempre se mantenga actualizada.

w) En el caso de existir un Encargado del Tratamiento de información de Datos Personales, la CORPONOR suministrará según el caso, información de Datos Personales únicamente cuyo Tratamiento realice en virtud de sus funciones legales y cuando excepcionalmente éstas no apliquen, con la autorización del Titular.

x) CORPONOR Informará al Encargado del Tratamiento de información de Datos Personales, de existir uno, cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

y) Cuando exista un Encargado del Tratamiento de información de Datos Personales, se exigirá que, en todo momento, se respeten las condiciones de seguridad y confidencialidad de la información del Titular establecidas por CORPONOR.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

RAFAEL NAVI GREGORIO ANGARITA LAMK

	Nombres y Apellidos	*Cargo*	*Firma*
Revisó:	*Melva Yaneth Álvarez Vargas*	*Subdirectora de Planeación y Fronteras*	
Revisó:	*Hilda Cristina Torres Castellanos*	*Profesional Especializado*	
Elaboró:	*Luis Omar Suescún Armesto*	*Asesor*	
Elaboró:	*Jesús Andrés Ovallos Ovallos*	*Profesional Contratista*	
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las disposiciones legales y/o técnicas vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma del Remitente.			

Dominio #3. Aviso de Privacidad. El tercer dominio del compendio de controles establecido en la metodología de implementación, detalla los controles enfocados al cumplimiento de las especificaciones relacionadas al aviso de privacidad, en el caso particular de los controles 3.2 y 3.3, estos se encuentran en procesos de implementación.

CORPONOR

AVISO DE PRIVACIDAD

La Corporación Autónoma Regional de la Frontera Nororiental - CORPONOR, con domicilio en la ciudad Cúcuta, se presenta y actúa como el responsable del tratamiento de datos personales, con la siguiente información de contacto:

a) Dirección de atención, Calle 13 Av. El Bosque No. 3E-278 Barrio Caobos - Cúcuta - Norte de Santander.
b) Correo electrónico corponor@corponor.gov.co
c) Teléfono 5828484.

Los datos recolectados, objeto de tratamiento, serán almacenados en nuestras bases de datos y serán utilizados de manera directa o indirecta a través de terceros aliados a la organización, teniendo como finalidad el cumplimiento del objeto y de los siguientes propósitos de Corponor:

a) Ejecutar la relación contractual existente con sus usuarios, proveedores y trabajadores, incluida el pago de obligaciones contractuales.

b) Proveer los servicios y/o los productos requeridos por sus usuarios.

c) Informar sobre nuevos productos o servicios y/o sobre cambios en los mismos.

d) Evaluar la calidad del servicio.

e) Desarrollar el proceso de selección, evaluación, y vinculación laboral.

f) Soportar procesos de auditoría interna o externa.

g) Registrar la información de empleados y/o pensionados (activos e inactivos) en las bases de datos de Corponor.

h) Los indicados en la autorización otorgada por el titular del dato o descritos en el aviso de privacidad respectivo, según sea el caso.

i) Suministrar, compartir, enviar o entregar sus datos personales a empresas filiales o vinculadas a Corponor, en el evento que dichas compañías requieran la información para los fines aquí indicados.

Corponor, les informa a los titulares de la información objeto de tratamiento, que pueden consultar la política de tratamiento de datos personales en su nivel de detalle, a través de la página web de la organización, así como los distintos procedimientos establecidos para el ejercicio de sus derechos de acceso, consulta, rectificación, actualización y supresión de los datos.

Dominio #4. Autorización de Tratamiento. El cuarto dominio del compendio de controles establecido en la metodología de implementación, especifica los controles relacionados a la recolección, almacenamiento y comunicación de la autorización de tratamiento de datos personales, la implementación de los controles se encuentra en la etapa del ciclo PHVA, planear y hacer, por lo tanto, no se han efectuado procesos de comunicación y mejora continua. Específicamente se da a entender que aún no se realiza el almacenamiento del aviso, es decir, los controles 4.2 y 4.3 se encuentran en proceso de implementación.

CORPONOR

CARTA DE AUTORIZACIÓN PARA EL USO Y ALMACENAMIENTO DE DATOS PERSONALES

Asunto: autorización para el uso y almacenamiento de datos personales

Dando cumplimiento a lo dispuesto en la ley 1581 de 2012, "Por el cual se dictan disposiciones generales para la protección de datos personales" y de conformidad con lo señalado en el Decreto 1377 de 2013, con la firma de este documento manifiesto que he sido informado por la Corporación Autónoma Regional de la frontera Nororiental (CORPONOR). NIT: 890505253-4 de lo siguiente:

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

b) Que me ha sido informada la(s) finalidad (es) de la recolección de los datos personales, la cual consiste en: Atención al ciudadano, Gestión de estadísticas internas, Gestión Administrativa, Gestión de clientes, Gestión de cobros y pagos, Gestión de facturación, Gestión tributaria y de recaudación, Procedimientos judiciales, Marketing, Publicidad propia, Comercio electrónico.

c) Es de carácter facultativo o voluntario responder preguntas que versen sobre datos sensibles o sobre menores de edad.

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

e) Los derechos pueden ser ejercidos a través de los canales dispuestos por
CORPONOR y observando la Política de Tratamiento de Datos Personales.
f) Mediante la página web de la entidad www.corponor.gov.co, a través del correo electrónico corponor@corponor.gov.co o al teléfono 5828484 podre radicar cualquier tipo de requerimiento relacionado con el tratamiento de mis datos personales.

g) CORPONOR garantizara la confidencialidad, libertad, seguridad, veracidad, transparencia, acceso y circulación restringida de mis datos y se reservara el derecho de modificar su Política de Tratamiento de Datos Personales en cualquier momento. Cualquier cambio será informado y publicado oportunamente en la página web.

h) Teniendo en cuenta lo anterior, autorizo de manera voluntaria, previa, explicita, informada e inequívoca a CORPONOR para tratar mis datos personales de acuerdo con su Política de Tratamiento de Datos Personales para los fines relacionados con su objeto y en especial para fines legales, contractuales, misionales descritos en la Política de Tratamiento de Datos Personales de CORPONOR.

i) La información obtenida para el tratamiento de mis datos personales la he suministrado de forma voluntaria y es verídica.

Se firma en la ciudad de _, a los días del mes de del año
Firma:
Nombre:
Identificación:

Dominio #5. Tratamiento de Datos. Se establecerán y formalizarán en la Corporación Autónoma Regional de la Frontera Nororiental – CORPONOR, el procedimiento “Recolección, uso, almacenamiento, circulación y supresión de datos” y la guía “ejercicio de los derechos de los titulares” dentro del proceso Gestión de la privacidad y seguridad de la información”.

Dominio #6. Registro Nacional de Bases de datos. El sexto dominio del compendio de controles establecido en la metodología de implementación, plantea los requerimientos necesarios para el cumplimiento de las disposiciones de ley, donde se establece que las

organizaciones o entidades de orden público deben registrar sus bases de datos físicas y digitales en el Registro Nacional de bases de datos.

Este proceso de registro de la organización y posterior ingreso de las bases de datos en la plataforma https://rnbd.sic.gov.co/, estuvo presidido de un conjunto de actividades desarrolladas en la entidad, que incluyó una fase diagnóstica de identificación de registros o bases de datos, dependencia por dependencia. A continuación, se demuestra el desarrollo de las actividades planteadas en los controles para este dominio.

Registro de la Entidad en el portal de la superintendencia para el RNBD.

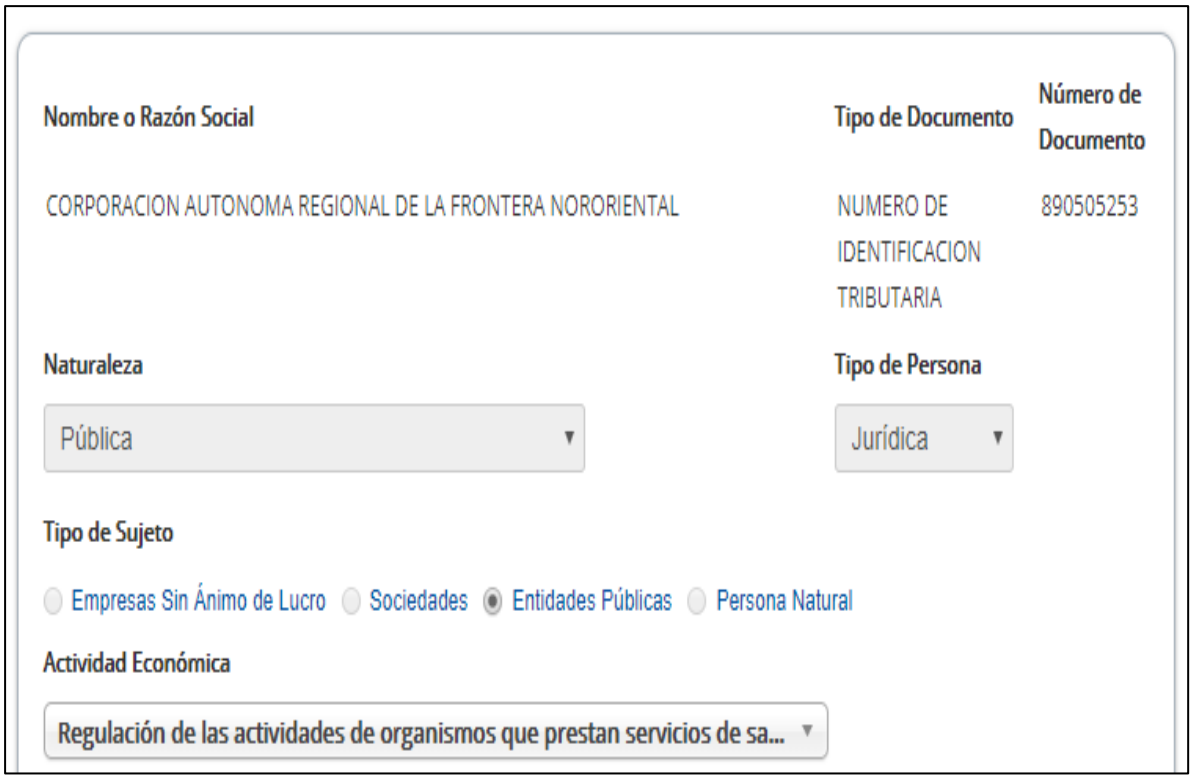


Figura 26. Evidencia registro de Corponor en el RNBD.
Fuente. Autor del proyecto

Registro de las bases de datos en el RNBD

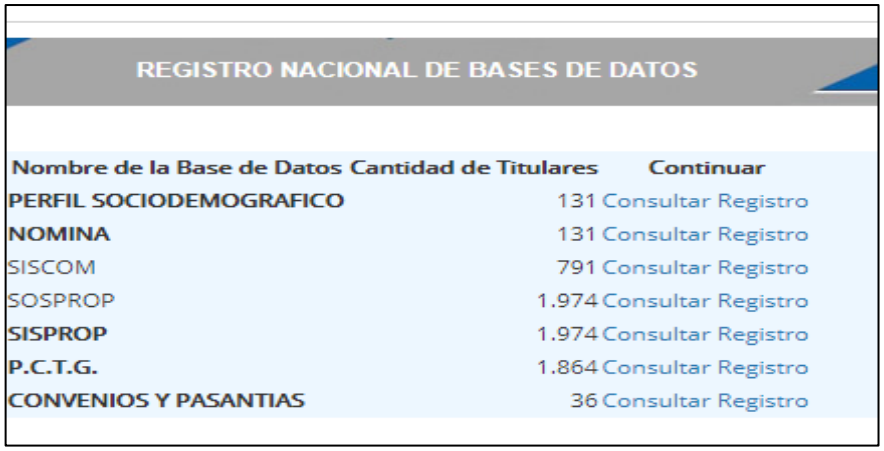


Figura 27. Evidencia de registro de bases de datos de CORPONOR en el RNBD.
Fuente. Autor del proyecto

Dominio #7. Seguridad de los datos. El séptimo dominio del compendio de controles establecido en la metodología de implementación, especifica que la organización, en este caso CORPONOR debe establecer buenas prácticas para la seguridad de la información. Para este requerimiento, Corponor como entidad pública se rige bajo las directrices dadas por el DAFP Departamento Administrativo de la Función pública y en el MinTIC - Ministerio de Tecnologías de la información. En cumplimiento de lo anterior CORPONOR, se encuentra implementando la política de Seguridad Digital y el Modelo de seguridad y privacidad de la información.

Actualmente se han desarrollo los siguientes documentos y estrategias y se encuentran anexos:

- Política de seguridad y privacidad de la información.
- Plan de seguridad y privacidad de la información.
- Plan de Tratamiento de riesgos de seguridad y privacidad de la información.
- Plan estratégico para el fortalecimiento de la infraestructura tecnológica.

Capítulo 5. Conclusiones.

Se logró realizar un proceso de identificación de estándares y metodologías relacionadas con la seguridad y privacidad de la información teniendo como referentes el estándar de seguridad de la industria de tarjetas de pago PCI-DSS, los controles del centro de seguridad de internet CIS Control, la familia ISO/IEC 27000, entre otros. Se identificó que los principios de privacidad o tratamiento de datos no se encuentran inmersos dentro de los estándares de seguridad, por lo tanto, cumplir con buenas prácticas de seguridad no garantiza el cumplimiento de los requisitos básicos de la privacidad de la información.

Los estándares de seguridad de la información tomados como referencia, permitieron construir la estructura básica para el establecimiento de controles de privacidad de la información. La revisión de las distintas normativas internacionales como el reglamento general para la protección de datos, los tratados internacionales como el convenio 108 de 1981, el tratado de Lisboa y la normativa nacional; evidencian un nuevo cambio de paradigma a la hora de regular, gestionar y controlar el tratamiento de datos personales en el mundo y Colombia.

Se diseñó un compendio de controles compuesto por siete dominios de privacidad, diseñados bajo las condiciones que establece la normativa colombiana. Estos fueron aplicados en la Corporación Autónoma Regional de la frontera Nororiental – CORPONOR, evidenciando la implementación de la guía sugerida en la metodología, demostrando la adopción de los requisitos de la ley 1581 de 2012, el decreto 1377 de 2013 y las disposiciones de la superintendencia de

industria y comercio. Se concluye que la metodología tuvo aceptación en el caso práctico propuesto, por la acreditación y aceptación recibida por la alta dirección de la entidad.

Capítulo 6. Recomendaciones

Se debe continuar con la implementación de la metodología de gestión de controles de privacidad, en las fases hacer, verificar y actuar del ciclo PHVA, con el fin de cumplir con todos los controles propuestos, garantizando el crecimiento en el nivel de madurez a través de la mejora continua.

Referencias

Ackerman, Sebastián; Com, S. (2013). *Metodología de la investigación*.

Andress, J. (2011). *What Is Information Security?* https://doi.org/10.1016/B978-1-59749-653-7.00001-3

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, *9*(1), 69–104. https://doi.org/10.1.1.85.3407

Computerworld. (2014). Forecast 2014: How to wring value from your IT budget.

Congreso de la república de Colombia. (2008). *Ley 1266 de 2008*. 1–9.

Congreso de la república de Colombia. *Ley 1273*. , (2009).

Congreso de la república de Colombia. *Ley 1581*. , (2012).

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162–176. https://doi.org/10.1016/j.cose.2014.12.006

Ernest Chang, S., & Lin, C. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, *107*(3), 438–458. https://doi.org/10.1108/02635570710734316

Europa, C. de. (1981). *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*.

Gehrmann, M. (2012). Combining ITIL , COBIT and ISO / IEC 27002 for structuring comprehensive information technology for management in organizations. *Navus - Revista de Gestao e Tecnologia.*, *2*, 66–77. https://doi.org/10.1109/AMS.2008.145

Guerrero, G. G. M. (2014). *Metodología de la Investigación* (Primera ed). México, D.F.: Grupo Editorial Patria.

Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la investigación. In *Journal of Chemical Information and Modeling* (Vol. 53). https://doi.org/10.1017/CBO9781107415324.004

Industria de Tarjetas de Credito PCI. (2016). *Requisitos y procedimientos de evaluación de Seguridad de Datos*.

ISO/IEC. (2015). *ISO/IEC 27002:2015 Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información*. (571).

ISO/IEC. (2017). *ISO/IEC 27000:2017 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información (SGSI). Visión general y vocabulario*. 39.

ISO. (2016). *ISO Survey of certifications to management system standards*. Retrieved from http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&vi%0AewType=1

Lerma, H. (2009). *Metodología de la investigación* (Cuarta edi). Bogotá.

Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, *30*, 803–814. https://doi.org/10.1016/j.cose.2011.07.003

Niño, M. (2011). *Investigación Diseño y ejecución*. Bogotá.

OEA, S. (2014). *Tendencias de seguridad cibernética en américa latina y el caribe*. 100. Retrieved from https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cybersecurity-%0Atrends-report-lamc.pdf

Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. (2013). *Norma Técnica Colombiana NTC-ISO/IEC 27001*. (571), 33.

Ross, R. S. (2014). *Assessing Security and Privacy Controls in Federal Information Systems and Organizations:* https://doi.org/10.6028/NIST.SP.800-53Ar4

Secure, S., & Secure, S. (2019). *Start Secure. Stay Secure. ® CIS Controls ™*. Retrieved from www.cisecurity.org/controls/

Trend Micro, & Oea. (2015). *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas*. 60. Retrieved from https://www.sites.oas.org/cyber/Certs_Web/OEA-Trend Micro Reporte Seguridad Cibernetica y Porteccion de la Inf Critica.pdf

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security. Fourth Edition*.