TRABAJO DE GRADO
MODELO DE PROTECCIÓN DE DATOS PERSONALES PARA UNA EMPRESA QUE CUMPLE EL ROL DE ENCARGADO

ANTONY FABIAN RODRIGUEZ RIOS
LUISA FERNANDA MAHECHA LESMES

UNIVERSIDAD CATÓLICA DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ D.C
2020

TRABAJO DE GRADO
MODELO DE PROTECCIÓN DE DATOS PERSONALES PARA UNA EMPRESA QUE CUMPLE EL ROL DE ENCARGADO

ANTONY FABIAN RODRIGUEZ RIOS
LUISA FERNANDA MAHECHA LESMES

Trabajo de grado presentado para optar al título de Especialista en Seguridad de la Información

Director
Alfonso Luque Romero
Magister

UNIVERSIDAD CATÓLICA DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ D.C
2020

TABLA DE CONTENIDO

Pág.

LISTA DE CUADROS

Pág.

LISTA DE FIGURAS

Pág.

1. INTRODUCCIÓN

El mundo se encuentra en la era de la información en la que los datos personales son la moneda del eje de actividades económicas, por este motivo las organizaciones se enfrentan al reto de proteger su información y cumplir con las normatividades vigente, así mismo, se centra en la ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales para empresas que cumplen el rol como encargado. Realmente, no es una ley para solo proteger la información personal, sino principalmente para exigir un tratamiento adecuado de los datos de las personas de manera que no se vulnere sus derechos.

Teniendo en cuenta las sanciones impuestas por la Superintendencia de Industria y Comercio por incumplimientos con el derecho de habeas data e incidentes se evidencia la necesidad de asegurar el cumplimiento frente al servicio que presta la compañía como encargada de la información personal. Dado lo anterior surge la necesidad de diseñar un modelo de protección de datos personales para una empresa que cumple el rol de encargada.

En este trabajo se brindan pautas con el objetivo de ayudar a las organizaciones a prepararse para el cumplimento de la ley 1581 de 2012 en protección de datos personales en el rol de encargado y de esta manera contar con la documentación básica requerida, además de identificar sus problemas de seguridad, riesgos y vulnerabilidades que le permitan tener un mejoramiento continuo logrando hacer que la protección de datos agregue valor para la organización, para esto se desarrollan seis fases que inicia en el diagnóstico, planeación, implementación, evaluación de riesgos, evaluación de desempeño y mejora continua, cada fase cuenta con elementos que ayudan a las organizaciones a entender cómo llevar a cabo cada una de estas.

Al finalizar este trabajo se encontrarán dos herramientas que apoyaran a las organizaciones con el rol de encargadas a realizar una auto evaluación de diagnóstico para ubicarse dentro del modelo de madurez propuesto y una matriz de riegos que apoyará toda la fase de gestión de los riesgos asociados a la protección de datos personales.

2. GENERALIDADES

1. LÍNEA DE INVESTIGACIÓN

El proyecto se encuentra dentro de la línea de Software Inteligente y Convergencia tecnológica.

2. PLANTEAMIENTO DEL PROBLEMA

Uno de los principales retos a los que se enfrentan las organizaciones es proteger sus datos personales, esto se debe al incremento de la información necesaria para la ejecución de los procesos de una organización y de las amenazas tanto internas como externas a la disponibilidad, confidencialidad e integridad de la misma, que pueden verse afectadas por atacantes que se aprovechen de vulnerabilidades, con el fin de obtener ilícitamente rentabilidad de estos; incluso, las organizaciones corren riesgo de empleados que por negligencia, desconocimiento o mala intención pueden afectar e impactar gravemente las operaciones, la imagen corporativa y su reputación.

Por esta razón se ha fortalecido la normatividad colombiana en los últimos años busca que las organizaciones protejan la información en todos sus frentes; en el 2012 el Congreso de la República de Colombia aprobó la ley 1581, por la cual se dictan disposiciones generales para la protección de datos personales. Esta ley es de obligatorio cumplimiento para entidad que cumplen el rol como encargadas, ya que al no acatar estas directrices se incurrirá en sanciones, hasta por un "equivalente 2000 SMLMV o al cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles"[1].

Teniendo en cuenta lo anterior, es de alta prioridad para la empresa gestionar los riesgos que afectan los datos personales en el servicio que presta de tercerización de nómina, además de este servicio, también ofrece servicios de auditoría y aseguramiento, consultoría, impuestos y servicios legales y que tiene presencia en toda Colombia y oficinas en Cali, Bogotá, Barranquilla y Medellín, en diversas industrias como los servicios financieros, turismo, salud, energía y recursos naturales, infraestructura y gobierno, y en el sector seguros, de una manera sistémica con el fin de reducir tanto la probabilidad de ocurrencia como el impacto que estos generan sobre la empresa a través de la definición de controles, estrategias y el monitoreo constante que permita mantener la continuidad del negocio.

[1] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá, 2012. no. 48.587, p. 12

2.1.1 ANTECEDENTES DEL PROBLEMA

En la actualidad en Colombia existen dos leyes en las cuales se ha reglamentado el derecho a la intimidad respecto al tratamiento de los datos personales:

En el año 2008 con ley 1266 “Habeas Data”, “… 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”[2].

Y en el 2012 con ley 1581, se regula la protección de datos personales en lo concerniente a la información de los ciudadanos en bases de datos y archivos. El objeto de la ley “es 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”[3]; a esta la regula la Superintendencia de Industria y Comercio la cual en lo últimos años ha sancionado a las organizaciones que cumple con el rol de responsables o encargadas por no cumplir con la normatividad con multas, en el 2018 impuso multas de un total de 5.723.806.408 millones de pesos y a julio de 2019 había impuesto mutas hasta por 7.148.168.221 millones de pesos.

Actualmente la organización como encargada de la información en el servicio que presta de tercerización de nómina no realiza la gestión de riesgos en el cual se definan, analicen, monitoricen y aseguren la protección de los datos personales en cuanto a su disponibilidad, integridad y confidencialidad que prevenga la materialización de los riesgos que ocasionen impacto negativo de carácter financiero o a la reputación de la organización mitigando los riesgos definidos hasta niveles aceptables de acuerdo al apetito de riesgo establecido. Por esta razón se establece la necesidad de definir un modelo de gestión de riesgos el cual se basará en estándares internacionales de Gestión de riesgos como metodología general, y la ley 1581 de 2012.

En este apartado muestre los desarrollos o investigaciones asociados a la temática que se han desarrollado previamente conservando la estructura histórica y diferenciándolos a nivel internacional, nacional, regional y/o local según el caso de aplicación.

---

[2] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 (31, diciembre 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. Bogotá, no. 47.219. p. 2

[3] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581, op. cit., p. 1

Para ello requiere la consulta de fuentes bibliográficas académicas, formales, apoye su investigación en las bases de datos digitales, libros, tesis, entre otros.

2.1.2 PREGUNTA DE INVESTIGACIÓN

¿Cómo asegurar el cumplimiento de la ley 1581 de protección de los datos en una empresa que asume el rol de encargado?

2.1.3 VARIABLES DEL PROBLEMA

• **Arreglo del incidente:** equivale al esfuerzo invertido en tiempo y dinero para la remediación del incidente, que está dada por la siguiente formula: tiempo total arreglo del incidente en horas por el número de colaboradores involucrados en el arreglo por la tarifa promedio hora mano de obra más pagos a terceros**.**

• **Aspectos legales:** Equivale al costo que se deriva de la afectación legal que se ocasione debido al incidente.

• **Multas:** Equivale al costo total real de las multas que se ocasionen por incumplimiento de la ley 1581 de 2012.

• **Afectación de imagen y reputación:** Equivale a la valoración del impacto del incidente en la imagen de la organización, debido a la perdida de la reputación y confianza fundamentalmente cuando el daño de la imagen afecta la relación con el cliente.

• **Costos por perdida de información o conocimiento:** Equivale al total de costos por perdida de información o conocimiento (cuando aplique).

3. JUSTIFICACIÓN

Teniendo en cuenta que en la actualidad las organizaciones usan datos personales como insumos fundamentales para casi todas sus actividades, esta información se ha convertido en un bien permanentemente comercializado con el fin de tomar e implementar decisiones de diversa naturaleza como económica, social, política, laboral, estadística, etc., por esta razón algunas empresas se dedican a venderlos, alquilarlos, analizarlos o sacar conclusiones a partir de los mismos.

En consecuencia, a esto, la regulación colombiana sanciona a las organizaciones que no conservan la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por este motivo se establece un modelo para asegurar el cumplimiento de la ley 1581 de 2012 artículo 18, el cual proporciona mejores prácticas que permiten a las organizaciones que cumplen con el rol de encargados de la información mejorar sus procesos e incrementar la confianza de sus clientes.

3. OBJETIVOS

1. OBJETIVO GENERAL

Generar un modelo que brinde lineamientos y buenas prácticas en la gestión de la protección de los datos personales, con base en la ley 1581, para una empresa que cumple el rol de encargada.

2. OBJETIVOS ESPECÍFICOS

- Definir las fases del modelo de protección de datos y las pautas que contribuyen a su implementación.

- Definir la herramienta y los criterios de evaluación de riesgos de protección de datos personales.

- Definir los criterios para el modelo de madurez de protección de datos personales.

4. MARCOS DE REFERENCIA

1. MARCO CONCEPTUAL

• **Titular:** persona natural cuyos datos personales sean objeto de Tratamiento"[4].

• **Tratamiento: c**ualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión" [5].

• **Datos personales:** es definido como cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"[6].

• **Datos públicos:** es aquel dato que no sea semiprivado, privado o sensible. Estos datos 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" [7]. Por ejemplo: datos relacionados con el estado civil de la persona, profesión u oficio a su calidad de comerciante o de servidor público, etc.

• **Datos semiprivados:** son datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios"[8]. Por ejemplo: datos financiero, crediticio, comercial, de servicios y provenientes de otros países, etc.

• **Datos privados:** "es el que por su naturaleza íntima o reservada sólo es relevante para el titular"[9]. Por ejemplo: Personas acogidas en programas de protección de testigos, victimas o en proceso penal, libros y papeles de comerciante, números telefónicos, direcciones correo electrónico personal, etc.

• **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, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derecho y garantías de partidos políticos de oposición así como los datos relativos a la salud a la vida sexual y los datos biométricos"[10].

---

[4] Ibíd., p. 2
[5] Ibíd., p. 2
[6] Ibíd., p. 2
[7] COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 1377 (27, junio 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Bogotá: La Presidencia, 2013. p. 2
[8] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581, Op. cit., p. 2
[9] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266, Op. cit., p., 1.
[10] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581, Op. cit., p. 3

• **Riesgos:** se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas. El nivel de riesgo se mide según su probabilidad de materializarse y el impacto que tiene en caso de hacerlo"[11].

• **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"[12].

• **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"[13].

• **Derecho de Hábeas Data:** es aquel que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivo y bancos de datos de naturaleza pública o privada"[14].

2. MARCO TEÓRICO

Este trabajo es fundamental identificar los tipos de datos personales; además, se debe verificar el cumplimiento de la legislación colombiana y contextualizar sobre los riesgos a los que está expuesto y el modelo de madurez de la organización que cumple el rol como encargado de la información. Es importante entender que los tipos de datos personales se clasifican como público, semiprivado, privado y sensibles como se explican a continuación (véase el Cuadro 1).

Cuadro 1. Clasificación de los Datos Personales

CLASIFICACIÓN	CATEGORIA
Público	•Datos generales de identificación de la persona. •Datos de ubicación relacionados con actividad comercial (Dirección, correo y teléfono empresarial).
Semiprivados	•Datos financieros. •Datos patrimoniales. •Datos de actividad económica.
Privados	•Datos de ubicación personal. •Datos socioeconómicos. •Datos tributarios. •Datos historia laboral. •Datos nivel educativo.

[11] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD [en línea]. Madrid: La Agencia [citado 2 mayo, 2020]. Disponible en Internet: <URL: https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf>

[12] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581, Op. cit., p. 4.

[13] Ibíd., p. 4

[14] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Manejo de información personal "Habeas data" [en línea]. Bogotá: La Superintendencia [citado 2 mayo, 2020]. Disponible en Internet: <URL: https://www.sic.gov.co/manejo-de-informacion-personal>

Cuadro 1. (Continuación)

CLASIFICACIÓN	CATEGORIA
	•Datos afiliación. •Datos sobre gustos y/o intereses particulares. •Fotografías y videos. •Datos de antecedentes.
Sensibles	•Datos biométricos de la persona. •Datos de descripción morfológica. •Datos relacionados con la salud. •Datos relacionados con el estado de salud. •Datos relacionados a pertenencias a sindicatos. •Datos relacionados organizaciones sociales. •Datos relacionados de derechos humanos, religiosas, políticas. •Datos de preferencia, orientación sexual, origen étnico-racial, etc. •Población en condición vulnerable. •Datos personas en discapacidad. •Datos acceso a sistemas de información. •Datos personales de niños, niñas o adolescentes sin autorización.

Fuente. Los Autores

Actualmente Colombia cuenta con dos leyes que reglamenta la protección de los datos, la primera es la ley 1266 de 2008 donde se evidenció deficiencia al momento proteger los datos personales diferentes a los de índole comercial y financiera, además no establece reglas obligatorias para la protección de los datos, y también para poder cumplir como un país seguro para autoridades europeas era necesaria la generación de una ley que contemplara la protección de los datos personales en todas las organizaciones del país, por esta razón nace la ley 1581 de 2012.

En el tratamiento de los datos se habla de tres actores como son el titular definido como "Persona natural cuyos datos personales sean objeto de tratamiento"[15], el responsable "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" [16] y el encardado "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"[17], por tanto este trabajo se centra en el papel que cumple la organización como encargada.

Los derechos como encargados de la información están contemplados en el artículo 18 de la ley 1581 de 2012, donde se deberá cumplir con las siguientes actividades:

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

- Conservar la información bajo las condiciones de seguridad necesarias para

[15] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581, op. cit., p. 4.
[16] Ibíd., p. 4
[17] Ibíd., p. 4

impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

•Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;

•Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;

•Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;

• 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;

• Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley;

• 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;

• Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;

• Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;

• 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;

• Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio[18].

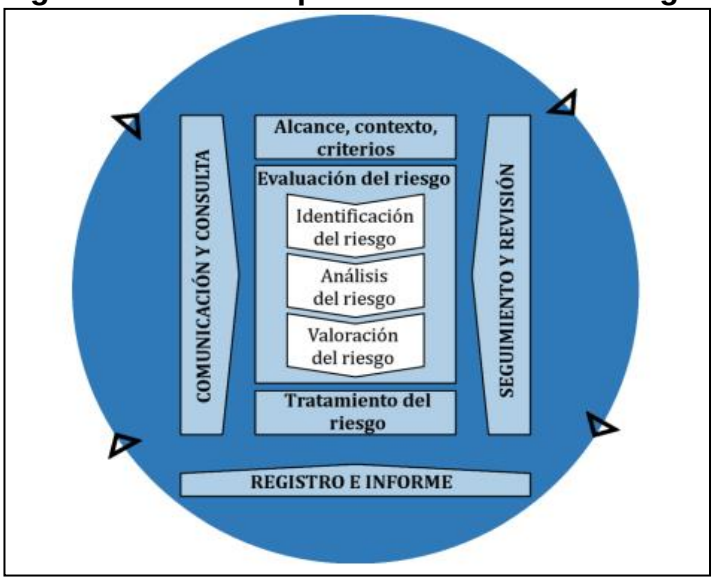
Seguidamente se utiliza como apoyo la norma ISO 27001 ya que esta brinda lineamientos para asegurar la confidencialidad, integridad y disponibilidad de la información, de igual manera se utiliza la 27002 la cual proporciona buenas prácticas o controles para la organización y la 27005 da un enfoque de gestión de riesgo, en este momento la organización se encuentra en proceso de certificación así que se busca alinearse a las política, controles y buenas prácticas del sistemas de seguridad de la información.

Finalmente, como marco general para realizar la gestión de riesgos este trabajo se basa en la NTC 31000. En esta norma, se usan las expresiones "gestión del riesgo" y "gestionar el riesgo". En términos generales, la "gestión del riesgo" se refiere a la

[18] Ibíd., artículo 18.

arquitectura (principios, marco y procesos) para a gestión eficaz del riesgo, mientras que "gestionar el riesgo" se refiere a la aplicación de esa arquitectura a riesgos particulares (véase la Figura 1).

Figura 1. Procesos para la Gestión del Riesgo



Fuente. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo: principios y directrices. NTC 31000. Bogotá: ICONTEC, 2018. p. 5

•**Identificación de activos:** en esta fase se identifica el conjunto de elementos que sostienen las actividades de la organización y que por su naturaleza se requiere un nivel de protección de acuerdo a su importancia en relación a los objetivos.

• **Evaluación del riesgo**: este proceso permite identificar las amenazas, los activos a los que pueden afectar junto con la identificación de vulnerabilidades de los activos valorados y el cálculo de la probabilidad de que ocurra y el impacto sobre los activos.

• **Tratamiento del riesgo**: en esta fase se establecen los controles que permitan mitigar el riesgo, pero que a su vez sean acordes al tipo de empresa y sus necesidades. El objetivo final es minimizar el riesgo al nivel que para la empresa sea aceptable.

El riesgo residual es el nivel de riesgo que queda después de la formulación de los controles, vulnerabilidad y amenazas relacionadas entre sí. Una vez identificado este riesgo residual el paso siguiente es identificar la manera más eficiente de reducirlo a un nivel aceptable definido por cada organización.
.

3. MARCO JURÍDICO

El marco jurídico cuenta de la siguiente normatividad colombiana:

•Ley 1266 del 31 de diciembre de 2008, “por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.

•Ley 1581 del 17 de octubre de 2012, “por la cual se disposiciones generales para la protección de datos personales”. Siguiendo la sentencia C-748 del 6 de octubre 2011 de la Corte Constitucional y el congreso de la Republica. Esta ley busca que las empresas que realizan tratamiento (Recolección, uso, almacenamiento, transferencia, supresión) de datos cumplan con unos deberes como responsable o encargados de la información.

•Decreto 1377 del 27 de junio de 2013, “por el cual se reglamenta parcialmente la ley 1581 de 2012”. Este decreto tiene como fin definir o explicar algunos términos o conceptos que no se incluyeron en la ley 1581 de 2012.

4. ESTADO DEL ARTE

Para el estado del arte del presente documento, se toma las referencias del repositorio de la biblioteca de la Universidad Católica de Colombia:

•”Regulación en materia de protección de datos personales o Habeas Data en Colombia a través de la Ley 1581 de 2012: Examen histórico y crítico sobre su ineficacia ante las administradoras de bases de datos, portales de Internet y motores de búsquedas”[19]

✓Objetivo: Regulación de protección de datos personales o Habeas en Colombia a través de la Ley 1581 de 2012.

✓Muestra: El documento nombra investigación frente a la línea de tiempo que ha tenido el crecimiento de la Ley de Protección de Datos Personales o Habeas Data, los motivos de la implementación de esta legislación en Colombia y la importancia que ha tenido para el sistema.

✓ Resultados: La legislación colombiana sea concentrada en proteger y vigilar a las organizaciones que tratan información personal de manera indebida, sancionar y penalizar uso abusivo de información. En el documento se encuentra referencia a

[19] RUÍZ, Betcy. Regulación en materia de protección de datos personales o Habeas Data en Colombia a través de la Ley 1581 de 2012: Examen histórico y crítico sobre su ineficacia ante las administradoras de bases de datos, portales de Internet y motores de búsquedas. Bogotá: Universidad Católica de Colombia. Faculta de derecho. Modalidad Trabajo de grado, 2016. p. 1

diferentes normatividades de la Unión Europe.

• “Evaluación de la gestión de riesgos del proceso de gestión humana en la empresa SUPPLA S.A. según la ley de 2012 y la ISO 31000”[20]

✓Objetivo: Evaluación de gestión de riesgos del proceso de gestión humana.

✓Muestra: En el trabajo identifica 31 bases de datos personales de titulares en el proceso de gestión humana, 13 de estas contienen datos de clasificación sensible, lo que equivale al 41% del total de las bases de datos.

✓ Resultados: Para el análisis de causas y consecuencias de la materialización del riesgo usaron la herramienta matriz de riesgos tomando como guía la NTC ISO 31000 Gestión del riesgo ya que esta permite clasificar y asignarles un estado de valoración dependiendo de su probabilidad de ocurrencia y el impacto. Además, se evidencia el uso de diferentes herramientas las cuales facilitaron la valoración de acciones correctivas y preventivas.

• “De la protección de datos personales en Colombia (Ley 1581 de 2012): un estudio comparado con el sistema canadiense”[21]

✓Objetivo: De la protección de datos personales en Colombia (Ley 1581 de 2012): un estudio comparado con el sistema canadiense. (María Paola Cuevas Rodríguez, 2016).

✓Muestra: Se evidencia los diferentes estudios que se realiza tanto a la legislación colombiana como la legislación canadiense, ya que Canadá se considera un país pionero en la protección de datos personales.

✓Resultados: En evidencia una comparación frente a las leyes de protección de datos que existen en Colombia y Canadá, teniendo en cuenta que este es reconocido como un país que cuenta con un nivel apropiado de protección de datos personales.

[20] MAHECHA, Luisa. Evaluación de la gestión de riesgos del proceso de gestión humana en la empresa SUPPLA S.A. según la ley de 2012 y la ISO 31000. Bogotá: Universidad Católica de Colombia. Faculta de Ingeniería. Modalidad Trabajo de grado, 2016. p. 1.

[21] RODRÍGUEZ, María. De la protección de datos personales en Colombia (Ley 1581 de 2012): un estudio comparado con el sistema canadiense. Bogotá: Universidad Católica de Colombia. Facultad de Derecho. Modalidad Trabajo grado, 201. p. 1

5. METODOLOGÍA

5.1 FASES DEL TRABAJO DE GRADO

Para la elaboración de este trabajo se llevará acabo las siguientes fases (véase el Cuadro 2).

Cuadro 2. Fases de Trabajo de Grado

FASES	ACTIVIDAD	MÉTODOS PROPUESTOS
Contexto de la PDP en Colombia.	Revisión documental de la normatividad colombiana actual en cuanto a protección de datos personales.	Consulta en páginas web y bases de datos de la Universidad. Legislación.
Consulta de estándares de gestión de riesgos.	Revisión de estándares internacionales que apoyen la gestión de riesgos asociados a la protección de datos personales.	Consulta de Guía Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD.
Definición de fases del modelo PDP.	Definir las siguientes fases del modelo de protección de datos personales para una empresa que cumple el rol de encargado: I. Diagnostico. II. Planeación. III. Implementación. IV. Evaluación de riesgos. V. Evaluación de desempeño. VI. Mejora continua.	Consulto el Modelo de seguridad y privacidad de la información MINTIC.
Definición de matriz de riesgos.	Definir de la matriz de riesgos de acuerdo con los criterios establecidos la identificación, evaluación, tratamiento y monitoreo de los riesgos en la protección de datos personales en el rol de encargado.	Consulta de normas ISO 31000, ISO 27001, 27005.
Definición de diagnóstico de madurez.	Definir la autoevaluación diagnostica del modelo de madurez frente a los deberes para el cumplimiento de PDP en el rol de encargado.	Ley 1581 de 2012. Guías publicadas por la SIC.
Entrega del modelo, matriz de riesgos y autoevaluación diagnostico modelo de madurez.	Entrega del modelo con las 6 fases definidas y la matriz de riesgos y autoevaluación diagnostico modelo de madurez.	Modelo de protección de datos personales para una empresa que cumple el rol de encargado. Matriz de riesgos. Autoevaluación diagnostico modelo de madurez.
Conclusiones finales.	Definir las conclusiones observadas resultantes del desarrollo de las anteriores fases.	Conclusiones.

Fuente. Los Autores

5.2 INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

•Se utilizará un a matriz de Excel donde se plantea un ejemplo de análisis de riesgo, en la que se encuentra una de matriz en la cual se llevará el registro de los riesgos identificados, la evaluación cualitativa y cuantitativa y los controles para cada uno de los riesgos junto con el seguimiento y monitoreo. También se incluirá una hoja

con la herramienta de mapa de calor utilizada para la priorización de los riesgos.

•Se utilizará una matriz de auto evaluación de diagnóstico de madurez con relación a los deberes para el cumplimiento de PDP en el rol de encargado.

•Para la documentación del modelo se utilizará Microsoft Word.

5.3 POBLACIÓN Y MUESTRA

Este proyecto está enfocado solo en empresas que cumplen el rol de encargados de la información de acuerdo con la ley 1581 de 2012.

5.4 ALCANCES Y LIMITACIONES

Este trabajo se centra en la definición de un modelo para las organizaciones que cuentan con el rol de encargado de la información frente a la ley 1581 de 2012.

6. PRODUCTOS A ENTREGAR

En este trabajo se entregará un modelo de protección de datos personales para una empresa que cumple el rol de encargado que se efectúa 6 fases, a continuación, un breve resumen de cada fase:

•Diagnóstico: su objetivo es apoyar a la organización a indagar en las bases de datos que tratan si son encargados de la información personal y que información trata y darle una clasificación, para esto se proponen unas tablas de guía que ayudara a la organización a investigar y clasificar su información.

•Planeación: busca dar una guía a la organización para abordar el cumplimiento del artículo 18 de la ley 1581 de 2012 como encargado, para esto se brinda una tabla donde se encuentra cada literal del articulo 18 y se proponen actividades específicas para dar cumplimiento al mismo.

•Implementación: brinda guías documentadas para la adopción por parte de la organización con el fin de dar cumplimiento al artículo 18. De acuerdo con las actividades propuestas en la fase de planeación, a continuación, se listan las siguientes guías:

✓Propuesta de documento de consulta y reclamos.

✓Propuesta de Bitácora de consulta y reclamos.

✓Tabla de validación de cumplimiento de medidas de seguridad de la información

✓Temas para incluir en el manual Interno en protección de datos personales de la compañía.

✓Tabla de validación de cumplimiento de la ley 1581 de acuerdo con las guías de documentos publicados por la SIC en su página Web.

•Evaluación de riesgos: con el fin de gestionar los riesgos asociados a la protección de datos personales en el rol de encargado se propone una metodología basada en la ISO 31000 e ISO 27005 la cual se apoya en una herramienta denominada Matriz de Riesgos en la cual se pueden desarrollar todas las fases de dicha metodología de una manera organizada intuitiva y sencilla.

•Evaluación de desempeño: tiene como fin informar a la organización de la importancia de la realización de auditorías, implementación y monitoreo de indicadores de gestión y adicionalmente se propone un modelo de madurez para medir el cumplimiento y gestión de los requisitos de la ley 1581 de 2012. Para esto se deja una guía de preguntas que ayudarán a la organización a realizar auditorías, además se incluyen ejemplos de indicadores a implementar y para el modelo de

madurez se explica cómo utilizar una herramienta que ayudará a la organización a posicionarse en una escala de acuerdo con su cumplimiento al artículo 18 de la ley 1581.

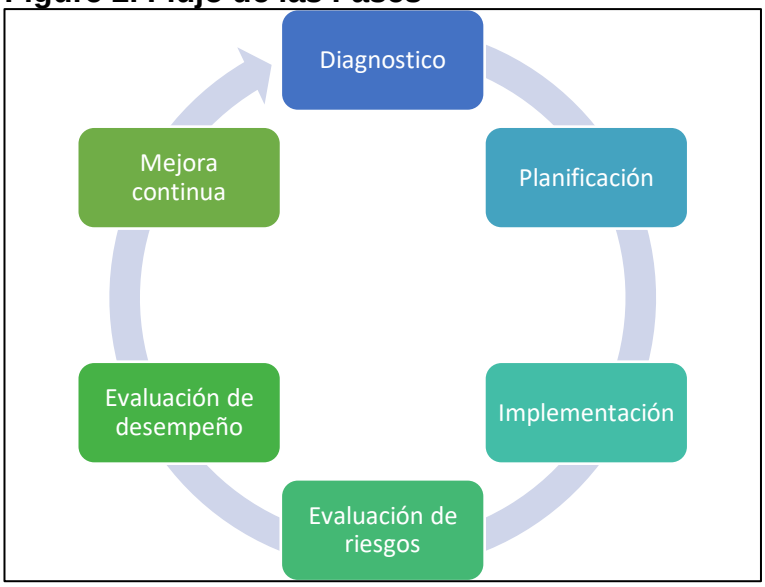
•Mejora continua: se busca ayudar a la organización a adoptar medidas correctivas y preventivas, que impulsen en mejoramiento continuo de todos los frentes que impactan en la protección de datos personales y gestionar los cambios y crear una cultura al interior de la organización hacía la protección de los datos personales a través de entrenamiento y capacitación sostenida en el tiempo.

7. ENTREGA DE RESULTADOS E IMPACTOS

7.1 FLUJO DE LAS FASES DEL MODELO

El modelo de protección de datos personales contempla 6 fases, en cada una se incluirá una guía que ayudará a realizar y comprender el cumplimiento frente a la ley 1581 de 2012 (véase la Figura 2).

Figure 2. Flujo de las Fases



Fuente. Los Autores

7.1.1 FASE UNO – DIAGNOSTICO

➢Identificar y clasificar. Para identificar y clasificar las bases de datos se debe indagar en los procesos que prestan servicios si estos cumplen el rol como encargados de la información, de acuerdo con lo anterior para tener claro el flujo de la información desde su recolección, uso, almacenamiento, transferencia y eliminación, tomando como guía el manual de Registro Nacional de Bases de Datos publicado por la SIC, a continuación, matriz (véase el Cuadro 3).

Cuadro 3. Descripción de Bases de Datos

Información								
Proceso	Subproceso	Nombre de base de datos	Cantidad de Titulares	Finalidad	¿Alguna norma lo obliga a realizar tratamiento de datos?	Tipo de norma BD	Número de norma	Año de expedición
Proceso al cual pertenece la base de datos	Subproceso donde se utiliza la base de datos	Nombre completo de la base de datos	Número total de personas naturales que se encuentran registradas en la base de datos.	Describa brevemente la finalidad para la cual usa esta base de datos, para esto tenga en cuenta la casilla anterior	Registre si conoce alguna normatividad diferente a la ley 1581 de 2012 la cual nos obligue a realizar el tratamiento de los datos de la base de datos	Si diligencio la casilla anterior con un SI, escoja alguna de las siguientes opciones:	Si diligencio la casilla anterior ingresar el número de la norma	Si diligencio la casilla anterior año de expedición de la norma

Fuente. Los Autores

El Cuadro 4 ayudara a dar una comprensión frente a que bases de datos se encuentra en el proceso, la finalidad de tratamiento y la existencia de normatividad que obligue a tratar la información con un fin específico o almacenar por tiempo determinado. En esta parte se identifica la primera parte del ciclo de la vida del dato como la recolección y uso.

Cuadro 4. Forma de Tratamiento

Forma de tratamiento						
Clasificación bases de datos	Ubicación de la base de datos si es Automatizada	País donde se encuentra el Servidor Externo	Ubicación de la base de datos si es física	Aplicativo	Retención	Propósito de Retención
Solo debe poner en esta casilla si la base de datos es Automatizada o física, recuerde que si maneja la misma bases en medio físico y electrónico, se deberán inscribir cada una en forma independiente.	Solo debe diligenciar esta casilla si en la anterior escogió la opción base de datos electrónico. La base de datos electrónicas es aquellas que se almacenan en herramientas electrónicas.	Si usted escogió la opción servidor externo en la casilla anterior, debe llenar esta casilla	Solo debe llenar esta casilla si en la casilla "Clasificación bases de datos" escogió la opción base de datos física. La base de datos físicas se identifica como manuales o archivos suya información se encuentra organizada y almacenada de manera física.	¿En qué aplicación se encuentra la base de datos?	Periodo de retención de la información en la base de datos. Ejemplo: x Meses, x Años Nota: Si el tiempo es menor al del ejemplo proporcione una explicación que describa como se administra la retención de datos.	Tener claro el propósito por el cual se almacena la información

Fuente. Los Autores

El Cuadro 4 ayuda a saber si la base de datos que se manejan en el proceso es físicas o electrónicas y donde se encuentra almacenadas.

Cuadro 5. Información que integra la Base de Datos

Información que integra la Base de Datos

Titular del dato	Datos Generales	Datos de identificación	Datos de Ubicación	Datos Sensibles	Datos de contenido socioeconómico	OTROS DATOS
Escoja alguna de las opciones: Colaborador Cliente Proveedor Candidato Otros_____	Para diligenciar esta casilla usted debe dirigirse a cuadro 9 Clasificación IP donde tendrá que escoger que tipo de datos personales se encuentran en la base de datos, Cuando finalice usted podrá ver en la casilla "Categoría" si esta contiene datos de generales.	Para diligenciar esta casilla usted debe dirigirse a cuadro 9 Clasificación IP donde tendrá que escoger que tipo de datos personales se encuentran en la base de datos, Cuando finalice usted podrá ver en la casilla "Categoría" si esta contiene datos de identificación.	Para diligenciar esta casilla usted debe dirigirse a cuadro 9 Clasificación IP donde tendrá que escoger que tipo de datos personales se encuentran en la base de datos, Cuando finalice usted podrá ver en la casilla "Categoría" si esta contiene datos de Ubicación.	Para diligenciar esta casilla usted debe dirigirse a cuadro 9 Clasificación IP donde tendrá que escoger que tipo de datos personales se encuentran en la base de datos, Cuando finalice usted podrá ver en la casilla "Categoría" si esta contiene datos Sensibles.	Para diligenciar esta casilla usted debe dirigirse a cuadro 9 Clasificación IP donde tendrá que escoger que tipo de datos personales se encuentran en la base de datos, Cuando finalice usted podrá ver en la casilla "Categoría" si esta contiene datos de contenido socioeconómico.	Para diligenciar esta casilla usted debe dirigirse a cuadro 9 Clasificación IP donde tendrá que escoger que tipo de datos personales se encuentran en la base de datos, Cuando finalice usted podrá ver en la casilla "Categoría" si esta contiene otros datos.

Fuente. Los Autores

El Cuadro 5 ayuda a identificar qué información se encuentra en la base de datos de acuerdo con la categoría dada por la SIC, para completar el Cuadro 5 se debe tomar como referencia el Cuadro 9.

Cuadro 6. Autorización de Titular

Autorización de titular			
Cuenta con la autorización del titular	Causales de Exoneración si es (No / Algunos casos)	Forma de obtención de los datos	Autorización
Diligencie esta casilla si usted cuenta con la autorización de tratamiento de datos personales.	Si diligencia la casilla anterior con la opción No o Algunos casos escoja alguna de las siguientes opciones: 1. Fuentes de acceso público. 2. Dada por un por un tercero. 3. Recolectado del titular.	Si diligencio la casilla "Cuenta con la autorización del titular", escoja alguna de las siguientes opciones	Se diligencio la casilla "Cuenta con la autorización del titular" nombre la autorización que usa

Fuente. Los Autores

El Cuadro 6 ayuda a identificar si en esa base de datos se recolecta o se obtiene de alguna manera la autorización de tratamiento de datos personales.

Cuadro 7. Responsable

Área interna		Receptor/Responsable del tratamiento									
Área interna	Acceso a la información	Nombre o Razón social	Tipo de documento del responsable	Número de documento	País	Dirección	Departamento	Ciudad	Correo electrónico	Teléfono fijo(indicativo-número)	Sitio Web
	De acuerdo con el acceso que tiene el área procesadora escoja que derechos tiene	Diligencie en esta casilla el número de identificación del responsable	Diligencie en esta casilla el país del responsable	Diligencie en esta casilla la dirección del responsable	Diligencie en esta casilla el Departamento del responsable	Diligencie en esta casilla la ciudad del responsable	Diligencie en esta casilla el correo electrónico del responsable	Diligencie en esta casilla el teléfono fijo del responsable	Diligencie en esta casilla el sitio Web del responsable	Diligencie en esta casilla el teléfono del responsable	Si esta transferencia se exceptúa de la prohibición general, seleccione la causal.

Fuente. Los Autores

El Cuadro 7 ayuda a identificar si en esa base de datos se recolecta o se obtiene de alguna manera la autorización de tratamiento de datos personales.

Cuadro 8.Transferencia Internacional / Clasificación

Transferencia Internacional			Clasificación
Se realiza Transferencia internacional	Caso de Excepción	Número de radicado	Clasificación
Si cuanta con Declaratorio de Conformidad emitida por la sic, ingrese el número de radicado			Clasificación ir

Fuente. Los Autores

El Cuadro 8 ayuda a identificar si se realizan transferencia y la clasificación final de la información.

Para realizar esta clasificación se sugiere tener en cuenta el Cuadro 9, ya que esta ayudara a hacer la clasificación de acuerdo con la caracterización que cada dato personal que se maneja en una empresa.

Cuadro 9. Tabla de Caracterización de la Información para Clasificarla

CATEGORIA	SUBCATEGORIA	CODIFICACIÓN	Clasificación 1581:2012
Identificación	Datos generales de identificación de la persona	Nombre completo	Publico
		Tipo de identificación	Publico
		Número de identificación	Publico
		Fecha de expedición	Publico
		Lugar de expedición	Publico
		Género	Publico
		Estado civil	Publico
	Datos específicos de identificación de la persona.	Número de la licencia para conducir	Publico
		Fecha de nacimiento	Publico
		Lugar de nacimiento	Publico
		Fecha de muerte	Privado
		Lugar de muerte	Privado
		Número de la tarjeta militar	Publico
		Origen Nacionalidad	Publico
		Ciudadanía/País de residencia	Publico
		Información de dependientes de Socio/Empleado (cónyuge/padres/otros)	Privado
		hijos(niños)	Sensible
		Tarjeta profesional	Publico
		Número Pasaporte	Privado
		Firma	Semiprivado
		Firma electrónica	Semiprivado
		Edad	Privado
		Fotografías	Privado
		Videos	Privado
		Voz	Sensible
	Datos de la descripción morfológica de la persona.	Estatura	Privado
		Peso	Privado

Cuadro 9. (Continuación)

CATEGORIA	SUBCATEGORIA	CODIFICACIÓN	Clasificación 1581:2012
Ubicación	Datos de ubicación relacionados con actividad comercial	Dirección de la empresa	Publico
		Número telefónico de la empresa	Publico
		Dirección del correo electrónico de la empresa	Publico
	Datos de ubicación personal	Dirección de la casa	Privado
		Número telefónico de la casa	Privado
		Dirección del correo electrónico personal	Privado
		Barrio/Vereda domicilio	Privado
		Teléfono celular personal	Privado
Datos sensibles	Datos relacionados con la salud	Reconocimiento médico / información de la salud	Sensible
	Datos relacionados con el estado de salud de la persona	Evaluaciones psicotécnicas	Sensible
		Data visita domiciliaria	Sensible
	Datos relacionados a pertenencias	Datos que revelan la opinión política	Sensible
		Datos que revelan religión o creencias filosóficas	Sensible
		Miembro de un gremio/Sindicato	Sensible
	Datos de preferencia, identidad y orientación.	Orientación sexual	Sensible
		Datos que revelan raza u origen étnico	Sensible
	Población en condición vulnerable	Condiciones vulnerables	Sensible
	Datos personas en discapacidad	Información sobre discapacidad	Sensible
Contenido socioeconómico	Datos financieros	Información financiera y crediticia	Semiprivado
	Datos socioeconómicos	Estrato	Privado
		propiedad de la vivienda	Privado
	Datos tributaria	Información tributaria	Privado
	Datos patrimoniales	Patrimoniales de la persona	Semiprivado
	Datos relacionados con la actividad económica de la persona	Número de las cuentas bancarias	Semiprivado
		Nombre de la entidad en donde tiene cuenta o inversión	Semiprivado
		Números de tarjetas de crédito	Semiprivado
		Información de la evaluación del desempeño del socio/empleado	Privado
	Datos historia laboral	Fecha de vinculación	Privado
		Tipo de contrato	Privado
		Salario	Privado
		Duración del contrato	Privado
		Cargo	Privado
		Historia laboral y referencias	Privado
	Datos nivel educativo	Educación, capacitación y/o historial académico	Privado
	Datos afiliación	Información de la seguridad social	Privado
Otros datos	Datos acceso a sistemas de información	Contraseñas de las cuentas o PINs	Sensible
	Datos sobre gustos y/o intereses particulares	Registros antecedentes penales - pasado judicial (sentencias ejecutoriadas, investigaciones disciplinarias luego del pliego de cargos)	Privado
	Datos de antecedentes	Hobbies/Intereses/Actividades/Hábitos	Privado

Fuente. Los Autores

7.1.2 FASE DOS – PLANIFICACIÓN

Una vez se han identificado las bases de datos que cumplen con las características de Encargado de la información en la Fase Uno – Diagnostico, se debe validar los deberes a implementar en la organización frente al artículo 18 “deberes del encargado de la información”, y planificar su cumplimiento de acuerdo a las acciones propuestas en el Cuadro 10 y en la Fase Tres - Implementación.

Cuadro 10. Articulo 18

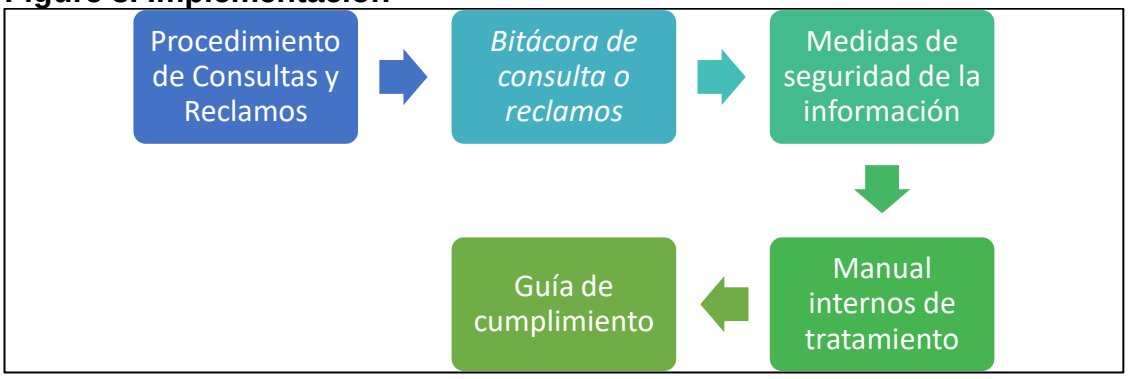
Artículo 18. Deberes de los Encargados del Tratamiento.	**Acciones**
a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;	Se debe tener un procedimiento de consultas y reclamos.
b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;	Se debe cumplir con las condiciones de seguridad dadas por el manual de RNBD
c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;	Se debe asegurar en el procedimiento de consultas y reclamos.
d) Actualizar la información reportada por los responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;	Se debe asegurar en el procedimiento de consultas y reclamos.
e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;	Se debe asegurar en el procedimiento de consultas y reclamos.
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;	Se debe incluir en el manual interno de tratamiento de datos personales de la empresa el cumplimiento frente a su responsabilidad como encargados de la información.
g) Registrar en la base de datos las leyendas "reclamo en trámite" en la forma en que se regula en la presente ley;	Se debe implementar tanto para bases de datos en físico y digital, se evidencia en la bitácora de consultas y reclamos.
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;	Se debe implementar tanto para bases de datos en físico y digital, se evidencia en la bitácora de consultas y reclamos.
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;	Se debe cumplir con las condiciones de seguridad dadas por el manual de RNBD.
j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;	Se debe cumplir con las condiciones de seguridad dadas por el manual de RNBD
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;	Se debe asegurar en el procedimiento de consultas y reclamos.
l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio	Se debe asegurar el cumplimiento tomando como referencia los documentos publicados por la SIC en su página Web

Fuente. Los Autores

7.1.3 FASE TRES – IMPLEMENTACIÓN

A continuación, se presenta el esquema de implementación del proyecto (véase la Figura 3)

Figure 3. Implementación



Fuente. Los Autores

De acuerdo con la sugerencia dadas frente al cumplimiento de la ley 1581 artículo 18 a continuación se lista las actividades a realizar:

7.1.3.1 DOCUMENTO DE CONSULTA Y RECLAMOS

El titular o responsable tiene derecho a solicitar al encargado del Tratamiento de la información personal el derecho de consulta y reclamo, para cumplir se sugiere tener en cuenta el siguiente procedimiento de acuerdo con su estructura organizacional y recursos (véase el Cuadro 11).

Cuadro 11. Procedimiento de Consultas y Reclamos

PROCEDIMIENTO DE CONSULTA Y RECLAMOS			
No	**ACTIVIDAD**	**DESCRIPCIÓN/ RESPONSABLE**	**DOCUMENTOS ASOCIADOS**
	Inicio		
1	**Recibir solicitud**	Se recibirá mediante correo buzón responsable de privacidad, la solicitud de ejercer el derecho de protección de datos personales. **RESPONSABLE:** Líderes de proceso que van a generar el cambio.	
2	**Clasificar Consulta**	Descripción: El titular y responsable y tiene derecho a solicitar al encargado del Tratamiento de la información: Conocer: o A ser informado respecto del uso que les ha dado a sus datos. o La prueba de la autorización concedida para tratar su información, salvo cuando ésta no sea necesaria. o El acceso a sus datos personales de forma gratuita. Tiempos de respuesta: Dependiendo del derecho de protección de datos personales, se deben tener cuenta las siguientes condiciones: Al recibir la solicitud de consulta se debe dar respuesta en diez (10) días hábiles.	

Cuadro 11. (Continuación)

No	ACTIVIDAD	DESCRIPCIÓN/ RESPONSABLE	DOCUMENTOS ASOCIADOS
		Cuando no pueda responder la consulta el tiempo dado por la ley, se informará al titular el motivo de la demora y se informara la fecha en que se atenderá, la cual no podrá superar los cinco (5) días hábiles. **RESPONSABLE**: Líderes de proceso que van a generar el cambio	
3	**Clasificar Reclamo**	Descripción: El titular y responsable y tiene derecho a solicitar al encargado del Tratamiento de la información: o Actualizar y/o rectificar: El titular de la información tiene derecho a actualizar y rectificar sus datos frente a los responsables de la información cuando estos son inexactos o cuando su tratamiento esté expresamente prohibido o no haya sido autorizado. o Revocar la actualización y/o Supresión: El titular de la información tiene derecho a revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. No procederá la revocatoria cuando el titular tenga un deber legal o contractual de permanencia en la base de datos. Tiempos de respuesta: Dependiendo del derecho de protección de datos personales, se deben tener cuenta las siguientes condiciones: Recibida la solicitud de reclamo se debe dar respuesta en un término de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no pueda responder el reclamo en el tiempo dado por la ley, se informará al titular el motivo de la demora y se informara la fecha en que se atenderá, la cual no podrá superar los ocho (8) días hábiles. La única excepción es actualizar la información reportada por los responsables dentro de los cinco (5) días hábiles. **RESPONSABLE:** Líderes de proceso que van a generar el cambio	
4	**Analizar consulta**	Conocer: Uso de los datos personales: El oficial de protección de información, deberá informar al titular el tratamiento que se da a su información personal, para esto se debe considerar la finalidad que se encuentra en el inventario de bases de datos. Solicitud de soporte de la autorización: El oficial de protección de información, deberá informar donde está la autorización para el tratamiento de datos ya sea en propuestas, contratos o recolectada directamente por el titular. Acceder de forma gratuita a sus datos personales: El oficial de protección de información, deberá recolectar la información del titular y obtener la copia de los datos personales. Se debe tener claro, que para las consultas cuya cantidad sea mayor a una por cada mes calendario, el encargado solo podrá cobrar al titular los gastos de envío, reproducción y certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente, con esto dando cumplimiento a lo estipulado en el art 21 decreto 1377 de 2013. Para tal efecto, el oficial de protección de información deberá demostrar el soporte de dicho gasto. **RESPONSABLE:** Líderes de proceso que van a generar el cambio	

Cuadro 11. (Continuación)

No	ACTIVIDAD	DESCRIPCIÓN/ RESPONSABLE	DOCUMENTOS ASOCIADOS
5	**Analizar reclamo**	Actualizar y/o rectificar: El oficial de protección de información, deberá actualizar o rectificar la información en la base de datos digital donde se encuentre almacenada dicha información. Dejar los soportes correspondientes de la actualización o rectificación según corresponda. Revocar la actualización y/o supresión: El oficial de protección de información, deberá identificar la siguiente información: a. ¿Qué información tiene del titular? Ejemplo: Hojas de vida, información de educación, certificados, etc. c. ¿Qué información digital tienen del titular? Ejemplo: correos electrónicos, formatos digitales, etc. El oficial de protección de información deberá recolectar la información digital del titular y hacer la destrucción segura de acuerdo con el Manual de tratamiento de datos personales parte "5.5 Requisitos de destrucción como responsable o encargado". El Manual lo podrá encontrar en la Intranet (M:\Proteccion de Datos Personales\Políticas, manuales y formatos\2. Manual de tratamiento de datos personales). Para el cual se estableció una conservación de los documentos por 2 años. **RESPONSABLE:** Líderes de proceso que van a generar el cambio.	
6	**Dar respuesta a consultas y reclamos**	Al momento de dar por finalizado la solicitud, se registrará la fecha de cierre en la "Bitácora consulta o reclamos" y debe asignar una numeración con la cual se adjuntará a la carpeta correspondiente los siguientes soportes: 1. Correo de la solicitud del titular. 2. Si corresponde al derecho de supresión se dejará el acta de la eliminación digital de la información. El acta con el soporte de la eliminación de la información digital donde se evidencie los pantallazos. 3. Respuesta de la solicitud al titular. **RESPONSABLE:** Líderes de proceso que van a generar el cambio.	
	Fin		
9	**Generación Lecciones Aprendidas**	Si en el proceso se identifican lecciones aprendidas estas deben registrar de acuerdo con los establecido en el instructivo de lecciones aprendidas **RESPONSABLE:** Líderes de proceso que van a generar el cambio, persona que autoriza el cambio.	Doc. Lecciones aprendidas
10	**Generación de acciones de mejora para el proceso**	Si en el proceso, se identifican acciones de mejora estas deben registrarse en SharePoint de acuerdo con lo establecido en el manual de manejo de solicitudes de mejora. **RESPONSABLE:** Líderes de proceso que van a generar el cambio, Asistente de recursos humanos, la persona que autoriza el cambio.	Doc. Manejo de solicitudes de mejora

CONTROL DE CAMBIOS		
VERSION No.	**DESCRIPCION DEL CAMBIO**	**FECHA**
1	Se crea documento	xx/xx/xx

ELABORADO	APROBADO:	REVISADO
NOMBRE **(CARGO)**	NOMBRE **(CARGO)**	NOMBRE **(CARGO)**

Fuente. Los Autores

7.1.3.2 BITÁCORA DE CONSULTA Y RECLAMOS

Cuando no se cuente con una aplicación para realizar el seguimiento de las consultas y reclamos se sugiere que se tenga encuentra la siguiente tabla, esta los ayudara a cumplir con la ley 1581 de 2012 articulo 18 punto "g" y "h" (véase el Cuadro 12)

Cuadro 12. Bitácora de Consulta o Reclamos

BITÁCORA CONSULTA O RECLAMOS											
Canal de la solicitud	Fecha de la solicitud	Solicitud	Estado de la solicitud	Validez de la solicitud	Fecha de respuesta	Días hábiles	Descripción	Nombre del solicitante	Papel del titular	Dato personal	Remediación / acción tomada
Descripción del mecanismo por el cual se recibió la solicitud, por ejemplo, a través de correo electrónico o teléfono	Fecha en la que el titular presentó la solicitud, en formato Día, mes y año	Registra la solicitud que realiza el titular, por ejemplo: Derecho Consulta, solicitar prueba de autorización, revocar la autorización, rectificar, solicitar la supresión del dato.	Si el derecho es de reclamos se debe contestar esta casilla. Registrar la leyenda " reclamo en trámite", "información en discusión judicial" o "finalizado" según corresponda.	Revisar en las bases de datos del área, si es válido la solicitud del titular. Ejemplo: en la base de datos no está el titular.	Fecha en la que el titular cerro la solicitud, en formato Día, mes y año.	Tiempo total para resolver y remediar, días desde la solicitud abierto hasta el cierre.	Descripción de la solicitud del titular.	Nombre del titular que realiza la solicitud	Descripción del rol de la parte del titular, por ejemplo: candidato, colaborador, cliente, etc.	Descripción de los datos personales que se tratan del titular, por ejemplo: Nombre, teléfono, correo, etc.	Puede incluir un resumen de las acciones tomadas y cualquier paso adicional para evitar que se vuelvan a presentar reclamos válidos

Fuente. Los Autores

7.1.3.3 MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo a las sugerencias dadas por la SIC, se sugiere cumplir con las condiciones de seguridad del manual de RNBD. Cabe resaltar que la aplicación de las medidas de seguridad dependerá de las necesidades, presupuesto y de la características propias de cada organización. (véase el Cuadro 13).

Cuadro 13. Medidas de Seguridad de la Información

#	SEGURIDAD DE LA INFORMACIÓN PERSONAL	EXPLICACIÓN	CONTROL ISO 27001	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS FÍSICAS	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS ELECTRÓNICAS
1	¿Tiene un documento de seguridad de la información personal o general aprobado?	Un documento de seguridad de la información personal es aquel que contiene los lineamientos y/o políticas administrativas, humanas y técnicas que se deben adoptar por todas las áreas de la organización y cada uno de sus integrantes en el cuidado de los datos personales, con el objeto de cumplir el principio de seguridad a que se refiere la Ley 1581 de 2012 que en su Artículo 4, literal g enuncia: “Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.”	A.5		
2	¿Ha realizado documentación de procesos en torno a la seguridad de la información personal?	Se refiere a si tiene documentos donde haya plasmado los procesos relacionados con seguridad de la información que involucren datos personales.	A.5		
3	¿Tiene procedimientos de asignación de responsabilidades y autorizaciones en el tratamiento de la información personal?	Hace referencia a si tiene por escrito o documentado de alguna manera quién tiene la responsabilidad en cuanto al tratamiento de datos personales en cada uno de los pasos de los procesos y/o procedimientos relacionados con dicho tratamiento.	A. 6.1.1		
4	¿Ha implementado acuerdos de confidencialidad con las personas que tienen acceso a la información personal?	Está relacionado con el principio de Confidencialidad contemplado por la Ley 1581 de 2012, que indica: "Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de	A.13.2.4		

		públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo			

Cuadro 13. (Continuación)

#	SEGURIDAD DE LA INFORMACIÓN PERSONAL	EXPLICACIÓN	CONTROL ISO 27001	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS FÍSICAS	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS ELECTRÓNICAS
		sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma."			
5	¿Tiene controles de seguridad en la tercerización de servicios para el tratamiento de la información personal?	Corresponde a aquellos controles implementados en los procesos o tratamiento de datos que se realizan a través de terceros ajenos a la organización, que corresponden a Encargados del tratamiento de datos personales.	A.15.1		
B	SISTEMAS DE SEGURIDAD DE LA INFORMACIÓN				
1	¿Tiene implementado herramientas de gestión de riesgos en el tratamiento de datos personales?	Herramientas de gestión de riesgo se denomina a la combinación de sistemas, controles, instrumentos, metodologías, etc., empleados para facilitar los procesos de prevención, mitigación y preparación de las capacidades de la organización para evitar, disminuir o transferir los efectos adversos o impactos negativos de las amenazas detectadas en un proceso de análisis del entorno durante cada una de las etapas del ciclo del dato y la naturaleza de estos. El responsable es libre de utilizar la herramienta o metodología que desee, de acuerdo con sus necesidades y capacidades organizacionales. Se debe tener una documentación de la metodología utilizada para la evaluación del riesgo.	Dominio. 6.1;8,2;8,3		
2	¿Tiene implementado un sistema de gestión de seguridad de la información o un programa integral de gestión de datos personales?	En términos generales un Sistema de Gestión de Seguridad de la Información o SGSI es un conjunto de lineamientos y/o políticas administrativas, humanas y técnicas de administración de la información. El concepto es utilizado por diferentes estándares, principalmente por la ISO/IEC 27001. En cuanto al Programa Integral de Gestión de Datos Personales PIGDP consiste en implementar al interior de la organización las medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012. Para lo cual el Decreto 1074 en su sección 6 desarrolla el principio de Responsabilidad demostrada frente al tratamiento de datos personales y la Superintendencia de Industria y comercio publicó la Guía para la implementación	A. 5		

Cuadro 13. (Continuación)

#	SEGURIDAD DE LA INFORMACIÓN PERSONAL	EXPLICACIÓN	CONTROL ISO 27001	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS FÍSICAS	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS ELECTRÓNICAS
		del principio de responsabilidad demostrada (Accountability) en las organizaciones, publicado en la página web de la SIC www.sic.gov.co. Por medio del SGSI o de un PIGDP, la organización realiza el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar de manera eficiente el acceso y uso de la información en general o específicamente de los Datos Personales, con base en los principios de la seguridad de la misma que son la confidencialidad, integridad y disponibilidad, para de esta manera minimizar los riesgos asociados al tratamiento de la información, de acuerdo con su clasificación y naturaleza de los datos.			
C	SEGURIDAD DE LA INFORMACIÓN PERSONAL EN TORNO AL RECURSO HUMANO				
1	¿Tiene implementados controles de seguridad de la información personal para el Recurso Humanos antes de la vinculación y una vez finalizado el contrato laboral?	Políticas y controles relacionados con el recurso humano vinculado a la organización que tendrá acceso a la información personal, antes, durante y posterior al desempeño de las funciones. Por ejemplo, acuerdos de confidencialidad de la información, estudios de seguridad previos a la contratación, cierre y control para perfiles de acceso a la información una vez finalizada la relación contractual, etc.	A.7		
D	CONTROL DE ACCESO A LA INFORMACIÓN PERSONAL				
1	¿Tiene una política de control de acceso a la información personal, tanto en las instalaciones físicas como a nivel tecnológico?	Se deben implementar medidas o controles para regular el acceso a la información personal, estas políticas deben contemplar tanto el acceso físico (a las instalaciones) como el acceso lógico (al software, aplicaciones, usuarios, IP´s, claves, etc.). Esto es definir quién tiene permisos sobre la información personal y qué puede hacer exactamente con los datos personales.	A.9.1.1.		

Cuadro 13. (Continuación)

#	SEGURIDAD DE LA INFORMACIÓN PERSONAL	EXPLICACIÓN	CONTROL ISO 27001	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS FÍSICAS	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS ELECTRÓNICAS
2	¿Cuenta con un procedimiento para la Gestión de usuarios con acceso a la información personal?	Es complemento del control de acceso a la información personal. Está relacionado con las políticas para el control de los usuarios que tienen acceso a los datos personales. Esto es definir quién es el responsable de crear los usuarios, autorizaciones, seguridad en cuanto a claves, notificaciones, eliminación, perfiles de acceso, permisos, entre otros.	A.9.4.2.		
3	¿Ha implementado una política específica para el acceso a la información personal de las bases de datos con información personal sensible?	Está relacionada con la política para regular el acceso a la información personal, pero donde se haga alusión específicamente al tratamiento de los datos sensibles (aquellos cuyo uso inadecuado puede generar discriminación) bien sea dentro de las políticas generales de acceso a la información o si se cuenta con políticas específicas para este tipo de datos. Estas políticas deben contemplar tanto el acceso físico (a las instalaciones) como el acceso lógico (al software, aplicaciones, usuarios, IP´s, claves, etc.), dentro de las cuales se define entre otros aspectos quién tiene permisos sobre dichos datos y qué puede hacer exactamente con ellos.	A. 8.2		
4	¿Tiene una política implementada de copia de respaldo de la información personal?	Hace referencia a si se tiene una política que indique a qué datos se les realiza una copia de seguridad, esto depende de la definición que la organización realice en cuanto a tipos de datos, tiempos de retención, datos a respaldar, medios de almacenamiento, ubicación de la copia, pruebas de restauración, entre otros aspectos.	A.12.4		
5	¿Ha implementado una política de protección para el acceso remoto a la información personal?	Se refiere a las medidas de seguridad que se implementen para garantizar una forma confiable de consulta, uso o extracción de la información de manera remota, es decir desde dispositivos que no se encuentren al interior de la organización. Lo anterior teniendo en cuenta las posibilidades que hoy existen de consultar los datos que una empresa tenga en sus servidores, equipos, data center, etc., desde diferentes puntos como dispositivos móviles, agilizando procesos de consulta, promoción y venta, etc. es importante asegurar dichos accesos a la red de la Organización.	A.9.1.1.		

Cuadro 13. (Continuación)

#	SEGURIDAD DE LA INFORMACIÓN PERSONAL	EXPLICACIÓN	CONTROL ISO 27001	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS FÍSICAS	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS ELECTRÓNICAS
E	PROCESAMIENTO DE INFORMACIÓN PERSONAL				
1	¿Cuenta con una política implementada para el correcto tratamiento de la información personal en las diferentes etapas del ciclo de vida del dato (recolección, circulación y disposición final)?	Está relacionado con la identificación de quién realiza qué y cómo lo hace en cada paso del tratamiento, para ello es importante elaborar una matriz de riesgo de los datos personales, identificar el ciclo del dato y en cada etapa, los riesgos asociados; una vez se realice esta tarea, se deben identificar los controles que se requieren para su gestión, demostrando así el correcto tratamiento en cada etapa. Para lo anterior puede apoyarse en la Guía para la implementación del principio de responsabilidad demostrada, que encuentra en la página de la SIC www.sic.gov.co.	A18.1.2		
2	¿Cuenta con un procedimiento implementado para la validación de datos de entrada y procesamiento de la información personal, para garantizar que los datos recolectados y procesados sean correctos y apropiados, como confirmación de tipos, formatos, longitudes, pertinencia, cantidad, uso, etc.?	Está relacionado con la veracidad del dato, el cual se debe garantizar desde su recolección, por lo tanto, es necesario minimizar el riesgo de error o ataques por inyección de código, utilizando técnicas de validación de los datos de entrada y procesamiento, al confirmar tipos, formatos, longitudes, pertinencia, cantidad, uso, entre otros.	A.14.2.2		
3	¿Cuenta con un control de seguridad de información para la validación de datos de salida?	Este control está relacionado con la veracidad e integridad del dato, las cuales se deben garantizar desde su recolección, procesamiento y busca tener resultados esperados. Los datos de salida son los datos esperados, que si se presume un campo con un tipo de dato definido sea ese el que se obtiene y no otro. Así como en un reporte, la pertinencia de la información reportada de acuerdo con la finalidad. Esta es una manera de controlar la veracidad, calidad y acceso no autorizado a la información.	A9		

Cuadro 13. (Continuación)

#	SEGURIDAD DE LA INFORMACIÓN PERSONAL	EXPLICACIÓN	CONTROL ISO 27001	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS FÍSICAS	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS ELECTRÓNICAS
4	¿Cuenta con una política implementada para el Intercambio físico o electrónico de datos (como por ejemplo durante el comercio electrónico para la compra y venta de productos o servicios), transporte y/o alimentación de información personal?	Se refiere a si existen medidas de seguridad que se apliquen para minimizar los riesgos asociados al intercambio de datos personales bien sea de manera física o electrónica, como interceptación, consulta no autorizada, fraude, pérdida o robo de la información	A.8.3.3 A.13.2.1		
5	¿Tiene un procedimiento o control implementado para la disposición final de la información personal (supresión, archivo, destrucción, etc.)?	Una vez identificados los riesgos asociados al tratamiento de datos en cada una de las etapas, debe implementar controles coherentes en cuanto a lo que se decida hacer finalmente con dicha información, que puede ser eliminación (borrado seguro), destrucción o conservación, de manera que nunca se expongan los datos a un uso no autorizado o fraudulento que conlleve a la materialización de un riesgo tanto para el titular como para el responsable del tratamiento.	A.8.3.2		
F	SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN PERSONAL				
1	¿Tiene implementado un procedimiento que contemple la definición de especificaciones y requisitos de seguridad de los sistemas de información personal?	Es documentar los pasos y metodología utilizada en la definición de las necesidades identificadas antes, durante y posterior al desarrollo de sistemas de información relacionados con el tratamiento de datos personales, en todo lo concerniente a seguridad de la información.			
2	¿Tiene implementados controles de seguridad de la información durante el mantenimiento (control de cambios) de los sistemas de información personal?	Se refiere a si existen controles implementados sobre la documentación que debe hacerse acerca de los cambios o modificaciones que requieran los sistemas de información en general o específicamente aquellos que incluyen el tratamiento de datos personales.	A.12.1.1		

Cuadro 13. (Continuación)

#	SEGURIDAD DE LA INFORMACIÓN PERSONAL	EXPLICACIÓN	CONTROL ISO 27001	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS FÍSICAS	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS ELECTRÓNICAS
3	¿Tiene un procedimiento implementado de auditoría de los sistemas de información personal?	Indicar si tiene procedimientos automatizados que permitan evaluar la eficiencia y suficiencia de los controles implementados a un sistema de información mediante el cual se traten datos personales para evitar su pérdida, uso o acceso no autorizado o fraudulento, de manera que se garantice la disponibilidad, integridad y confidencialidad de los datos personales.	Dominio 9.2		
4	¿Las bases de datos con información personal poseen Monitoreo de consulta?	Permite efectuar trazabilidad o seguimiento de cualquier consulta que realice sobre la base de datos con información personal. Lo cual se definirá dependiendo del riesgo a que esté expuesta esta información y la naturaleza de los datos que se estén tratando.	A.9.4.1		
G	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PERSONAL				
1	¿Cuenta con una política y procedimientos implementados de gestión de Incidentes de seguridad de la información personal?	Teniendo en cuenta que un Incidente de seguridad de datos personales se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de datos personales bien sea en manos del responsable del Tratamiento o de su Encargado, se refiere a la documentación de los pasos a seguir una vez se detecte la comisión del incidente, tanto a nivel correctivo como preventivo. Dentro de los cuales se deben determinar tiempos, roles y responsabilidades.	A.16.1.1 A. 16.1.5 A.16.1.7		
2	¿Tiene implementada una política para mejorar la seguridad de la información personal a partir de los incidentes o vulnerabilidades detectados?	Una vez se han determinado las causas e impacto del incidente detectado relacionado con datos personales, es importante identificar oportunidades de mejora e implementar controles que redunden en la prevención de la ocurrencia de otros hechos relacionados con las vulnerabilidades detectadas.	A. 12.6.1		

Cuadro 13. (Continuación)

#	SEGURIDAD DE LA INFORMACIÓN PERSONAL	EXPLICACIÓN	CONTROL ISO 27001	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS FÍSICAS	DOCUMENTO DE CUMPLIMIENTO FRENTE A LA BASE DE DATOS ELECTRÓNICAS
H	AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN PERSONAL				
1	¿Tiene una política de auditorías de seguridad de la información personal?	Indicar si tiene documentada una política de auditoría de seguridad de la información personal o en general, que permita evaluar el cumplimiento, resultados y la documentación de acciones correctivas y/o preventivas, relacionadas con el tratamiento de datos personales.	Dominio 9.2		
2	¿Dentro de las auditorías de seguridad de información personal, tiene en cuenta el cumplimiento de requisitos, políticas y normas que específicamente le apliquen a la base de datos?	Indicar si tiene implementada una política de auditoría de seguridad de la información personal o en general, que permita evaluar el cumplimiento, resultados y la documentación de acciones correctivas y/o preventivas, sobre tratamiento de datos personales, donde sea posible evaluar el cumplimiento de requisitos, políticas y normas que específicamente le apliquen a la base de datos con información personal que está registrando.	Dominio 9.2		

Fuente. Los Autores

7.1.3.4 MANUAL INTERNO EN PROTECCIÓN DE DATOS PERSONALES

Para cumplir con el numeral f). de la ley 1581 de 2012 artículo 18, se sugiere incluir los siguientes temas en el Manual interno de la organización para el cumplimiento del tratamiento de la ley:

•Procedimiento de consultas y reclamos.

•Procedimientos implementados de gestión de Incidentes.

•Plan de sensibilización.

•Proceso de auditoría de seguridad de la información personal que permita evaluar el cumplimiento, resultados y la documentación de acciones correctivas y/o preventivas, relacionadas con el tratamiento de datos personales.

•Procedimiento o control implementado para la disposición final de la información personal (supresión, archivo, destrucción, etc.)

•Procedimientos de asignación de responsabilidades

•Control de acceso a la información personal, tanto en las instalaciones físicas como a nivel tecnológico.

•Proceso de respaldo de la información personal

•Proceso para el acceso remoto a la información personal

•Proceso para el tratamiento de la información en la recolección, uso, almacenamiento, transferencia y eliminación.

•Procedimiento implementado donde se realice la validación de datos de entrada y tratamiento de la información personal, que garantice que los datos recolectados y procesados sean correctos y apropiados, en cuanto a la confirmación de los tipos, los formatos, la cantidad, el uso, etc.

•Proceso para validación de datos de salida

7.1.3.5 DOCUMENTO GUÍA DE CUMPLIMIENTO TOMANDO COMO REFERENCIA LOS DOCUMENTOS PUBLICADOS POR LA SIC EN SU PÁGINA WEB

La SIC no ha publicado guías específicas para el cumplimiento de la ley 1581 de 2012 frente al rol de encargado de la información, pero se tomará como referencias las dos guías publicada para el cumplimiento con la ley 1581 de 2012 y

responsabilidad demostrada (véase el Cuadro 14).

Cuadro 14. Cuestionario Diagnóstico para el Cumplimiento ley 1581 de 2012

Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las MIPYMES	
PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES	SI/NO
Se recolecto información personal para finalidades legítimas y se informa al titular esas finalidades	
Se cuenta con el consentimiento para tratar los datos del titular del cual se recolecta información.	
Si hay casos en los que se recolecta o información personal sin el consentimiento de los titulares, existe un mandato legal o judicial que habilite a organización para hacerlo	
Se conserva información personal veraz, completa, exacta, actualizada, comprobable y comprensible.	
Se cuenta con medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a la información personal para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.	
Se garantiza la confidencialidad de la información por las personas de la organización que interviene en el tratamiento de datos personales, incluso después de que han finalizado si relación con alguna de las labores desempeñadas.	
TRATAMIENTO DE DATOS SENSIBLES Y DE MENORES DE EDAD	SI/NO
Se cuenta con autorización explícita de los titulares para el tratamiento de sus datos sensibles	
Se informa al titular que por tratarse de datos sensibles no está obligados a autorizar su tratamiento	
Se informa al titular cuáles de los datos serán objeto de tratamiento en su organización son sensibles y para qué finalidad(es) se utilizan	
Se efectúa tratamiento de datos personales de menores de edad únicamente para actividades que responden y respetan el interés superior de los menores	
En el tratamiento de datos personales de menores de edad se asegura el respeto de sus derechos fundamentales	
Se cuenta con la autorización del representante legal del menor de edad para el tratamiento de sus datos	
DERECHOS DE LOS TITULARES DE LA INFORMACIÓN	SI/NO
Se permite el ejercicio del derecho de los titulares a conocer, actualizar y rectificar los datos personales que recolecta	
Se da respuesta a las solicitudes presentadas por los titulares dentro de la oportunidad prevista en la ley general de protección de datos personales	
Se entrega a los titulares copias de la autorización otorgada por ellos para el tratamiento de sus datos personales cuando así lo solicitan estos.	
Se informa a los titulares qué uso les ha dado la organización a sus datos personales cuando así lo solicitan estos	
Se permite a los titulares el acceso gratuito a los datos personales que han sido objeto de tratamiento al menos una vez cada mes calendario y cada vez que se hagan modificaciones sustanciales a la política de tratamiento de la información.	
AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES	SI/NO
Se cuenta con la autorización de los titulares de los datos contenidos en las bases de datos que tiene la organización para el tratamiento de estos	
Se conocen los casos en los que no es necesario contar con autorización de los titulares para el tratamiento de su información personal	
Se cuenta con procedimiento efectivos y eficientes para solicitar, a más tardar en el momento de la recolección de los datos personales, las autorizaciones de los titulares para el tratamiento de estos	
Se informa a los titulares qué datos personales serán recolectados y todas las finalidades específicas del tratamiento para las cuales la organización obtiene el consentimiento	
Se obtiene nuevas autorizaciones de los titulares, cuando la organización realiza cambios sustanciales en las políticas de tratamiento de información personal	
Se estable mecanismos que garantizaran la consulta posterior de la autorización otorgada por los titulares para el tratamiento de sus datos personales	
Se ponen a disposición de los titulares mecanismos gratuitos y de fácil acceso para presentar solicitudes de supresión de datos o la revocación de la autorización otorgada	

Cuadro 14. (Continuación)

Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las MIPYMES	
INFORMACIÓN MÍNIMA A LOS TITULARES	SI/NO
Se informa de manera clara y expresa a los titulares, al momento de solicitar la autorización para el tratamiento de datos personales, el tratamiento al cual serán sometidos los mismos y la finalidad.	
Se informa de manera clara y expresa a los titulares, al momento de solicitar la autorización para el tratamiento de datos personales, el carácter facultativo de la respuesta a las preguntas que se hacen, cuando se relacionan con datos sensibles a datos de niñas, niños y adolescentes.	
Se informa de manera clara expresa a los titulares, al momento de solicitar la autorización para el tratamiento de datos personales, los derechos que les asisten	
Se informa de manera clara y expresa a los titulares, al momento de solicitar la autorización para el tratamiento de datos personales, la identificación, dirección física y electrónica y teléfono de responsable del tratamiento	
Se conserva prueba de haber informado a los titulares lo mencionado anteriormente	
SUMINISTRO DE LA INFORMACIÓN PERSONAL	SI/NO
La información personal que se suministra al titular o a quien éste autorice es de fácil lectura, sin barreras técnicas que impidan su acceso y corresponde en un todo a aquella que reposa en la base de datos	
Se suministra únicamente información personal a los titulares, sus causahabientes o sus representantes legales, a las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial y a los terceros autorizados por el titular o por la ley	
ATENCIÓN DE CONSULTAS Y RECLAMOS DE LOS TITULARES	SI/NO
Se cuenta con canales o mecanismos sencillos y ágiles y que estén permanentemente habilitados para la atención de las consultas y reclamos de los titulares o sus causahabientes	
Se dan a conocer a los titulares e interesados los canales habilitados para la atención de consultas y reclamos en la política de tratamiento de datos personales dispuesta por la organización	
Se atiende, dentro de los diez (10) días hábiles contados a partir de su recibo, las consultas de información personal presentadas por los titulares, sus causahabientes y las personas autorizadas	
Se informa a los peticionarios el motivo de la no atención oportuna a su consulta de información personal y se señala la fecha de respuesta de la solicitud, sin exceder el término de cinco (5) días adicionales a los (10) días iniciales para contestar	
Se atiende, dentro de los diez (15) días hábiles contados a partir de su recibo, las reclamaciones presentadas por los titulares o sus causahabientes que consideran que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley.	
Se informa a los peticionarios el motivo de la no atención oportuna a su reclamo y se señala la fecha de respuesta de la solicitud, sin exceder el término de ocho (8) días adicionales a los quince (15) días iniciales para contestar.	
Se adoptan medidas para asegurar que los datos personales que reposan en las bases de datos Dean precisos y suficientes y, cuando así lo solicite el titular o cuando haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del tratamiento	
Se ha designado a una persona a área para que asume la función de protección de datos personales y dé trámite a las solicitudes de los titulares para el ejercicio de sus derechos	
Se da a conocer a los titulares los procedimientos dispuestos por la organización para el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización, y los mismos son fácilmente accesibles.	
Se incluye dentro de la política de tratamiento de datos personales los procedimientos dispuestos para garantizar el acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización	
Se cuenta con un manual interno de políticas y procedimientos para garantizar la atención de consultas y reclamos presentados por los titulares y para garantizar, en general, el adecuado cumplimiento de la ley	
Se han adoptado procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, con respecto a cualquier aspecto de tratamiento de sus datos personales	
POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES	SI/NO
Se cuenta con una política para el tratamiento de los datos personales	
La política para el tratamiento de datos personales consta en medio físico o electrónico, en un lenguaje claro y sencillo, y es puesta en conocimiento de los titulares	

Cuadro 14. (Continuación)

Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las MIPYMES	
Se cuenta con una política para el tratamiento de los datos personales que incluye el nombre o razón social, domicilio, dirección, correo electrónico y teléfono de la organización.	
La política para el tratamiento de datos adoptada por la organización incluye información sobre el tratamiento al cual serán sometidos los datos personales y la finalidad de este.	
Incluye la política para el tratamiento de datos personales información sobre los derechos que le asisten a los titulares respecto de su información personal	
Se informa en la política para el tratamiento de datos personales sobre la persona o área responsabilidad de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.	
Se indica en la política para el tratamiento de datos personales cuál o cuáles son los procedimientos para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización	
En la política para el tratamiento de datos personales está incluida la fecha de entrada en vigor y el periodo de vigencia de la o las bases de datos que tiene la organización.	
AVISO DE PRIVACIDAD	SI/NO
Se informa a los titulares la existencia de la política para el tratamiento de datos personales por medio de un aviso de privacidad	
El aviso de privacidad publicado por la organización incluye el nombre o razón social y los datos de contacto de esta	
En el aviso de privacidad publicado se incluye la descripción del tratamiento al cual serán sometidos los datos personales recolectados y la finalidad de tal recolección	
El aviso de privacidad incluye un listado de los derechos que tienen los titulares cuya información es recolectada por la organización	
Se informa a los titulares en el aviso de privacidad publicado, cómo acceder o consultar la política de tratamiento de datos personales dispuesta por la organización	
En el aviso de privacidad publicado se señala expresamente la facultad que tienen los titulares de contestar o no las preguntas que versen sobre datos personales sensibles o sobre los datos de niños, niñas y adolescentes.	
Se conserva el modelo de aviso de privacidad utilizado para cumplir con la obligación legal de dar a conocer las políticas de tratamiento de la información personal	
REPORTE DE VIOLACIONES A LOS CÓDIGOS DE SEGURIDAD	SI/NO
Informa a la Superintendencia cuando se presentan violaciones a los códigos de seguridad que generen riesgos en la administración de la información de los titulares	
GESTIÓN DE ENCARGADOS DEL TRATAMIENTO	SI/NO
Se han establecidos procedimientos internos para asegurar que los Encargados del tratamiento garanticen la protección de los datos personales que le son entregados y que su tratamiento se haga acorde con los principios y deberes establecidos en la ley	
Se suscriben contratos con los Encargados que incluyen expresamente el tratamiento que éste podrá realizar a los datos personales	
Se suscriben contratos con los Encargados que incluyen cláusulas de confidencialidad de la información entregada	
Se exige a los encargados tener y mantener políticas de seguridad de la información y de tratamiento de datos personales antes de entregar las bases de datos	
Se informa al encargado de forma oportuna todas las novedades respecto de los datos que previamente le fueron suministradas	
Se cuenta con medidas necesarias para que la información suministrada al encargado se mantenga actualizada	
Se comunica al encargado cuando se ha rectificado la información incorrecta	
Se comunica al encargado si determinada información se encuentra en discusión por parte del titular, una vez éste presenta una reclamación y no ha finalizado el trámite respectivo	
Se verifica que el encargado actualice y rectifique la información personal en los términos legales.	
TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES	SI/NO
Se transfieren datos personales a países que garantizan niveles adecuados de protección de datos, según lo establecido en el numeral 3.2 de capítulo tercero del título V de la circular única de la Superintendencia de Industria y Comercio	

Cuadro 14. (Continuación)

Cuestionario de diagnóstico para el cumplimiento de la Ley 1581 de 2012 en las MIPYMES	
Se han implementado medidas a apropiadas y efectivas para garantizar el adecuado tratamiento de los datos personales que se transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia	
Se transfieren datos personales fuera del territorio colombiano con base en alguna de las causales de excepción establecidas en el artículo 26 de la ley 1581 de 2012	
Se transfiere datos personales fuera del territorio colombiano con base en una declaración de conformidad emitida por esta Superintendencia	
Se han suscrito contratos con los responsables del tratamiento destinatarios de los datos personales a transferir fuera del territorio colombiano o se implementan otros instrumentos jurídicos en los que se señalen las condiciones que regirán la transferencia	
Internacional de datos personales, mediante las cuales se garantizará el cumplimiento de los principios que rigen el tratamiento, así como de las obligaciones que tienen a cargo	
Se transmiten datos personales fuera del territorio colombiano a un encargado para que realice el tratamiento indicado por la organización como responsable del tratamiento y para ello han suscrito contratos de transmisión de datos personales en los que se señalen los alcances del tratamiento, las actividades que el encargado realizará y obligaciones de este respecto de los titulares y el responsable.	
Se incluyen en el contrato de transmisión internacional de datos personales celebrado con el Encargado cláusulas mediante las cuales este se compromete a dar aplicación a las obligaciones del responsable bajo su política de tratamiento de la información y a realizar el tratamiento de datos de acuerdo con la finalidad que los titulares han autorizado y con las leyes aplicaciones	
Se incluyen en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación de dar tratamiento, a nombre del responsable, a los datos personales conforme a los principios establecidos en la ley general de protección de datos personales	
Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación para este de salvaguardar la seguridad de las bases de datos que contengan datos personales	
Se incluye en el contrato de transmisión internacional de datos personales celebrado con el Encargado la obligación para este de guardar confidencialidad respecto del tratamiento de los datos personales	
RESPONSABILIDAD DEMOSTRADA	SI/NO
Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el decreto único 1074 de 2015 de manera proporcional a la naturaleza jurídica de la organización y su tamaño empresarial	
Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la ley 1581 de 2012 y el decreto único 1074 de 2015 de manera proporcional a la naturaleza de los datos personales objeto del tratamiento	
Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la ley 1581 de 2012 y el decreto único 1074 de 2015 de manera proporcional al tipo de tratamiento que realice con los datos personales	
Se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la ley 1581 de 2012 y el decreto único 1074 de 2015 de manera proporcional a los riesgos potenciales que el tratamiento podrías causar sobre los derechos de los titulares	
Se conserva evidencia sobre la implementación efectiva de medidas de seguridad apropiadas para el cumplimiento del régimen de protección de datos personales	
Se han adoptado mecanismos internos para poner en práctica las políticas establecidas en los que se incluyan herramientas de implementación, entrenamiento y programas de educación en materia de protección de datos personales	
REGISTRO NACIONAL DE BASES DE DATOS	SI/NO
Se han registrado las bases de datos con información personal de la organización en el Registro Nacional de Bases de datos (RNBD) administrado por la Superintendencia de Industria y comercio	

Fuente. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Cuestionario de diagnóstico para el cumplimiento de la ley 1581 de 2012 en las MIPYMES [en línea]. Bogotá: La Superintendencia [citado 27 octubre 2020]. Disponible en Internet: <URL: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cuestionario_de_diagnostico_para_el_cumplimiento_de_la_Ley_1581_de_2012_en_las_Mipymes.pdf>

Cuadro 15. Accountability

Compromisos de la organización	
DESDE LA ALTA DIRECCIÓN	SI/NO
Se cuenta con el compromiso de la organización para la implementación de un programa integral de gestión de datos personales	
Existe en la organización una cultura de respeto a la protección de los datos personales que se recogen o tratan	
Se han comprometido recursos económicos y de personal en la organización, acorde a su tamaño y estructura, así como al tipo de información a la que se le realiza Tratamiento, para la implementación del Programa Integral de Gestión de Datos Personales	
Se cuenta con el apoyo y compromiso de la Alta Dirección para generar una cultura organizacional de respeto a la protección de datos personales	
La Alta Dirección de la organización designó a la persona o área que asumirá la función de protección de datos dentro de la organización	
La Alta Dirección de la organización aprobó el Programa Integral de Gestión de Datos Personales	
La Alta Dirección de la organización realiza un monitoreo del Programa Integral de Gestión de Datos Personales.	
La Alta Dirección de la organización informa de manera periódica a los órganos directivos sobre la ejecución del programa Integral de Gestión de Datos Personales	
La Alta Dirección de la organización destina recursos suficientes al área o persona encargada de diseñar e implementar el Programa Integral de Gestión de Datos Personales para desempeñar sus funciones.	
A través del área o persona encargada de diseñar e implementar el Programa Integral de Gestión de Datos Personales se establecen las responsabilidades específicas para otras áreas de la organización respecto de la recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales que se tratan.	
OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	SI/NO
Se cuenta con una persona o área que asume la función de protección de datos personales y que da trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el Decreto Único Reglamentario 1074 de 2015.	
Se cuenta con una persona o área que vele por la implementación efectiva de las políticas y procedimientos adoptados por la organización para cumplir las normas de protección de datos personales.	
Se cuenta con una persona o área que establezca los controles del Programa Integral de Gestión de Datos Personales, así como la evaluación y revisión permanente de dichos controles.	
La persona o área que asume la función de protección de datos personales ha promovido la elaboración e implementación de un sistema que permita administrar los riesgos del Tratamiento de datos personales.	
La persona o área que asume la función de protección de datos personales sirve de enlace y coordina las demás áreas de la organización para asegurar la implementación transversal del Programa Integral de Gestión de Datos Personales.	
La persona o área que asume la función de protección de datos personales impulsa dentro de la organización una cultura de protección de datos.	
La persona o área que asume la función de protección de datos personales mantiene un inventario de las bases de datos personales en poder de la organización y las clasifica de acuerdo con su tipo.	
La persona o área que asume la función de protección de datos personales ha solicitado la declaración de conformidad de las operaciones de transferencia internacional de información personal ante la Superintendencia, cuando ha sido requerida, de conformidad con las instrucciones impartidas por esa entidad.	
La persona o área que asume la función de protección de datos personales revisa los contenidos de los contratos de transmisiones internacionales de datos, suscritos por la organización con los Encargados del Tratamiento no residentes en Colombia.	
La persona o área que asume la función de protección de datos personales ha diseñado un programa de entrenamiento en protección de datos personales acorde con las responsabilidades de cada cargo de la organización.	

Cuadro 15. (Continuación)

Compromisos de la organización	

La persona o área que asume la función de protección de datos personales realiza un entrenamiento general a todos los empleados y colaboradores de la compañía en protección de datos personales.	
La persona o área que asume la función de protección de datos personales realiza un entrenamiento a los nuevos empleados o colaboradores de la organización que, por las condiciones de su empleo, tengan acceso a los datos personales que se gestionan al interior de esta.	
La persona o área que asume la función de protección de datos personales integral las políticas de protección de datos personales dentro de las actividades de las demás áreas de la organización.	
La persona o área que asume la función de protección de datos personales mide la participación de los empleados y colaboradores en los entrenamientos en protección de datos y califica su desempeño.	
La persona o área que asume la función de protección de datos personales requiere que se complete satisfactoriamente el entrenamiento en protección de datos personales para realizar el analista del desempeño de los empleados y colaboradores.	
La persona o área que asume la función de protección de datos personales acompaña y asiste a la organización en la atención de las visitas y requerimientos realizados por la Superintendencia de Industria y Comercio.	
La persona o área que asume la función de protección de datos personales realiza seguimiento al Programa Integral de Gestión de datos personales.	
PRESENTACIÓN DE INFORMES	SI/NO
Se cuenta con planes de auditoría interna para verificar el cumplimiento de las políticas de Tratamiento de datos personales y señalar el procedimiento a seguir en caso de que se presenten violaciones a los códigos de seguridad o se detecten riesgos en la administración de la información personal de los Titulares.	
De define la estructura de la generación de reportes en la que se establezca qué empleado o persona genera qué tipo de reporte y se asignan responsabilidades claras ante una queja de los Titulares o una violación a los códigos de seguridad.	
Se documenta el proceso de generación de reportes como parte del Programa Integral de Gestión de Datos Personales.	
Se generan reportes para los accionistas o socios de manera periódica y se informa a estos el estado del Programa Integral de Gestión de Datos Personales.	
CONTROLES DEL PROGRAMA	
PROCEDIMIENTOS OPERACIONALES	SI/NO
Se cuenta con procedimientos administrativos consistentes con las políticas generales de protección de datos personales y con las disposiciones legales vigentes, para manejar adecuadamente los riesgos inherentes al Tratamiento de datos personales dentro de la gestión operacional.	
INVENTARIO DE BASES DE DATOS CON INFORMACIÓN PERSONAL	SI/NO
Se tienen identificadas e inventariadas las bases de datos dentro de la organización.	
Se tiene claridad sobre el medio en el que se conservan las bases de datos al interior de la organización (manual o automatizado). Se tiene claridad de cuántos Titulares o personas naturales existen en cada base de datos.	
Se tiene identificado qué tipo de datos personales reposan en cada base de datos (datos de identificación, datos de ubicación, datos sensibles, datos de contenido socioeconómico, etc.)	
Se tiene establecido claramente para qué se utiliza cada base de datos y si realmente los datos que allí reposan son necesarios, teniendo en cuenta la finalidad para la que se recolectan.	
Se han identificado cómo se obtienen los datos personales en la organización, si se debe solicitar la autorización de los Titulares para obtener esos datos y, de ser así, sí se conserva prueba de tal autorización para su posterior consulta.	
Se informa a los Titulares la finalidad de la recolección de sus datos personales y el Tratamiento al que tales datos serán sometidos, así como los derechos que tienen como titulares.	
Se protege la calidad de la información personal al momento de su recolección.	
Si se recolectan datos de menores de edad, se han imprentado medidas adecuadas para garantizar una protección reforzada de dicha información.	

Cuadro 15. (Continuación)

Compromisos de la organización	

Si se recolectan datos menores de edad, la organización informa al Titular o a quien corresponda (tutores o representantes de los menores), que no existe obligación de suministrar tales datos.	
Se ha identificado qué áreas de la organización utilizan los datos personales y de qué forma los utilizan.	
Se han implementado medidas de seguridad para tratar y conservar los datos personales recolectados.	
Se han implementado procedimientos para actualizar, rectificar y depurar los datos personales en las bases de datos.	
Se entregan o comparten las bases de datos con información personal a terceros ubicados dentro o fuera del país.	
Se ha identificado para qué entregan o comparte las bases de datos con información personal con terceros dentro o fuera del territorio nacional.	
Se ha identificado por cuánto tiempo se conservan los datos personales y qué medios se utilizan para su disposición final (archivo físico, digitalización, eliminación, etc.)	
Se cuenta con medidas técnicas que garanticen la seguridad de los datos personales una vez se ha definido cuál será su disposición final.	
POLÍTICAS	SI/NO
Se cuenta con políticas internas debidamente documentadas e implementadas que incluyan las obligaciones señaladas en la Ley de protección de Datos Personales y se dan a conocer a los empleados o colaboradores.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la recolección o recopilación, el mantenimiento, uso y eliminación o disposición final de los datos personales.	
Se cuanta con procedimientos debidamente documentados e implementados que establezcan los requisitos para obtener la autorización de los Titulares.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la conservación y eliminación de información personal.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para el uso Responsables de la información, incluyendo controles administrativos, físicos y tecnológicos que garanticen la seguridad de la información.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la inclusión en todos los medios contractuales de la empresa de una cláusula de confidencialidad y de manejo de información, donde se afirme que se conoce la política de la empresa, se acepta, y se permite a la compañía utilizar dicha información de forma Responsable.	
Se cuenta con procedimientos debidamente documentados e implementados donde se establezcan reglas para la presentación de quejas, denuncias y reclamos por parte de los Titulares y la forma de tramitarlas y atenderlas de manera adecuada, congruente y oportuna.	
Se incluye en las políticas de la organización, diferentes a la de protección de datos personales (talento humano, contratos, transparencia, etc.), elementos que permitan cumplir las normas sobre protección de datos.	
SISTEMA DE ADMINISTRACIÓN DE RIESGOS	SI/NO
Cuenta con un sistema de administración de riesgos, acorde con la estructura organizacional, los procedimientos internos asociados al tratamiento de datos personales, la cantidad de bases de datos y los tipos de datos personales tratados por la empresa, que le permita identificar, medir, controlar y monitorear aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos los datos personales.	
Se ha identificado a qué riesgos se ven expuestos los datos personales a los que se realiza Tratamiento al interior de la organización (ej.: riesgo de pérdida o fuga de información, riesgo de mantener información desactualizada o no veraz, riesgo de acceso indebidos a la información, etc.).	
Se ha determinado la posibilidad de ocurrencia de los riesgos identificación y el impacto que podría ocasionar la materialización de estos, tanto para los Titulares como para la organización.	
Se ha establecidos qué acciones se deben tomar para controlar y/o mitigar los riesgos identificados, con el fin de disminuir la posibilidad y/o el impacto de la materialización de dichos riesgos.	

Cuadro 15. (Continuación)

Compromisos de la organización	

Los controles establecidos son suficientes, efectivos y oportunos para disminuir la posibilidad y/o el impacto de la materialización de los riesgos.	
Se realiza seguimiento constante para velar porque las medidas adoptadas sean efectivas	
Se realiza una evaluación de riesgos constante en la organización y desde el diseño en cada proyecto en él se involucre el Tratamiento de datos personales.	
FORMACIÓN Y EDUCACIÓN	SI/NO
Se tiene implementado un programa de capacitación para los empleados y contratistas de la organización en materia de protección de datos personales.	
Se realizan jornadas de capacitación al personal en materia de protección de datos personales, con periodicidad.	
Las capacitaciones realizadas a los empleados, contratistas y colaboradores en general de la organización involucrados directamente en las actividades de Tratamiento de datos personales se adaptan específicamente a las funciones, obligaciones y tareas que tienen a cargo.	
Existen dentro de los contratos suscritos por los empleados de la organización acuerdos de cumplimiento de las políticas internas desarrolladas por esta para el adecuado Tratamiento de los datos personales.	
PROTOCOLOS DE RESPUESTA EN EL MANEJO DE VIOLACIONES E INCIDENTES DE SEGURIDAD	SI/NO
Se cuenta con un procedimiento documentados e implementado y una persona o área encargada de manejar los incidentes o violaciones a los sistemas de información donde se gestionan datos personales y a los archivos físicos.	
Los empleados y contratistas de la organización tienen conocimiento sobre qué hacer antes, durante y después de que se presente un incidente de seguridad.	
Dentro del protocolo de incidentes de seguridad adoptado por la organización está previsto reportar a la Superintendencia de Industria y Comercio la ocurrencia de tales incidentes.	
Se cuenta con mecanismos, herramientas o procedimientos para la elaboración de informes internos y para informar tanto a los Titulares como a la Superintendencia de Industria y Comercio cuando se presenten incidentes de seguridad que involucren datos personales.	
Se cuenta con mecanismos, herramientas o procedimientos que permitan, además de informar a los Titulares la ocurrencia de un incidente de seguridad con sus datos personales y las posibles consecuencias, dar a conocer opciones o alternativas a dichos Titulares para minimizar el daño potencial o el daño causado.	
Se cuanta con mecanismos o procedimientos que permitan informar a la Superintendencia el tipo de incidente ocurrido la fecha en la que ocurrió y la fecha en la que se tuvo conocimiento de este, la causal del incidente, el tipo de datos personales comprometidos y la cantidad de Titulares afectados.	
GESTIÓN DE LOS ENCARGADOS DEL TRATAMIENTO EN LAS TRANSMISIONES INTERNACIONALES DE DATOS PERSONALES.	SI/NO
Se han implementado medidas para asegurar la protección de los datos personales cuyo Tratamiento es realizado por los Encargados.	
Los contratos suscritos con los Encargados del tratamiento incluyen requisitos para que estos cumplan las normas colombianas de protección de datos y las políticas de Tratamiento de la información adoptadas por la organización.	
Se cuenta con mecanismos para que los Encargados reporten a la organización los incidentes de seguridad de la información que se presentan.	
Se verifica si los Encargados del Tratamiento de la información personal cuentan con política de Tratamiento de datos personales y programas de formación o educación en temas de protección de datos para sus empleados.	
Se exige la realización de auditoría internas y/o externas a las actividades desarrolladas por el Encargado del Tratamiento.	
Existen acuerdos con los Encargados y sus empleados o colaboradores aceptando que cumplirán con las políticas y protocolos de Tratamientos de datos de su organización.	
Se exige a los Encargados que utilizan subcontratistas que se establezcan obligaciones para éstos de adherencia a las políticas de Tratamiento de la organización.	

Cuadro 15. (Continuación)

Compromisos de la organización	
COMUNICACIÓN EXTERNA	SI/NO

Se han implementados procedimientos para informar a los Titulares sus derechos.	
Se dirigen comunicaciones claras y comprensibles a los Titulares.	
Se cuenta con un área o persona encargada de la atención de las quejas y reclamos relacionados con el ejercicio del derecho de hábeas data.	
Se informa a los Titulares cuáles son los canales de atención que la organización tiene dispuestos para la presentación de sus reclamaciones o consultas.	
EVALUACIÓN Y REVISIÓN CONTINUA	
PLAN DE SUPERVISIÓN Y REVISIÓN	SI/NO
Se ha desarrollado dentro de la organización un plan de supervisión y revisión anual del Programa Integral de Gestión de Datos Personales.	
El plan de supervisión y revisión implementado establece las medidas de desempeño e incluye un calendario para las revisiones de las políticas y los controles del Programa Integral de Gestión de Datos Personales, por lo menos una vez al año.	
EVALUACIÓN Y REVISIÓN DE LOS CONTROLES DEL PROGRAMA	SI/NO
Se revisan y evalúan periódicamente los controles establecidos para minimizar o evitar la materialización de los riesgos en el Tratamiento de datos personales.	
Los controles establecidos tienen en cuenta las nuevas amenazas, los motivos de las quejas más recientes presentadas por los Titulares, los hallazgos en las auditorías o las orientaciones de la autoridad de protección de datos.	
Se hace seguimiento a los servicios prestados por la organización que involucran recolección, uso, divulgación y, en general, cualquier Tratamiento de información personal para determinar que estén cumpliendo las políticas y procedimientos adoptados.	
Se realizan capacitaciones idóneas y acordes con las políticas y procedimientos dispuestos por la organización.	
La persona o área que asume la función de protección de datos personales controla y actualiza el inventario de información personal continuamente para identificar y evaluar nuevas recolecciones, usos y divulgaciones.	
La persona o área que asume la función de protección de datos personales revisa las políticas de acuerdo con los resultados de las evaluaciones o auditoría.	
La persona o área que asume la función de protección de datos personales mantiene como documentos históricos las evaluaciones de impacto y las de amenazas a la seguridad y riesgos.	
La persona o área que asume la función de protección de datos personales revisa y actualiza, en forma periódica, los programas de formación y educación para todos los empleados de la organización como resultado de evaluaciones continuas.	
La persona o área que asume la función de protección de datos personales revisa y adapta los protocolos de respuesta al manejo de violaciones e incidentes de seguridad e implementa las mejores prácticas y recomendaciones de las revisiones que se efectúan posterior a la ocurrencia de esos incidentes.	
La persona o área que asume la función de protección de datos personales revisa y, si es el caso, modifica los requisitos establecidos en los contratos suscritos por la organización con los Encargados del Tratamiento.	
La persona o área que asume la función de protección de datos personales actualiza y clara las comunicaciones externas para explicar las políticas de Tratamiento de datos.	
La persona o área que asume la función de protección de datos personales reporta semestralmente al representante legal de la empresa la evolución del riesgo, los controles implementados, el monitoreo y, en general, los avances y resultados del Programa Integral de Gestión de Datos Personales.	

Fuente. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Guía para la implementación del principio de responsabilidad demostrada (Accountability) [en línea]. Bogotá: La Superintendencia [citado 27 octubre, 2020]. Disponible en Internet: <URL: https://issuu.com/quioscosic/docs/guia_accountability_6e79bc4c4b6fef.>

7.1.4 FASE CUATRO- EVALUACIÓN DE RIESGOS

7.1.4.1 IDENTIFICACIÓN RIESGOS, AMENAZAS Y EL ESTADO DE LA PROTECCIÓN DE DATOS PERSONALES DE LA ORGANIZACIÓN

Cuanto mayor sea entendimiento de los riesgos de los datos personales aumenta la seguridad en la protección de estos, el riesgo no se puede eliminar en su totalidad, pero con el apoyo de la mejora continua se pueden reducir en gran medida hasta hacerlo aceptables para la organización.

Esta fase tiene como fin que los responsables identifiquen las características de los riesgos que podrían tener mayor impacto sobre la protección de los datos personales que tratan, con el fin de tomar decisiones para el tratamiento y la priorización de los riesgos más relevantes e inmediatos a implementar.

De esta manera se presenta las siguientes fases para gestión de los riesgos de la protección de datos personales (véase la Figura 4).

Figura 4. Proceso para Monitorear Riesgos

Fuente. Los Autores

➢Identificar riesgos. Los riesgos tienen variación y dependen de la exposición a amenazas de la actividad de tratamiento, de acuerdo con esto es de gran importancia disponer de una descripción detallada del tratamiento, los elementos más relevantes que intervienen y su contexto. En esta etapa es necesario identificar los activos de información que hacen parte de la protección de datos personales tales como la información propiamente dicha, así como los activos de soporte en los que se almacenan, procesan y que ayudan a mantener toda la seguridad necesaria para dicha información.
El riesgo se materializa a raíz de la exposición a amenazas y por esta razón, es fundamental entender cuáles actúan sobre los datos personales teniendo en cuenta los siguientes aspectos:

• El riesgo inherente a cada de dato personal de acuerdo a su tipología.
• El desarrollo de la infraestructura tecnológica
• Las consecuencias de la materialización de una vulneración para los titulares de los datos personales.

Adicionalmente, se debe tomar en cuenta los siguientes puntos:

• La cantidad de titulares;

• Los incidentes ocurridos previamente en los sistemas de tratamiento;

• Otros factores que puedan afectar el nivel la valoración del riesgo o que surjan a partir de nuevas regulaciones.

➢Evaluar los riesgos. La evaluación de riesgos consiste en valorar el impacto de la materialización de un evento, junto a la probabilidad de ocurrencia de este. El impacto se mide con relación a los posibles daños que se pueden producir si una amenaza se materializa. Para realizar la evaluación de riesgos es uno de los pasos que se utiliza en un proceso de gestión de riesgos es necesario definir las escalas cuantitativas y/o cualitativas de los dos parámetros que lo determinan, la magnitud de la pérdida o daño posible (impacto) y la probabilidad que dicha pérdida o daño llegue a ocurrir, además de estos dos parámetros también se debe definir el apetito del riesgo y la tolerancia al riesgo de la organización. Dentro de esta etapa se incluye la generación de mapas de calor las cuales apoyan a la visualización y priorización de los riesgos inherentes y residuales de acuerdo con el resultado en cada cuadrante de dicho gráfico.

➢Tratar los riesgos. Una vez realizado el análisis de riesgos de la protección de datos personales es necesario que se seleccionen e implementen las respectivas medidas que permitan disminuir los riesgos, para elegir las medidas de seguridad efectivas se pueden tomar en cuenta los siguientes criterios que:

•Impidan la divulgación no autorizada de los datos personales.

•Protejan los datos personales contra su destrucción, alteración, daño o su pérdida.

•Impidan el acceso, uso o tratamiento no autorizado de los datos personales.

Para realizar el análisis de brechas de las medidas de seguridad previamente se debe realizar la identificación de los procesos y los activos asociados a los datos personales, así como las amenazas, vulnerabilidades y los eventos o incidentes relacionados y consiste en identificar los siguientes puntos:

•Las medidas de seguridad implementadas.

•Las medidas de seguridad implementadas que eficaces.
•Las medidas de seguridad aun no existentes.

Es importante identificar los controles que ya están se están ejecutando en la organización de manera efectiva, así como las medidas identificadas como faltantes, para generar un plan de trabajo enfocado en las actividades a ejecutar, los responsables, y las fechas compromiso para su implementación.

Los controles efectivos pueden ser identificados teniendo en cuenta su cumplimiento de los siguientes aspectos:

•**Documentación.** Se han documentado las características y los objetivos del control, así como las políticas que soportan su cumplimiento.

✓No Documentado
✓Documentado no actualizado
✓Documentado
✓Documentado desplegado

•**Implementación.** El control se encuentra activo a través de una o más medidas de privacidad. Las opciones de implementación de los controles son:

✓Manual
✓Combinado
✓Automatizado

•**Tipo.** Los tipos de controles son los siguientes:

✓Detectivo
✓Preventivo
✓Correctivo.

•**Percepción de Efectividad.** Los niveles de percepción de la efectividad de los controles son:

✓Ninguna
✓Poca
✓Media
✓Alta

➢Monitorizar los riesgos. Teniendo en cuenta que los riesgos son variables en el tiempo y pueden cambiar ante variaciones en las actividades de tratamiento es de gran importancia garantizar una adecuada monitorización continua de los riesgos y realizar evaluaciones periódicas de la efectividad de los controles definidos para reducir su impacto o su probabilidad de ocurrencia.

Se recomienda revisar de una manera sistemática el análisis de riesgos realizado para detectar cualquier cambio significativo en las actividades de tratamiento que pueda generar la aparición de nuevos riesgos o su incidencia sobre el impacto y su probabilidad de ocurrencia.

➢Guía de uso de la herramienta “Matriz de Riesgos”. La primera hoja de la herramienta contiene el menú general para desplazarse por las distintas fases de la gestión de riesgos para la protección de datos personales. Como se muestra a continuación (véase la Figura 5)

Figura 5. Menú Guía de uso de la herramienta “Matriz de Riesgos

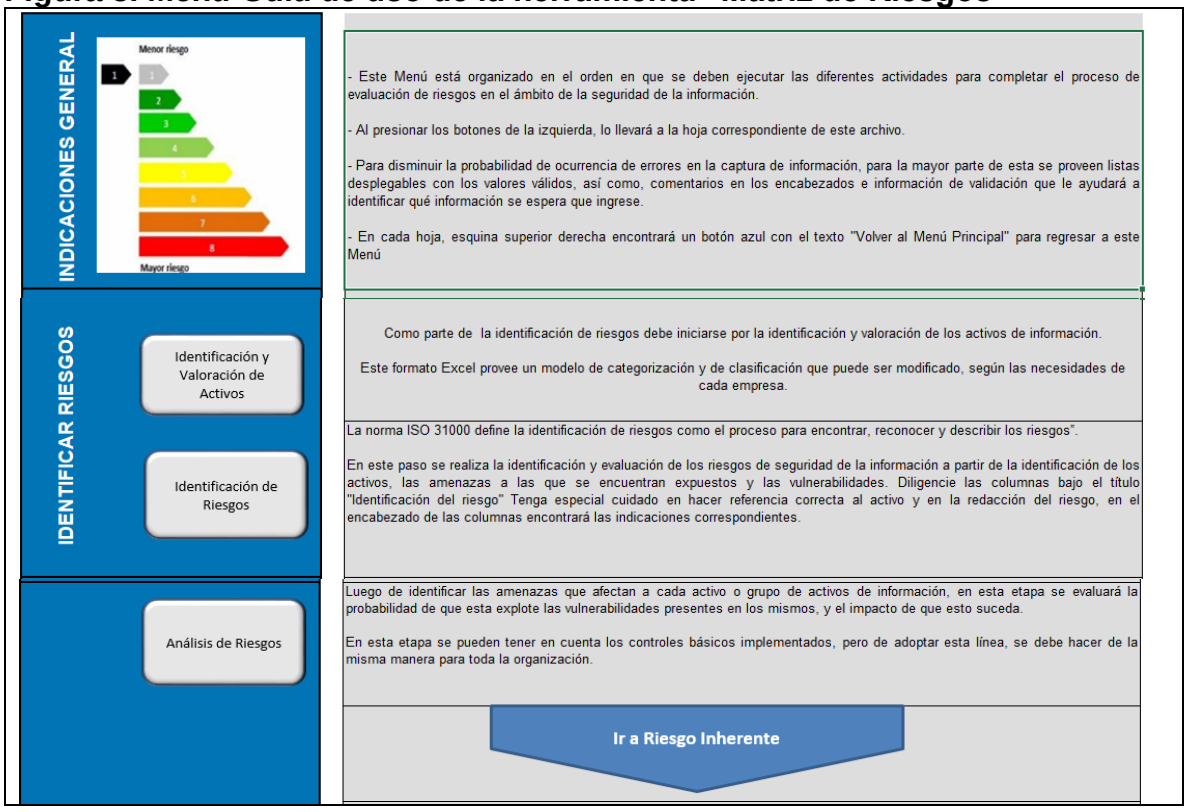
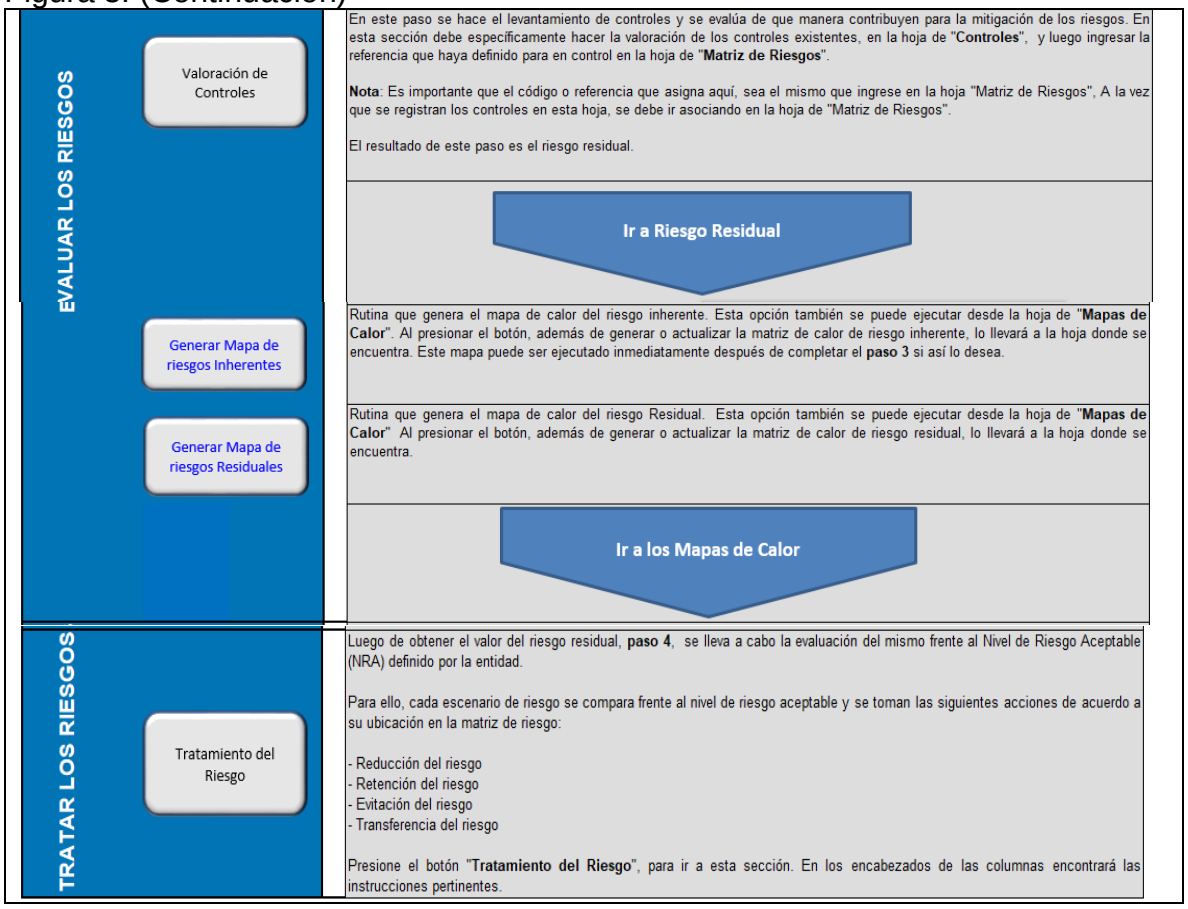


Figura 5. (Continuación)



Fuente. Los Autores

A continuación, se muestra el desarrollo de la identificación y valoración de activos de información, así como el propietario de los riesgos, el proceso asociado y la fecha de elaboración (véase el Cuadro 16).

Cuadro 16. Inventario y Valoración de Activos de Información

Inventario y Valoración de Activos de Información	
PROPIETARIO DE LOS RIESGOS (Nombre y cargo del responsable del proceso):	Juan Perez - Gerente Comercial
PROCESO RESPONSABLE	Vicepresidencia Comercial
FECHA DE ELABORACIÓN/VALIDACIÓN:	10/10/2020

Fuente. Los Autores

En esta fase se debe identificar el activo de información, su categoría su impacto frente a la CIA y su nivel de clasificación de acuerdo a los datos contenidos, en esta fase también es necesario identificar quienes tienen acceso a esta información y cuáles son sus privilegios frente a la misma, así como su ubicación y propietarios, custodios y responsables (véase los Cuadros 17 y 18)

Cuadro 17. Nivel de Clasificación

Nombre del Activo	Descripción	Tipo de Activo	Categoria Activo ISO/IEC 27005:2009, ANEXO B	Confidencialidad	Integridad	Disponibilidad	Valoración	A1	A2	A3	A4	Nivel de Clasificacion
CRM	Gestion de las relaciones del cliente	Sistema de Información	De soporte	4	4	4	4	1	0	0	0	Semiprivado
Datos Clientes	Información de clientes de entidad financiera porpietarios de tarjeta de credito	Información	Primario	5	3	2	3	0	1	0	0	Privado

Fuente. Los Autores

Cuadro 18. Responsables

Acceso		Soporte	Ubicacion		Propietario	Responsable	Custodio
Usuarios	Privilegios		Fisico	Electrónico			
Gerente Comercial	PN1	Digital	NA	Servidor Jupiter	Vicepresidencia Comercial	Vicepresidente Comercial	Gerente Comercial
Asesor Comercial	PN4						
Ejecutivo Comercial	PN2						
Gerente Comercial	PN1	Digital	NA	Base de Datos	Vicepresidencia Comercial	Vicepresidente Comercial	Gerente Comercial
Asesor Comercial	PN2						

Fuente. Los Autores

Esta fase busca identificar los posibles riesgos asociados a un activo de información, así como las amenazas y vulnerabilidades de estos (véase el Cuadro 19)

Cuadro 19. Identificación de Riesgos

Matriz de Riesgos

Código Riesgo	Nombre del Activo	Descripción Activo	Tipo Activo	Categoria Activo ISO/IEC 27005:2009, ANEXO B	Amenaza	Vulnerabilidades
R-001	CRM	Gestion de las relaciones del cliente	Sistema de Información	De soporte	Procesamiento ilegal de los datos	Habilitación de servicios innecesarios
R-002	Datos Clientes	Información de clientes de entidad financiera porpietarios de tarjeta de credito	Información	Primario	Falsificación de derechos	Gestión deficiente de contraseñas

Fuente. Los Autores

En esta misma hoja se debe evaluar el nivel del riesgo inherente de un activo de información en función de la probabilidad de ocurrencia y del impacto a la imagen, a la información, legal y financiero que genere un evento identificado si este se llegara a materializar, así como los controles implementados y su respectiva evaluación para dar como resultado un riesgo residual al cual se le aplicará un tratamiento en particular de acuerdo al apetito y tolerancia al riesgo que defina la organización (véase los Cuadros 20, 21, 22, 23 y 24).

Cuadro 20. Evaluación de Riesgo

Redacción del Riesgo	Evaluar el Riesgo									
	Probabilidad de Ocurrencia		Impacto Credibilidad e Imagen	Impacto Información	Impacto Legal	Impacto Financiero	Impacto Total	Descripción Impacto	Nivel de Riesgo Inherente	
Se presenta afectacion a la integridad del sistema de informacion de gestion de clientes CRM debido a la asignaciòn de privilegios inadecuados a modulos que no corresponden con el rol del funcionario generando perdida de la imagen de la organización.	3	Posible	3	3	2	2	3	Moderado	A	Alto
Posible afectaciòn sobre la integridad de la informaciòn manejada en las bases de datos de clientes por una gestiòn deficiente de contraseñas que le permita la suplantaciòn y acceso a personal malintencionado.	2	Improbable	4	4	3	2	3	Moderado	M	Medio

Fuente. Los Autores

Cuadro 21. Descripción de Controles

Valoracion de controles						
Control	Descripción Control	Control 2	Descripción	Control 3	Descripción	Control 4
ctrl-TI-16	Establecer y comunicar políticas y procedimientos para identificar, autenticar y autorizar derechos de acceso para todos los usuarios, basados en la necesidad de conocer los mínimos privilegios.					
ctrl-TI-17	Definición y asignación de un ID unico por usuario.					

Fuente. Los Autores

Cuadro 22. Calificación del Control

Código del Control	NOMBRE Y DESCRIPCIÓN DE CONTROLES	Tipo	Implementación	Calificación	Documentación	Calificación	Percepción de Efectividad	Calificación	Puntaje Total Control	Calificación del Control
Ctrl-TI-15	Clasificar las áreas fisicas acorde a su sensibilidad	Correctivo	Manual	1	Documentado	2	Media	2	5	Moderado
Ctrl-TI-16	Establecer y comunicar políticas y procedimientos para identificar, autenticar y autorizar derechos de acceso para todos los usuarios, basados en la necesidad de conocer los mínimos privilegios.	Preventivo	Combinado	2	Documentado	2	Alta	3	7	Efectivo
Ctrl-TI-17	Definición y asignación de un ID unico por usuario.	Correctivo	Automatizado	3	Documentado	2	Alta	3	8	Efectivo
Ctrl-TI-18	Trazabilidad/Auditoría de las actividades de los usuarios acorde con su sensibilidad/criticidad.									
Ctrl-TI-19	Asegurar que la información de cambios/novedades de personal (ejemplo ingresos, retiros, retiro temporal, vacaciones, traslados, promociones) es comunicada oportunamente a los responsables de la administración de accesos.									
Ctrl-TI-20	Clasificar la información por su sensibilidad y criticidad.									
Ctrl-TI-21	Definir e implementar políticas para proteger la información sensible, ejemplo cifrado, códigos de autenticación, totales hash.									

Fuente. Los Autores

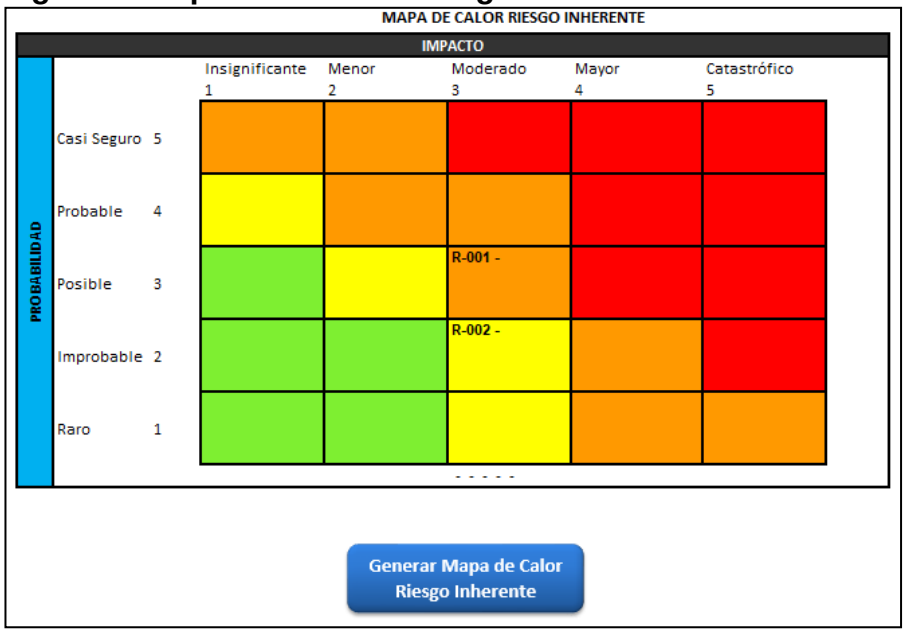
Cuadro 23. Tratamiento de Riesgo

			Tratamiento del Riesgo				
			Tratamiento	Plan de Manejo del Riesgo			
Impacto	Nivel de Riesgo Residual		Opción a Aplicar	Acciones a Realizar	Responsable	Fecha Terminación	Registro de evidencias
Moderado	M	Medio	**Reducción del riesgo**	Establecer plan de seguimiento y control respecto a los roles y perfiles que acceden a la BD de clientes.	Director de Infraestructura	2021/02/15	Bitacora de seguimiento y control de usuarios
Menor	B	Bajo	Retención del riesgo				

Fuente. Los Autores

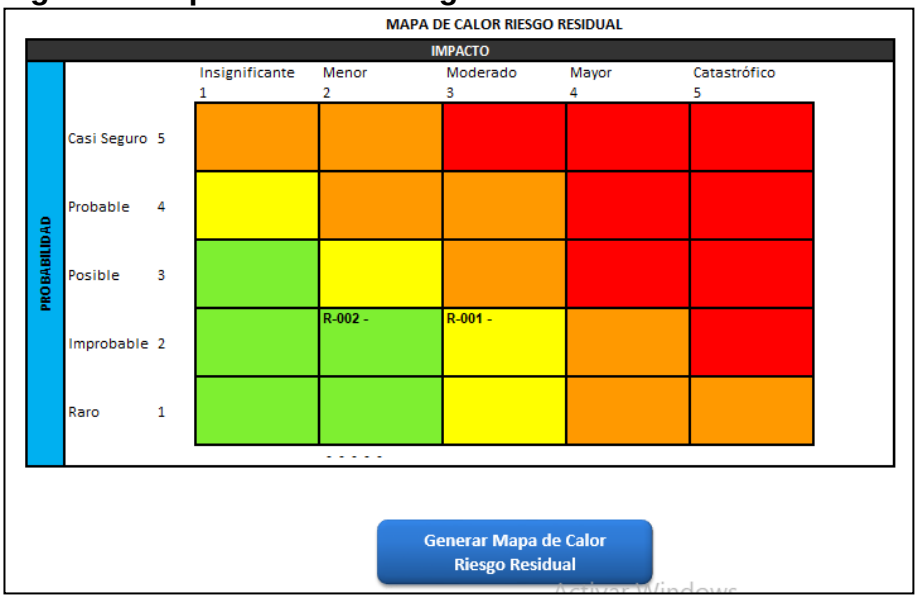
También se encontrará un mapa de calor tanto para el riesgo inherente como para el riesgo residual que permitirá visualizar de manera clara la prioridad con que se deben tratar los riesgos de acuerdo con su ubicación en el mismo y de acuerdo al apetito y tolerancia del riesgo de la organización, así como visualizar la efectividad que tienen los controles implementados sobre los riesgos identificados (véase las Figuras 6 y 7).

Figure 6. Mapa de Calor de riesgo Inherente



Fuente. Los Autores

Figure 7. Mapa de Calor Riesgos Residual



Fuente. Los Autores

7.1.5 FASE CINCO – EVALUACIÓN DE DESEMPEÑO

7.1.5.1 AUDITORIA

La organización debe considerar la planeación y ejecución de auditorías internas o externas para validar el cumplimiento de los requisitos de una manera objetiva y evitando siempre el conflicto de interés.

Las auditorias deben tener una programación periódica donde se asegure que la organización esté ejecutando de acuerdo con la política, manual de tratamiento de datos personales, procedimientos definidos e implementando todos los acuerdos de servicios y tecnológicos, de acuerdo con lo anterior en la tabla 15 se encontrará una guía de preguntas que podrían utilizarse para realizar una auditoría interna.

Es esencial guardar la información documentada como evidencia de los resultados de las auditorías, y esta deben ser socializada con la alta dirección. Los riesgos obtenidos de los resultados de las auditorias se emplear como medidas preventivas o como observaciones que solicitan medidas correctivas inmediatas contribuyendo así al ciclo de mejora continua en la protección de datos personales de la organización (véase el Cuadro 24).

Cuadro 24. Guía de Preguntas para Realizar Auditoría

Temas	Preguntas
Requisitos Básicos	¿Su organización tiene un programa integral de datos personales?
	¿La alta dirección ampara y lidera el cumplimiento de la ley de Protección de datos personales?
	¿Existe Política de tratamiento de datos personales? Este cumple con:
	a. Contiene el nombre o razón social, domicilio, dirección, correo electrónico y teléfono del responsable?
	b. Tratamiento al cual serán sometidos los datos y finalidad de este cuando ésta no se haya informado mediante el Aviso de privacidad.
	c. Menciona de manera completa los derechos del titular del dato.
	d. Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.
	e. Describe el procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.
	f. Indica la fecha de entrega en vigencia de la política de tratamiento de información y período de vigencia de la base de datos.
	¿Su política realiza actualizaciones periódicas?
	¿Su política es conocida por sus empleados, clientes, proveedores, socios de negocios y accionistas?
	¿Existe un área a cargo del sistema de protección de datos personales?
	¿Ya ha sido nombrado un Oficial de Protección de Datos Personales?
	¿En las diferentes áreas de la organización existen responsabilidades específicas para recolección, uso, almacenamiento, transfiere y suprime los datos personales?
	¿Existe una cultura de protección de datos en su organización?
	Cuentan con un Manual interno de políticas y procedimientos.
	¿Cuenta con un aviso de video Aviso de videovigilancia? Este cumple con:
	a. Nombre o razón social y datos de contacto del Responsable de Tratamiento.
	b. El tratamiento al cual serán sometidos los datos y la finalidad de este.
	c. Los derechos que le asisten al Titular.
	d. Los mecanismos dispuestos por el responsable de los datos para que el titular conozca la política y los cambios que se produzcan en ella o en el aviso de privacidad.
	¿Los empleados, practicante, temporales y contratistas en sitio están capacitados?
	¿Ha evaluado a su equipo humano respecto de la normatividad, su comprensión del alcance, riesgos, procesos y reclamaciones?
	¿El análisis de desempeño del equipo humano de su empresa incluye calificación por conocimientos en Protección de datos personales?
	¿Envía comunicaciones de concientización a los titulares datos?
	¿Existe un proceso de atención de reclamación de los titulares de datos?
	¿Se generan informes de reclamaciones por Protección de datos personales?
	¿Ha habido retroalimentación basadas en las reclamaciones para evitar que se repitan?
	¿Tiene políticas y procesos especiales para manejo de información de niños, niñas y adolescentes?
	¿Su empresa genera informe de cumplimiento con de la ley 1581 de 2012 de PDP para la gerencia, accionistas informes anuales a supe sociedades y entes de control?
	¿Los datos personales que manejan cuentan con autorización de los titulares? Este cumple con:
	a. El tratamiento al cual serán sometidos sus datos personales y la finalidad de este.

Cuadro 24. (Continuación)

Temas	Preguntas
	b. El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando éstas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes
	c. Los derechos que le asisten como Titular.
	d. La identificación, dirección física o electrónica y teléfono del responsable del tratamiento.
	¿Conserva la información de forma segura?
	¿Tienen un inventario de BD electrónicas?
	¿Tienen un inventario de BD físicas?
	¿Tienen las BD actualizadas?
	¿Su empresa y realizó el Registro Nacional de Bases de Datos -RNBD-?
Terceros	¿Tienen contratos de transmisión y transferencia de datos?
	¿Hace revisiones de cumplimiento de la política a sus proveedores?
	¿Conoce el nivel de capacitación de los terceros de Protección de datos personales?
	¿Sus subcontratistas se han adherido a sus políticas de Protección de datos personales?
	¿Tienen cláusulas de confidencialidad y manejo de información personal en todos los contratos realizados con encargados del tratamiento?
Riesgos	¿Han realizado un análisis de riesgos por Protección de datos personales?
	Tienen un sistema de administración de riesgos que contemple: ¿Identificación, medición, control y monitoreo de riesgos de privacidad?
	¿Tienen políticas de seguridad de la información?
	¿Tienen procesos probados de seguridad de la información?
	¿Tienen cláusulas de confidencialidad y manejo de información en todos los contratos pertinentes?
	¿Su empresa audita los avances en Protección de datos personales?
	¿Han analizado como impacta la ley de PDP en el cumplimiento de otras normas tales como SARLAFT, ley de transparencia, ley del consumidor, etc.?

Fuente. Los Autores

7.1.5.2 INDICADORES.

Las organizaciones se deben plantear implementar indicadores que permita medir el cumplimiento de sistema de protección de datos personales de acuerdo con los objetivos cumpliendo con los siguientes aspectos que sean específicos, medibles, alcanzables, realistas y temporizados. En la tabla 16 se deja dos ejemplos guía de indicadores (véase el Cuadro 25).

Cuadro 25. Indicadores

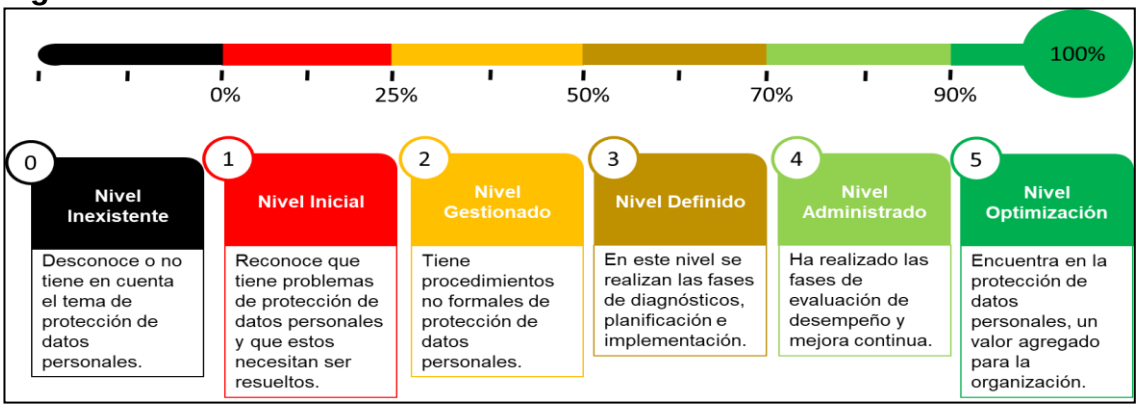
INDICADOR	MEDICIÓN
Gestión de respuesta a Consultas y reclamos.	= (Número total de requerimientos atendidos/ Número total de requerimientos recibidos) *100%
Gestión de incidentes de Protección de datos personales.	= (Número total de incidentes atendidos/ Número total de incidentes recibidos) *100

Fuente. Los Autores

7.1.5.3 MODELO DE MADUREZ

La siguiente figura muestra un esquema que permite identificar los niveles de madurez de privacidad en la organización, midiendo el nivel actual versus cada uno de los niveles del modelo (véase la Figura 8).

Figura 8. Nivel de Madurez



Fuente. Los Autores

En la Figura 8 se evidencian los niveles de madurez de la implementación de la protección de datos, los cuales buscan establecer los criterios de valoración para determinar el estado actual de la privacidad en una organización que cumple el rol de encargado.

En el siguiente cuadro, se presenta la descripción completa de calificación que se aplica al programa de evaluación de protección de datos personales y su relación con el literal del artículo 18 “DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO.” de la ley 1581 de 2012, se presenta a continuación:

Cuadro 26. Características de los Niveles de Madurez

Nivel	Literal artículo 18	Descripción
Inexistente		Los procesos no han sido documentados.
		No existen procesos estandarizados y tienen a ser aplicados de forma individual o en casos específicos.
		En estado de cambio dinámico.
		Aunque no se tiene un modelo de seguridad, se han implementado controles en su infraestructura de TI.
		La información no se identifica como un activo que contribuye al logro de su misión y objetivos estratégicos.
		No se genera conciencia sobre la importancia de la protección de datos personales en la entidad.
Inicial	a)	Existe una documentación mínima.
	a)	Se basa en gran medida en el conocimiento de las personas, por lo que los errores son probables.
		No se realiza entrenamiento formal, divulgación o despliegue de los procesos estándar.
	b) j) k) l)	Se identifican las posibles debilidades en la protección de datos personales y la seguridad de la información.

Cuadro 26. (Continuación)

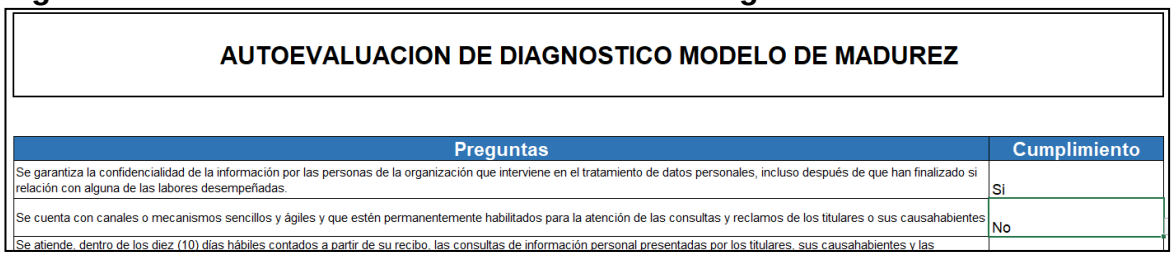
Nivel	Literal artículo 18	Descripción
	k) l)	Los incidentes que se presentan en la protección de datos se tratan de forma correctiva.
	a) b) c) d) e) f) g) h) i) l)	Se define políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre la privacidad de datos se presentan en la Entidad.
Repetible	a) c) d) e) f) l)	Los procesos son repetibles y posiblemente con resultados consistentes de personas diferentes que hacen la misma tarea.
	a) b) c) d) e) f) g) h) i) j) k) l)	Hay entrenamiento formal o comunicación de los procesos estándar.
	b) l)	La organización determina en forma general los activos de privacidad.
	b) j) l)	Se genera conciencia en los colaboradores sobre la protección de datos personales.
	b) k) l)	Los temas de seguridad de la información y protección de los datos personales se tratan en los comités de rendición de cuentas.
Definido	a) c) d) e) f) g) h) i) l)	Existen procedimientos documentados estándar, los cuales son mejorados constantemente.
	b) j) g) h) i) l)	Existen controles formales para garantizar que los procedimientos son efectivos.
	l)	Las actividades se llevan a cabo consistentemente dentro de algunas áreas.
	l) f)	Se han determinado los objetivos, alcance y límites de la protección de datos personales.
	l) f) g) h) i)	Se han establecido formalmente políticas de protección de datos personales.
	a) c) d) e) f) j) l)	Se tienen definidos los roles y responsabilidades asignados en protección de datos personales.
	b) l)	Se ha realizado un inventario de la información aplicando técnicas definidas.
	b) k) l)	Se tratan los riesgos de Protección de datos personales a través de una metodología.
Administrado	a) c) d) e) f) l)	Se llevan a cabo procesos formales de revisión y aprobación y son comunicados constantemente en toda la organización.
	a) b) c) d) e) f) g) h) i) j) k) l)	Las actividades son coherentes y bien comunicadas al interior de la organización.
	j) l) b)	Se revisa y monitorea periódicamente los activos de información.
	a) b) c) d) e) f) g) h) i) j) k) l)	Se usan indicadores para establecer el cumplimiento de las políticas de protección de datos personales.
	k) b) j) k)	Se valora la efectividad de los controles implementados y las medidas necesarias para reducir los incidentes y prevenir su ocurrencia.
Optimizado	a) c) d) e) f) g) h) i)	La eficiencia y eficacia de los procesos es evaluada mediante procedimientos y mediciones formales.
	a) b) c) d) e) f) g) h) i) j) k) l)	Se realizan cambios para mantener la eficiencia en el tiempo.
	a) c) d) e) f) l)	Los procesos están integrados a lo largo de los límites de la Organización.
	a) b) c) d) e) f) g) h) i) j) k) l)	La protección de datos personales es un valor agregado para la organización.
	a) b) c) d) e) f) g) h) i) j) k) l)	Se usan indicadores de efectividad para establecer si la organización halla retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos estratégicos.
	a) b) c) d) e) f) g) h) i) j) k) l)	La mejora continua es parte de la cultura organizacional.

Fuente. Los Autores

7.3 GUÍA DE USO DE LA HERRAMIENTA "AUTOEVALUACIÓN DE DIAGNÓSTICO MODELO DE MADUREZ"

La hoja "Autoevaluación" de la herramienta contiene un listado de preguntas en las cuales la compañía deberá a conciencia responder sí o no cumplen con lo descrito, como se muestra en la Figura 9.

Figura 9. Cuestionario de Autoevaluación de Diagnóstico



AUTOEVALUACION DE DIAGNOSTICO MODELO DE MADUREZ

Preguntas	Cumplimiento
Se garantiza la confidencialidad de la información por las personas de la organización que interviene en el tratamiento de datos personales, incluso después de que han finalizado si relación con alguna de las labores desempeñadas.	Si
Se cuenta con canales o mecanismos sencillos y ágiles y que estén permanentemente habilitados para la atención de las consultas y reclamos de los titulares o sus causahabientes	No
Se atiende, dentro de los diez (10) días hábiles contados a partir de su recibo, las consultas de información personal presentadas por los titulares, sus causahabientes y las	

Fuente. Los Autores

Cuando se termine de responder el cuestionario este dará un nivel de cumplimiento actual de la compañía de acuerdo con el Cuadro 26 "Características de los Niveles de Madurez", como se muestra en la Figura 10

Figura 10. Nivel de Cumplimiento Actual de la Organización

NIVEL DE CUMPLIMIENTO ACTUAL
Nivel_Inexistente

Fuente. Los Autores

De igual manera se evidencia una gráfica que ayuda a la organización a visualizar que porcentaje le falta para poder llegar al siguiente nivel de maduración, como se muestra en la Figura 10.

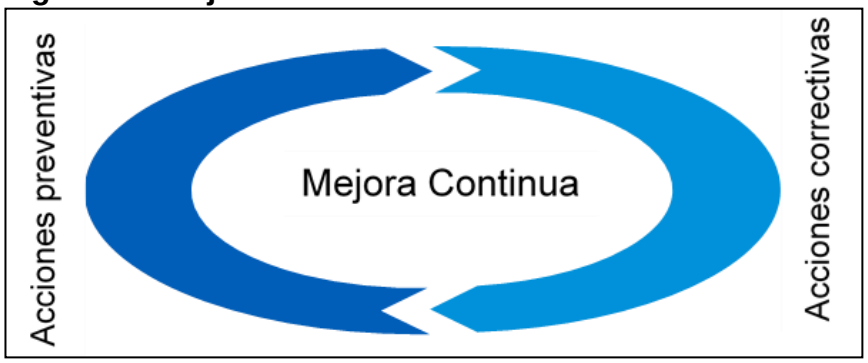
Se debe tener en cuenta que se debe escalar nivel a nivel del modelo de madurez para llegar a óptimo ya que no es posible saltarse un nivel porque esto implicaría que la organización no está contestando las preguntas correctamente.

7.1.6 FASE SEIS - MEJORA CONTINUA Y CAPACITACIÓN

Para originar la mejora continua es necesario adoptar la medidas correctivas y preventivas, de acuerdo con los resultados de la fase de evaluación de riesgos.

La mejora continua se puede dividir en dos tipos (véase la Figura 11).

Figura 11. Mejora Continua



Fuente. Los Autores

7.1.6.1 MEJORA CONTINUA

•Acciones correctivas: Son actividades que buscan suprimir las causas de los incidentes con el objetivo de prevenir que se vuelvan a materializar. Para atender estas acciones se debe tener en cuenta lo siguiente:

✓Análisis y revisión del incidente.
✓Causas que originen el incidente
✓Acciones que adopta para evitar que el incidente se vuela a originar.
✓Implementar dichas acciones.
✓Documentar las consecuencias de las actividades implementadas.
✓Evaluar la eficacia de las actividades implementadas

•Acciones preventivas: Son actividades enfocadas a suprimir las causas de los incidentes con relación a las amenazas potenciales. Para atender estas acciones se debe tener en cuenta lo siguiente:

✓Análisis de las amenazas
✓Posibles incidentes que podrían generarse por una amenaza
✓Acciones necesarias para evitar que el incidente ocurra
✓Implementación de las actividades necesarias
✓Documentar los resultados de las actividades
✓Evaluar la eficacia de las actividades implementadas.

La implementación de estas acciones puede realizarse periódicamente de acuerdo con la importancia de la mejora y los recursos disponibles o tratarse de inmediato ante su detección, por ejemplo, ante auditorías externas.

Una parte esencial de la mejora continua es la capacitación, aportando conciencia de su responsabilidad y deberes frente a la protección de datos personales a los colaboradores, así mismo ayudan a identificar cuál es su aporte para el logro de cumplimento de los objetivos de la organización. Accountability propone establecer

campañas de concienciación, entrenamiento y educación a sus colaboradores garantizando su entrenamiento periódico, de acuerdo con las necesidades identificadas de acuerdo a su rol en el cumplimiento de la protección de la información y evaluar su eficacia mediante la aplicación de exámenes prácticos o periódicos con el objetivo de medir el nivel de conocimiento proporcionado.

8. CONCLUSIONES

El trabajo de proyecto de grado actual presenta un modelo para la implementación de la Ley de protección de datos personales 1581 en el rol de encargado de la información basado en la norma ISO 27001, 27005 y 31000, el cual aporta una guía para que todo tipo de organización en Colombia logre reconocer su estado frente al cumplimiento de la norma y cumplir ante la SIC de forma correcta, siguiendo con el proceso de gestión de protección de datos personales y su vez gestione los riesgos y brinde la seguridad de la información asociada a los mismos.

El cumplimiento de la Ley de protección de datos personales en las organizaciones es un proceso que demanda tiempo, organización y recursos de esta manera una de las pautas iniciales es la identificación y clasificación de los datos, que si se hace de manera correcta y siguiendo las fases propuestas de este modelo se puede lograr de una manera progresiva y generando valor a la organización y estableciendo un punto diferenciador frente a la competencia y una solidez de la imagen organizacional.

Toda organización que siga las pautas brindadas en este modelo podrán prepararse para el cumplimiento de la normatividad en protección de datos personales en el rol de encargado y de esta manera contar con la documentación básica requerida para evitar hacerse acreedores de las multas y sanciones de los entes regulatorios en materia de protección de datos personales, además de identificar sus problemas de seguridad, riesgos y vulnerabilidades que le permitan tener un mejoramiento continuo logrando hacer que la protección de datos personales agregue valor a la organización .

Es de gran importancia entender que más que con carácter impositivo, esta ley puede abordarse como una oportunidad para mejorar nuestros niveles de protección de datos y seguridad de la información, incluyendo estrategias de concientización a los colaboradores, lo que permitirá tener una cultura de protección y cuidado por los datos personales, aportando para tener un país más responsable y de altos niveles de seguridad y confianza para sus clientes y generar para sus accionistas la rentabilidad y productividad esperada.

9. BIBLIOGRAFÍA

1. COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581 (17, octubre 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá, 2012. no. 48.587, p. 12

2. COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266 (31, diciembre 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. Bogotá, no. 47.219.

3. COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 1377 (27, junio 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Bogotá: La Presidencia, 2013.

4. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD [en línea]. Madrid: La Agencia [citado 2 mayo, 2020]. Disponible en Internet: <URL: https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf>

5. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Manejo de información personal “Habeas data” [en línea]. Bogotá: La Superintendencia [citado 2 mayo, 2020]. Disponible en Internet: <URL: https://www.sic.gov.co/manejo-de-informacion-personal>

6. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del riesgo: principios y directrices. NTC 31000. Bogotá: ICONTEC, 2018.

7. RUÍZ, Betcy. Regulación en materia de protección de datos personales o Habeas Data en Colombia a través de la Ley 1581 de 2012: Examen histórico y crítico sobre su ineficacia ante las administradoras de bases de datos, portales de Internet y motores de búsquedas. Bogotá: Universidad Católica de Colombia. Faculta de derecho. Modalidad Trabajo de grado, 2016.

8. MAHECHA, Luisa. Evaluación de la gestión de riesgos del proceso de gestión humana en la empresa SUPPLA S.A. según la ley de 2012 y la ISO 31000. Bogotá: Universidad Católica de Colombia. Faculta de Ingeniería. Modalidad Trabajo de grado, 2016.

9. RODRÍGUEZ, María. De la protección de datos personales en Colombia (Ley 1581 de 2012): un estudio comparado con el sistema canadiense. Bogotá: Universidad Católica de Colombia. Facultad de Derecho. Modalidad Trabajo grado, 201.

10. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Cuestionario de diagnóstico para el cumplimiento de la ley 1581 de 2012 en las MIPYMES [en línea]. Bogotá: La Superintendencia [citado 27 octubre 2020]. Disponible en Internet: <URL: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cuestionario_de_diagnostico_para_el_cumplimiento_de_la_Ley_1581_de_2012_en_las_Mipymes.pdf>

11. BERNAL PULIDO, Carlos. Corte Constitucional explica los principios del derecho al habeas data [en línea. Bogotá: Noticio Oficial [citado 31 mayo, 2020]. Disponible en Internet: <URL: https://www-noticieroficial-com.ucatolica.basesdedatosezproxy. com/noticias/Corte-Constitucional-explica-los-principios-del-derecho-al-habeas-data/129618?b=true>

12. COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Modelo de seguridad y privacidad de la información. Bogotá: MinTic, 2016. 58p.

13. DELTA. Ley de Delitos Informáticos en Colombia [en línea]. Bogotá: La Empresa [citado 2 mayo, 2020]. Disponible en Internet: <URL: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia>

14. DETERMANN, Lothar. Protección global de datos personales Guía de aplicación práctica [en línea]. Bogotá: Astreavirtual [citado 2 mayo, 2020]. Disponible en Internet: <URL: https://www-astreavirtual-com-ar.ucatolica.basesdedatosezproxy.com/panel.php?b=0089600>

15. GARCÍA GONZÁLEZ, Aristeo. Hacia una cultura en materia de protección de datos personales [en línea]. Bogotá: Metarevistas [citado 30 mayo, 2020]. Disponible en Internet: <URL: https://www-metarevistas-com.ucatolica.basesdedatosezproxy. com/Record/oai:ojs.revistas.juridicas.unam.mx:articleojs-6816>

16. GARCIA MOLINA, Carolina. Información que se debe brindar para la autorización del tratamiento de datos personales [en línea]. Bogotá: Noticiero Oficial [citado 31 mayo, 2020]. Disponible en Internet: <URL: https://www-noticieroficial-com.ucatolica.basesdedatosezproxy.com/noticias/Informacion-que-se-debe-brindar-para-la-autorizacion-del-tratamiento-de-datos-personales/300160?b=true>

17. GARRIGA DOMÍNGUEZ, Ana. Tratamiento de datos personales y derechos fundamentales [en línea]. Bogotá: ELibro [citado 30 mayo, 2020]. Disponible en Internet: <URL: https://elibro-net.ucatolica.basesdedatosezproxy.com/es/lc/ucatolica/titulos/56784>

18. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información. Técnicas de seguridad. Sistema de gestión de la

seguridad de la información. Requisitos. NTC-ISO IEC 27001. Bogotá: ICONTEC, 2013. 26 p.

19. ------. Tecnología de la información. Técnicas de seguridad. Código de practica para controles de seguridad de la información. NTC-ISO IEC 27002. Bogotá: ICONTEC, 2015. 107 p.

20. ------. Tecnología de la información. Técnicas de seguridad. Gestión de riesgos en la seguridad de la información. NTC-ISO IEC 27005. Bogotá: ICONTEC, 2009. 67p.

21. MARTÍNEZ VÁZQUEZ, Francisco. El reciente marco de la protección de datos personales (RGPD y la nueva LOPDP). [en línea]. Bogotá: Meta Revistas [citado 30 mayo, 2020]. Disponible en Internet: <URL: https://www-metarevistas-com.ucatolica.basesdedatosezproxy.com/Record/oai:ojs.revistas.uca.es:articleojs-5424>

22. MARZO PORTERA, Ana. Guía práctica para la protección de datos de carácter personal [en línea]. Bogotá: ELibro [citado 30 mayo, 2020]. Disponible en Internet: <URL: https://elibro-net.ucatolica.basesdedatosezproxy.com/es/ereader/ucatolica/41971>

23. ------. La auditoría de seguridad en la protección de datos de carácter personal [en línea]. Bogotá: ELibro [citado 30 mayo, 2020]. Disponible en Internet: <URL: https://elibro-net.ucatolica.basesdedatosezproxy.com/es/lc/ucatolica/titulos/41972>

24. MURILLO DE LA CUEVA, Pablo. Informática y protección de datos personales [en línea]. Bogotá: Meta Revistas [citado 30 mayo, 2020]. Disponible en Internet: <URL: https://www-metarevistas-com.ucatolica.basesdedatosezproxy.com/Record/oai:ojs. revistas.uchile.cl:articleojs-10656>

25. NYMITY innovating compliance. Manual Nymity para Demostrar el cumplimiento legal: una aproximación estructurada a la gestión de protección de datos. Bogotá: NYMITY, 2016. 29p.

26. OFICINA DEL COMISIONADO DE INFORMACIÓN Y PRIVACIDAD DE ALBERTA. dEntendiendo la Responsabilidad Demostrada con un Programa de Protección e Datos. Alberta: La Oficina, 2012. 40 p.

27. PESO NAVARRO, Emilio. La seguridad de los datos de carácter personal [en línea]. Bogotá: Elibro [citado 30 mayo, 2020]. Disponible en Internet: <URL: https://elibro-net.ucatolica.basesdedatosezproxy.com/es/lc/ucatolica/titulos/57477>

28. PUCCINELLI, Oscar R. Protección de datos de carácter personal [en línea]. Bogotá: Meta Revistas [citado 30 mayo, 2020]. Disponible en Internet: <URL:

https://www-astreavirtual-com-ar.ucatolica.basesdedatosezproxy.com/panel.php?b=0056100>

29. REMOLINA ANGARITA, Nelson. Tratamiento de datos personales, aproximación internacional y comentarios a la ley 1581 de 2012. Bogotá: LEGIS, 2013. 375p.

30. RODRIGUEZ AYUSO, Juan. Figuras y responsabilidades en el tratamiento de datos personales [en línea]. Bogotá: Elibro [citado 30 mayo, 2020]. Disponible en Internet: <URL: https://elibro-net.ucatolica.basesdedatosezproxy.com/es/ereader/ucatolica/ 127035>

31. ROJAS BEJARANO, Marcela. Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales [en línea]. Bogotá: Universidad Católica de Colombia [citado 30 mayo, 2020]. Disponible en Internet: <URL: https://editorial.ucatolica.edu.co/index.php/Juridica/article/view/652>

32. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Cartilla formatos modelo para el cumplimiento de obligaciones establecidas en la ley 1581 de 2012 y sus decretos reglamentarios. [en línea]. Bogotá: ISSUU [citado 30 mayo, 2020]. Disponible en Internet: <URL: https://issuu.com/quioscosic/docs/cartilla_formatos_datos_personales_>

33. ------. Guía para la implementación del principio de responsabilidad demostrada (Accountability) [en línea]. Bogotá: La Superintendencia [citado 27 octubre, 2020]. Disponible en Internet: <URL: https://issuu.com/quioscosic/docs/guia_accountability_6e79bc4c 4b6fef>

34. ------. Preguntas frecuentes [en línea]. Bogotá: SIC [citado 30 mayo, 2020]. Disponible en Internet: <URL: http://www.sic.gov.co/drupal/ preguntas-frecuentes-pdp>

35. VV.AA. La protección de datos personales en la era digital. Corporación [en línea]. Bogotá: Foro: Revista de Derecho [citado 30 mayo, 2020]. Disponible en Internet: <URL: https://ebookcentral.proquest.com/lib/biblioucatolicasp/reader.action?docID=5425768&query=datos+personales>