PREVI PASO
CASA DE FUNERALES
La atención nos distingue
NIT: 901.722.843

MANUAL DE TRATAMIENTO DE DATOS PERSONALES

1. OBJETIVO

El objetivo del presente documento denominado Manual de Tratamiento de Datos Personales, (en adelante "Manual"), es describir la forma en que se deben llevar a cabo los diferentes Tratamientos que comprenden el Ciclo de Vida del Dato Personal, en aras de dar cabal cumplimiento a la Ley Estatutaria No. 1581 de 2012, su Decreto Reglamentario 1074 de 2015 (Capítulo 25) y demás normas que rigen la Protección de Datos Personales, o aquellas que las complementen, sustituyan, modifiquen o deroguen y, en particular, del principio de responsabilidad demostrada en materia de protección de datos personales.

2. ALCANCE

Este Protocolo es aplicable a **PREVIPASO S.A.S** en calidad de Responsable del Tratamiento y a sus empleados directos e indirectos (en adelante "Operativos"), como a todas aquellas terceras personas naturales o jurídicas que realicen un Tratamiento sobre Datos Personales de los Titulares que comprenden los Grupos de Interés del Responsable del Tratamiento, por Encargo de éste.

3. DEFINICIONES

Para los efectos de este Protocolo, se entenderá por:

ADOLESCENTE: Personas entre 12 y 18 años de edad (Código de la Infancia y de la Adolescencia, artículo 3).

AUTORIZACIÓN: Consentimiento previo, expreso e informado del Titular de Datos Personales para llevar a cabo el Tratamiento de sus datos personales, la cual puede ser recolectada de manera (i) escrita, (ii) oral o (iii) mediante conductas inequívocas, que permitan concluir de manera razonable que este otorgó la autorización.

AVISO DE PRIVACIDAD: Documento físico, electrónico o en cualquier otro formato generado por el Responsable del Tratamiento, que se pone a disposición del Titular para el Tratamiento de sus datos personales. En el Aviso de Privacidad se comunica al Titular la información relativa a la existencia de las políticas de tratamiento de información que le

serán aplicables, la forma de acceder a las mismas y las características del tratamiento que se pretende dar a los Datos Personales.

BASE DE DATOS: Conjunto organizado de datos personales físico o electrónico (digital) que sea objeto de Tratamiento manual o automatizado.

CICLO DE VIDA DEL DATO: Etapas por las que pasan los Datos Personales, desde su recolección, hasta la disposición final de los mismos.

DATOS PERSONALES: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. La naturaleza de los Datos Personales puede ser pública, semiprivada, privada o sensible.

Clases de Datos Personales	Ejemplos
Datos de Identificación	Datos generales de identificación de la persona, familiares, beneficiarios o terceros. Ej: Nombre, apellido, tipo de identificación, número de identificación, fecha y lugar de expedición, nombre, estado civil, sexo, etc.
Datos específicos de Identificación	Firma, nacionalidad, datos de familia, firma electrónica, otros documentos de identificación, lugar y fecha de nacimiento o muerte, edad, etc.
Datos Biométricos	Huella, ADN, iris, Geometría facial o corporal, fotografías, videos, fórmula dactiloscópica, voz, etc
Datos de contacto empresariales o profesionales	Dirección, teléfono, correo electrónico, etc.
Datos de contacto personales	Domicilio, teléfono, correo electrónico, etc.

Datos órdenes para procedimientos médicos	Órdenes y relación de pruebas complementarias como laboratorio, imagen, endoscópicas, patológicas, estudios, etc. NO INCLUYE RESULTADOS NI DIAGNÓSTICOS.
Datos Resultados y diagnósticos médicos	Resultados de pruebas, laboratorios, estudios, diagnósticos médicos, generales o especializados, psicológicos o psiquiátricos, medicamentos y/o tratamientos médicos o terapéuticos de cualquier tipo, etc.
Datos de Asociación	Datos relacionados con la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, religiosas, políticas
Datos sexualidad	Datos orientación sexual y preferencias sexuales
Datos de Origen	Datos de origen étnico-racial
Datos de población vulnerable	Personas de la tercera edad o menores de 18 años en condición de pobreza, personas con limitaciones sicomotoras, auditivas y visuales en condiciones de pobreza, personas víctimas de la violencia, personas en situación de desplazamiento forzado por violencia, madres gestantes o lactantes o cabeza de familia en situación de vulnerabilidad, menores en condición de abandono o protección, etc.
Datos de algún tipo de discapacidad	Personas con limitaciones sicomotoras, auditivas y visuales, etc.

Datos económicos	Datos financieros, crediticios y/o derechos de carácter económico de las personas.
Datos socioeconómicos	Estrato, propiedad de la vivienda, etc.
Datos de información tributaria	Declaración de impuestos, régimen común o simplificado, etc.
Datos patrimoniales	Bienes muebles e inmuebles, ingresos, egresos, inversiones, etc
Datos actividad económica	Actividad económica NIT
Datos laborales	Datos relacionados con la historia laboral de la persona, experiencia laboral, cargo, fechas de ingreso y retiro, anotaciones, llamados de atención, etc.
Datos educación	Datos relacionados con el nivel educativo, capacitación y/o historial académico de la persona, etc.
Datos seguridad social	EPS, IPS, ARL, fechas de ingreso/retiro EPS, AFP, etc.

Datos de acceso a Sistemas de Información	Usuarios, IP, claves, perfiles, etc.
Datos gustos y hobbies	Deportivos, ocio, gastronómicos, turismo, moda, lectura, etc.
Datos Antecedentes	Datos de antecedentes judiciales y/o disciplinarios

DATO PRIVADO: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el Titular.

DATO PÚBLICO: Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y aquel que no sea semiprivado, privado o sensible. Son públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio, a su calidad de comerciante o de servidor público y aquellos que puedan obtenerse sin reserva alguna. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, que no estén sometidos a reserva.

DATOS SENSIBLES: Son aquellos que afectan la intimidad del Titular de Datos Personales o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos (huella dactilar, el iris del ojo, voz, forma de caminar, palma de la mano o los rasgos del rostro, fotografías, videos, entre otros).

A los Datos Personales de Niños, Niñas y/o Adolescentes, se les aplicarán las mismas normas y procedimientos que a los Datos Sensibles, y no se le dará Tratamiento alguno que pueda vulnerar o amenazar su desarrollo físico, mental y emocional.

DATOS SEMIPRIVADOS: Son aquellos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. Se entiende por dato semiprivado, entre otros, la información relacionada con seguridad social y con el comportamiento financiero y crediticio.

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.

FUENTE DE INFORMACIÓN: Persona, entidad u organización que recibe o conoce Datos Personales de los Titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del Titular, suministra esos datos a un Operador de Información, el que a su vez los entregará al usuario final.
Para los efectos de este Procedimiento, se entenderá que la Fuente es el Responsable del Tratamiento.

INVENTARIO DE BASES DE DATOS: Documento mediante el cual se identifican las Bases de Datos del Responsable del Tratamiento y se caracterizan de acuerdo al Grupo de Interés, Tipos de Datos y finalidades para el Tratamiento.

LEY 1266 DE 2008: por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

LEY 1581 DE 2012: Ley Estatutaria por la cual se dictan disposiciones generales para la protección de datos personales.
GRUPOS DE INTERÉS: Para los efectos de este Procedimiento, se entenderán como Grupos de Interés todos los grupos de personas naturales respecto de las cuales el Responsable del Tratamiento y/o los Encargados del Tratamiento realicen algún Tratamiento de Datos Personales.

NIÑO O NIÑA: Personas entre los 0 y 12 años (Código de la Infancia y de la Adolescencia, artículo 3).

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES: Persona o Área Responsable de velar por la implementación efectiva de las políticas y procedimientos adoptados para cumplir el Régimen de Protección de Datos Personales y la implementación de buenas prácticas de gestión de datos personales dentro de la empresa.

OPERADOR DE LA INFORMACIÓN: Persona, entidad u organización que recibe de la Fuente de Información, Datos Personales comerciales, financieros o crediticios, sobre varios Titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la Ley 1266 de 2008.

Para los efectos de este Procedimiento, se entenderán como Operadores de la Información las Centrales de Riesgo Legalmente establecidas.

OPERATIVO: Empleado directo o indirecto del Responsable del Tratamiento que realiza algún tipo de Tratamiento sobre Datos Personales.

PROTECCIÓN DE DATOS: son todas 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.

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.

Para los efectos de este Procedimiento, se entiende como Responsable del Tratamiento a **PREVIPASO S.A.S**

TITULAR: Para los efectos de la Ley 1266 de 2008, es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías consagrados en dicha Ley y las normas que la complementen, modifiquen, sustituyan o deroguen. Para los efectos de la Ley 1581 de 2012, es la persona natural cuyos datos personales sean objeto de Tratamiento.

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

TRANSMISIÓN: Tratamiento de Datos Personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

TRATAMIENTO: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, actualización, uso, circulación, Transferencia, Transmisión o supresión.

4. PRINCIPIOS RECTORES

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

Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la ley.

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la ley.

Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

ESTRUCTURA ORGANIZACIONAL

El cumplimiento y ejecución de las actividades tendientes a lograr el adecuado y oportuno funcionamiento del Manual de Protección de Datos Personales, es responsabilidad tanto de la alta dirección y gerencia, del oficial de protección de datos personales, como de los demás empleados y áreas de la organización.

Gerencia

Para el adecuado y oportuno funcionamiento del Programa de Protección de Datos Personales, se requiere el compromiso de la Gerencia, brindando el apoyo para consolidar la cultura organizacional respecto a la protección y tratamiento de datos.

Sus principales responsabilidades son:

Designar a la persona o área que asumirá la función de protección de datos personales.

Aprobación y monitoreo del Programa de Protección de Datos Personales.

Realizar el acompañamiento para el diseño e implementación del programa.

Presentar ante el órgano directivo y mantener informados los avances y resultados de la implementación del Programa de Protección de Datos Personales en la organización.

Establecer 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

Será el funcionario responsable dentro de la compañía de velar por la implementación efectiva de las políticas y procedimientos adoptados por ésta para cumplir las normas, así como la implementación y buenas prácticas de gestión de datos personales dentro de la organización. Sus funciones son las siguientes:

- Estructurar, diseñar y administrar el programa que permita a la organización cumplir las normas sobre protección de datos personales, así como establecer los controles a ese programa, su evaluación y revisión permanente.
- Impulsar la cultura de protección de datos de dentro de la organización.
- Dar trámite a las solicitudes de los titulares, para el ejercicio de sus derechos.
- Coordinar la definición e implementación de los controles en materia de protección de datos personales, así como las acciones tendientes para su sostenibilidad.
- Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa de Protección de Datos Personales.
- Inscribir las bases de datos de la organización en el Registro Nación de Bases de Datos (según el caso) y, actualizar la información según las instrucciones que en el futuro imparta la Superintendencia de Industria y Comercio.
- Analizar las responsabilidades de cada cargo de la organización, para diseñar y velar por la implementación de un programa de entrenamiento en protección de datos personales específico para cada uno de ellos.
- Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización.
- Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal.

- Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio.
- Realizar seguimiento al Programa de Protección de Datos Personales, verificando el envío de los reportes a que haya lugar.
- En conclusión, el Oficial de Protección de Datos Personales tendrá el control y la responsabilidad de la implementación transversal del Programa de Protección de Datos Personales en la organización.

Otras áreas de la organización

Con el fin de asegurar una implementación transversal del presente programa, el personal adscrito a la organización que realice algún tipo de tratamiento de datos personales deberá implementar las medidas de protección de datos personales, de acuerdo al cargo que ocupe y a las responsabilidades y obligaciones inherentes al mismo. Deberán consultar al Oficial de Protección de Datos Personales cuando se tomen decisiones con implicaciones para la protección de datos personales. Toda la información pertinente debería de transmitírsele al Oficial a su debido tiempo, con el fin de que pueda prestar una asesoría adecuada. Se consultará al Oficial con prontitud una vez que se haya producido una brecha a los códigos de seguridad de la organización o cualquier incidente que afecte la información.

En los procesos de inducción de cada colaborador se deberá incluir una capacitación en materia de Protección de Protección de Datos Personales, la cual podrá ser dictada por un agente interno o externo a la organización y en la cual se deberán socializar y poner a su disposición los formatos y políticas de la organización en esa materia, para que sean utilizados por estos.

5. TRATAMIENTOS

Para realizar cualquier Tratamiento, el Responsable del Tratamiento, los Operativos y los Encargados del Tratamiento, deberán seguir los pasos específicos que se definen a continuación, para cada Ciclo de Vida del Dato Personal.

5.1. RECOLECCIÓN

Para la recolección de Datos Personales, sin importar cuál sea la técnica a utilizar, se deberán seguir los siguientes pasos:

5.1.1. Identificar el Grupo de Interés

Se debe identificar el Grupo de Interés al cual pertenecen los Titulares cuyos Datos Personales serán recolectados y validar si ya existe una Base de Datos creada para estos dentro del Inventario de Bases de Datos.

En caso de estar obligado el Responsable del Tratamiento por las normas vigentes a inscribir las Bases de Datos en el Registro Nacional de Bases de Datos (en adelante "RNBD"), deberá adicionalmente verificar si la Base de Datos ya se encuentra registrada. Si no está registrada, deberá inscribirla dentro de los dos (2) meses siguientes a su creación.

5.1.2. Identificar las Finalidades para las cuales se requiere recolectar Datos Personales:

Se deben tener Finalidades para las cuales se van a recolectar los Datos Personales claras, proporcionales, pertinentes y adecuadas, y se debe verificar que éstas se encuentren incluidas dentro de la Política de Privacidad y Protección de Datos Personales vigente (en adelante "Política de Privacidad").

En caso de no estar incluidas dentro de la Política de Privacidad, deberán incluirse antes de realizar el proceso de recolección.

En caso de estar obligado el Responsable del Tratamiento por las normas vigentes a inscribir las Bases de Datos en el RNBD, deberá validar que la finalidad para la cual se van a recolectar los datos haya sido reportada y en caso de que no se haya reportado, deberá reportarla previo a la recolección de la información.

5.1.3. Identificar los Datos Personales que se van a recolectar para cumplir con las Finalidades previamente identificadas y la naturaleza de los mismos:

Se debe identificar qué Datos Personales se van a recolectar e identificar su naturaleza:

Datos Personales	**Naturaleza del Dato**
Datos de Identificación	Público
Datos de contacto empresariales o profesionales	Público
Datos actividad económica	Público
Datos específicos de Identificación	Semiprivado

Datos económicos	Semiprivado
Datos de información tributaria	Semiprivado
Datos patrimoniales	Semiprivado
Datos laborales	Semiprivado
Datos educación	Semiprivado
Datos seguridad social	Semiprivado
Datos Antecedentes	Semiprivado
Datos de contacto personales	Privado
Datos órdenes para procedimientos médicos	Privado
Datos socioeconómicos	Privado
Datos de acceso a Sistemas de Información	Privado
Datos gustos y hobbies	Privado
Datos Biométricos	Sensible
Datos Resultados y diagnósticos médicos	Sensible
Datos de Asociación	Sensible
Datos sexualidad	Sensible
Datos de Origen	Sensible
Datos de población vulnerable	Sensible
Datos de algún tipo de discapacidad	Sensible
Datos Niños, Niñas y/o Adolescentes	Sensible

Los Datos de contacto empresariales o profesionales son de naturaleza Pública, siempre y cuando se utilicen para los fines propios de la empresa o profesión. Sin embargo, adquieren el carácter de privados, cuando se utilizan para otras finalidades.

Cualquier Dato Personal puede ser Dato Sensible, si tiene la potencialidad de generar discriminación.

5.1.4. Identificar si se requiere Autorización para el Tratamiento de los Datos Personales

Se debe identificar según la Naturaleza de los Datos Personales que se pretenden recolectar, si se requiere contar con Autorización para el Tratamiento de los mismos:

Naturaleza del Dato	Autorización
Público	No requiere
Semiprivado	Requiere
Privado	Requiere
Sensible	Requiere

No se podrán recolectar Datos Personales sin Autorización del Titular, salvo en los casos en los que alguna norma vigente obligue su Tratamiento.

Los Datos Personales que se encuentren en fuentes de acceso público, con independencia del medio por el cual se tenga acceso, entendiéndose por tales aquellos datos o Bases de Datos que se encuentren a disposición del público, pueden ser Tratados por cualquier persona siempre y cuando, por su naturaleza, sean datos públicos.

5.1.5. Identificar Titulares

Se debe identificar si los Titulares cuyos Datos Personales serán recolectados, son mayores o menores de edad (Niños, Niñas y/o Adolescentes).

En caso de ser mayores de edad, la Autorización para el Tratamiento de Datos Personales, debe provenir directamente del Titular, sus causahabientes, o un apoderado.

En caso de ser menores de edad o tratarse de una persona incapaz la Autorización deberá provenir de sus padres o de quienes representen legalmente al menor, previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

En cualquier caso, se deberá verificar la identidad de quien otorga la autorización, y requerir la acreditación de la calidad en la que actúa.

En caso tal que el Titular sea una persona incapaz, deberá otorgar la Autorización quien lo represente legalmente.

5.1.6. Recolectar la Autorización

La autorización deberá solicitarse a más tardar en el momento de la recolección de los Datos Personales y deberá informarse al Titular o a su representante, los datos personales que serán recolectados, así como todas las Finalidades específicas y Tratamientos para los cuales se obtiene el consentimiento.

En el Tratamiento de datos personales sensibles, deberán cumplirse las siguientes obligaciones:

a. Informar al Titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.
b. Informar al Titular de forma explícita y previa, además de los requisitos generales de la Autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.

Ninguna actividad podrá condicionarse a que el Titular suministre Datos Personales sensibles, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización, o que sea imposible desarrollar la actividad sin el Tratamiento de dichos datos.

En caso de haber cambios sustanciales en el contenido de la Política de Privacidad en relación con la identificación del Responsable y las Finalidades del Tratamiento de los Datos Personales, estos deberán ser comunicados al Titular y se deberá obtener una nueva Autorización a más tardar al momento de implementar los nuevos cambios introducidos en la Política de Privacidad.

La Autorización podrá ser recolectada por escrito, de forma oral o mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la Autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.

Para que se entienda que hubo Autorización mediante conducta inequívoca, se debe demostrar como mínimo que al momento de recolectar la Autorización se le informó al Titular acerca de la existencia de la Política de Privacidad, la forma de acceder a ésta, las Finalidades y Tratamientos que se pretende dar a los Datos Personales, nombre o razón social y datos de contacto del Responsable del Tratamiento y derechos que le asisten como Titular.

Asignación de roles y responsabilidades en la recolección de la Autorización:

GRUPO DE INTERÉS		**ÁREAS O DEPENDENCIAS**
1	ASPIRANTES, EMPLEADOS DIRECTOS E INDIRECTOS, ACTIVOS E INACTIVOS Y FAMILIAS	TALENTO HUMANO SALUD Y SEGURIDAD EN EL TRABAJO MARKETING
2	CLIENTES (ACTIVOS E INACTIVOS), POTENCIALES CLIENTES Y SUS COLABORADORES, Y BENEFICIARIOS	COMERCIAL MARKETING CALL CENTER CALIDAD ADMINISTRATIVA O SISTEMAS
3	PROVEEDORES, CONTRATISTAS Y SUS COLABORADORES – ALIADOS O SOCIOS COMERCIALES	COMPRAS GERENCIA
4	ACCIONISTAS Y MIEMBROS DE JUNTA DIRECTIVA / ADMINISTRADORES	GERENCIA
5	VIDEOVIGILANCIA	TECNOLOGÍA O SISTEMAS GERENCIA
6	VISITANTES	TALENTO HUMANO

Sin perjuicio de lo anterior, es posible que excepcionalmente, otras áreas de la organización requieran recolectar información de algún grupo de interés en ejercicio de sus funciones, para lo cual, antes de recolectar el dato, se deberá verificar si la finalidad se encuentra dentro del alcance de la autorización para el tratamiento de datos personales dada por el respectivo titular, de lo contrario, deberá ser obtenida la autorización, al momento de la recolección del dato personal respectivo.

Los datos recolectados se limitan a aquellos que son pertinentes y necesarios para las finalidades que se describen en la Política de Protección de Datos Personales y de acuerdo al grupo de interés de que se trate.

5.1.7. Conservación de la Autorización

Sea cual sea la forma de obtención de la Autorización, se debe conservar prueba de la existencia de la misma.

5.1.8. Política de Privacidad y Avisos de Privacidad

Todas las finalidades deberán estar incluidas en la Política de Privacidad, previo al uso de los Datos Personales.

Se deberán conservar todas las versiones de las políticas que se adopten, así como constancia de la publicación de cada una de ellas y la puesta en conocimiento de las mismas a los Titulares.

En caso de haber cambios sustanciales en el contenido de la Política de Privacidad en relación con la identificación del Responsable y las Finalidades del Tratamiento de los Datos Personales, estos deberán ser comunicados al Titular y se deberá solicitar autorización previa, para usar los datos con las nuevas finalidades introducidas.

En caso de estar obligado el Responsable del Tratamiento por las normas vigentes a inscribir las Bases de Datos en el RNBD, deberá actualizar la Política de Privacidad en dicha plataforma, siempre que se presenten actualizaciones a la misma.

En los casos en los que no sea posible poner a disposición del Titular la Política de Privacidad, el Responsable del Tratamiento deberá informar a este último de manera oportuna y en todo caso a más tardar al momento de la recolección de los Datos Personales, por medio de un Aviso de Privacidad, el nombre o razón social y datos de contacto del Responsable del Tratamiento, existencia de dicha Política y la forma de acceder ella, Tratamiento al cual serán sometidos los datos y la finalidad del mismo, derechos que le asisten al Titular.

En caso de recolectar Datos Sensibles, el Aviso de Privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos.

El Responsable del Tratamiento deberá conservar el modelo del Aviso de Privacidad que utilice, mientras se Traten Datos Personales conforme al mismo y perduren las obligaciones que de este se deriven. Para el almacenamiento del modelo, el Responsable podrá emplear medios informáticos, electrónicos o cualquier otra tecnología que garantice el cumplimiento de lo previsto en la Ley 527 de 1999, o las normas que la complementen, sustituyan, modifiquen o deroguen.

5.1.9. Tratamiento de Datos Personales de Niños, Niñas y/o Adolescentes

Para el Tratamiento de Datos Personales de Niños, Niñas y/o Adolescentes, se requerirá la Autorización de los padres o de quien lo represente legalmente, atendiendo siempre el principio del interés superior del menor de edad y la prevalencia de sus derechos fundamentales.

El Responsable del Tratamiento deberá velar por que los Operativos y Encargados del Tratamiento den un uso adecuado a los Datos Personales de Niños, Niñas y/o Adolescentes.

5.1.10. Preceptos

No se podrán utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de datos personales

En caso de que la recolección de Datos Personales la realice un Encargado del Tratamiento, se debe cumplir con lo dispuesto en el punto 4.4.2 del presente Protocolo.

5.2. ALMACENAMIENTO Y USO

Los Datos Personales podrán ser almacenados en medios físicos y/o magnéticos dentro o fuera del país, mientras subsista la finalidad para la cual se recolectaron, adoptando las medidas de seguridad requeridas para la Protección de Datos Personales.

Se deberán implementar mecanismos y procedimientos para salvaguardar los datos, respetando la privacidad, creando confianza, y disponiendo los canales o medios al titular para acceder a ella bajo los siguientes criterios de seguridad y calidad de la información.
Seguridad de la Información:

- Confidencialidad: Hace referencia a la protección de información cuya divulgación no está autorizada.
- Integridad: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.
- Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

Calidad de la información:

- Efectividad: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.
- Eficiencia: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.
- Confiabilidad: La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

Cada área que realice tratamiento de datos personales de cualquier grupo de interés, deberá cumplir con las medidas de seguridad técnicas, humanas y administrativas dispuestas en el presente documento, con el fin de otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta o acceso no autorizado o fraudulento.

MEDIDAS DE SEGURIDAD

1. CLASIFICACIÓN DE LAS MEDIDAS DE SEGURIDAD

Las medidas de seguridad se clasifican en tres (3) niveles (Alto, Medio o Bajo), según la Naturaleza del Dato (Público, Semiprivado, Privado, Sensible):

Naturaleza del Dato	**Nivel Medida de Seguridad**
Público	Bajo
Semiprivado	Medio
Privado	Medio
Sensible	Alto

Los niveles de seguridad son acumulativos, de forma que las medidas de seguridad para Datos Sensibles incluyen también las medidas de seguridad para los Datos Semiprivados, Datos Privados y Datos Públicos.

2. TIPOS DE DATOS Y NIVEL DE SEGURIDAD

Datos Personales	**Naturaleza del Dato**	**Nivel Medida de Seguridad**
Datos de Identificación	Público	Bajo
Datos de contacto empresariales o profesionales	Público	Bajo
Datos actividad económica	Público	Bajo
Datos específicos de Identificación	Semiprivado	Medio
Datos económicos	Semiprivado	Medio
Datos de información tributaria	Semiprivado	Medio
Datos patrimoniales	Semiprivado	Medio
Datos laborales	Semiprivado	Medio
Datos educación	Semiprivado	Medio
Datos seguridad social	Semiprivado	Medio
Datos Antecedentes	Semiprivado	Medio
Datos de contacto personales	Privado	Medio
Datos órdenes para procedimientos médicos	Privado	Medio
Datos socioeconómicos	Privado	Medio
Datos de acceso a Sistemas de Información	Privado	Medio
Datos gustos y hobbies	Privado	Medio
Datos Biométricos	Sensible	Alto
Datos Resultados y diagnósticos médicos	Sensible	Alto
Datos de Asociación	Sensible	Alto

Datos sexualidad	Sensible	Alto
Datos de Origen	Sensible	Alto
Datos de población vulnerable	Sensible	Alto
Datos de algún tipo de discapacidad	Sensible	Alto
Datos Niños, Niñas y/o Adolescentes	Sensible	Alto

Los Datos de contacto empresariales o profesionales son de naturaleza Pública, siempre y cuando se utilicen para los fines propios de la empresa o profesión. Sin embargo, adquieren el carácter de privados, cuando se utilizan para otras finalidades. En ese orden de ideas, si los datos se utilizan para otras finalidades, se deberán adoptar medidas de seguridad de nivel Medio.

3. CLASIFICACIÓN BASES DE DATOS

Tipo de Bases de Datos	
Física	**Automatizada**
Archivo físico	Digital Electrónica Medios magnéticos

Las siguientes son las medidas de seguridad que se aplican en la organización:

Medida de seguridad	**Tipo de Bases de Datos**	
	Física	**Automatizada**
Elaboración, adopción e implementación de Políticas de Protección de Datos Personales	x	x
Designación de un Oficial de Protección de Datos Personales quien se encargue de velar por el cumplimiento de las normas de	x	x

Protección de Datos Personales por parte de los Operativos y Encargados del Tratamiento		
Designación de Responsables por Base de Datos, dentro de la organización	x	x
Elaboración, seguimiento y control periódico del Inventario de las Bases de Datos de la organización y clasificación según la Naturaleza de Datos Personales que se Traten	x	x
Capacitación a los Operativos y a los Encargados del Tratamiento actuales y nuevos ingresos, en materia de Protección de Datos Personales	x	x
Elaboración y suscripción de Contratos de Confidencialidad y Transmisión de Datos Personales con los Encargados del Tratamiento	x	x
Elaboración y suscripción de Contratos de Confidencialidad y Transferencia de Datos Personales con otros Responsables del Tratamiento a quienes se Transfieran Datos Personales	x	x
Elaboración y suscripción de Contratos de Confidencialidad y Protección de Datos Personales con los Operativos	x	x
Elaboración, adopción e implementación de Medidas de Seguridad según la Naturaleza de los Datos Personales que se Traten y el Tipo de Base de Datos	x	x
Elaboración, adopción e implementación de procedimientos que garanticen una correcta conservación, localización y consulta de la información	x	x

Implementación de medidas que eviten el acceso indebido o no autorizado de datos o la recuperación de los que hayan sido descartados, borrados o destruidos garantizando los derechos de los Titulares	x	x
Implementación de medidas que permiten la recuperación de datos que hayan sido descartados, borrados o destruidos por error	x	x
Implementación de controles y restricciones de acceso a los Datos Personales que reposen en Bases de Datos Físicas, tales como llaves, códigos de seguridad, carnés para el ingreso, entre otros, y definición de roles y perfiles según los cargos y funciones asignadas a quienes tengan acceso a la información	x	
Implementación de controles y restricciones de acceso a los Datos Personales que reposen en Bases de Datos Automatizadas, tales como creación de usuarios y contraseñas y definición de roles y perfiles según los cargos y funciones asignadas a quienes tengan acceso a la información		x
Elaboración de lista de usuarios y accesos autorizados e implementación de mecanismos para evitar el acceso a datos distintos de los autorizados	x	x
Asignación de deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos.	x	
Autorización del Responsable del Tratamiento para la salida de documentos o soportes por medio físico o electrónico	x	x

Elaboración de una matriz de riesgos y elaboración, adopción e implementación de un protocolo de violaciones y atención de incidentes en materia de protección de datos personales	x	x
Identificación personalizada de usuarios y contraseñas alfanuméricas secretas para acceder a los sistemas de información, servidores, carpetas compartidas, etc.		x
Implementación de medidas de acceso a datos y búsqueda de información a través redes y buscadores seguros. Por medio del antivirus y el firewall se restringe el acceso a ciertas páginas que se consideran de alto riesgo.	x	x
Implementación de auditorías ordinarias internas o externas una vez al año y extraordinarias cuando se realicen modificaciones sustanciales en los sistemas de información, así como la conservación del resultado de las mismas y de la prueba de implementación de los planes de acción correspondientes	x	x
Implementación de registros de entrada y salida de documentos y reportes que incluyan como mínimo: fecha, emisor y/o receptor, número de documento, tipo de información, forma de envío, responsable de la recepción o entrega	x	x
Implementación de mecanismos que limiten el número de intentos reiterados de accesos		x

Implementación de medidas para la confidencialidad y acceso no autorizado de terceros en el envío de documentos con contenido semiprivado, privado o sensible (ejemplo: sobre sellado)	x	x
Implementación de un sistema de copia o back up de la información	x	x
Recolección inmediata de copias en el uso de impresoras, escáneres y otros dispositivos de copia	x	
No reutilizar papel que contenga información personal semiprivada, privada o sensible	x	
Implementación de cultura de bloqueo de equipos de cómputo cuando no se encuentren en uso y creación de contraseñas alfanuméricas secretas para el ingreso a la información contenida en los mismos		x
Limitación al uso de internet mediante bloqueo de páginas inseguras. Cuando se reciba un correo que es de dudosa procedencia, la primera acción tiene que ser avisar a TI antes de abrir archivos o descargar		x
Limitación a las formas de extracción de información, bloqueando puertos de USB y unidad de CD y/o DVD.		x
Protección de contraseñas siendo las mismas secretas y de carácter intransferible		x
Compra e implementación de softwares antivirus, antispyware y firewalls que impidan el acceso no autorizado de terceros y la destrucción de la información		x

Actualización periódica de parches de seguridad		x
Utilización y compra de licenciamiento de Software original		x
Implementación de medidas de seguridad en la descarga de archivos adjuntos, como validación de extensiones del archivo (pdf, doc, .xlsx, png, etc.)		x
Establecimiento de políticas de protección para el acceso remoto a los sistemas de información		x
Para la atención de requerimientos realizados por alguna autoridad, validación de norma que faculta a la entidad para realizar el requerimiento y verificación de finalidades y proporcionalidad de las mismas según la naturaleza de los datos requeridos y la facultad contenida en las normas	x	x
Formateo de equipos de cómputo, destrucción de los discos duros antes de darles de baja a los mismos		x
Copia oculta de los contactos en el envío de correos masivos		x
Medidas de seguridad ADICIONALES para datos sensibles: Además de lo anterior, respecto de las bases de datos que contengan datos personales sensibles se tendrán las siguientes medidas de seguridad:		
Adopción de medidas que faciliten el control de cambios de la información contenida en las Bases de Datos		x
Implementación de sistema de etiquetado confidencial	x	x
Implementación de mecanismos de cifrado de datos para desarrollos y mantenimientos		x

de equipos informáticos, software, hardware, etc.		
Implementación de control y registro de accesos, que contenga información asociada a las gestiones realizadas.	x	x
Custodia de los soportes. Mientras la documentación con datos de carácter sensible no se encuentre archivada en los dispositivos de almacenamiento, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.	x	x
En cualquier intercambio de información sensible que se encuentre previamente o autorizada o legitimada por la ley, se deberá cifrar el acceso a los archivos correspondientes y en caso de envío físico, los documentos deberán ir en sobres debidamente cerrados y sellados, con sello de confidencialidad e información sensible, que sólo podrá ser abierta por su destinatario	x	x
Se cuenta con un sistema de análisis de datos en virtud del cual se restringe el cargue de datos sensibles a la herramienta. Dicha información se encuentra a cargo de un área específica de la organización y únicamente se utiliza con fines de alimentación de la herramienta omnicanal.		x

Asignación de responsabilidades y autorizaciones en el tratamiento de información personal, en las diferentes etapas del ciclo de vida del dato.

Como medida de seguridad asociada al tratamiento de datos personales, se define la asignación de responsabilidades en el tratamiento información personal de sus grupos de interés, en cada uno de los procedimientos relacionados con el dato al interior de la empresa, de la siguiente manera:

- **Responsabilidad en la Recolección, Almacenamiento, Uso y Circulación de datos personales**

La recolección, almacenamiento, uso y circulación de la información personal de la cual es responsable PREVIPASO S.A.S, se regirá de conformidad con lo dispuesto en el presente documento.

- **Responsabilidad en la Atención de consultas y reclamos (acceso y corrección)**

El Oficial de Protección de Datos Personales será el responsable de la atención de consultas y reclamos efectuados por los titulares en ejercicio de sus derechos, las cuales deberán ser atendidas en los términos de ley, conforme al procedimiento establecido en este documento.

- **Responsabilidad en la Conservación y/o Supresión de datos personales**

Para la supresión o destrucción de información contentiva de datos personales se deberá garantizar la confidencialidad e imposibilidad de recuperación de la información PREVIPASO S.A.S, y el área encargada será el área de Sistemas, con apoyo y supervisión del Oficial de Protección de Datos Personales, conforme al procedimiento de conservación y supresión establecido en este documento.

En caso de resultar procedente la supresión de los datos personales del titular de la base de datos conforme a reclamaciones presentadas por el titular PREVIPASO S.A.S, deberá realizar operativamente la supresión de tal manera que la eliminación no permita la recuperación de la información, sin embargo, en aquellos casos en que cierta información deba permanecer en registros históricos por cumplimiento de deberes legales o contractuales de la organización, su supresión versará frente al tratamiento activo de los mismos y de acuerdo a la solicitud del titular, lo cual será responsabilidad de las áreas que tengan acceso a la respectiva información de acuerdo al grupo de interés de que se trate.
En caso de que el Almacenamiento de Datos Personales la realice un Encargado del Tratamiento, se debe cumplir con lo dispuesto en el punto 4.4.2 del presente Protocolo.

PROCEDIMIENTO DE GESTIÓN DE RIESGOS E INCIDENTES DE SEGURIDAD ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES:

De conformidad con la estructura organizacional y procedimientos internos para el tratamiento de datos personales de PREVIPASO S.A.S, gestionará los riesgos asociados al tratamiento de datos personales con el propósito de evaluar y/o anticipar el incumplimiento de las normas de protección de datos personales, de la siguiente manera:

1. **Identificación.** Consiste en establecer los riesgos a que se ven expuestos los datos personales en desarrollo de su tratamiento.

- Se ha documentado los procedimientos que se implementen dentro del ciclo de vida de los datos personales, los cuales se describen en el presente documento.
- Se identifican los riesgos e incidentes ocurridos o que pudiesen ocurrir, respecto a este tipo de información, de acuerdo a lo dispuesto en este documento.
- Se ha identificado la persona o área que tenga a cargo la función de protección de datos personales en el diseño de nuevas iniciativas, servicios o programas.

Identificación de los riesgos e incidentes de seguridad de datos personales

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 que sean tratados bien sea por el Responsable del Tratamiento o por su Encargado.

Causales de los incidentes

Fraude interno. Delito no violento efectuado con la participación de los empleados o personas de confianza de PREVIPASO S.A.S, o Encargado del Tratamiento, bien sea en forma directa o indirecta, a saber:

- Cualquier apropiación, acceso o uso indebido o no lícito de los datos personales a los cuales PREVIPASO S.A.S, o sus Encargados les realice tratamiento, a través de engaños, gestiones no reales, falsificación o adulteración de documentos, administración mal intencionada, cometido por los empleados o personas de confianza dentro de la organización; quienes valiéndose de su posición o de la información privilegiada de la que disponen, realizan un manejo indebido de los datos personales o cualquier tipo de infraestructura que pueda incidir o representar un riesgo en el tratamiento de los mismos.

Fraude externo. Cualquier acto efectuado por una persona ajena PREVIPASO S.A.S, o Encargado del tratamiento, buscando acceder, apropiarse, causar adulteración o eliminación a los datos personales a los cuales estos les realizan tratamiento, a saber:

- Cualquier apropiación, acceso o uso indebido o no lícito de los datos personales a los cuales el Responsable o Encargado les realice tratamiento, a través de los sistemas informáticos, robo, atraco, engaños, falsificación o adulteración de documentos, cometido por personas que no pertenecen a la organización.

Daños a activos físicos. Pérdida, deterioro o cualquier afectación de los datos personales a los cuales el Responsable o Encargado realicen tratamiento, causados por daños a los activos físicos de los mismos, a saber:

- Daño físico en los computadores de la empresa, archivos físicos como papel, cintas, discos, etc., causados por cualquier tipo de incidencia como fenómenos naturales, accidentales o por problemas de orden público.

Falla de tecnología informática. Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales el Responsable o Encargado realicen tratamiento, causados por fallas en la infraestructura tecnológica de uno u otro, a saber:

- Daño en el funcionamiento de los sistemas de información, daño en las redes de datos, problemas con los canales de transmisión de información, VPN, aplicaciones, etc.

Ejecución y/o administración de procesos. Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales PREVIPASO S.A.S., o sus Encargados realicen tratamiento, causados por fallas en la ejecución, aplicación y/o administración de procesos, procedimientos, protocolos, políticas de uno u otro, a saber:

- Toda vulneración que se detecte por la mala aplicación o ejecución de un procedimiento ya establecido, el cual debe estar documentado y llevar una trazabilidad de su correcta ejecución.

Falla por negligencia o actos involuntarios de los titulares. Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales PREVIPASO S.A.S, o sus Encargados realicen tratamiento, causados por negligencia o actos involuntarios del mismo titular, que puede ver afectados tanto sus propios datos como los de otros titulares.

- Por lo general, este riesgo se materializa cuando el titular no acata las recomendaciones de seguridad frente al manejo de sus propios datos personales, como el uso de contraseñas de acceso a sistemas de información o cuentas bancarias, cuentas de correo electrónico, números de tarjetas bancarias, utilización de éstos en medios no

seguros o excesiva confianza en la entrega de sus datos personales o de otros titulares a personas no autorizadas.

Tipo de incidente de seguridad

Afecta la Confidencialidad de los datos personales. Todos aquellos incidentes que afecten el principio de seguridad relacionado con la Confidencialidad de los datos personales, siendo ésta, la característica que evita la divulgación de la información a personas o procesos que no estén debidamente autorizados.

- Cualquier acceso no autorizado a los datos personales.

Afecta la Disponibilidad de los datos personales. Todos aquellos incidentes que afecten el principio de seguridad relacionado con la Disponibilidad de los datos personales, que es la característica que garantiza el acceso a la información por las personas o procesos autorizados, siempre que sea requerida.

- Caída en los sistemas de información, ataques de denegación de servicio.

Afecta la Integridad de los datos personales. Todos aquellos incidentes que afecten el principio de seguridad relacionado con la Integridad de los datos personales que es aquél que garantiza que la información se mantenga, tal como fue recolectada o generada, sin alteraciones o modificaciones no solicitadas o autorizadas.

- Alteración en los datos personales frente a los datos entregados por el titular, sin trazabilidad de solicitud de actualización.

Afecta Confidencialidad y disponibilidad de los datos personales. Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la confidencialidad y disponibilidad de los datos personales.

- Acceso no autorizado a la base de datos personales y eliminación de algunos o todos los datos personales encontrados en la misma.

Afecta Confidencialidad e Integridad de los datos personales. Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la confidencialidad e Integridad de los datos personales.

- Acceso no autorizado a la base de datos personales y adulteración de algunos o todos los datos personales encontrados en la misma.

Afecta Disponibilidad e Integridad de los datos personales. Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la disponibilidad e Integridad de los datos personales.

- Acceso autorizado a la base de datos personales con adulteración de algunos o todos los datos personales encontrados en la misma y que para perpetrar el hecho, se realice cualquier acción en forma temporal o definitiva en la que se evite el acceso a la información del (los) titular (es) por parte de personas o procesos autorizados.

Afecta la Confidencialidad, Disponibilidad e Integridad de los datos personales. Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la confidencialidad, disponibilidad e integridad de los datos personales.

- Acceso no autorizado a la base de datos con información personal y adulteración de algunos o todos los datos personales encontrados en la misma y que para perpetrar el hecho, se realice cualquier acción en forma temporal o definitiva en la que se evite el acceso a la información del (los) titular (es) por parte de personas o procesos autorizados.

2. Medición y evaluación (Impacto y Probabilidad).

Tiene por objetivo determinar la posibilidad de ocurrencia de los riesgos relacionados con el tratamiento de bases de datos personales y su impacto en caso de materializarse.

Un incidente de seguridad puede tener una variedad de efectos adversos sobre las personas que puede dar lugar a problemas de discriminación, suplantación de identidad o fraude, pérdidas financieras, daño reputacional, pérdida del carácter confidencial de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo. El nivel de riesgo del incidente de seguridad frente a los Titulares de la información se cuantifica y/o califica así:

- **Bajo riesgo:** es improbable que el incidente de seguridad tenga un impacto en las personas, y de generarlo, este sería mínimo. Esto será de aplicación para incidentes de seguridad atinentes a datos de carácter público.
- **Riesgo medio:** el incidente de seguridad puede tener un impacto en las personas, pero es poco probable que el impacto sea sustancial. Esto será de aplicación para incidentes de seguridad atinentes a datos de carácter semiprivado de cualquier grupo de interés.
- **Riesgo alto:** el incidente de seguridad puede tener un impacto considerable en las personas afectadas. Esto será de aplicación para incidentes de seguridad atinentes a datos de carácter privado de cualquier grupo de interés.

- **Riesgo grave:** el incidente de seguridad puede tener un impacto crítico, extenso o peligroso en las personas afectadas. Esto será de aplicación para incidentes de seguridad atinentes a datos sensibles de cualquier grupo de interés.

Sin perjuicio de la clasificación anterior, en cada caso concreto se analiza el nivel de riesgo no sólo de acuerdo al grupo de interés, sino también de acuerdo al tipo de incidente de seguridad ocurrido, teniendo en cuenta los siguientes criterios:

En los Titulares de la información:

¿Qué cantidad de personas fueron afectadas? ¿Qué categoría de personas fueron afectadas? ¿Cuáles son las características especiales de las personas afectadas? Por ejemplo: niños, niñas y/o adolescentes; personas en estado de vulnerabilidad; personal del sindicato, etc.

En los datos personales: ¿Cuál fue el volumen de los datos afectados? ¿Cuál fue el periodo durante el cual los datos fueron afectados o estuvieron comprometidos? ¿Qué tipo de información personal fue afectada? Por ejemplo, identificación personal, datos biométricos, historia clínica, datos genéticos, pruebas académicas, registros de localización, direcciones IP, mensajes de texto, información financiera y crediticia, datos genéticos, perfiles de comportamiento, puntajes de crédito, etc. ¿Qué tan sensible es la información comprometida? Por ejemplo: datos de niños, niñas y/o adolescentes; datos biométricos, genéticos o de salud; perfiles de comportamiento; resultados de decisiones automatizadas; orientación sexual; datos políticos; etc. ¿Cuál es el contexto de la información personal comprometida? ¿Estaba la información personal adecuadamente cifrada, anonimizada? ¿Era inaccesible? ¿Cómo se puede utilizar la información personal afectada? ¿Existe un riesgo a una mayor exposición de la información personal? ¿Está la información personal disponible públicamente en internet? ¿Se puede utilizar la información personal para fines fraudulentos o puede causar cualquier tipo de daño material y/o inmaterial al Titular? ¿Se ha recuperado la información personal?

En la organización: ¿Qué causó el incidente de seguridad? ¿Cuándo y con qué frecuencia ocurrió el incidente de seguridad? ¿Es este un problema sistémico o aislado? ¿Cuál fue el alcance del incidente de seguridad? ¿Qué medidas se han tomado para mitigar el daño? ¿Cuáles son las actividades y operaciones que desarrolla la organización? Por ejemplo: entidades financieras, entidades públicas, etc. ¿Los datos comprometidos afectarán las transacciones que debe realizar la organización con terceros externos?

3. Control y gestión de incidentes

Se relacionan las acciones que se deben tomar para controlar y/o mitigar los riesgos a los que se ven expuestos los datos personales, con el fin de disminuir la posibilidad y/o las consecuencias de la materialización de los mismos; de igual forma, 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 continuación, se describen de forma general los controles que deberá verificar el Oficial de Protección de Datos Personales de PREVIPASO S.A.S, para asegurar que las políticas adoptadas por la organización se implementen al interior de la compañía:

Procedimientos operacionales:

a. Controles Preventivos

PREVIPASO S.A.S, ha elaborado procedimientos alusivos a la recolección, almacenamiento, utilización, supresión y disposición final de los datos personales al interior de la compañía, mediante la definición de funcionarios, roles y actividades que deberán observarse para cumplir con las actividades propuestas, los cuales se encuentran descritos en el presente manual.

De igual manera, PREVIPASO S.A.S, cuenta con medidas de seguridad en materia de protección de datos personales encaminadas a prevenir y mitigar el riesgo de ocurrencia incidentes de seguridad respecto de los mismos.

b. Gestión de incidentes de seguridad

Una vez detectado el incidente, el área que lo haya detectado deberá comunicar inmediatamente al Oficial de Protección de Datos Personales, quien deberá de forma simultánea:

- **Adoptar las medidas que correspondan para contener el incidente y efectuar una evaluación preliminar.**

En esta primera etapa se hará una investigación inicial sobre el evento u ocurrencia, en la que se deberá indagar acerca de: ¿Cómo se produjo? ¿Cuándo y dónde tuvo lugar? ¿Cuál fue la naturaleza y quién lo detectó? ¿Se continúa compartiendo o divulgando información personal sin Autorización? ¿Quién tiene acceso a la información personal? ¿Qué se puede hacer para asegurar la información o detener el acceso, divulgación o disponibilidad no autorizada y reducir el riesgo de daños a los afectados? ¿Es un incidente de seguridad relacionado con Datos Personales que requiere la notificación a las personas tan pronto como sea posible?

- **Evaluar los riesgos e impactos asociados al incidente e identificar daños para las personas, organizaciones y público en general.**

En este punto, se deberán tener en cuenta los criterios de medición y evaluación indicados en el punto 2 de este acápite, y adicionalmente los siguientes:

Daños para las personas que podrían resultar de un incidente de seguridad

- Riesgo en su seguridad física o psicológica.
- Extorsión económica o sexual
- Hurto de identidad
- Suplantación de identidad.
- Pérdida financiera.
- Negación de un crédito o seguro.
- Perfilamiento con fines ilícitos.
- Pérdida de negocios u oportunidades de empleo.
- Discriminación.
- Humillación significativa o pérdida de dignidad y daño a la reputación.

Daños para la organización que podrían resultar de un incidente de seguridad

- Pérdida reputacional
- Pérdida de clientes o usuarios
- Pérdida de confianza en la organización
- Honorarios de consultores e ingenieros forenses
- Pérdida de activos
- Sanciones, órdenes e instrucciones administrativas
- Exposición financiera
- Órdenes judiciales
- Demandas judiciales

Daños para el público podría resultar de un incidente de seguridad

- Riesgo para la salud pública
- Riesgo para la seguridad pública
- Pánico económico
- Alteración de los pilares constitucionales de un país

- **En caso de ser necesario, comunicar de manera eficiente a los titulares afectados sobre el incidente ocurrido y proporcionar herramientas para minimizar el daño potencial o causado.**

Las comunicaciones en caso de ser necesario informarle al titular, deben ser suficientes claras y precisas para permitir que los Titulares de la información comprendan la importancia del incidente y que tomen las medidas, si es posible, para reducir los riesgos que podría resultar de su ocurrencia. Es primordial no incluir información personal innecesaria en el aviso para evitar una posible divulgación no autorizada.

- **Independientemente de su impacto, el Oficial de Protección de Datos Personales deberá reportar a la Superintendencia de Industria y Comercio todos los incidentes ocurridos, informando como mínimo:**

  - El tipo de incidente ocurrido.
  - Fecha en que ocurrió.
  - Fecha en que se tuvo conocimiento del mismo.
  - La causal.
  - Tipo de datos personales comprometidos.
  - Cantidad de titulares afectados.

El reporte deberá efectuarse dentro de los quince (15) días hábiles siguientes a la fecha de ocurrencia del incidente o a la fecha en que se detecte, a través del enlace establecido por la Superintendencia de Industria y Comercio para ello.

c. Control y prevención de <u>nuevos</u> incidentes de seguridad

Se implementarán las siguientes medidas para controlar y disminuir la posibilidad y/o las consecuencias de la materialización de incidentes de seguridad.

Conservación de registros internos

Cuando ocurra un incidente de seguridad, el Oficial de Protección de Datos Personales documentará todos los aspectos de cada incidente de seguridad en los registros internos de la organización, con el fin de evitar que esos incidentes ocurran nuevamente.

Dichos registros documentales deberán incluir lo siguiente:

- Una descripción general de las circunstancias del incidente de seguridad (incluidas las Bases de Datos y las clases de datos -sensibles, privados, etc.- comprometidos).
- Las categorías de Titulares de la información afectados.
- La fecha y hora del incidente de seguridad y del descubrimiento del mismo.
- Las indagaciones preliminares e investigaciones realizadas por la organización.
- Las medidas correctivas.
- Los Responsables del manejo del incidente de seguridad.
- La prueba del reporte efectuado ante la SIC, así como la comunicación realizada a los Titulares de la información, si fue necesario.

- La evaluación del nivel de riesgo derivado del incidente de seguridad en los Titulares y los factores tenidos en cuenta.
- La inclusión de detalles personales, cuando deban establecerse.

Se adoptarán otras medidas como:

- Reforzar los programas de capacitación y educación del personal.
- Identificar y mejorar los controles internos que no tuvieron el efecto esperado en la contención de la brecha de seguridad.
- Identificar y eliminar malware o desactivar cuentas de usuarios vulnerables.
- Realizar un contraste con las medidas adoptadas para solucionar el incidente de seguridad en cuestión, y garantizar un análisis pormenorizado de las soluciones que pudieron haberse adoptado.
- Actualizar el antivirus de la organización.
- Analizar con el antivirus todo el sistema operativo, incluidas aquellas secciones que no se vieron afectadas.

4. Monitoreo y evaluación

Sostenibilidad del Programa de Protección de Datos Personales. El Programa de Protección de Datos Personales exige una evaluación y revisión continúa de los controles que lo integran, con el fin de determinar la pertinencia y eficacia del plan de gestión. En consecuencia, el Oficial de Protección de Datos Personales será el encargado al interior de la organización de desarrollar un plan de supervisión y revisión anual que tome en cuenta las siguientes etapas:

Fase de diagnóstico: En ella deberá evaluarse en qué estado de cumplimiento se encuentra la organización, acudiéndose, entre otras, a: (i) elaboración de auditorías internas; (ii) debilidades identificadas en la atención de consultas y reclamos, e incidentes de seguridad y; (iii) Revisión de las tendencias y obligaciones legales que surjan con ocasión a la protección de datos personales.

Fase de adecuación: Consiste en determinar las acciones a implementar por la organización, en aras de hacer más efectivo el Programa de Protección de Datos Personales. En PREVIPASO S.A.S, se implementarán las siguientes medidas preventivas:

A. Entrenar periódicamente al equipo humano de la organización para actuar frente al incidente de seguridad. Se podrán realizar simulacros preventivos como se hacen, por ejemplo, para casos de incendios o temblores. Frente a un incidente de seguridad, la gente debe estar preparada para actuar de inmediato, profesionalmente e inteligentemente.

B. Precisar exactamente cuándo se está ante un incidente de seguridad que afecte Datos Personales. No todas las fallas de seguridad necesariamente involucran la confidencialidad, integridad y disponibilidad de información de carácter personal.
C. Aplicar las medidas y el procedimiento descrito en este documento para el manejo de los incidentes de seguridad.
D. Aplicar la metodología para la evaluación del impacto de los incidentes de seguridad en los Titulares de la información.
E. Conocer los procesos de respuesta a incidentes de seguridad, sistemas de corrección y de recuperación, incluidos aquellos establecidos por los Encargados del Tratamiento.
F. Cumplir con lo establecido en la Ley 1581 de 2012, así como con las órdenes y/o instrucciones que imparta la SIC.
G. Reportar el incidente de seguridad tanto a la SIC como a otras autoridades públicas, según sea el caso.
H. Preparar al equipo de comunicaciones frente a las posibles preguntas e inquietudes de Titulares de la información, accionistas, clientes, proveedores, empleados y medios de comunicación, respecto del incidente de seguridad.

Fase de implementación: Previa aprobación de la alta dirección de la organización, efectuar los cambios que resulten pertinentes en los componentes del Programa de Protección de Datos Personales. Junto con acciones de capacitación al personal.

Fase de revisión: El Oficial de Protección de Datos Personales debe supervisar, evaluar y revisar el programa por lo menos una vez a año, para asegurar que siga siendo pertinente y eficaz, debiendo determinar:

- Cuáles son las últimas amenazas y riesgos respecto del tratamiento de datos personales detectados en la organización.
- Si los controles del programa están teniendo en cuenta las nuevas amenazas y reflejando las quejas más recientes o los hallazgos de las auditorias, o las orientaciones de la autoridad de protección de datos.
- Si se están ofreciendo nuevos servicios que involucran una mayor recolección, uso o divulgación de la información personal.
- Si se está llevando a cabo capacitación eficaz, se está siguiendo las políticas y procedimientos, y el programa se encuentra actualizado.

Con base en los resultados del proceso de evaluación, se deben tomar las medidas para actualizar y revisar los controles del programa y los cambios deben ser comunicados a los empleados y autorizados cuando sea procedente.

Incidentes de seguridad cuando se acude a encargados del tratamiento

En los contratos de transmisión de datos personales suscritos por PREVIPASO S.A.S, con los encargados del tratamiento, se incluirán cláusulas asociadas al manejo y reporte de incidentes de seguridad.

1.1. USO

Para el uso de los Datos Personales de los Titulares, se deberán tener en cuenta las siguientes indicaciones:

1.1.1. Finalidades Autorizadas

Sólo se podrán usar los Datos Personales para las finalidades que hayan sido autorizadas por el Titular o su representante, salvo que se trate de Datos Públicos que no requieran Autorización o que exista alguna norma que obligue su Tratamiento.

Se deberá establecer un mecanismo para verificar qué finalidades autorizó el Titular y cuáles no, o sobre cuáles revocó su Autorización.

1.1.2. Encargados del Tratamiento

En caso de que el Uso de Datos Personales la realice un Encargado del Tratamiento, se debe cumplir con lo dispuesto en el punto 4.4.2 del presente Protocolo.

1.2. CIRCULACIÓN

La circulación de los Datos Personales, se realizará cumpliendo las siguientes reglas:

1.2.1. Circulación entre Operativos

El Operativo sólo podrá acceder o consultar la información o Datos Personales que reposen en las Bases de Datos del Responsable del Tratamiento cuando sea estrictamente necesario para el ejercicio de sus funciones.

El Operativo podrá utilizar la información a la que tenga acceso en ejercicio de su cargo, para la ejecución de las labores y funciones asociadas al mismo, por lo que le está prohibido usarla para fines distintos y deberá abstenerse de suministrarla, cederla o comercializarla a terceras personas naturales o jurídicas, públicas o privadas, salvo que la misma sea de

naturaleza pública sin sujeción a reserva, o sea requerida por una autoridad competente en el ejercicio de sus funciones legales, caso en el cual deberá avisar de inmediato a la persona o área encargada de la Protección de Datos Personales, conforme a lo establecido en la Política de Privacidad y Protección de Datos Personales, para que sea ésta quien defina cómo atender el requerimiento realizado por la autoridad competente.

El Responsable del Tratamiento cuenta con medidas de seguridad para el control de acceso de los Operativos a los Datos Personales a los que, por sus funciones, no requieran tener acceso.

1.2.2. Transmisión de Datos Personales

El Responsable del Tratamiento podrá Encargar a una tercera persona natural o jurídica el Tratamiento de Datos Personales de los Titulares que componen sus Grupos de Interés, dentro o fuera del país.

PREVIPASO S.A.S, podrá transmitir los datos personales a terceros con quienes tenga relación operativa que le provean de servicios necesarios para su debida operación, o de conformidad con las funciones establecidas a su cargo en las leyes.

En dichos supuestos, se adoptarán las medidas necesarias para que las personas que tengan acceso a sus datos personales cumplan con la presente Política y con los principios de protección de datos personales y obligaciones establecidas en la Ley.
Transmisión de datos personales

En todo caso, cuando PREVIPASO S.A.S, transmita los datos a uno o varios encargados ubicados dentro o fuera del territorio de la República de Colombia, establecerá cláusulas contractuales o celebrará un contrato de transmisión de datos personales en el que indicará:

Alcances del tratamiento, 2. Las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales y, 3. Las obligaciones del Encargado para con el titular y el responsable.

Mediante dicho contrato el Encargado se comprometerá a dar aplicación a las obligaciones del responsable bajo la política de Tratamiento de la información fijada por este y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares hayan autorizado y con las leyes aplicables vigentes.

Además de las obligaciones que impongan normas aplicables dentro del citado contrato, deberán incluirse las siguientes obligaciones en cabeza del respectivo encargado: 1. Dar

Tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan. 2. Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales. 3. Guardar confidencialidad respecto del tratamiento de los datos personales.

1.2.3. Transferencia de Datos Personales

El Responsable del Tratamiento podrá realizar Transferencia de Datos Personales a otros Responsables del Tratamiento, previa autorización del Titular, salvo que estos sean de naturaleza pública o exista alguna norma vigente que obligue su Transferencia.

Cuando se realicen Transferencias Internacionales de Datos Personales, se debe verificar que el país al cual se Transfieren los datos, cuente con niveles adecuados de Protección de Datos Personales, conforme a los estándares que fije la Superintendencia de Industria y Comercio.

Lo anterior no aplica en los siguientes casos:

a. Exista autorización previa y expresa del Titular para la Transferencia Internacional;
b. Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública;
c. Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;
d. Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;
e. Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular;
f. Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; o
g. Se cuente con una Declaración de Conformidad expedida por la Superintendencia de Industria y Comercio.

Sin perjuicio de lo anterior, el Responsable del Tratamiento Remitente deberá suscribir un Contrato de Transferencia de Datos Personales con los Responsables del Tratamiento a quienes Transfiera Datos Personales, que contenga como mínimo: los alcances del tratamiento, las actividades para las cuales se Transfiere la información, la obligación del Responsable del Tratamiento Receptor de cumplir con las normas de Protección de Datos Personales y de dar Tratamiento únicamente para las finalidades autorizadas por el Titular en aplicación de los principios establecidos en las normas vigentes, la obligación de adoptar

las medidas de seguridad que se requieran para proteger los Datos Personales y el deber de guardar estricta confidencialidad respecto del Tratamiento de los Datos Personales.

PROCEDIMIENTO DE ATENCIÓN DE CONSULTAS Y RECLAMOS DE LOS TITULARES DE LA INFORMACIÓN

1. **Consultas.**

Los titulares o sus causahabientes podrán consultar la información personal del titular que repose en la base de datos de la Empresa, previa validación y acreditación de su identidad, las cuales deberán contener como mínimo: i) la identificación completa del titular, ii) los datos personales que quieren ser consultados, ii) dirección, iii) correo electrónico, y; iv) en caso de ser causahabientes anexar el respectivo documento que lo demuestre.

La consulta será atendida por la compañía, en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo del correo electrónico o del documento físico.

Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado expresando los motivos de la demora y señalará la fecha en que se atenderá su solicitud en un tiempo máximo de cinco (5) días hábiles siguientes al vencimiento del primer término.

2. **Reclamos.**

El Titular o sus causahabientes que consideren 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, podrán presentar un reclamo ante PREVIPASO S.A.S, como Responsable o Encargado del Tratamiento, el cual será tramitado bajo las siguientes reglas:

1. El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

1.2.4. Titulares y personas legitimadas en ejercicio del Derecho de Hábeas Data

Los Titulares o aquellas personas que se encuentren legitimadas por normas vigentes, pueden presentar Peticiones, Consultas y Reclamos a través de los canales establecidos en la Política de Privacidad y Protección de Datos Personales del Responsable del Tratamiento.

Las siguientes, son las personas facultadas para presentar PQR´s en ejercicio del Derecho de Hábeas Data, conforme a lo dispuesto por el artículo 2.2.2.25.4.1.del Decreto 1074 de 2015:

a. El Titular, quien deberá acreditar su identidad en forma suficiente.
b. Los causahabientes del Titular, quienes deberán acreditar tal calidad.
c. El representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
d. Por estipulación a favor de otro o para otro, siempre que medie la aceptación por parte del Titular, de lo cual, se deberá presentar constancia en la solicitud.

Los derechos de los Niños, Niñas o Adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Las consultas y reclamos serán resueltos dentro de los términos establecidos en las Leyes 1266 de 2008 y 1581 de 2012, o aquellas que las sustituyan, modifiquen o deroguen.

1.2.5. Tipos de reclamos

Las consultas y reclamos que pueden presentar los Titulares, según la Ley 1581 de 2012, se clasifican por códigos y se deben reportar de esta manera ante la Superintendencia de Industria y Comercio.

Los códigos de consultas y reclamos ante el Responsable del Tratamiento son los que se indican en el Manual del Registro Nacional de Bases de Datos emitido por la Superintendencia de Industria y Comercio.

1.2.6. Reporte de información comercial, financiera y crediticia (Ley 1266 de 2008)

El Responsable del Tratamiento o Fuente de Información, podrá realizar reportes positivos de los Titulares en cualquier tiempo.

Para realizar reportes negativos a los diferentes Operadores de Información, el Responsable del Tratamiento deberá enviar comunicación previa a los Titulares con una antelación de veinte (20) días calendario, en la cual se le informe a éste último de la mora presentada, para que el mismo pueda demostrar o efectuar el pago de la obligación, así como controvertir aspectos tales como el monto de la obligación o cuota y fecha de exigibilidad.

Pasados los veinte (20) días calendario antedichos, sin que el Titular cancele las obligaciones pendientes, el Responsable del Tratamiento podrá realizar el reporte respectivo.

En caso que el Titular presente una solicitud de rectificación o actualización, el Responsable del Tratamiento deberá informar al Operador de Información que la información reportada se encuentra en discusión por parte del Titular.

1.2.7. Requerimiento de información por autoridad administrativa o judicial competente

Cuando una autoridad administrativa o judicial competente requiera información personal, se deberá validar que en el requerimiento incluya:

1. La norma que los faculta a requerir la información;
2. La finalidad para la cual se requiere la información; y
3. La forma en que debe ser enviada la información, para garantizar la protección de los Datos Personales.

1.3. ACTUALIZACIÓN

La Actualización de Datos Personales se podrá llevar a cabo, bien sea por una reclamación del Titular o de las personas que se encuentren legitimadas, o por la adopción de

mecanismos por parte del Responsable del Tratamiento que le permitan actualizar periódicamente la información:

1.3.1. Otros mecanismos de actualización

El Responsable del Tratamiento podrá implementar mecanismos tales como encuestas, campañas de actualización, cruce de información con bases de datos públicas, entre otras, previa Autorización del Titular.

1.3.2. Encargado del Tratamiento

En caso de que la Actualización de Datos Personales la realice un Encargado del Tratamiento, se debe cumplir con lo dispuesto en el punto 4.4.2 del presente Protocolo.

1.4. SUPRESIÓN

La supresión de los Datos personales deberá llevarse a cabo de la siguiente forma:

1.4.1. Culminación finalidad

Los Responsables del Tratamiento y los Encargados del Tratamiento podrán Tratar los Datos Personales mientras subsistan las finalidades para las cuales fueron recolectados, y atendiendo aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

Una vez cumplida la o las finalidades para las cuales se recolectaron los datos, el Responsable del Tratamiento y el Encargado del Tratamiento, deberán proceder a la supresión de los mismos, salvo que se requiera su conservación para el cumplimiento de una obligación legal o contractual.

A continuación, se señalan los términos establecidos en algunas normas vigentes para la conservación de los siguientes documentos y/o soportes:

MATERIA	TIPO DE DOCUMENTO	NORMA	TIEMPO
CONTABLES Y CONTRACTUALES	Contabilidad, libros, registros contables, inventarios y estados financieros en general	Ley 962 de 2005	Periodo mínimo diez (10) años contados a partir de la fecha del último asiento, documento o comprobante. La conservación en físico por un tiempo mayor dependerá de la valoración documental que se realice. En todo caso deberán conservarse los soportes en medios magnéticos.
	Comprobantes que sirvan de respaldo a las partidas asentadas en los libros, así como la correspondencia directamente relacionada con los negocios		
	El comprobante de contabilidad es el documento que debe elaborarse previamente al registro de cualquier operación y en el cual se indicará el número, fecha, origen, descripción y cuantía de la operación, así como las cuentas afectadas con el asiento. A cada comprobante se anexarán los documentos que lo justifiquen.		
	Copia fiel de la correspondencia que dirija en relación con los negocios, por cualquier medio que asegure la exactitud y duración de la copia. Asimismo, conservará la correspondencia que reciba en relación con sus actividades comerciales, con anotación de la fecha de contestación o de no haberse dado respuesta.		
	El comerciante conservará archivados y ordenados los comprobantes de los asientos de sus libros de contabilidad, de manera que en cualquier momento se facilite verificar su exactitud.		

FISCALES	Libros de contabilidad junto con los comprobantes de orden interno y externo que dieron origen a los registros contables (que permitan la verificación de activos, pasivos, patrimonio, ingresos, costos, deducciones, rentas exentas, descuentos, impuestos y retenciones)	Estatuto Tributario (Decreto 624 de 1989)	Período mínimo de cinco (5) años, contados a partir del primero (10.) de enero del año siguiente al de su elaboración, expedición o recibo
	Las informaciones y pruebas específicas contempladas en las normas vigentes, que dan derecho o permiten acreditar los ingresos, costos, deducciones, descuentos, exenciones y demás beneficios tributarios, créditos activos y pasivos, retenciones y demás factores necesarios para establecer el patrimonio líquido y la renta líquida de los contribuyentes, y en general, para fijar correctamente las bases gravables y liquidar los impuestos correspondientes.		
	La prueba de la consignación de las retenciones en la fuente practicadas en su calidad de agente retenedor		
	Copia de las declaraciones tributarias presentadas, así como de los recibos de pago correspondientes		
	Las facturas, documentos equivalentes y documentos sustitutivos		

	Los archivos magnéticos y el software utilizados para el intercambio de documentos a través de la red, tratándose de la factura electrónica		
	Los medios magnéticos que contengan la información, así como los programas respectivos, el comprobante informe diario y la cinta testigo magnética, cuando se expidan facturas por computador o se utilice el sistema POS (Punto de Venta o terminal de punto de venta)		
	La identificación tanto del emisor de la factura como del receptor, con indicación de la fecha de transmisión o recepción, por parte de los administradores de la red de valor agregado		
	Los registros, comprobantes informes diarios, comprobantes Z, listas genéricas y los comprobantes resumen denominados informes fiscales de control en ellas adoptados		
	El registro que deben llevar quienes elaboran facturas o documentos equivalentes de las personas o entidades que hayan solicitado el servicio, y copia de las resoluciones de autorización de la numeración o constancias del vencimiento del término para decidir, entregadas por el usuario del servicio		

LABORALES	Historias laborales y nóminas activas e inactivas (Hoja de vida, Contrato de trabajo, Documentos de identidad, Certificados académicos, Exámenes médicos, Llamados de atención, descargos, Afiliaciones y retiros, Liquidación del contrato, Certificaciones laborales, Afiliación a Sindicatos, Bono pensional, Resolución de nombramiento, encargo, comisión, vacaciones, licencias, incapacidad, asignación de funciones, encargos, Formato de solicitud de autorización de ausencia temporal, Notificación, Laborales, Cesantías, Inscripciones, Resolución de elegibles, Resolución nombramiento en periodo de prueba, Notificación de Nombramiento, Solicitud de Inscripción en Carrera Administrativa, Acta de posesión, Evaluación del desempeño Laboral, Resolución de Inscripción en Carrera Administrativa, Llamados de atención, Investigación, Informe de gestión, Embargos varios, Cuota alimentaria, Notificación de retiro, Beneficios madres y/o padres cabeza de familia, Actualización hoja de vida, Actualización de bienes y rentas)	Sentencia T-470 de 2019	Permanente

	Documentos relacionados con pagos de seguridad social	Constitución Política Artículo 48 Corte Constitucional Sentencia SU-298 de 2015	Permanente

SALUD Y SEGURIDAD EN EL TRABAJO	Los resultados de los perfiles epidemiológicos de salud de los trabajadores, así como los conceptos de los exámenes de ingreso, periódicos y de retiro de los trabajadores, en caso que no cuente con los servicios de médico especialista en áreas afines a la seguridad y salud en el trabajo Cuando la empresa cuente con médico especialista en áreas afines a la seguridad y salud en el trabajo, los resultados de exámenes de ingreso, periódicos y de egreso, así como los resultados de los exámenes complementarios tales como paraclínicos, pruebas de monitoreo biológico, audiometrías, espirometrías, radiografías de tórax y en general, las que se realicen con el objeto de monitorear los efectos hacia la salud de la exposición a peligros y riesgos; cuya reserva y custodia está a cargo del médico correspondiente	Decreto 1072 de 2015	Mínimo veinte (20) años contados a partir del momento en que cese la relación laboral del trabajador con la empresa

	Resultados de mediciones y monitoreo a los ambientes de trabajo, como resultado de los programas de vigilancia y control de los peligros y riesgos en seguridad y salud en el trabajo		
	Registros de las actividades de capacitación, formación y entrenamiento en seguridad y salud en el trabajo		
	Registro del suministro de elementos y equipos de protección personal		

1.1.1. Requerimiento de autoridad competente

Los Datos Personales deberán suprimirse, en el evento que así lo requiera una autoridad administrativa o judicial competente, dentro del término establecido por ésta.

1.2. Tablas de retención documental

El Responsable del Tratamiento, deberá adoptar Tablas de Retención Documental, las cuales se elaborarán, teniendo en cuenta los siguientes pasos:

1.2.1. Inventario documental

El Responsable del Tratamiento deberá realizar un inventario de los documentos o Datos Personales incluidos en las Bases de Datos, sobre las cuales decida o en las que actúe en calidad de Encargado del Tratamiento.

1.2.2. Valoración documental

Una vez levantado el inventario, el Responsable del Tratamiento deberá adelantar un análisis sobre los documentos o Datos Personales incluidos en las Bases de Datos, con el fin de determinar cuáles son necesarios para su operación diaria y/o para atender las solicitudes realizadas por autoridades administrativas y/o judiciales competentes, proveedores, trabajadores, contratistas, clientes, y demás Grupos de Interés (*Valor Primario*);y cuáles son útiles para fines históricos, científicos y/o culturales (*Valor Secundario*).

Valor Primario:

Entre estos se encuentran los siguientes:

- **VALOR ADMINISTRATIVO:** Cualidad que tienen los documentos o Datos Personales del Responsable del Tratamiento, dado que son testimonio y soporte de sus procedimientos y actividades.

- **VALOR JURÍDICO O LEGAL:** Valor del que se derivan derechos y obligaciones legales, regulados por el derecho común y que sirven ante la ley como testimonio.

- **VALOR FISCAL:** Utilidad de los documentos de archivo para el tesoro o hacienda pública.

- **VALOR CONTABLE:** Cualidad de los documentos que soportan el conjunto de cuentas y de registros de los ingresos, egresos, y los movimientos económicos de una entidad pública o privada.

- **VALOR TÉCNICO:** Atributo de los documentos producidos y recibidos por una institución en virtud de sus funciones misionales.

Valor Secundario:

Entre estos se encuentran los siguientes:

- **VALOR HISTÓRICO:** Cualidad atribuida a los documentos que por ser útiles para la reconstrucción de la historia o memoria de una comunidad deben conservarse.

- **VALOR CIENTÍFICO:** Cualidad de los documentos que registran información relativa a la creación de conocimiento en cualquier área del conocimiento.

- **VALOR CULTURAL:** Cualidad de los documentos que por su contenido son testimonios de los hechos, vivencia, tradiciones, costumbres, hábitos, valores, modos de vida o desarrollos económicos, sociales, políticos, religiosos o estéticos propios de una comunidad y útiles para el conocimiento de su identidad.

1.2.3. Definición de tiempos de retención documental

El Responsable del Tratamiento deberá definir el tiempo que desea conservar los documentos de Valor Primario y los documentos de Valor Secundario.

1.2.4. Tiempos de retención documental

Los tiempos de retención documental que deberán aplicarse, serán los contenidos en las Tablas de Retención documental, las cuales se adoptarán, en atención a los:

1. Tiempos establecidos por orden legal o judicial;
2. Tiempos definidos por el Responsable del Tratamiento para los documentos o Datos Personales de Valor Primario;
3. Tiempos definidos por el Responsable del Tratamiento para los documentos o Datos Personales de Valor Secundario.

Los tiempos definidos para los documentos de Valor Primario y Valor Secundario no podrán en ningún momento ser inferiores a los tiempos establecidos por orden legal o judicial y podrán ser superiores, siempre y cuando la decisión de definir un tiempo superior, esté debidamente fundamentada.

1.3. Definición de proceso de supresión

Presentada alguna de las causales establecidas en el numeral 4.2 del presente documento, se deberá proceder a la supresión o eliminación del documento o Dato Personal, según el Tipo de Base de Datos y su forma de almacenamiento:

Tipo de Bases de Datos	
Física	**Automatizada**
Archivo físico	Digital

	Electrónica Medios magnéticos
Formas de supresión	
Trituración del documento	Eliminación del archivo Eliminación del contenido Destrucción o Formateo del dispositivo

1.4.2. Revocatoria de autorización o reclamo de supresión

En caso de revocatoria de la autorización o reclamo de supresión, Responsable del Tratamiento deberá Suprimir la información dentro de los quince (15) días hábiles siguientes a la presentación del mismo, comunicando de forma oportuna al Encargado del Tratamiento, la obligación de suprimir los datos.

El término anterior podrá extenderse por ocho (8) días más, siempre que se informen al interesado las causas de la demora y la nueva fecha para resolver su reclamo.

El Encargado del Tratamiento deberá Suprimir la información dentro de los cinco (5) días hábiles siguientes a que el Responsable del Tratamiento le comunique la obligación de supresión.

La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos; la eliminación de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas; o los datos sean necesarios para proteger los intereses jurídicamente tutelados del Titular para realizar una acción en función del interés público o para cumplir con una obligación legalmente adquirida por el Titular, por lo que su supresión versará frente al tratamiento activo de los mismos y de acuerdo a la solicitud del titular.

1.4.3. Documentación

La supresión de los Datos Personales deberá quedar consignada en un Acta debidamente firmada por el Oficial de Protección de Datos Personales del Responsable del Tratamiento y por el o los Operativos Responsables de la Base de Datos de la cual se suprime el Dato Personal.

1.4.4. Encargado del Tratamiento

En caso de que la Supresión de Datos Personales la realice un Encargado del Tratamiento, se debe cumplir con lo dispuesto en el punto 4.4.2 del presente Protocolo.

Asimismo, deberá quedar consignada un Acta debidamente firmada por el Oficial de Protección de Datos Personales del Responsable del Tratamiento y por el Encargado del Tratamiento o por quienes éste designe para llevar a cabo dicha labor.

REGISTRO NACIONAL DE BASES DE DATOS

Mientras PREVIPASO S.A.S, se encuentre obligado a efectuar el registro de las bases de datos en el Registro Nacional de Bases de Datos, el Oficial de Protección de Datos Personales debe realizar la actualización permanente de los cambios sustanciales y no sustanciales de las bases de datos, así como el reporte de los incidentes de seguridad y reclamos de los titulares, de la siguiente manera:

<table>
<tr><td colspan="2">Registro de nuevas bases de datos</td></tr>
<tr><td colspan="2">Deben registrarse dentro de los dos (2) meses siguientes a su creación</td></tr>
<tr><td colspan="2">Cambios sustanciales</td></tr>
<tr><td>Son cambios sustanciales los que se relacionen con la finalidad de la base de datos, el Encargado del Tratamiento, los canales de atención al Titular, la clasificación o tipos de datos personales almacenados en cada base de datos, las medidas de seguridad de la información implementadas, la Política de Tratamiento de la Información y la transferencia y transmisión internacional de datos personales.</td><td>Deben actualizarse dentro de los primeros diez (10) días hábiles de cada mes, a partir de la inscripción de la base de datos.</td></tr>
<tr><td colspan="2">Cambios no sustanciales</td></tr>
</table>

Cantidad de titulares, ubicación, número de bases de datos, si se cuenta o no con la autorización en cada caso, manual o automatizada, forma de obtención de la autorización (directamente o a través de terceros, fuentes de acceso público)	Anualmente, entre el 2 de enero y el 31 de marzo, a partir de 2020.
Reclamos presentados por los Titulares	
Corresponde a la información de los reclamos presentados por los Titulares ante el Responsable y/o Encargado del tratamiento, según sea el caso. El reporte deberá ser el resultado de consolidar los reclamos presentados por los Titulares ante los Responsables del Tratamiento que se encuentran obligados a registrar sus bases de datos en el RNBD y sus respectivos Encargados del Tratamiento.	Debe ser reportado dentro de los quince (15) primeros días hábiles de los meses de febrero y agosto de cada año, a partir de su inscripción.
Incidentes de seguridad	
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 que sean tratados bien sea por el Responsable del Tratamiento o por su Encargado.	Deberán reportarse al RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

Los líderes o directores de cada área deberán apoyar al Oficial de Protección de Datos Personales en el mantenimiento y actualización del inventario de bases de datos.

AUDITORÍA DEL PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES

El Oficial de Protección de Datos Personales será el responsable dentro de la compañía de velar por la implementación efectiva de las políticas y procedimientos adoptados por ésta

para cumplir las normas, así como la implementación de buenas prácticas de gestión de datos personales dentro de la organización.

En consecuencia, deberán supervisar, evaluar y revisar el programa por lo menos una vez al año, para asegurar que siga siendo pertinente y eficaz, debiendo determinar:

- Cuáles son las últimas amenazas y riesgos respecto del tratamiento de datos personales detectados en la organización.
- Si los controles del programa están teniendo en cuenta las nuevas amenazas y reflejando las quejas más recientes o los hallazgos de las auditorias, o las orientaciones de la autoridad de protección de datos.
- Si se están ofreciendo nuevos servicios que involucran una mayor recolección, uso o divulgación de la información personal.
- Si se está llevando a cabo capacitación eficaz, se está siguiendo las políticas y procedimientos, y el programa se encuentra actualizado.
- Evaluación de los criterios establecidos en el Protocolo de Gestión de Incidentes de Seguridad.

Con base en los resultados del proceso de evaluación, se deben tomar las medidas para actualizar y revisar los controles del programa.

DIVULGACIÓN

Este documento se encuentra articulado con los demás documentos, políticas y procedimientos de PREVIPASO S.A.S

Una vez aprobado el presente Manual, debe ser socializado y aplicado conforme a su mandato.

El incumplimiento de cualquiera de las disposiciones señaladas en este manual será considerado como falta grave conforme a lo dispuesto en el numeral 6 del artículo 62 del Código Sustantivo del Trabajo. Las sanciones aplicables al personal y sus procedimientos respectivos se regirán por lo establecido en el régimen sancionatorio y disciplinario adoptado por la PREVIPASO S.A.S.