1. OBJETIVO

Definir los lineamientos generales para la implementación, aplicación, monitoreo, sostenimiento y mejora continua de las políticas y procedimientos internos para el correcto manejo y la efectiva protección de los datos personales, suministrados por los correspondientes titulares a la Fiduciaria, de conformidad con lo dispuesto en la Ley de Protección de Datos Personales y, las demás normas que, actualmente o en el futuro la reglamenten.

2. ALCANCE

Las disposiciones contenidas en este Manual se aplicarán al tratamiento de datos personales efectuado en territorio colombiano, o cuando le sean aplicables las normas al Responsable y/o Encargado que se encuentre ubicado fuera del territorio colombiano, esto, en virtud de los tratados internacionales vigentes en esa materia o las relaciones contractuales existentes, entre otros.

En todo caso, los principios se aplicarán a cualquier base de datos personales que se encuentre bajo custodia o tratamiento de Fiduprevisora S.A., bien sea en calidad de Responsable y/o como Encargada del tratamiento.

La puesta en práctica de este Manual es obligatoria para todos los funcionarios y el personal que se encuentre al servicio de la Fiduciaria, sin perjuicio de la observancia de las disposiciones legales vigentes sobre protección de datos. En caso de existir alguna contradicción entre este Manual y la normatividad vigente para el efecto, primará lo establecido en la Ley.

3. GLOSARIO

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales. El consentimiento puede otorgarse por escrito, de forma oral o mediante conductas inequívocas del Titular que permitan concluir que otorgó la autorización.

Aviso de Privacidad: Comunicación verbal o escrita cuyo fin es informar al titular de los datos sobre la existencia de un manual de políticas de tratamiento que le será aplicable al procesamiento de su información.

Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento (ej. Base de Datos de clientes, entre otras).

Causahabiente: Persona que ha sucedido a otra por causa del fallecimiento de ésta (heredero o legatario).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Datos Personales Privados: Aquellos cuyo conocimiento es restringido al público.

Datos Sensibles: Son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos, entre otros, la captura de imagen fija o en movimiento, huellas digitales, fotografías, iris, reconocimiento de voz, facial o de palma de mano, etc.

Datos Públicos: Dato que no sea semiprivado, privado o sensible, que puede ser tratado por cualquier persona, sin necesidad de autorización para ello. Son públicos, entre otros, los datos contenidos en el registro civil de las personas (p.ej. si se es soltero o casado, hombre o mujer) y aquellos contenidos en documentos públicos (p.ej. contenidos en Escrituras Públicas), en registros públicos (p.ej. el registro de antecedentes disciplinarios de la Procuraduría), en gacetas y boletines oficiales y en sentencias judiciales ejecutoriadas que no estén sometidas a reserva.

Delegado de Privacidad: Encargado de administrar bases de datos personales, para control, tratamiento, monitoreo y gestión; relacionadas con las funciones y responsabilidades de su cargo.

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.

Titular de la Información: Persona natural cuyos datos personales sean objeto de Tratamiento.

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

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.

Transferencia: Envío de datos, dentro o fuera del territorio nacional, cuyo remitente y, a su vez, destinatario, es un Responsable del Tratamiento de Datos.

Transmisión: Comunicación de Datos, dentro o fuera del territorio colombiano, cuyo remitente es el Responsable y su receptor es el Encargado del Tratamiento de Datos.

Oficial de Protección de Datos Personales: Encargado de vigilar, controlar y promover la aplicación de la Política de Protección de Datos Personales al interior de La Compañía.

4. MARCO NORMATIVO

- **Constitución Política de Colombia:**

- **Artículo 15,** De los Derechos, las Garantías y los Deberes. "*Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas*."

- **Leyes:**

- **Ley 1266 de 2008,** Por la cual se dictan las disposiciones generales de 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,** la cual se dictan disposiciones generales para la Protección de Datos Personales.

- **Ley 1712 de 2014,** Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones". Publicada en el Diario Oficial No. 49.084 del 6 de marzo de 2014.

- **Decretos:**

- **Decreto 1727 de 2009,** Por el cual se determina la forma en la cual los operadores de los Bancos de Datos de Información Financiera, Crediticia, Comercial, de Servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.

- **Decreto 2952 de 2010,** Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008.

- **Decreto 1377 de 2013,** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- **Decreto 886 de 2014,** Por el cual se reglamenta el artículo de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.

- **Decreto 1074 de 2015**, Decreto Único del Sector Comercio, Industria y Turismo, Capitulo 25 sobre protección de datos.

- **Resoluciones:**

- **Resolución 76434 de 2012,** Por la cual se deroga el contenido del Título V de la Circular Única de la Superintendencia de Industria y Comercio, sobre Acreditación y se imparten instrucciones relativas a la Protección de Datos Personales, en particular, acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, las cuales se incorporan en el citado Título.

- **Circular Externa:**

- **Circular Externa 005 de 2017** de la Superintendencia de Industria y Comercio, por la cual se fijan estándares de un nivel adecuado de protección en el país receptor de la información personal

- **Circular Externa 008 de 2017** de la Superintendencia de Industria y Comercio, por el cual se incluye un país en la lista de aquellos que cuentan con un nivel adecuado de protección de datos personales

- **Guías**

- Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability) emitido por la Superintendencia de Industria y Comercio

5. DOCUMENTOS RELACIONADOS

FuenteplanMIaGTH-03-001 Administración de Perfiles y Estructura Organizacional

FuenteplanMIaPLA-01-005 Guía Metodológica Para la Gestión de Proyectos

FuenteplanMIaGRI-02-002 Sistema de Administración de Riesgo Operativo (SARO)

FuenteplanMIaESC-05-001 Política de Seguridad de la Información y Ciberseguridad

FuenteplanMPaGCL-01-007 Gestión a PQRSD Solicitudes

FuenteplanMPaGAD-04-007 Comunicaciones Oficiales

Fuente: MPaESC-05-003 Gestión de Incidentes de Seguridad de la Información

Fuente: MPaESC-01-006 Auditorías al Sistema de Control Interno

Fuente: MPaESC-03-003 Auditoría Interna SIG

Fuente: MPaGRI-02-003 Administración de Riesgo Operativo

6. POLÍTICAS Y LINEAMIENTOS

6.1 PRINCIPIOS GENERALES

- La Fiduciaria garantiza la protección de derechos como el Habeas Data, la privacidad, la intimidad, el buen nombre, honra e imagen personal, con tal propósito, todas las actuaciones se regirán por los postulados de la buena fe, la legalidad, la autodeterminación informática, la libertad y la transparencia.
- Quien en ejercicio de su actividad suministre cualquier tipo de información o dato personal a la Fiduciaria en su condición de encargado o responsable del tratamiento, podrá ejercer sus derechos como titular de la información para conocerla, actualizarla y rectificarla conforme a los procedimientos establecidos en la ley aplicable y la presente política.
- La Fiduciaria reconoce que su legítimo derecho al tratamiento de los datos personales de los titulares de información debe ser ejercido dentro del marco específico de la legalidad y del consentimiento del titular, procurando en todo momento preservar el equilibrio entre los derechos y deberes de titulares, responsables y encargados del tratamiento vinculados a su operación.

6.2 PRINCIPIOS ESPECIFICOS

Para el debido tratamiento de datos personales, Fiduprevisora S.A. aplicará los principios específicos que se establecen a continuación, los cuales constituyen las reglas a seguir en la recolección, almacenamiento, uso, intercambio, archivo, eliminación y/o destrucción de datos personales:

Principio de Legalidad en materia de Tratamiento de Datos: El Tratamiento 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 y a lo indicado en el presente documento.

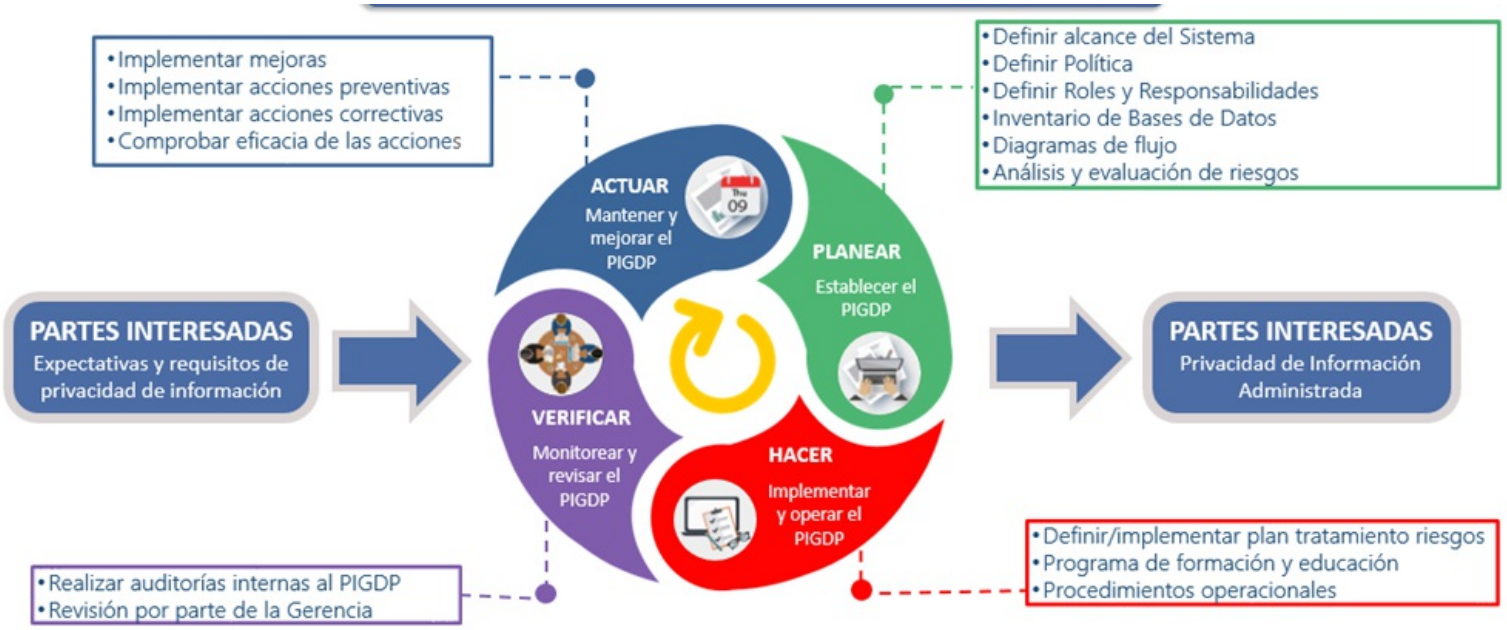
Principio de Seguridad: La información sujeta a Tratamiento por el Responsable o Encargado del Tratamiento a que se refiere la ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, 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.

7. PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

La implementación de un Programa Integral de Gestión de Datos Personales, que incluya un adecuado manejo de los datos personales que son objeto de tratamiento por parte de Fiduprevisora S.A. en desarrollo de sus actividades, así como elevar los estándares de protección de estos, constituyen una obligación legal en cumplimiento de la responsabilidad demostrada y un compromiso para satisfacer las necesidades de los titulares de la información y, en general, de los demás grupos de interés.

En ese sentido, el referido programa contempla el desarrollo de las siguientes actividades:



7.1 PLANEACIÓN

En esta etapa se traza la estrategia con el objetivo de organizar el trabajo adelantado por Fiduprevisora S.A., para acercarla a un nivel de cumplimiento adecuado que permita salvaguardar la información privada y, de manera concomitante, responder a los retos de disponibilidad a la información pública por parte de la ciudadanía, así como para ajustar los roles del personal designado para cumplir con las responsabilidades de seguridad y privacidad de la información.

7.1.1 Política de protección de datos personales y aviso de privacidad

Con el objeto de dar cumplimiento al Capítulo VI Responsabilidad demostrada frente al tratamiento de datos personales del Decreto 1377 de 2013, Fiduprevisora S.A. cuenta con un Programa Integral de Datos Personales. Así mismo, promueve a nivel institucional la generación de una cultura organizacional de respeto frente a la protección de los datos personales, ajustada y concordante con otros sistemas de gestión de riesgo y de calidad.

La Fiduciaria ha puesto a disposición de los Titulares la Política de tratamiento y el aviso de privacidad, los cuales se encuentran publicados en la página web de la entidad.

7.1.2 Deberes de Fiduprevisora S.A.

7.1.2.1 Cuando obra como Responsable del tratamiento

Fiduprevisora S.A. como Responsable del Tratamiento deberá cumplir los siguientes deberes:

Deberes respecto del Titular del dato

- Solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el Titular.
- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data, es decir, conocer, actualizar o rectificar sus datos personales.
- Informar a solicitud del Titular sobre el uso dado a sus datos.
- Tramitar las consultas y reclamos formulados en los términos señalados en la ley.

Deberes respecto de la calidad, seguridad y confidencialidad de los datos personales

- Observar los principios de veracidad, calidad, seguridad y confidencialidad en los términos establecidos en este manual.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Actualizar la información cuando sea necesario.
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

Deberes cuando realiza el tratamiento a través de un Encargado

- Suministrar al Encargado las instrucciones y el alcance del tratamiento del dato.
- Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la ley. Cuando se trate de transmisiones nacionales e internacionales se deberá suscribir un contrato de transmisión de datos personales o pactar cláusulas contractuales que contengan lo dispuesto en el artículo 25 del decreto 1377 de 2013 o las normas que lo modifiquen o reglamenten;
- Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Comunicar de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.
- Informar de manera oportuna al Encargado del tratamiento las rectificaciones realizadas sobre los datos personales para que éste proceda a realizar los ajustes pertinentes.
- Exigir al Encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- Exigir al Encargado el cumplimiento de lo establecido a través del manual interno de políticas y procedimientos, para garantizar el adecuado cumplimiento de la ley y, en especial, para la adecuada atención de PQRSD.

Deberes respecto de la Superintendencia de Industria y Comercio

- Informarles las eventuales violaciones a los códigos de seguridad y cuando existan riesgos en la administración de la información de los Titulares;
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

7.1.2.2 De Fiduprevisora S.A. como Encargado del Tratamiento

Fiduprevisora S.A. como Encargado del tratamiento deberá cumplir los siguientes deberes:

- Garantizar al Titular, en todo tiempo el pleno y efectivo ejercicio del derecho de hábeas data.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la ley.
- Actualizar la información reportada por los Responsables del tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
- Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la ley.
- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares.
- Cuando corresponda, registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la Ley.
- Cuando corresponda, insertar en la base de datos la leyenda "información en discusión judicial" una vez notificada por parte de la autoridad competente, sobre la existencia de procesos judiciales relacionados con la calidad del dato personal.
- Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
- Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Nota: En el evento en que concurran las calidades de Responsable del tratamiento y Encargado del tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno de los roles referidos.

7.1.3 Roles, responsabilidades y autoridad

Las políticas de Administración y Gestión del Talento Humano se encuentran orientadas al cumplimiento de los objetivos organizacionales e individuales, contemplan directrices frente a la estructura organizacional de la Entidad, dependencias, cargos, perfiles de cargos y requisitos exigidos para el desempeño de los mismos, establecidos en el ML-GTH-03-001 Administración de Perfiles y Estructura Organizacional.

Complementariamente Fiduprevisora S.A., ha establecido responsabilidades frente al Programa Integral de gestión de Protección de Datos Personales, los cuales están incorporados en los respectivos manuales de funciones de cada cargo, a continuación, se detallan los cargos o áreas que tienen el rol de "Delegado de Privacidad", al tener injerencia en la administración de las diferentes bases de datos personales que se administran en la Entidad.

Base de datos	Delegado de Privacidad
Base de Datos Junta Directiva y Accionistas	La Vicepresidencia Jurídica es la encargada de la administración y tratamiento de la base de datos lógica
Base de Datos de Clientes	Servicio al cliente es la encargada de la administración y tratamiento de la base de datos tanto física como lógica. Unidad de Vinculados y Unidad de SARLAFT, encargados de registrar la información de clientes en el

	sistema core de la Entidad y la documentación que respalda dichos registros. La oficina de impuestos recibe y consolida información de terceros.
Base de Datos relacionado con Trabajadores	La Gerencia Talento Humano es la encargada de la administración y tratamiento de las siguientes bases de datos personales tanto físicas como lógicas de: - Funcionarios - Beneficiarios - Postulantes
Base de Datos de Proveedores	La Gerencia de Adquisiciones y Contratación es la encargada de la administración y tratamiento de la base de datos tanto física como lógica
Base de Datos Videograbación	La Dirección de Recursos Físicos es la encargada de la administración y tratamiento de la base de datos lógica
Base de Datos Visitantes	La Dirección de Recursos Físicos es la encargada de la administración y tratamiento de la base de datos lógica
Base de Datos Monitoreo	La Vicepresidencia de Tecnología de la Información es la encargada de la administración y tratamiento de la base de datos lógica

Además, se han definido las autoridades y grupos de interés especial con las que se debe mantener contacto y los casos en que esto debe ocurrir. La privacidad de la información es parte integral de los proyectos de Fiduprevisora S.A., los requerimientos de este aspecto que se han definido en ML-PLA-01-005 Guía Metodológica Para la Gestión de Proyectos.

7.1.4 Inventario Bases de Datos

Son las bases de datos en medio físico o sistematizado que contengan información de carácter personal. El tratamiento de estos datos requerirá autorización previa e informada de las finalidades de su tratamiento por parte del titular, bajo los formatos que para tal efecto defina la Fiduciaria.

La Fiduciaria ha identificado, clasificado y definido las bases datos personales de la Entidad y son registradas y actualizadas cada año en la página de la Superintendencia de Industria y Comercio.

7.1.5 Diagramas del flujo de la información

La descripción de los flujos de información por base de datos sirve para determinar qué información está siendo recolectada, con qué propósito, cómo, en qué cantidad y si la misma es objeto de transmisión y/o transferencia (nacional y/o internacional). De igual forma, determina el tiempo de conservación de la información.

Los diagramas sirven como insumo al identificar qué información se tiene, dónde y en cabeza de quién. Este ejercicio tiene que ser complementado con la documentación de los procesos relacionados con la gestión de la información que la entidad haya levantado, para poder hacer una valoración sobre la circulación de la información, identificando que en la misma no se afecten derechos de los titulares de información o se ponga en riesgo su privacidad.

Los diagramas de flujo o el ciclo de vida de los datos se pueden dividir en las siguientes etapas:

- **Captura de datos**: Proceso de obtención de datos para su almacenamiento y posterior procesamiento. Dentro de esta categoría se pueden encontrar diversas técnicas: formularios web, formularios en papel, toma de muestras y realización de encuestas, grabaciones de audio y video,

redes sociales, captación mediante sensores, etc.

- **Clasificación / Almacenamiento**: Establecer categorías y asignarlas a los datos para su clasificación y almacenamiento en los sistemas o archivos.

- **Uso / Tratamiento**: Operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos de los datos automatizados o manuales.

- **Cesión o transferencia de los datos a un tercero para su tratamiento**: Traspaso o comunicación de datos realizada a un tercero, definido como aquella persona física o jurídica, pública o privada u órgano administrativo. Este concepto es muy amplio, puesto que recoge tanto la entrega, comunicación, consulta, interconexión, transferencia, difusión o cualquier otra forma de acceso a los datos.

- **Destrucción**: Eliminar los datos que puedan estar contenidos en los sistemas o archivos, de manera que no puedan ser recuperados de los soportes de almacenamiento (disposición final de la información).

7.1.6 Análisis de riesgos

Para la definición de la metodología para gestionar los riesgos de la información, se definió dar adherencia a la metodología definida en el manual ML-GRI-02-002 - Sistema de Administración de Riesgo Operativo (SARO).

En desarrollo de este numeral, se da alcance a los siguientes aspectos:

- Se realiza un análisis de riesgos con el fin de establecer medidas de seguridad y control para garantizar los derechos y libertades de los titulares.
- Se realiza una gestión continua de los riesgos potenciales asociados al tratamiento desde su diseño.
- La gestión de riesgos se realiza en tres etapas básicas La identificación, la evaluación y el tratamiento de los riesgos.
- Se establecen procedimientos de control que garanticen cumplir los principios de protección desde el diseño y, por defecto:
- Se definen y establecen medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado al riesgo, de acuerdo con las particularidades de las actividades de tratamiento

8. IMPLEMENTACIÓN

En esta fase se deben ejecutar las acciones trazadas en la etapa previa de planeación de manera que Fiduprevisora S.A. diseñe un modelo de privacidad que le permita cumplir con los mínimos legales, generar una política privacidad que le permita la correcta gestión de la información, definir los procedimientos de privacidad y realizar el registro de las bases de datos en el Registro Nacional de Bases de Datos (RNBD).

8.1 Programas continuos de formación y educación

En concordancia con el Plan Institucional de capacitación (PIC), la Gerencia de Riesgos de modo conjunto con la Gerencia de Gestión Humana define la programación de capacitación de Datos Personales y coordina los planes específicos dirigidos a todos los funcionarios. Las capacitaciones podrán desarrollarse de manera presencial o virtual según se requiera.

8.1.1 Toma de Conciencia

Ver numeral 7.3.3 Toma de conciencia del ML-ESC-05-001 Política de Seguridad de la Información y Ciberseguridad.

8.1.2 Procedimientos operacionales

8.1.2.1 Autorización expresa

Fiduprevisora S.A. obtiene la autorización por medio de un documento físico, electrónico, mensaje de datos, Internet, sitio web, o también de manera verbal o telefónica o en cualquier otro formato que permita su posterior consulta, o mediante un mecanismo técnico o tecnológico idóneo, mediante el cual se pueda concluir de manera inequívoca, que, de no haberse surtido una conducta del titular, los datos nunca hubieren sido capturados y almacenados en la base de datos. La autorización es generada por Fiduprevisora S.A. y puesta a disposición del titular de manera expresa, previa e informada al tratamiento de sus datos personales.

Fiduprevisora S.A. informa al titular de los datos en la política de protección de datos personales y el aviso de privacidad:

- El tratamiento al que serán sometidos sus datos personales y la finalidad específica del mismo.
- Los derechos que le asisten como titular.
- La página web, correo electrónico, dirección física y demás canales de comunicación a través de los cuales podrá formular consultas y/o reclamos ante el Responsable o Encargado del tratamiento.

Fiduprevisora S.A. utiliza los mecanismos con que cuenta actualmente, e implementa y adopta las acciones tendientes y necesarias para mantener registros o mecanismos técnicos o tecnológicos idóneos de cuándo y cómo obtuvo autorización por parte de los titulares de datos personales para el tratamiento de los mismos. Para dar cumplimiento a lo anterior, se podrán establecer archivos físicos o repositorios electrónicos realizados de manera directa o a través de terceros contratados para tal fin.

8.1.2.2 Almacenamiento, uso y circulación de información personal

La recolección, almacenamiento, uso y circulación de información de datos personales se hará de acuerdo con los procedimientos descritos en el presente manual garantizando el cumplimiento de las políticas definidas en el manual ML-ESC-05-001 - Manual de Políticas de Seguridad de la Información.

8.1.2.3 Procedimiento para que los titulares del Dato puedan ejercer sus Derechos

El procedimiento para que los Titulares de los datos puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información o revocar la autorización está documentado en MP-GCL-01-007 Gestión a PQRSD Solicitudes y MP-GAD-04-007 Comunicaciones Oficiales.

Los derechos de los titulares podrán ejercerse por las siguientes personas legitimadas de conformidad con el artículo 20 del decreto 1377 de 2013:

- Por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición Fiduprevisora S.A.;
- Por sus causahabientes, quienes deberán acreditar tal calidad;
- Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento;
- Por estipulación a favor de otro o para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Todas las consultas y reclamos se deben canalizar a través de los medios habilitados por Fiduprevisora S.A., quien adoptará mecanismos de prueba de la radicación y trámite de los mismos.

8.1.2.4 Pautas para atender consultas y reclamos

- **Consultas:** Todas las consultas que realicen las personas legitimadas para conocer los datos personales que reposen en Fiduprevisora S.A. se canalizarán a través de los medios que tiene para el efecto. En todo caso es necesario dejar prueba de lo siguiente:

  - Fecha de recibo de la consulta;
  - Identidad del solicitante.

- **Reclamos:** Los reclamos tienen por objeto corregir, actualizar, o suprimir datos o elevar una queja por el presunto incumplimiento de cualquiera de los deberes contenidos en la ley 1581 de 2012 y en esta política.

8.1.2.5 Comunicación con los titulares

La base de la comunicación externa de Fiduprevisora S.A. es el respeto hacia el otro, y debe ser clara y entendible para las partes, de tal forma que no haya lugar a equívocos. Se respetarán siempre los canales, así como los conductos regulares para establecer comunicación con los titulares.

Los canales dispuestos para la comunicación con los titulares se encuentran disponibles en la página web de Fiduprevisora S.A. y son los siguientes:

- Página web: formulario definido para atención a PQR y son radicadas a través de Orfeo
- Presencial: Calle 72 #10-03 Bogotá D.C. de lunes a viernes en horario de 8:30 a.m. a 5:30 p.m.
- Teléfono: Bogotá: (57+1) 7562444 y Resto del país: (57) 018000180510

8.1.2.6 Gestión de Encargados

En los eventos en los que Fiduprevisora S.A. entregue una base de datos a un tercero para que éste realice por cuenta de la Fiduciaria como Responsable el tratamiento de la misma, el tercero se obliga a cumplir con lo establecido en la Ley 1581 de 2012 y demás normas reglamentarias, y especialmente en lo que respecta a los deberes y responsabilidades de los Encargados (artículo 17 de la ley 1581 de 2012) y en el marco de las políticas y directrices contenidas en el presente documento.

Cuando se vaya a realizar un tratamiento por cuenta de un Responsable del tratamiento, este elegirá únicamente un Encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la SIC y garantice la protección de los derechos del interesado.

El Encargado del tratamiento no recurrirá a otro Encargado sin la autorización previa por escrito, específica o general, de Fiduprevisora S.A. como

Responsable. En este último caso, el Encargado informará al Responsable de cualquier cambio previsto en la incorporación o sustitución de otros Encargados, dando así al Responsable la oportunidad de oponerse a dichos cambios

El tratamiento por el Encargado se regirá por un contrato u otro acto jurídico, que vincule al Encargado respecto del Responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del Responsable.

El Encargado de tratamiento pondrá a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del Responsable o de otro auditor autorizado por dicho Responsable.

8.1.2.7 Transferencias internacionales

Está prohibida la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos. Se entienden países seguros aquellos que cumplan con los estándares fijados por la Superintendencia de Industria y Comercio.

De manera excepcional se podrán realizar transferencias internacionales de datos por Fiduprevisora S.A. cuando:

- El titular del dato haya otorgado su autorización previa, expresa e inequívoca para realizar la transferencia.
- La transferencia sea necesaria para la ejecución de un contrato entre el titular y Fiduprevisora S.A. como Responsable y/o Encargado del tratamiento.
- Se trate de transferencias bancarias y bursátiles acorde con la legislación aplicable a dichas transacciones.
- Se trate de transferencia de datos en el marco de tratados internacionales que hagan parte del ordenamiento jurídico colombiano.
- Transferencias legalmente exigidas para salvaguardar un interés público.

Al momento de presentarse una transferencia internacional de datos personales, previo envío o recepción de los mismos, Fiduprevisora S.A. suscribirá los acuerdos que regulen en detalle las obligaciones, cargas y deberes que surgen para las partes intervinientes.

Los acuerdos o contratos que se celebren deberán atender lo dispuesto en esta norma, así como en la legislación y jurisprudencia que fuera aplicable en materia de protección de datos personales.

Corresponderá al Oficial de Protección de Datos Personales revisar el contenido de los contratos que conlleven una transferencia internacional de datos personales, atendiendo como directrices los principios aplicables y recogidos en este manual, con el respectivo apoyo del área jurídica de la Fiduciaria. Así mismo le corresponderá asegurar la calidad de un "país seguro" definido por Superintendencia de Industria y Comercio en relación con el territorio de destino y/o procedencia de los datos. En caso contrario, deberá tramitar ante la SIC la Declaración de Conformidad para la transferencia internacional.

8.1.2.8 Protocolos de respuesta en el manejo de violaciones e incidentes

La gestión de incidentes para el tratamiento de datos personales es un proceso para garantizar la protección de la información a través de la solución de posibles vulnerabilidades, motivo por el cual Fiduprevisora S.A. lo desarrolla de acuerdo o como se encuentra descrito en MP-ESC-05-003 - Gestión de Incidentes de Seguridad de la Información.

Fiduprevisora S.A. a través del Oficial de Protección de Datos, deberá informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares, cuyos informes serán soporte de verificación en las visitas que realice la Superintendencia de Industria y Comercio.

8.1.2.9 Registro Nacional de Bases de Datos

Fiduprevisora S.A. debe realizar el registro de sus bases de datos, por tener activos totales superiores a 610.000 Unidades de Valor Tributario (UVT).

Fiduprevisora S.A. debe actualizar la información registrada, como se indica a continuación:

- Dentro de los primeros diez (10) días hábiles de cada mes, a partir de la inscripción de la base de datos, cuando se realicen cambios sustanciales en la información registrada.
- Anualmente, entre el 2 de enero y el 31 de marzo.

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.

8.1.2.10 Registro de Novedades

Se debe realizar el mantenimiento al programa integral implementado el año anterior, por lo cual debemos presentar los informes de acuerdo con la siguiente periodicidad definida:

- Reclamos presentados por los titulares

  - Periodicidad: semestral

  - Dentro de los quince (15) primeros días hábiles de los meses de febrero y agosto de cada año

- Gestionar y reportar los incidentes

  - Periodicidad: 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 entenderlos.

- Registrar nuevas bases de datos

  - Las bases de datos que se creen después del registro deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación.

- Eliminación bases de datos

  Se deben dar de baja las bases de datos que ya no se utilicen en la entidad y se documentará el motivo del mismo:

  - Cesión de información

  - Cumplimiento de las Tablas de retención documental

  - Depuración de información

  - Desuso / inhabilitación de datos

  - Fusión de datos

  - Liquidación de persona jurídica

  - Orden judicial o administrativa

  - Por no contar con autorización del titular para el tratamiento de datos personales

  - Por término legal

  - Terminación de la finalidad para la que fue creada

9. EVALUACIÓN DE DESEMPEÑO

En esta fase se define el monitoreo, medición y revisión continua del desempeño (eficiencia y eficacia) del Programa Integral. Se desarrollará un plan de supervisión y revisión anual que tome en cuenta las siguientes etapas:

9.1 Auditorías internas

Fiduprevisora S.A. ha definido el proceso de Auditoría con el fin de establecer disposiciones específicas para la planificación, preparación y ejecución de las Auditorías Internas para verificar la conformidad del Programa Integral.

Este proceso se encuentra documentado a través del procedimiento MP-ESC-01-006 Auditorías al Sistema de Control Interno y MP-ESC-03-003 Auditoría Interna SIG.

9.2 Revisión por parte de la Alta Dirección

La revisión por la dirección del Programa Integrado se realiza atendiendo lo establecido para sistemas de gestión de la Fiduciaria, para garantizar la adecuación, conveniencia y eficacia del Programa.

Adicionalmente, semestralmente el Oficial de Protección de Datos Personales presentará ante el Representante Legal y a la Junta Directiva el informe de gestión de las actividades realizadas en desarrollo del Programa Integral de Gestión de Datos Personales.

10. MEJORA CONTINUA

Lo relacionado con mejora continua está documentado mediante salidas no conformes y acciones correctivas.

Las salidas no conformes en Fiduprevisora S.A., son consideradas eventos de riesgo operativo (ERO), por tanto, deberán ser gestionadas de acuerdo con lo establecido en el procedimiento MP-GRI-02-003 - Administración de Riesgo Operativo.

11. DEMOSTRACIÓN

La acreditación de cumplimiento se puede hacer mediante la documentación que se haya generado para determinar las medidas destinadas a cumplir con las obligaciones de la Ley, así como las evidencias del correcto funcionamiento de las mismas, lo que en el argot de los Sistemas de Gestión son medidas y controles.

Esta forma de demostrar o acreditar el cumplimiento con base a la documentación interna y las evidencias no resultarán muy complicada, dado que tenemos la obligación de guardar las pruebas que demuestren, por ejemplo, que hemos informado correctamente o que aplicamos unas determinadas medidas de índole técnicas u organizativas para cumplir con el principio de seguridad. Esto se traduce en que tendremos documentación como: Procedimientos o protocolos internos, cláusulas de información, contratos de encargado del tratamiento, registro de actividades del tratamiento, análisis de riesgo, etc.

12. DISPOSICIONES FINALES

El presente manual deberá ser objeto de revisión por parte del oficial por lo menos durante una vez al año o inmediatamente ante la ocurrencia de un incidente que afecte o comprometa la seguridad de la información o el adecuado nivel de cumplimiento del programa integral de gestión de protección de datos personales.

0. LISTA DE VERSIONES

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
2	09/Feb/2022	- Se incorporaron ajustes relacionados con la inclusión del programa integral de gestión de datos personales. - Actualización Gobierno de Datos Personales.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Martin Ramirez Angelica María **Cargo:** Porfesional de Seguridad de la Informacion y Ciberseguridad **Fecha:** 09/Feb/2022	**Nombre:** Quiroga Munoz Fredy Ivan **Cargo:** Tecnico de Organizacion y Metodos **Fecha:** 10/Feb/2022	**Nombre:** Perez Mesa Sergio Andres **Cargo:** Directivo 6 **Fecha:** 11/Feb/2022 **Nombre:** Quiroga Munoz Fredy Ivan **Cargo:** Tecnico de Organizacion y Metodos **Fecha:** 15/Feb/2022 **Nombre:** Suarez Calderon Juan Pablo **Cargo:** VICEPRESIDENTE JURIDICO **Fecha:** 14/Feb/2022