TABLA DE CONTENIDO:

1. OBJETO

Como medida de cumplimiento a la Política de Protección de Datos Personales de la organización aprobada por la Alta Dirección, PROTECCIÓN S.A. ha implementado el presente documento denominado Manual Interno de Procedimientos del Programa de Protección de datos Personales, el cual, tiene como propósito establecer al interior de la organización procedimientos fundamentados en la gestión del riesgo de privacidad y la asignación de responsabilidades, que permitan garantizar la protección efectiva de la información confiada por aquellos individuos pertenecientes a nuestros grupos de interés, por lo tanto, se describen las medidas adoptadas por la compañía para el cumplimiento de la normativa aplicable, además de ser un manual interno de procedimientos para la gestión de los datos.

2. TÉRMINOS Y DEFINICIONES

A continuación, se presentan algunas definiciones de los principales conceptos utilizados en el presente documento:

Alta dirección: la estructura organizacional de PROTECCIÓN S.A. está diseñada para garantizar el cabal desarrollo de su objeto social y la independencia entre sus principales áreas, con el objetivo de generar entre ellas un adecuado ambiente de control y coordinación. Para tales efectos cuenta con los siguientes órganos:

- Órgano de Dirección: es encabezada por la Asamblea General de Accionistas.
- Órganos de Administración y representantes legales: la gestión administrativa de la organización se encuentra en cabeza de la Junta Directiva a través de sus comités de apoyo; y la Alta Gerencia, integrada por el representante legal, los Comités de dirección, las vicepresidencias y, en general, la estructura interna que soporta la gestión operativa de PROTECCIÓN S.A.

Sin embargo, para los efectos del presente documento la Alta Dirección hará referencia a los órganos de administración y los representantes legales de la organización.

Colaboradores: son todas aquellas personas naturales que le prestan un servicio a la organización en virtud de un contrato de trabajo.

Bases de datos: depósito ordenado (físico o digital) en donde se realiza el tratamiento de datos personales.

Dato personal: aspecto exclusivo y propio de una persona natural que permite identificarla en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos.

Organización: la organización es el conjunto de recursos humanos y económicos que interactúan conjuntamente para lograr unos objetivos comunes. Para los efectos del presente documento la organización se refiere a los recursos gestionados por PROTECCIÓN S.A.

Partes de interés: son las personas naturales y/o jurídicas, o los grupos de personas que pueden afectar, verse afectadas, o percibirse como afectadas por una decisión tomada o una actividad ejecutada en el marco del sistema de gestión del compliance de PROTECCIÓN S.A.

Titular: es la persona natural cuyos datos personales están siendo objeto de tratamiento.

Tratamiento: cualquier operación o conjunto de operaciones manuales o automáticas que apliquen sobre los datos de carácter personal.

Transmisión: tratamiento de datos personales por un tercero encargado en representación o por cuenta del responsable.

Transferencia: envío de datos a un tercero que también actúa como responsable del tratamiento de datos personales por cuenta propia. Esta puede ser nacional o internacional.

3. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES:

El presente Manual de Procedimientos Internos reglamenta la Política de Tratamiento de Datos Personales de PROTECCIÓN S.A. para su aplicación práctica en la organización. La Política de Tratamiento de Datos Personales y el presente manual de procedimientos están definidos y estructurados por el equipo de Cumplimiento Legal y son aprobados por la Alta Dirección, encargada del establecimiento de políticas y directrices institucionales.

La Política de Protección de Datos Personales se encuentra publicada en la página web de la organización, y puede ser consultada en el siguiente link: https://www.proteccion.com/contenidos/persona/cesantias/ley-proteccion-datos-personales

4. COMPROMISO DE LA ORGANIZACIÓN

En PROTECCIÓN S.A somos conscientes de que no basta con adoptar políticas y procedimientos que busquen el cumplimiento de las normas de protección de datos personales; sino que debemos velar por una efectiva implementación de estos.

Conocedores del gran compromiso que tenemos como responsables en el tratamiento de los datos personales que nos han confiado aquellos individuos pertenecientes a nuestros grupos de interés, hemos decidido adoptar el presente Programa de Protección de Datos Personales. Por ello, destinaremos todos los recursos económicos y el talento humano necesario para la implementación de este programa, con el único propósito de robustecer la cultura de respeto a la protección de datos personales que recogemos y tratamos.

Para tales efectos, hemos decidido disponer la siguiente estructura en materia de protección de datos personales:

- Junta Directiva

- Presidente
- Representantes Legales
- Gerente de Auditoría
- Vicepresidencias
- Oficial de Protección de Datos Personales
- Todos los colaboradores

Alta Dirección: En consonancia con el compromiso anterior, desde la alta dirección de PROTECCIÓN S.A. se apoya a cabalidad el fomento de una cultura organizacional de respeto a la protección de datos personales, por tal motivo, la Alta Dirección en cabeza del representante legal:

- Designa como Oficial de Protección de Datos personales en la organización a la persona que ocupe el cargo de Líder de Cumplimiento Legal, a quien se le destinarán los recursos necesarios y suficientes para el diseño y la implementación del presente Programa de Protección de Datos Personales que responda a la estructura y tamaño de nuestra organización, así como al tipo de datos personales que tratamos.

- Aprueba el presente Programa de Protección de Datos Personales y personalmente monitoreará su cumplimiento.

- Aprueba el Plan de Comunicación y Sensibilización anual estructurado y presentado por el Oficial de Protección de Datos Personales.

- La Alta Dirección informa anualmente a la Junta Directiva sobre la ejecución y desarrollo del presente programa.

Oficial de Protección de Datos Personales: En virtud de la designación de la Alta Dirección, el rol del Oficial de Protección de Datos será asumido por el Líder de Cumplimiento Legal de la organización, quien será el encargado de velar por la implementación efectiva de las políticas y procedimientos adoptados por PROTECCIÓN S.A., así como de aplicación de buenas prácticas en materia tratamiento de datos personales.

En este sentido, el Oficial deberá estructurar, diseñar y administrar este programa, permitiendo a PROTECCIÓN S.A. dar cumplimiento a las normas sobre protección de datos personales. De igual manera tendrá a su cargo las siguientes funciones:

- Promover la estructuración e implementación de un sistema que permita gestionar los riesgos del tratamiento de datos personales y privacidad.

- Coordinar la definición e implementación de los controles del Programa de Protección de Datos Personales.

- Deberá establecer responsabilidades específicas en cabeza de otras áreas de la compañía para el tratamiento de la información.

- Servir de enlace y coordinar con las demás áreas de la organización para asegurar una implementación transversal del Programa de Protección de Datos Personales.

- Impulsar una cultura de protección de datos dentro de la organización.

- Mantener un inventario de las bases de datos personales en poder de PROTECCIÓN S.A. y clasificarlas según su tipo.

- Registrar y actualizar las bases de datos en el Registro Nacional de Bases de Datos, atendiendo a las instrucciones que para el particular emita la SIC.

- Obtener las autorizaciones o declaraciones de conformidad de la SIC cuando sean requeridas.

- Revisar los contenidos de los contratos de transferencia o transmisión de datos que se suscriban, remitidos por la Gerencia de Regulación.

- Integrar en las políticas de protección de datos a los terceros o proveedores.

- Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realicen las entidades de control.

- Analizar las responsabilidades de los cargos de la Compañía, con el propósito de diseñar un programa de entrenamiento en protección de datos personales focalizado a cada uno de ellos. De manera general la organización se ha subdividido en tres macro grupos de cara a la diferenciación del entrenamiento en materia de tratamiento de datos, a saber: la Estructura Comercial, el área Administrativa y las Oficinas de Servicio.

- Realizar un entrenamiento general en protección de datos personales para todos los empleados de la organización.

- Estructurar y presentar al Comité de Ética anualmente el Plan de Comunicación y Sensibilización anual, así mismo, realizar el entrenamiento a los nuevos empleados, independientemente de la función que vayan a desempeñar en el día a día.

- Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la Organización.

- Medir la participación y evaluar el desempeño en los entrenamientos de protección de datos.

- Requerir que dentro de los análisis de desempeño de los empleados se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales.

- Velar por la implementación de planes de auditoría interna que tengan como objetivo la verificación del cumplimiento de las políticas de tratamiento de datos personales.

- Acompañar y revisar desde su diseño, de conformidad con el régimen de protección de datos personales, la creación y estructuración de nuevos servicios, productos o soluciones en la organización.

- Realizar seguimiento al Programa de Protección de Datos Personales.

Presentación de Informes: Las siguientes áreas de la organización deberán presentar informes al Oficial de Protección de Datos, quien se encargará de transmitir los resultados generales del Programa de Protección de Datos Personales a la Alta Dirección a través de los informes periódicos de cumplimiento establecidos en el programa de compliance de PROTECCIÓN S.A.

- El equipo de Gestión de Riesgos de Negocio e Información en conjunto con el equipo de Gestión de Ciberseguridad, deben dar cuenta inmediata de los incidentes o vulneraciones donde se hayan visto comprometidos datos personales de los grupos de interés de la organización. Además, deberán dar un concepto sobre cómo están operando los controles, y las actualizaciones que puedan llegar a implementarse sobre estos; de acuerdo con lo

establecido en la política "PO – POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD" de la organización.

- El equipo de Atención de Solicitudes y PQR, durante los meses de enero y julio de cada año, deberán remitir un informe de las solicitudes, peticiones, quejas o reclamos que se hubieran recibido en materia de tratamiento de datos personales, especificando a su vez el porcentaje de casos recibidos por causa de contacto comercial no autorizado. En dicho informe, detallarán el área o subproceso que ocasionó el requerimiento y la solución dada al solicitante en los términos de la Ley 1581 de 2012, así como los tiempos de atención para cada una de las solicitudes.

- El equipo de Regulación deberá informar durante el periodo de actualización de las bases de datos en el Registro Nacional de Bases de Datos, la cantidad de contratos de transmisión de información suscritos con encargados del tratamiento de datos personales durante el semestre inmediatamente anterior, indicando el nombre del encargado, el tiempo de vigencia de la relación y si existieron incidentes con dichos terceros relacionados con el tratamiento de datos personales.

Igualmente, dentro del ciclo de auditoría de PROTECCIÓN S.A se incluirá la revisión de las actividades relacionadas con el cumplimiento del Programa de Protección de Datos Personales. En este sentido, los hallazgos preliminares que se identifiquen durante el desarrollo de esta auditoría serán reportados al Oficial de Protección de Datos con el objeto de que se adopten los correctivos necesarios para solventar los riesgos asociados a dicho hallazgo.

5. PROCESOS INTERNOS DE GESTIÓN DE DATOS PERSONALES

PROTECCIÓN S.A en cumplimiento de disposiciones normativas emanadas del Sistema de la Seguridad Social colombiano y en atención a las instrucciones impartidas por la Superintendencia Financiera de Colombia a través de su Circular Básica Jurídica; se encuentra obligada a realizar tratamiento sobre los siguientes datos personales de los individuos pertenecientes a sus grupos de interés:

- **Datos de identificación:** Son aquellos datos que permiten determinar directa o indirectamente la identidad de una persona.

- **Datos de contacto:** Son aquellos datos que permiten establecer comunicaciones de manera directa con una persona.

- **Datos clínicos:** Son aquellos datos que permiten analizar el recorrido médico de una persona.

- **Datos biométricos:** Son aquellos datos relativos a las características físicas, fisiológicas y/o asociadas al comportamiento e ideología de las personas.

- **Datos financieros:** Son aquellos datos que permiten analizar la situación financiera y/o jurídica de una persona natural.

Todas las operaciones sobre estos datos personales se ejecutan a través de diferentes ciclos internos de información que se encuentran a cargo de cada uno de los procesos de la organización; lo cual permite garantizar que la gobernanza sobre estos sea realizada de forma eficaz, eficiente y oportuna.

Equipos que intervienen en la gestión y custodia del tratamiento de los datos personales:

Dirección de Riesgos de Negocio e Información: Todas las Bases de datos que sean utilizadas por la organización deben ser reportadas a la Dirección de Riesgos de Negocio e Información, como parte del inventario y clasificación de activos de información, con el fin de garantizar que estas cumplan con todas las condiciones mínimas de seguridad.

Adicionalmente, este inventario será el insumo para garantizar que todos los datos existentes cumplan con la reglamentación de protección de datos, labor que se encuentra a cargo del equipo de Cumplimiento Legal.

Equipo de Ciberseguridad: Este equipo está encargado de la infraestructura tecnológica para la defensa de la Compañía frente a posibles intrusiones y brechas de ciberseguridad.

Equipo de Gestión de la Información: La administración y custodia de las bases de datos de clientes (Apolo) se encuentra a cargo del equipo de Gestión de la Información, quienes cuentan con la ayuda de los terceros que se han subcontratado para tal fin.

En el marco de dichas funciones, se encuentran encargados de mantener la información de clientes actualizada y corregida, con la ayuda de herramientas tecnológicas que les permiten llevar a cabo depuración de datos personales, entre otras acciones.

Adicionalmente, se encargan de atender las solicitudes de eliminación de información contenida en la base de datos de APOLO, y llevar un monitoreo mensual de dicho procedimiento, con el fin de detectar y subsanar inconsistencias.

Por su parte, en conjunto con el área de Ciberseguridad son responsables de reportar al equipo de Cumplimiento Legal cada uno de los incidentes que se presentan en el marco del tratamiento de la información de clientes de la administradora.

Esta área también es la responsable de mantener actualizado el registro que permite saber a los diferentes procesos de la Organización, el alcance de la autorización de tratamiento de datos que suscribe el usuario. Esto con el fin de que no se envíe información comercial a quien no lo ha autorizado, o que no se compartan los datos con terceros para fines distintos a la gestión del vínculo que se tiene con PROTECCIÓN S.A.

De igual forma, son los responsables de la marcación de los afiliados que se encuentran en cabeza del empleador, así como de aquellos que presentaron el extravío del formulario de vinculación, de conformidad con las alertas emitidas por otras áreas. Esto con el fin de evitar que dichos afiliados, sean contactados para cuestiones distintas a las referentes al producto que tienen contratado con la Administradora.

Este equipo se encarga de verificar que la información generada en los extractos que emite la Administradora se encuentre correcta antes de ser transmitida a sus destinatarios.

Por otro lado, este proceso se encarga de la Administración de los repositorios de información de la organización, función dentro de la cual se encuentra la recepción y conservación de los documentos que contienen información personal de las diferentes contrapartes de PROTECCIÓN S.A., en especial de clientes actuales. Esta área cuenta con un protocolo de digitalización y gestión documental, así como un procedimiento de atención frente a las pérdidas de información que puedan llegar a darse durante el proceso de custodia de esta.

Equipo de Administración del producto mandatorio: Esta área está encargada de la generación de las vinculaciones de afiliados por su empleador. Es decir, que no suscribieron un formulario, sino que la empresa los vinculó a esta Administradora realizando cotizaciones a su nombre. Esta generación se realiza en consonancia con el reporte mensual que emite Asofondos para dar a conocer los nombres de los afiliados que cuentan con dicha particularidad en su vinculación.

Esta área se encargará de remitir el listado de afiliados cuya vinculación fue realizada por su empleador, al equipo comercial con el fin de que se obtenga la autorización expresa, libre e informada del titular para su afiliación.

Asimismo, son los encargados de notificar al equipo de Gestión de la Información los casos de vinculación en cabeza del empleador, con el fin de que quede debidamente registrada esta novedad en Apolo o el aplicativo correspondiente.

Atracción y Desarrollo: Esta área se encuentra encargada de la contratación de nuevo personal para la Organización, proceso dentro del cual se hace recolección de información personal de candidatos, frente a los cuales somos responsables del tratamiento.

En este sentido, el equipo de atracción y desarrollo es el responsable de la administración de la base de datos de los candidatos que participan en los procesos de selección de la Administradora, así como de los datos de los colaboradores actuales.

Comunicaciones y Marca: Este proceso se encarga de posicionar a la organización dentro del mercado, así como de la atracción de nuevos clientes. Con ocasión de dicha labor, Comunicaciones y Marca recolecta información personal de clientes potenciales que es transmitida a la Estructura Comercial con el fin de perfeccionar las ventas. Esta información, debe ser manejada conforme a la Política de Tratamiento de Datos Personales de PROTECCIÓN S.A.

Por su parte, en el marco de las campañas que realiza el área con clientes actuales o potenciales, esta se cerciora en Apolo o los aplicativos a que haya lugar, de las finalidades del tratamiento de datos que hubiera autorizado el titular de la información antes de incluirlo en cualquier proyecto comercial de la organización.

Este equipo es el encargado de dar cumplimiento a las disposiciones de contactabilidad dispuestas en la legislación colombiana como la Ley 2300 de 2023 (dejen de fregar).

Estructura Comercial (ahorro para el retiro y gestión patrimonial): La Estructura Comercial está encargada del crecimiento de los afiliados de PROTECCIÓN S.A. en cada uno de sus productos y servicios. Para dicha labor, cuentan con el insumo que les proporciona Comunicaciones y Marca, así como otras áreas que se dedican al relacionamiento externo de la Compañía.

Así las cosas, la Estructura es la encargada de garantizar que en la consecución de clientes se haga uso únicamente de las bases de datos proporcionadas por la Administradora, las cuales, a su vez, deben contar con la autorización de tratamiento por parte de los clientes prospectos. Lo anterior implica, no hacer uso de bases de datos paralelas, ni independientes a las recolectadas por los procesos encargados de dicha labor, y realizar las actividades de tratamiento de datos personales, únicamente con las herramientas, medios y canales establecidos por la organización.

Adicionalmente y al igual que Comunicaciones y Marca, deben cerciorarse en Apolo o los aplicativos a que haya lugar, de las finalidades de tratamiento de datos que hubiera autorizado el titular de la información antes de incluirlo en cualquier proyecto comercial de la organización. En caso de que lleven a cabo el proceso de actualización de datos de clientes actuales o potenciales, deben velar por que se suscriba el formato de autorización de tratamiento de datos personales. Este equipo es el responsable de la Administración de la base de datos de clientes potenciales de la organización.

Equipo de Experiencia de Estrategia Digital: Esta área lleva a cabo iniciativas de fidelización, atracción de clientes potenciales, entre otras campañas en las que se recolecta información de carácter personal. Esta debe ser utilizada de conformidad con nuestra Política de Protección de Datos Personales.

Adicionalmente, esta área deberá cerciorarse en Apolo o los aplicativos a que haya lugar, de las finalidades de tratamiento de datos que hubiera autorizado el titular de la información antes de incluirlo en cualquier proyecto comercial de la organización.

En caso de que lleven a cabo el proceso de actualización de datos de clientes actuales o potenciales, deben velar por que se suscriba el formato de autorización de tratamiento de datos personales.

Este equipo es el responsable de la Administración de la base de datos de clientes potenciales de la organización.

Canal personas: Este proceso se encarga de llevar a cabo todas las interacciones con clientes actuales y prospectos, terceros, beneficiarios y apoderados a través de nuestros canales de servicio. En dichos eventos, recolectan información personal y documentación que es transmitida al equipo de Gestión de la Información para su custodia.

Este equipo tiene a su cargo entre otras cosas, la actualización de datos de afiliados, proceso dentro del cual deben velar por que los titulares de información otorguen la autorización de tratamiento de datos personales y por qué la misma quede debidamente registrada en los aplicativos establecidos para ello.

Por su parte, deben retomar a los usuarios sobre los que se hubiera reportado una pérdida del formulario de afiliación, con el fin de que se pueda formalizar nuevamente el vínculo con la Administradora.

Equipo de Atención de Solicitudes y PQR: Este equipo tiene a cargo la atención de los requerimientos que realizan tanto clientes, como usuarios externos o beneficiarios frente a productos y servicios de la Compañía.

En lo que se refiere al tema de protección de datos, son los encargados de reportar a Cumplimiento Legal, las quejas y reclamos que llegan sobre esta materia para efectos de seguimiento e implementación de mejoras dentro de los procesos involucrados.

Por su parte, deben contar con un protocolo de atención de requerimientos específico sobre datos personales, en el cual deben quedar establecidos los tiempos de respuesta para este tipo de peticiones, de conformidad con lo regulado en la Ley 1581 de 2012.

Equipo de Soluciones Digitales y Relacionamiento para Clientes: Este equipo desarrolla proyectos e iniciativas que pretenden fortalecer la relación con clientes, así como con proveedores y colaboradores. En dicho marco de actuación se recolecta información personal que es utilizada de conformidad con nuestra Política.

Por su parte, esta área debe cerciorarse en Apolo o los aplicativos a que haya lugar, de las finalidades de tratamiento de datos que hubiera autorizado el titular de la información antes de incluirlo en cualquier proyecto comercial de la Organización.

Experiencia del colaborador: Esta área realiza actividades de formación y crecimiento tanto para colaboradores como para clientes actuales y potenciales a través de eventos, webinarios y contenido en la Universidad Protección. La información sobre clientes potenciales es remitida al Equipo Comercial y de Experiencia del Cliente para el robustecimiento del insumo para su gestión.

En caso de que lleven a cabo el proceso de actualización de datos de colaboradores o clientes actuales o potenciales, deben velar por que se suscriba el formato de autorización de tratamiento de datos personales.

Equipo de Responsabilidad Social y Empresarial y Equipo de Sostenibilidad: Esta área se encarga de generar iniciativas y voluntariados sociales a los que puede acceder cualquier tipo de público, incluso personas externas a la Administradora. En dichos eventos se recolecta información personal que es tratada conforme a nuestra Política de Protección de Datos.

En caso de que lleven a cabo el proceso de actualización de datos de colaboradores o clientes actuales o potenciales, deben velar por que se suscriba el formato de autorización de tratamiento de datos personales.

Abastecimiento: Dentro de la labor de este proceso, se encuentra la contratación de proveedores que pueden ser personas naturales. En este sentido, la información personal recolectada es utilizada de acuerdo con nuestra Política de Tratamiento de Datos.

Adicionalmente, esta área se encarga de realizar las auditorías que se consideren necesarias para establecer la idoneidad y el cumplimiento del encargado o responsable del tratamiento de datos en el ejercicio de sus funciones y la no extralimitación de las finalidades establecidas para el tratamiento de los datos personales por este encargado o responsable, según sea el caso. Esta obligación deberá cumplirse en conjunto con el proceso de la organización responsable de la transferencia o transmisión de los datos personales.

Bien Estar: Esta área recibe la información de colaboradores de parte del equipo de Atracción de Talento como administradores de las bases de datos de candidatos y trabajadores de la organización. Dentro de esta se encuentra comprendida la información personal, familiar y profesional, así como la referente a la historia clínica ocupacional, a la cual solo se podrá tener acceso con autorización expresa del colaborador. Adicionalmente, esta área se encuentra a cargo del corredor de seguros de la organización, al cual se le remite información personal y financiera de los colaboradores, siguiendo los lineamientos de nuestra Política de tratamiento de Datos.

Dirección de Procesos Jurídicos y Regulación: Este equipo tiene a cargo la interpretación y divulgación de normatividad relacionada con el tratamiento de datos personales. De igual forma, son responsables de llevar a cabo los contratos de transmisión o transferencia de información con los encargados, así como de la inclusión de cláusulas penales y otras garantías frente a los proveedores que incumplan obligaciones en esta materia.

Equipo de Gobierno Corporativo y Relaciones Institucionales: Este equipo tiene a cargo la información los accionistas, miembros de junta y miembros externos de comités de la organización, la cual es recolectada por un tercero, pero Administrada por PROTECCIÓN S.A. para los efectos pertinentes.

Equipo Oferta de Valor: Este subproceso se distribuye de acuerdo con el ciclo de vida de nuestros clientes (jóvenes / independientes, intermedios, adulto mayor y pensionados) con el fin de realizar iniciativas y proyectos que aporten a la oferta de la Administradora frente a clientes actuales o potenciales. En dicha gestión se recolectan datos personales, los cueles son remitidos a las áreas comerciales para poblamiento de sus bases de datos y retoma posterior.

Equipo de Diseño Organizacional y Compensación: Este equipo recibe la base de datos de colaboradores del área de, quien administra la información de candidatos y trabajadores actuales. Con dichos datos, el área de compensación lleva a cabo las actividades de nómina de la Administradora, entre las cuales se encuentra la transmisión de datos personales a entidades externas con las cuales se tramitan, créditos, alianzas, pagos de seguridad social entre otros.

6. CONTROLES DEL PROGRAMA

Con el objeto de garantizar la implementación efectiva de las políticas y procedimientos establecidos por PROTECCIÓN S.A en materia de protección de datos personales, se han establecido los siguientes controles:

6.1 Metodología para la gestión del riesgo: PROTECCIÓN S.A. ha definido adoptar una metodología para identificar, valorar, controlar y monitorear el riesgo de uso o tratamiento indebido o injustificado de datos personales y afectación de la privacidad de los titulares con el objetivo de minimizar incidentes, garantizar el cumplimiento normativo, y proteger la reputación de la organización. Esta metodología se establece acorde con los parámetros determinados por la norma técnica internacional ISO 31000:2018 y las mejores prácticas en materia de gestión de riesgos empresariales. La metodología de gestión de riesgos se documenta en la "Matriz de Riesgos del Programa de Protección de Datos Personales", la cual, es parte integral del Programa de Protección de Datos Personales, da cuenta de la ejecución efectiva de las etapas de gestión del riesgo anteriormente mencionadas, y se encuentra a cargo del Oficial de Protección de Datos Personales, quien estará a cargo

también de su actualización periódica como mínimo, cada dos años. La estructura de la matriz de riesgos, los criterios, las escalas de probabilidad e impacto para la valoración del riesgo y de efectividad de los controles, se establecen de conformidad con las directrices dispuestas por el equipo de Riesgos de Negocio e Información en cuanto a la metodología a aplicar.

6.2. Procedimientos Operacionales: Los controles operacionales relacionados con la protección de los datos personales tratados por la organización se encuentran establecidos en la "Matriz de Riesgos del Programa de Protección de Datos Personales".

6.3. Inventario de Bases de Datos Personales: Como resultado del proceso de debida diligencia adelantado por PROTECCIÓN S.A para determinar los ciclos internos de gestión de datos personales, se han identificado las siguientes bases de datos:

- Clientes Potenciales: Los datos de identificación y de contacto de las personas que podrían convertirse en clientes de la organización son recolectados a través de los eventos de comunicaciones y marca, los formularios en redes sociales y el portal web, el cruce periódico con bases de datos con aliados, y a través de referencias comerciales. Asimismo, estos son almacenados a través de sistemas como: Pragma, Salesforce, la Nube u otros.

  Estos datos son utilizados para las finalidades descritas en nuestra Política de Tratamiento de Datos Personales.

- Beneficiarios, Curadores y Apoderados: Los datos de identificación y de contacto de las personas que por disposición legal y/o contractual se encuentran legitimadas para actuar en representación de un cliente de la organización, y/o han adquirido un derecho en virtud de la consanguineidad con un cliente de la organización, son recolectados a través de la radicación de trámites prestacionales, peticiones, quejas y/o reclamos. Asimismo, estos son almacenados a través de aplicativos como Salesforce u otros.

  Estos datos son utilizados para las finalidades descritas en nuestra Política de Tratamiento de Datos Personales.

- Clientes: Los datos de identificación, de contacto y financieros de las personas que se encuentran vinculadas a los diferentes fondos administrados por la organización (Pensión Obligatoria, Pensión Voluntaria y/o Cesantías), son recolectados a través del proceso de afiliación, las compañas de actualización de datos, los eventos de universidad protección y otros micrositios, la radicación de tramites asociados a los productos contratados, y la interposición de peticiones, quejas y/o reclamos. Asimismo, estos son almacenados a través de aplicativos como Apolo, Salesforce, Filenet, Imagine, Advance, Altius y otros.

  Estos datos son utilizados para las finalidades descritas en nuestra Política de Tratamiento de Datos Personales.

- Candidatos: Los datos de identificación y de contacto de las personas que aspiran vincularse laboralmente a la organización son recolectados a través de la inscripción que estos realizan en el portal de empleo de PROTECCIÓN S.A. Asimismo, estos son almacenados a través de aplicativos como Talentum y otros.

  Estos datos son utilizados para las finalidades descritas en nuestra Política de Tratamiento de Datos Personales.

- Colaboradores: Los datos de identificación y de contacto de las personas que se encuentran vinculadas laboralmente a la organización son recolectados a través de la suscripción del respectivo contrato laboral y de la inscripción en voluntariados o iniciativas sociales. Asimismo, estos son almacenados a través de Talentum, Qerix7, los repositorios internos del equipo de bienestar y otros.

  Estos datos son utilizados para las finalidades descritas en nuestra Política de Tratamiento de Datos Personales.

  Miembros de Junta Directiva y Miembros de Comités de Apoyo: Los datos de identificación y de contacto de los integrantes de la Junta Directiva de la organización y los comités de apoyo, son recolectados a través de Dilitrust. Asimismo, estos son almacenados a través de los repositorios internos de la Secretaría General.

Estos datos son utilizados para las finalidades descritas en nuestra Política de Tratamiento de Datos Personales.

- Proveedores: Los datos de identificación, de contactos y financieros de las personas naturales que prestan y/u ofrecen directamente sus servicios y/o productos a la organización son recolectados a través de la suscripción de los documentos de vinculación como proveedores de la organización. Estos datos son recolectados por el área de abastecimiento.

  Estos datos son utilizados para las finalidades descritas en nuestra Política de Tratamiento de Datos Personales.

- Accionistas: Los datos de identificación y de contacto de los integrantes de los accionistas de la organización son recolectados a través de Deceval. Estos son almacenados a través de los repositorios internos de la Secretaría General.

6.4. Disposiciones para la protección de datos sensibles y datos de menores de edad

El tratamiento de la información personal sensible y/o los datos personales de niños, niñas y adolescentes, se realizará exclusivamente en cumplimiento de las disposiciones normativas emanadas del sistema de seguridad social (Ley 100 de 1993) y de las instrucciones impartidas por la Circular Básica Jurídica de la Superintendencia Financiera de Colombia; y para la materialización de los propósitos y finalidades descritas en nuestra Política de Protección de Datos Personales para esta información.

Asimismo, como parte de la protección reforzada sobre este tipo de información, en PROTECCIÓN S.A se desarrollarán continuamente las siguientes acciones:

- Se efectuarán capacitaciones al personal en las que se enfatice la obligatoriedad de una mayor protección a estos datos sensibles.

- Se buscará mejorar las condiciones de seguridad de este tipo de información.

- Se priorizará la atención de quejas que versen sobre este tipo de información.

6.5. Procedimientos para el ciclo de vida del tratamiento de los datos personales

PROTECCIÓN S.A establece los siguientes procedimientos para el aseguramiento del ciclo de vida de los datos personales de aquellos individuos pertenecientes a nuestros diferentes grupos de interés, quienes han autorizado el tratamiento de su información personal.

6.5.1. Recolección y autorización

Toda captura, recolección, uso, almacenamiento o cualquier otro tratamiento que realice PROTECCIÓN S.A respecto de los datos personales requiere de los titulares un consentimiento libre, previo, expreso, inequívoco e informado. PROTECCIÓN S.A. solo realizará actividades de tratamiento de datos personales frente a aquellos clientes que lo hayan autorizado, o en los eventos que la Ley lo autorice.

PROTECCIÓN S.A. entiende y presume que todos los datos entregados por parte del titular son veraces, completos, exactos, actualizados, comprobables y comprensibles. En ese sentido, PROTECCIÓN S.A. no tratará datos parciales, incompletos,

fraccionados o que induzcan a error, por lo que se reservará el derecho de eliminar o suprimir de sus bases de datos este tipo de información.

Para esto, PROTECCIÓN S.A. cuenta con formatos de autorización de tratamiento de datos personales y un Aviso de Privacidad que según sea el caso, dependiendo del tipo de información, las finalidades y el tipo de titular, pondrá a disposición de los titulares para que estos se informen sobre la captura de sus datos personales, el tratamiento al que serán sometidos incluyendo sus finalidades, sus derechos, los canales para ejercer sus derechos y la información relacionada con la Política de Protección de Datos Personales.

En todos los casos, la obtención de la autorización se realizará bajo las diferentes modalidades que establece la ley, teniendo en cuenta la naturaleza de cada uno de los canales de captura de la información y el modo en que la misma es obtenida, es decir, si es a través de un canal escrito, verbal o mediante una conducta inequívoca.

Finalmente, es de vital importancia almacenar y custodiar las autorizaciones obtenidas para el tratamiento de los datos personales, dado que ésta hace parte de las pruebas exigidas por la autoridad competente. Así las cosas, se deberán guardar los formatos físicos en donde existan autorizaciones, el registro de llamadas o de los formularios web en los que se da trazabilidad de la aceptación del tratamiento. Esta retención se hará de acuerdo con las políticas y procedimientos para la retención y disposición de la compañía y será deber del área o proceso encargado de la recolección de la autorización respectiva

Adicionalmente, en virtud del Principio de Privacidad por Diseño, será deber de todos los colaboradores, previo a la estructuración o creación de un producto, servicio o solución, evaluar en conjunto con el Área de Cumplimiento Legal, si para ese nuevo producto, servicio o solución se requiere un flujo de captura de la autorización para el tratamiento de los datos personales con su respectiva conexión a la base de datos de clientes, a partir de las actividades de tratamiento que se vayan a realizar y del público objetivo del mismo.

En los eventos en que el dato personal sea recolectado por un proveedor o tercero, se deberá validar que la entidad recolectora cuente con una autorización válida para compartir dicha información con PROTECCIÓN S.A, así como las finalidades autorizadas por el titular del dato y la suscripción del respectivo Acuerdo de Tratamiento de Datos Personales.

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

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las Personas.
- Información necesaria para las actuaciones relacionadas con el Sistema General de Seguridad Social que sean de obligatorio cumplimiento para la correcta administración de los recursos de los afiliados en los Fondos de Pensiones y Cesantías, en el entendido que estas acciones buscan proteger el interés superior de la seguridad social del afiliado y son actuaciones exigidas por la misma ley.

<u>Deber de los colaboradores:</u> Todos los colaboradores se comprometen a tratar únicamente los datos personales que el titular haya autorizado. Cualquier tratamiento de datos personales no autorizado por el titular o que su tratamiento no se encuentre enmarcado en el cumplimiento de las obligaciones legales a cargo de PROTECCIÓN S.A. es considerado un incumplimiento del contrato laboral.

6.5.1.1. Procedimientos de obtención de la autorización:

Los modelos de autorización de tratamiento de datos personales pueden ser tramitados a través de formatos web, documentos físicos, llamadas o cualquier otro soporte que permita guardar prueba de dicha autorización.

Cuando se trate de Formatos Web, debe tenerse en cuenta los siguientes aspectos necesarios para su captura:

- Solicitar sólo aquellos datos personales necesarios conforme con la finalidad del tratamiento.
- Relacionar en el formato, un aviso de privacidad que incorpore la autorización del tratamiento por parte del titular en los casos donde no se pueda poner toda la información necesaria para que la autorización sea válida.
- Condicionar el envío de la información a través del formulario a la previa aceptación de la autorización de tratamiento del dato.
- Validar que en la autorización se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos personales.
- Validar que la plataforma que soporta el formulario web tenga la capacidad técnica, operativa y de seguridad para almacenar las autorizaciones, y poder tener la trazabilidad en ellas.
- Incluir fecha en la que se obtuvo la autorización para temas de trazabilidad.

Cuando se trate de Formatos Físicos, debe tenerse en cuenta los siguientes aspectos:

- Solicitar sólo aquellos datos personales necesarios conforme con la finalidad de la captura.
- Relacionar en el formato, la autorización completa de acuerdo con los requisitos legales.
- Para que PROTECCIÓN S.A. pueda realizar el tratamiento de los datos capturados en el formulario, el titular debe dar la autorización.
- Validar que en la autorización se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos personales.
- Realizar el adecuado almacenamiento o digitalización del documento para posterior consulta.

Cuando se trate de llamadas, debe tenerse en cuenta los siguientes aspectos:

- Solicitar sólo aquellos datos personales necesarios conforme con la finalidad de la captura
- Desde el primer momento del contacto, se debe parametrizar en el dialogo con el cliente, la captura de la autorización para el tratamiento de datos personales, informando las finalidades para las cuáles serán utilizados los datos y los canales para el ejercicio de los derechos por los titulares. Para la creación de estos diálogos prediseñados, el encargado de la implementación del flujo de captura de la autorización deberá solicitar acompañamiento del Área de Cumplimiento Legal.
- Garantizar la documentación y almacenamiento de las conversaciones que soporten el otorgamiento de la autorización de tratamiento de datos personales por parte de los titulares.

En los 3 medios de captura de la autorización mencionados anteriormente (formularios físicos, web o llamadas) el responsable del proceso encargado de la captura de la información personal debe estructurar una conexión con la base de datos de clientes de la compañía (APOLO), para que allí se refleje la autorización otorgada por el cliente, la fecha de dicha autorización, y si el cliente autoriza compartir sus datos con aliados y el envío de información publicitaria y comercial. Para esta actividad el responsable deberá solicitar apoyo del equipo de Gestión de la Información - Información para Clientes y del Área de Cumplimiento Legal.

6.5.1.2. Tipos de autorizaciones de tratamiento de datos personales:

Autorización para el tratamiento de datos sensibles:

Son aquellos datos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, como aquellos que revelen el origen racial o étnico; la orientación política, las convicciones religiosas o filosóficas; la pertenencia a sindicatos u organizaciones sociales, de derechos humanos, que promuevan 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.

Este tipo de datos exige un tratamiento especial, por lo que, para su recolección, se debe tener en cuenta que:

- El titular de forma explícita debe autorizar el tratamiento de los datos sensibles. Actualmente PROTECCIÓN cuenta con un texto para la autorización del tratamiento de datos sensibles, el cual, se encuentra incluido dentro de la Política de Protección de Datos Personales aprobada por la organización y a cargo del Área de Cumplimiento Legal.
- El titular no se encuentra obligado a suministrar este tipo de datos, y ninguna actividad puede estar condicionada a la entrega de datos sensibles salvo que exista obligación legal que implique el tratamiento de estos.
- El acceso a bases de datos que tengan información sensible debe ser de circulación restringida, por lo que solamente aquellas personas que deban estrictamente realizar tratamiento de estos deben tener acceso.
- Se deben aplicar técnicas de seudonimización o anonimización de la data cuando la identificación directa del titular no sea necesaria para la finalidad prevista o no se requiera el análisis de datos sensibles.

Autorización para el tratamiento de datos personales de menores de edad:

La obtención de datos de menores de edad se realiza previa autorización de quien tenga la representación legal y patria potestad del menor, a través de mecanismos electrónicos o físicos dispuestos para tal efecto.

Para obtener la autorización para el tratamiento de datos personales de menores de edad, se debe tener presente que dicho tratamiento está prohibido, excepto cuando se trate de datos de naturaleza pública, conforme a lo establecido en el artículo 7 de la Ley 1581 de 2012 y en los artículos 6 y 12 del Decreto 1377 de 2013. También será permitido cuando cumpla con los siguientes parámetros y requisitos:

- Solicitar la autorización de forma previa al tratamiento de los datos personales al representante legal del menor.
- Recolectar únicamente los datos que sean estrictamente necesarios para las finalidades para las cuales se recogen y estas sean informadas al menor y sus representantes legales.
- Limitar el envío de información a aquella que sea estrictamente necesaria para las finalidades autorizadas.
- Realizar toda interacción con el menor a través de sus representantes legales.
- Recordar que la respuesta a preguntas acerca de los datos de niños, niñas o adolescentes tiene carácter facultativo y no obligatorio.
- Respetar el interés superior de los menores y garantizar la protección de sus derechos fundamentales

Cumplidos los requisitos anteriores, el representante legal del niño, niña o adolescente otorgará la autorización a PROTECCIÓN S.A., previo ejercicio del menor de su derecho a ser escuchado. La opinión del menor será valorada teniendo en cuenta su madurez, autonomía y capacidad para comprender el asunto. Se informará explícitamente cuáles son los datos objeto de tratamiento y la finalidad del mismo.

En el tratamiento de datos personales de menores de edad, se deberán desplegar las siguientes actividades o procedimientos:

- Los medios de captura de la autorización deben garantizar la firma expresa por parte de los representantes legales.

- La autorización deberá digitalizarse y documentarse conforme a las políticas de gestión documental de la organización.
- Se deberán implementar medidas para validar la patria potestad o representación legal, lo anterior a través del Registro Civil de Nacimiento del menor o el documento legal que haga sus veces.
- Si bien se debe propender por la firma de la autorización por parte de ambos padres, en caso de existir solo uno de ellos, este podrá otorgar la autorización para el tratamiento de los datos personales del menor.
- Capacitaciones al personal en las que se enfatice la obligatoriedad de una mayor protección a estos datos sensibles.
- Mejora de las condiciones de seguridad de este tipo de información.
- Priorización de la atención de quejas que versen sobre este tipo de información.

El Área de Cumplimiento Legal será quien estructure el formato de autorización de tratamiento de datos personales de menores de edad

Autorización para el tratamiento de información personal – Formato General

El formato general de Autorización de Tratamiento de Datos Personales se encuentra a cargo del Área de Cumplimiento Legal. En este formato se contemplan las finalidades específicas de acuerdo con el público objetivo y el tratamiento que se le vaya a dar a los datos personales, los derechos ARCO de los titulares, las medidas de seguridad, y los canales para el ejercicio de dichos derechos. Así mismo, se contemplan las autorizaciones particulares de compartir la información con aliados y de envío de información publicitaria y comercial.

Autorización para el tratamiento de la información personal Empleados

El formato para solicitar autorización para el tratamiento de datos personales de empleados de PROTECCIÓN deberá recolectarse desde el contrato de trabajo y/o de manera independiente de este. En esta autorización solo se contemplan aquellas finalidades que no sean de obligatorio cumplimiento por disposiciones legales, ya que para estas no se necesitará autorización expresa de los colaboradores.

Aviso de Privacidad:

De acuerdo con las disposiciones normativas, los avisos de privacidad mediante los cuales se obtiene la autorización de los titulares deben tener los siguientes elementos:

- Nombre o razón social y datos de contacto del responsable del tratamiento
- El Tratamiento al cual serán sometidos los datos y la finalidad de este.
- Los derechos que le asisten al titular.
- Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información.
- En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información.

Los avisos de privacidad suelen ser utilizados en lugares donde no se puede incluir el texto completo de la autorización, para los casos de video vigilancia, o cuando se requiere entregar conocimiento sencillo y simplificado sobre los aspectos relacionados con la autorización de tratamiento de datos personales. PROTECCIÓN S.A. cuenta con un aviso de privacidad que se publica en el siguiente link de la página web: https://www.proteccion.com/contenidos/persona/cesantias/ley-proteccion-datos-personales

Autorización para la transferencia de información dentro del ecosistema de Finanzas Abiertas (Open Finance):

En virtud de las operaciones que realice la compañía a través del sistema de Finanzas Abiertas (Open Finance), se deberá solicitar en todos los casos, y para cada operación de transferencia de datos personales, la autorización previa, expresa e informada por parte del titular. Esta autorización debe contemplar como mínimo, la finalidad de la operación de transferencia, los datos que serán tratados, la vigencia de dicha autorización, los derechos del titular y los canales o medios por los cuáles podrá ejercerlos. Esta autorización deberá ser recolectada tanto en los casos donde la organización actúa como receptor como operador de los datos.

El área o proceso interesado en recibir o entregar los datos a través del ecosistema de Open Finance, deberá dar cumplimiento al procedimiento de captura de la autorización y a las disposiciones dispuestas en la Política de Vinculación de Terceros Receptores de Datos, con apoyo de las demás áreas o procesos competentes.

6.5.2. Almacenamiento

Tanto la información personal de nuestros grupos de interés como la prueba de la autorización de tratamiento de datos que se haga de manera escrita (sea física o digital) se guardarán en el aplicativo respectivo, con todos los requisitos de seguridad establecidas por las áreas de Riesgos de Negocio e Información y Ciberseguridad en la Política de Seguridad en la Información y Ciberseguridad de la organización.

La custodia deberá contar con medidas de seguridad idóneas para el mantenimiento de la confidencialidad de la información y la prevención de fuga o robo de información. Así mismo, la información deberá estar de forma organizada para que esta pueda ser puesta a disposición de la autoridad competente en el evento que se requiera.

Deber de los colaboradores: Todos los colaboradores se comprometen a almacenar los datos personales exclusivamente conforme las reglas, sistemas y herramientas establecidas por la compañía. Cualquier almacenamiento de información personal a la que los colaboradores accedan en virtud de sus funciones, en sistemas o herramientas no establecidas por la organización, o de uso personal, es considerado un tratamiento no autorizado e injustificado de la información, y se entiende como un incumplimiento del contrato laboral.

6.5.3. Uso

Los datos recolectados por PROTECCIÓN S.A tendrán como propósito principal, el cumplimiento de las funciones inherentes a la Administradora. No obstante, también podrá hacerse uso de los datos recolectados para gestión comercial de los productos y servicios ofrecidos por la organización, finalidad que deberá quedar explícita en la autorización que suscribe el titular y que además se enuncia en la Política de tratamiento de Datos Personales aprobada y publicada por la organización.

En los casos en que PROTECCIÓN S.A requiera del apoyo de terceros para el ofrecimiento de productos o servicios, se compartirá la información personal que se requiera, previa autorización por parte del titular y previa suscripción del respectivo Acuerdo de Tratamiento de Datos Personales, el cual, debe ser estructurado o revisado por la Gerencia de Regulación de la compañía

Las finalidades indicadas en la cláusula de autorización de tratamiento constituyen el límite para el uso de la información y serán las dispuestas en la Política de Protección de Datos de PROTECCIÓN S.A.

Deber de los colaboradores: Todos los colaboradores se comprometen a usar la información personal únicamente para las finalidades comprendidas en la autorización otorgada por el titular y en la Política de Protección de Datos Personales de PROTECCIÓN S.A. Cualquier uso de información personal a la que acceda el colaborador en el ejercicio de sus funciones y sea utilizada para fines particulares, no autorizados por el titular o que no se encuentre en el marco del cumplimiento de las

obligaciones legales a cargo de PROTECCIÓN S.A., es considerado un tratamiento no autorizado e injustificado de la información, y se entiende como un incumplimiento del contrato laboral.

6.5.4. Circulación

PROTECCIÓN S.A no realizará transmisión de información de sus clientes con terceros a menos que se haya estipulado el tratamiento de los datos a través de un encargado, se haya suscrito el respectivo Acuerdo de Tratamiento de Datos Personales, y así haya sido autorizado por el titular.

Deber de los colaboradores: Todos los colaboradores se comprometen a transferir o transmitir la información personal de los titulares conforme las reglas establecidas en el presente manual, de conformidad con la autorización otorgada por el titular y/o las obligaciones legales a cargo de PROTECCIÓN S.A. Cualquier envío de información personal a un correo o sistema de información de uso particular, o cualquier transferencia o transmisión de datos no autorizada o a un tercero no autorizado, es considerado un tratamiento indebido e injustificado de la información, y se entiende como un incumplimiento del contrato laboral.

6.5.5. Actualización

La posibilidad de rectificar la información que reposa en una base de datos es uno de los derechos con que cuentan los titulares de estos. En este sentido, al momento de realizar una actualización deberá incluirse un procedimiento de validación de identidad, a través de cualquiera de los medios que sean aprobados por la Dirección de Riesgos de Negocio e Información, con el fin de garantizar que quien requiera el cambio de los datos personales sea en efecto el titular de estos.

Deber de los colaboradores: Todos los colaboradores se comprometen a actualizar los datos personales de los titulares de conformidad con su voluntad y la autorización otorgada. Cualquier actualización de datos personales que no se encuentre autorizada por el titular, no sea solicitada por este, o no se encuentre dentro de las competencias de PROTECCIÓN S.A. en el marco del cumplimiento de sus obligaciones legales, es considerada un tratamiento indebido e injustificado de la información, y se entiende como un incumplimiento del contrato laboral.

6.5.6. Supresión

Los titulares de la información podrán solicitar en todo momento, por medio de cualquiera de nuestros canales de atención, la supresión de sus datos personales, solicitud que será atendida por parte de PROTECCIÓN S.A. de la siguiente forma:

Una vez recibida la solicitud, deberá ser ingresada a través de la aplicación Salesforce o la que haga sus veces, clasificándola de acuerdo con el flujo establecido para las solicitudes asociadas a la protección de datos por parte del Equipo de Atención de Solicitudes

Trámite de la solicitud: el equipo de Atención de Solicitudes activará al área encargada de la administración de la base de datos, para que proceda a la destrucción de los datos personales que el usuario solicitó eliminar con sus respectivos soportes, para efectos de conservación de pruebas del requerimiento.

- Seguimiento a la solicitud: el Equipo de Atención de Solicitudes informará al área de Cumplimiento Legal las peticiones que ingresan al relacionadas con Protección de datos, con el fin de llevar la trazabilidad de este tipo de requerimientos.

- Reporte al titular: una vez realizada la destrucción de la información, el Equipo de Atención de Solicitudes notificará al usuario por los medios que este último hubiera informado en su petición. Por su parte, mientras no exista una solicitud de eliminación de los datos por parte del afiliado, PROTECCIÓN S.A como responsable del tratamiento, conservará los datos por los términos establecidos en Ley y por el tiempo que sea necesario con el fin de garantizar el acceso a la información del expediente pensional y evitando que en un futuro se pueda ver afectado el derecho fundamental a la Seguridad Social.

Adicionalmente, el Decreto 1377 de 2013 que reglamenta la Ley 1581 de 2012, consagra en su artículo 9º la posibilidad que tiene el titular de solicitar al responsable la revocatoria de la autorización o supresión del dato; no obstante, es de resaltar que dicha acción no procede cuando el titular tenga un deber legal o contractual de permanecer en la base de datos de conformidad con la normativa vigente, especialmente dentro del Sistema de Seguridad Social.

Acceso y corrección de datos personales

De conformidad con la Ley 1581 de 2012, Protección garantiza el derecho de acceso a la información personal, únicamente a los Titulares de datos privados, previa acreditación de la identidad del titular o de su representante, poniendo a disposición de éste, sin costo o erogación alguna, de manera pormenorizada y detallada, los respectivos datos personales tratados, a través de cualquier medio de comunicación, incluyendo los electrónicos. Dicho acceso, se sujeta a los límites establecidos en el artículo 21 del Decreto 1377 de 2013.

En caso de que el titular de la información advierta y pruebe debidamente alguna inconsistencia en los datos tratados a su nombre, deberá Protección corregir la información requerida en los términos establecidos en el artículo 15 de la Ley 1581 de 2012.

Conservación y eliminación de información personal

La Administradora preservará la información de sus contrapartes durante el tiempo necesario para cumplir las finalidades para las que fueron recogidos, incluso luego de finalizado el vínculo, si existe una obligación legal para hacerlo y en atención a la normatividad vigente en materia de responsabilidad demostrada, la cual dependerá de la clasificación del dato o del documento que lo contenga, así:

- La información relacionada con el expediente pensional deberá ser conservada por 20 años desde la extinción del derecho del último beneficiario, debido al carácter imprescriptible del derecho fundamental a la Seguridad Social.
- Se conservarán por un período no menor de diez (10) años los documentos relativos a la prevención de lavado de activos y financiación del terrorismo (SARLAFT).

En general, los documentos que contengan datos personales y se incluyan en las tipologías documentales que se relacionan a continuación, deberán ser conservados incluso así el titular haya solicitado su eliminación, o haya culminado el vínculo con este. Lo anterior, en virtud de las obligaciones legales a cargo de PROTECCIÓN S.A:

Tipo de documento con información personal	Tiempo mínimo sugerido	Fundamento normativo
Expediente pensional	20 años desde extinción del derecho del último beneficiario.	Acuerdo 001 de 2024 AGN
Documentos contables	10 años desde el cierre o asiento.	Código de Comercio

Documentos generales de operación financiera	5 años desde el asiento.	Decreto 663 de 1993 EOSF
Contratos y condiciones aceptadas por clientes	5 años desde terminación de la relación	Decreto 663 de 1993 EOSF
Comunicaciones con valor probatorio (como asesorías por WhatsApp)	Dependerá de la naturaleza de la información	Todos los anteriores

- Frente a los datos para los cuales no exista un plazo específico de almacenamiento y sean requeridos para determinar responsabilidades derivadas, se les aplicará las reglas de conservación establecida en los artículos 60 del Código de Comercio y el 11 del Decreto 1377 de 2013 según aplique y de conformidad con las directrices emanadas por parte de la Gerencia de Regulación.

Por su parte, la información de clientes potenciales se conservará hasta por un año después de su recolección. En el evento de no concretar una vinculación durante el tiempo establecido, PROTECCIÓN S.A deberá eliminar los datos adquiridos.

Revocatoria de la autorización de tratamiento de datos

Todo titular de datos personales puede revocar en cualquier momento, el consentimiento al tratamiento de éstos, siempre y cuando, no lo impida una disposición legal o contractual. Para ello, el titular de la información deberá interponer una petición en la que informe que revoca su autorización para el tratamiento de datos de forma total o parcial a saber:

- Total: Sobre la totalidad de finalidades consentidas, esto es, que Protección debe dejar de tratar por completo los datos del Titular.
- Parcial: Sobre ciertas finalidades consentidas como por ejemplo para fines publicitarios o de estudios de mercado. En este caso, Protección deberá suspender parcialmente el tratamiento de los datos del titular. Se mantienen entonces otros fines del tratamiento que el responsable puede llevar a cabo, de conformidad con la autorización otorgada, y con los que el titular está de acuerdo.

Deber de los colaboradores: Todos los colaboradores se comprometen a revocar y suprimir los datos personales de los titulares de conformidad con su voluntad y la autorización otorgada. Cualquier revocatoria de datos personales que no se encuentre autorizada por el titular, no sea solicitada por este, o no se encuentre dentro de las competencias de PROTECCIÓN S.A. en el marco del cumplimiento de sus obligaciones legales, es considerada un tratamiento indebido e injustificado de la información, y se entiende como un incumplimiento del contrato laboral.

6.6. Uso responsable de información

La información tratada por PROTECCIÓN S.A será objeto de los siguientes controles y medidas de seguridad en la información:

- Administrativos y físicos: Dentro de nuestras políticas de seguridad física, contamos con procedimientos y controles que mitigan los accesos no autorizados a las oficinas, y a las áreas definidas como de control especial, los cuales se relacionan a continuación:

    a. Estándar de Seguridad Física: este documento tiene como objetivo definir los parámetros que deben cumplir las oficinas respecto de temas como: vigilancia, sistemas de control de acceso, sistemas de alarmas, CCTV, control de activos, servicios de suministro (energía, acueducto, etc.), mantenimientos, etc.

b. Definición de Áreas restringidas para el ingreso del personal: Protección cuenta con algunas áreas con acceso restringido, ya sea por requerimiento de las entidades de control o por que la información contenida en éstas es confidencial y no debe ser conocida por terceros (Mesa de Dinero, Tesorería, Centro de Servicios).
c. Controles de ingreso de terceros (Visitantes, proveedores, Outsorcing): se tienen definidos los requerimientos que deben cumplir todos los terceros que vayan a ingresar a las instalaciones.
d. Validaciones de seguridad física para proveedores estratégicos: los proveedores que prestan servicios que sean considerados como estratégicos, según los lineamientos del área de Abastecimiento, deberán tener implementado en sus instalaciones, esquemas de seguridad que garanticen la confiabilidad de dichos servicios, y la seguridad en la custodia de la información.
e. Política de apertura y cierre de oficinas: se tienen definidos los horarios, responsables, y el proceso de activación de alarmas para evitar intrusiones.
f. Monitoreo a los sistemas de seguridad: contamos con una central de seguridad propia que opera 7 x 24 x 365, la cual se encarga de validar el cumplimiento de las políticas de seguridad física, y de administrar los sistemas de seguridad electrónica (alarmas, control de acceso, CCTV; ente otros).

- Controles de seguridad tecnológicos: Entre las metodologías utilizadas para garantizar la seguridad de la información a nivel tecnológico se encuentran las siguientes:

a. Realización de inventario de activos de información en función del proceso encargado de la recolección de la autorización de tratamiento de datos.
b. Identificación de posibles brechas de seguridad y procedimentales.
c. Optimización y seguimiento a los subprocesos que requieran intervención.
d. Antispam y limpieza de correo en la nube.
e. Uso de plataforma de aseguramiento de servidores.
f. Herramienta de autenticación y autorización, así como de manejo de roles y perfiles.
g. Uso de plataforma para seguridad del datacenter y red desde el perímetro.
h. Portal de procesos de recuperación de infraestructura tecnológica.
i. Modelo de madurez en el aseguramiento de aplicaciones.
j. Control de identidad en canales de servicio.
k. En general, todas aquellas que definan las áreas de Ciberseguridad y Seguridad de la Información.
l. Monitoreo detectivo mediante Data Loss Prevention (DLP).
m. Enmascaramiento y anonimización de datos en algunos sistemas de información.

6.7. Confidencialidad

Al momento de la vinculación de un colaborador a PROTECCIÓN S.A., se suscribirá dentro de los formatos de ingreso, el acuerdo de confidencialidad y de manejo de información, dentro de los cuales el trabajador deberá informar que conoce, entiende y acepta la obligación de reserva que existe con la información a la que se tiene acceso durante la relación contractual al igual que los terceros que puedan tener acceso a los datos.

Adicionalmente, dentro de la inducción corporativa se exigirá a los nuevos colaboradores adelantar el curso de Protección de Datos, en el que se encuentra expuesta Política de Protección de Datos Personales.

6.8. Ejercicio del derecho de Habeas Data por los titulares

El Titular de datos personales privados o sensibles que considere que la información contenida o almacenada en una base de datos puede ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes y principios contenidos en la normatividad sobre protección de datos personales, podrán presentar

peticiones, quejas y denuncias siguiendo el procedimiento indicado en la Política de Protección de Datos Personales. En este sentido, la respuesta a dichos requerimientos quedará a cargo del área de Atención de Solicitudes o quien haga sus veces. Este equipo otorgará respuesta a través del medio que hubiera indicado el peticionario en su reclamación.

De no haber quedado explícito, se notificará a la(s) direcciones físicas o digitales que el usuario tenga registradas en Protección; sin embargo, en caso de no encontrar un mecanismo de comunicación con el interesado, se dejará la respuesta a disposición de los canales de atención, previendo un eventual contacto del solicitante con PROTECCIÓN S.A para requerir su respuesta.

6.9. Formación y cultura: En PROTECCIÓN S.A somos conscientes de que las políticas para ser verdaderamente robustas y efectivas deben contar con un programa de formación adecuado dirigido a los colaboradores, encargados y cualquier otra contraparte que tenga acceso a la información recopilada por la Administradora.

El Área de Cumplimiento Legal, estructurará anualmente un plan de Comunicación y Sensibilización con alcance al Programa de Protección de Datos Personales, el cual, contemplará las medidas de comunicación interna, externa y formación que se desplegarán en el año, relacionadas con la Protección de Datos Personales. Este Plan de Comunicación y Sensibilización, será presentado cada año al Comité de Ética de la organización para su aprobación.

Adicionalmente, de forma anual, el área de Talento y Cultura en conjunto con el equipo de Cumplimiento Legal impartirá una formación general en materia de datos personales a toda la Compañía, así mismo, desplegará capacitaciones focales a aquellos procesos que traten datos personales directamente, de acuerdo con sus funciones.

Entre otras acciones se enviará información como cápsulas informativas y noticias relevantes sobre el tratamiento de datos personales, se realizarán capacitaciones con los equipos que intervienen en el tratamiento de datos personales, se entregará documentación clara sobre el tratamiento y se realizará sensibilización permanente sobre los diferentes procesos procedimientos para el correcto tratamiento de los datos personales.

Al momento de ingresar nuevos colaboradores, en su contrato de trabajo o en documentos anexos, suscribirán acuerdos de cumplimiento de las políticas internas adoptadas en materia de tratamiento de datos personales.

Por su parte, se suministrará el material para realizar las acciones de comunicación y sensibilización con los proveedores y encargados externos de tratamiento de datos personales, con el apoyo del área de abastecimiento, con el fin de mantener alineadas a todas las contrapartes de la organización con la Política de Protección de Datos de PROTECCIÓN S.A.

6.10. Protocolo de respuesta en el manejo de violaciones e incidentes de seguridad en la información que involucren datos personales:

Teniendo en cuenta que las vulneraciones de nuestros códigos de seguridad en la información exacerban el riesgo de tratamiento indebido de los datos de los titulares, y eventualmente pueden impactar la reputación de PROTECCIÓN S.A., se ha definido un protocolo de respuesta conjunto entre las áreas responsables de propender la seguridad en la información y el debido tratamiento de datos personales, para atender de forma oportuna los incidentes y vulneraciones a los sistemas de información donde se almacenen datos personales.

En este sentido, PROTECCIÓN S.A dispone como área encargada a la Dirección de Riesgos de Negocio e Información, a quien en todos los casos, y de conformidad con las disposiciones de la Política de Seguridad en la Información y Ciberseguridad de la organización, es deber de todos los colaboradores reportar de forma inmediata todos los incidentes de fuga o pérdida de custodia de información, incluyendo aquellos que involucre datos personales, o cualquier otro evento en los sistemas de

información o bases de datos manuales o sistematizadas, que atente contra la seguridad de los datos personales en ellos almacenados.

En los casos en que la Dirección de Riesgo de negocio, confirme que el incidente involucra datos personales bajo la responsabilidad y custodia de PROTECCIÓN S.A., reportará el suceso al equipo de Cumplimiento Legal de forma inmediata, quien tiene el deber de estudiar el incidente, adquirir la mayor cantidad de información posible que permita conocer las causas del incidente, y en el caso que se confirme y se compruebe el incidente de seguridad, podrá determinar la oportunidad de notificar a los titulares de los datos, especificando los hechos ocurridos, las posibles consecuencias y los mecanismos que puede activar el titular para minimizar el daño potencial o causado por el responsable o encargado del tratamiento, en caso de que esto último sea posible.

Asimismo, el Área de Cumplimiento Legal, comunicará a la Superintendencia de Industria y Comercio dentro de los 15 días hábiles siguientes al momento del conocimiento del incidente por parte de la Dirección de Riesgo de Negocio, cuando se compruebe el acontecimiento y existencia del incidente. Este reporte debe contener la fecha de ocurrencia, fecha en la que se tuvo conocimiento de este, causal, tipo de datos personales comprometidos, la cantidad de titulares afectados, y se deberá realizar mediante el portal del Registro Nacional de Bases de Datos dispuesto por la autoridad

6.11. Gestión de los encargados y responsables del tratamiento en las transmisiones y transferencias de datos personales nacionales e internacionales:

En PROTECCIÓN S.A. somos conscientes de que, para el cumplimiento de nuestro objeto social, es necesario apoyarnos en terceros que realizan tareas con una experticia fundamental. Por esa razón, debemos transferir o transmitirles datos para que puedan lograr el encargo propuesto por nosotros como responsables del tratamiento de datos. Sin embargo, en esas operaciones se debe tener presente lo siguiente:

Es obligación de todos los colaboradores de PROTECCIÓN S.A. de informar y solicitar acompañamiento de forma previa al Área de Cumplimiento Legal, cuando se encuentre en el marco de una transferencia o transmisión de información personal a terceros. Este acompañamiento consistirá en revisar los aspectos relacionados con:

- La implementación de las medidas de seguridad de la información necesarias para garantizar su adecuado tratamiento.
- Si la transferencia es internacional, se debe verificar que la Superintendencia de Industria y Comercio ha incluido al país de domicilio del tercero, en la lista de países que ofrecen un nivel adecuado de protección de datos, o en su defecto, se deberá revisar la normativa vigente del país que recibe la información para incluir cláusulas contractuales con el tercero que blinden la transferencia de una forma más estricta.
- Suscribir el contrato de transferencia o transmisión, clausula contractual u otro instrumento jurídico que garantice la protección de los datos personales que se transfieren y regule las finalidades del encargo o transferencia, las condiciones de seguridad, custodia, y eliminación de la información personal.

Adicional a lo anterior, la Gerencia de Regulación velará por que, en el contrato o acuerdo de tratamiento de datos con el tercero, quede expresa la disposición de que el encargado o responsable, según sea el caso, cumplirá a cabalidad tanto la normatividad colombiana en materia de protección de datos, como las políticas de tratamiento de datos personales de PROTECCIÓN S.A. Así mismo, que se haga explícita la obligación del encargado o responsable, según sea el caso, de reportar a Protección como responsable, aquellos incidentes de seguridad con la información que hayan ocurrido, así mismo, en dicho contrato o acuerdo, se deberá incluir la divulgación y aceptación de la Política de Protección de Datos Personales, donde se encuentran los deberes de los encargados y/o terceros responsables.

El equipo de Abastecimiento y el proceso organizacional responsable de la transferencia o transmisión de datos personales deberán implementar mecanismos de monitoreo y seguimiento que permitan verificar que el tercero encargado o

responsable del tratamiento cumpla con las finalidades autorizadas y las condiciones establecidas en el acuerdo o contrato correspondiente.

En caso de identificar cualquier desviación en el uso de los datos personales —como finalidades no autorizadas o tratamientos no previstos—, dicha situación deberá ser reportada de forma inmediata al equipo de Cumplimiento Legal.

Para estos fines, el proceso organizacional responsable y el equipo de Abastecimiento podrán requerir al tercero toda la información que considere necesaria para verificar el cumplimiento de las finalidades pactadas y el uso adecuado de los datos personales.

6.12. Comunicaciones externas:

Es deber de la organización divulgar a Política de Protección de Datos Personales. Esta divulgación se realizará a través del Portal Web, en donde quedará a disposición de todos los interesados en el siguiente link: https://www.proteccion.com/contenidos/persona/cesantias/ley-proteccion-datos-personales

Esta política se encuentra en un lenguaje claro y comprensible para los titulares de los datos, pues esta tiene como objetivo informar de sus derechos de acceso, actualización, corrección, eliminación y revocatoria de la autorización; así como exponerles los mecanismos dispuestos para el ejercicio de tales derechos.

Adicionalmente, en virtud de la protección de la intimidad de los titulares, PROTECCIÓN S.A. ha definido adoptar las siguientes medidas aplicables a los procesos de contactabilidad de marketing, publicitario o de cobranza, de conformidad con la Ley 2300 de 2023:

- Horarios de contacto: De lunes a viernes de 7:00 am a 7:00 pm, sábados de 8:00 am a 3:00 pm, domingos y festivos no se podrán realizar contactos publicitarios, de marketing o de cobranza.
- Canales de contacto: El contacto con los titulares solo podrá efectuarse a través de los canales previamente autorizados por estos, asegurando su consentimiento informado. Durante una misma semana, se deberá utilizar exclusivamente un mismo canal de contacto por cliente.
- Periodicidad de contacto: No se podrá contactar a un mismo cliente más de una vez al día, incluso si el canal es el mismo. El principio de moderación y respeto a la privacidad debe prevalecer en todas las gestiones.

Estas disposiciones solo serán aplicables a las comunicaciones que sean consideradas de carácter publicitario, de mercadeo o de cobranza. Se entiende como comunicación o contacto publicitario o de mercadeo, cuando el contacto tenga la finalidad de ofrecer un producto o servicio, incidir en la toma de decisiones del consumidor, promover la imagen o reputación de la organización, y/o se relacionen con productos o servicios no adquiridos por el destinatario de la comunicación. Aquellas comunicaciones que sean solicitadas por el cliente, de carácter transaccional, que se relacionen con los productos o servicios ya adquiridos por el consumidor o sean obligatorias por mandato legal, no serán objeto de aplicación de las disposiciones aquí previstas.

6.13. Actualización del Registro Nacional de Bases de Datos:

- En Colombia, existe la obligación de realizar de forma periódica una actualización en el Registro Nacional de Base de Datos, dichas actualizaciones se darán en diferentes periodos del año de acuerdo con lo siguiente: Creación de nueva base de datos: en los casos donde se cree una base de datos que no se enmarque en las ya registradas, se deberá realizar el registro dentro de los primeros (10) diez días hábiles del mes.

- Cantidad de registros: cada año entre el 2 de enero y el 31 de marzo, se deberá realizar una actualización anual de la cantidad de registros que contienen la base de datos registrada, para esto, se deberá solicitar al responsable o administrador de cada base de datos, que se indique la cantidad de registros de la base de datos e ingresarlo en el Registro Nacional. Junto con la actualización de la base de datos, deberá actualizarse el listado de encargados del tratamiento de datos personales de dicha base de datos, y la demás información relacionada con la clasificación del tipo de datos almacenados, medidas de seguridad, entre otros aspectos requeridos.

- Reporte de PQR sobre los datos personales: esta actualización se debe realizar una vez por semestre, en el mes de febrero y agosto. En esta actualización se deberá ingresar la cantidad de reclamos interpuestos por los clientes, es decir, solicitudes de actualización, y/o consulta o eliminación de datos que se ingresaron en el semestre inmediatamente anterior.

- Reporte de incidentes: se deberá reportar dentro de los (15) quince días hábiles siguientes al conocimiento de la materialización d un incidente de seguridad que involucre datos personales.

- Cambios sustanciales: se deberá reportar los cambios relacionados con la finalidad, encargado del tratamiento, canales de atención al titular, clasificación del tipo de datos almacenados, medidas de seguridad, política de tratamiento o transmisión o transferencia de datos personales, en los (5) días hábiles siguientes al cambio sustancial desplegado.

Procedimiento interno para la actualización en el RNBD:

Con al menos 15 días de anticipación a la fecha en la que se debe remitir el reporte, el Analista de Cumplimiento Legal, deberá solicitar a las diferentes áreas la información requerida de acuerdo con el reporte que se debe realizar.

- Para actualización de bases de datos: se debe solicitar la cantidad de registros de personas naturales que se encuentran inscritos al momento de la actualización.
- Clientes: la información se recolecta con el equipo de Gestión de la Información.
- Proveedores: la información se recolecta con el equipo de Abastecimiento.
- Colaboradores: la información se recolecta con el equipo de Experiencia al Colaborador.
- Para el reporte de PQR sobre datos personales la información se recolecta con el Equipo de Atención de Solicitudes y PQR.
- Para el reporte de incidentes de seguridad, la información se recolecta con el equipo de Riesgo de Negocio – Seguridad en la Información y con el equipo de Ciberseguridad.

6.14. Inteligencia Artificial y Protección de Datos Personales:

Cualquier desarrollo con Inteligencia Artificial que se despliegue en la compañía, debe atender en todos los casos a criterios de idoneidad (capacidad para alcanzar el objetivo), necesidad (ausencia de alternativas menos intrusivas), razonabilidad (alineación con fines constitucionales) y proporcionalidad estricta (los beneficios no pueden superar el riesgo al Habeas Data).

En caso de que exista incertidumbre sobre posibles riesgos a la privacidad con la implementación de un desarrollo que implique Inteligencia Artificial en la organización, el responsable del desarrollo debe abstenerse de la ejecución de dicho desarrollo o adoptar medidas de prevención que protejan la dignidad y los derechos fundamentales de los titulares.

Antes de diseñar o desplegar este tipo de desarrollos, el responsable del desarrollo debe en todos los casos documentar un estudio de impacto respecto del riesgo de privacidad que describa detalladamente las operaciones de tratamiento de datos personales, evalúe y clasifique los riesgos para los derechos y libertades de los titulares, y defina medidas técnicas,

organizativas y de seguridad, incluyendo diseño de software y mecanismos preventivos, para mitigarlos. Para este tipo de revisiones, debe solicitar acompañamiento del equipo de Cumplimiento Legal.

Deberes en cuanto a los desarrollos con inteligencia artificial que involucren tratamiento de datos personales:

El responsable del desarrollo de forma previa a la producción debe:

- Cerciorarse de que los datos utilizados son veraces, completos, actualizados, comprobables y comprensibles; se prohíbe el tratamiento de información parcial o que induzca a error.
- Debe contemplar la incorporación de mecanismos que garanticen la conformidad del desarrollo con el Régimen de Protección de Datos Personales, lo previsto en la Política de Protección de Datos Personales de la organización, y en el presente manual de procedimientos internos.
- Debe verificar la existencia del otorgamiento de la autorización para el tratamiento de datos personales por parte de los titulares respecto de los cuales serán utilizados sus datos personales en el modelo de Inteligencia Artificial en desarrollo.
- En caso de que el desarrollo del modelo de Inteligencia Artificial requiera transmitir información personal de los titulares a terceros encargados del desarrollo, se deberá suscribir el respectivo Acuerdo de Tratamiento de Datos Personales con el tercero encargado del tratamiento, de conformidad con lo dispuesto en el capítulo "6.11. Gestión de los encargados y responsables del tratamiento en las transmisiones y transferencias de datos personales nacionales e internacionales" del presente manual de procedimientos internos. Lo anterior, con el acompañamiento de la Gerencia de Regulación y el equipo de Cumplimiento Legal.

7. EVALUACIÓN DEL PROGRAMA

El seguimiento y la evaluación del Programa de Protección de Datos Personales de la Compañía son fundamentales para determinar los resultados de su implementación. A continuación, se presentan las actividades de evaluación del Programa, que se deberán realizar al menos anualmente por parte del Área de Cumplimiento Legal.

De igual forma, el área de Auditoría Interna deberá realizar auditorías internas mínimo cada dos años al programa, de conformidad con lo establecido en su plan de auditoría.

7.1. Indicadores de efectividad del programa

Nivel de cumplimiento normativo: con este indicador se mide el grado en que la organización cumple con las Leyes y regulaciones del proceso de protección de datos personales. Se evalúa la documentación relacionada al proceso y la implementación del Programa en general.

El resultado para el presente indicador se medirá en porcentaje de 0% a 100%, partiendo de dos mediciones.

(I) Cumplimiento de la normatividad existente, tiene un peso del 80% sobre el resultado del indicador.
(II) Cumplimiento de la normatividad sugerida, tiene un peso del 20% sobre el resultado del indicador.

Incidentes de Seguridad de datos personales: El resultado esperado para el presente indicador deberá ser del 100%.

- Número de incidentes donde se comprometan datos personales al año / Total de incidentes reportados a la Superintendencia de Industria y Comercio en el año * 100.

PQRS: El porcentaje máximo aceptado para este indicador corresponderá al 100% para la respuesta a las PQR de titulares sobre sus datos personales recibidas durante el año.

- Tiempo legalmente establecido (10 días hábiles) / Promedio de días para la respuesta a peticiones de Consultas de datos personales * 100.
- Tiempo legalmente establecido (15 días hábiles) / Promedio de días para la respuesta a reclamos (actualización o supresión de datos personales) sobre el tratamiento de datos personales * 100.

Autorizaciones: Para los siguientes indicadores se requiere del 100% de las autorizaciones para el tratamiento de datos personales durante el año.

- Número de afiliados durante el año / Número de autorizaciones de tratamiento de datos personales durante el año * 100.
- Número de proveedores (Personas naturales) contratados durante el año / Número de autorizaciones de tratamiento de datos personales durante el año * 100.
- Número de colaboradores que ingresaron durante el año / Número de autorizaciones de tratamiento de datos personales durante el año * 100.

Capacitaciones: El resultado esperado del presente indicador deberá ser del 100%.

- Número de personas que aprobaron la capacitación anual sobre datos personales / Total de colaboradores * 100.
- Número de equipos con reunión de preguntas y respuestas/total de equipos que se presupuestaba impactar*100 (se tendrá en cuenta el cronograma de reuniones que se plantee en el año).

7.2. Acreditación del principio de responsabilidad demostrada

Para realizar un adecuado tratamiento de los datos personales, el Oficial de Protección de Datos Personales deberá validar los siguientes elementos de manera periódica:

- Revisar las actividades que generan algún tipo de tratamiento de los datos personales para tener un mapeo general y control del ciclo de vida de los datos personales.
- Validar los puntos de captura de información personal, identificando el tipo de información que se recolecta y sus finalidades, con el fin de mitigar riesgos sobre el tratamiento.
- Actualizar permanentemente el inventario de las bases de datos identificadas.
- Realizar seguimiento del cumplimiento de las medidas de seguridad de las bases de datos y repositorios de información que se encuentren en el inventario y en la matriz de riesgos.
- Identificar terceros que realizarán el tratamiento de datos personales para que se cumplan con los requisitos para compartir la información.
- Documentar y almacenar los procesos y actividades desplegadas.

Estos elementos son la base para la determinación e incorporación de coberturas jurídicas y técnicas de la compañía, para que se pueda llevar a cabo un adecuado tratamiento de los datos personales en cumplimiento de las disposiciones legales y reglamentarias.

Adicionalmente, como parte de un análisis integral, PROTECCIÓN S.A procurará mantener relaciones con terceros que reflejen un compromiso por la protección de los datos personales y la operación que ellos implican. Para este efecto, en los contratos que la compañía suscriba se incorporarán cláusulas de protección de datos personales, y adicionalmente, se podrá solicitar a los terceros en el desarrollo del vínculo comercial o contractual, información que permita validar el cumplimiento de las directrices contenidas en la Política de Protección de Datos Personales de la compañía, así como aquellas directrices legales y reglamentarias, cuando se estime necesario.

Los terceros que realicen un tratamiento de datos personales de los cuales la compañía es responsable, deberán acreditar el cumplimiento de los requisitos del régimen de protección de datos personales, aportando i) la política de protección de datos personales; ii) información sobre los canales habilitados para el trámite de consultas y reclamos y iii) el cumplimiento sobre

el registro y actualización de las bases de datos ante el Registro Nacional de Bases de Datos de la autoridad competente cuando sea necesario.

8. PLAN DE AUDITORÍA:

Se realizará una auditoría al menos cada dos años a este programa de la mano del área de Auditoría Interna, donde se definirá el plan de auditoría a realizar, el método, las responsabilidades y los informes a entregar.

Para cada auditoría se tendrá en cuenta:

- Realizar la auditoría de acuerdo con los criterios, objetivos y alcance de determinados.
- Realizar un plan de trabajo para cerrar las brechas encontradas y se establezca el plan de mejora continua.
- Documentar y almacenar todos los documentos respectivos.
- Los controles y documentos establecidos para el cumplimiento del programa.

9. MEJORA CONTINUA

Los lineamientos establecidos para la mejora continua del Programa Integral de Compliance de PROTECCIÓN S.A se aplicarán al presente programa, como parte integrante del mismo.

De forma anual, el equipo de Cumplimiento Legal realizará una actividad de monitoreo al cumplimiento normativo de los principales elementos del programa, para identificar brechas y oportunidades de mejora que sirvan para la actualización y propender la conformidad con los principales requisitos legales y mejores prácticas en la materia.

Control de cambios

Fecha de Actualización: diciembre 2025	**Nombre del documento** MANUAL DE PROCEDIMIENTOS INTERNOS PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES-PROTECCIÓN S.A.
Versión del manual	V3 - 2025
Persona que elaboró el documento	Daniel Ramírez Barrios – Analista de Cumplimiento Legal
Persona que revisó el documento	Juan Felipe Moreno – Oficial de Cumplimiento
Persona que aprobó el documento	Juan Pablo Arango – Representante Legal

Principales cambios de la versión	Se actualiza la descripción del objetivo del manual y se ajustan redacciones generales para mayor entendimiento del documento. Se incluye lo relativo a la metodología de gestión de riesgos y matriz de riesgos. Se modifican algunas definiciones. Se incluye el desarrollo del principio de privacidad por diseño en las operaciones de transferencia o transmisión de datos personales. Se especifica la obligación de Regulación de acompañar la suscripción de los acuerdos de tratamiento de datos personales. Se incluyen los horarios, periodicidad y canales previstos por la Ley 2300 de 2023 para los contactos publicitarios, de marketing o de cobranza. Se integra el procedimiento en el marco de desarrollos que involucren modelos de inteligencia artificial y que involucren el tratamiento de datos personales de conformidad con las recomendaciones de la SIC. Se integra la estructuración y aprobación del plan de comunicación y sensibilización anual. Se integra en las funciones del oficial de cumplimiento, el deber de acompañar la estructuración de nuevos productos, soluciones y servicios desde su diseño. Se integra el deber de validar con el Área de Cumplimiento Legal, desde el diseño, los nuevos flujos de autorización para el tratamiento de los datos personales. Se incluyen expresamente los deberes de los colaboradores en cada etapa del ciclo de vida del dato personal, y su incumplimiento, como un incumplimiento al contrato laboral. Se integra lo relativo a la autorización, finalidades y políticas de terceros receptores de información para el ecosistema Open Finance. Se incluye la actividad de monitoreo a los elementos del programa, como proceso de mejora continua. Se aclara el apartado de autorización de tratamiento de datos de menores de edad y tratamiento de datos sensibles. Se adicionan algunas medidas de seguridad en la información. Se identifica en mayor medida la obligación de la Auditoría Interna de evaluar el programa de forma periódica conforme su plan de auditoría. Se estructura el protocolo y paso a paso para la gestión de incidentes de seguridad en la información que involucren datos personales.

	Se actualiza lo relativo al plazo de conservación de los datos personales.