1. CARACTERIZACIÓN DE LA POLÍTICA

- Nivel de la Política: Estratégico
- Tipo Normativo: Si
- Procesos Asociados del Sistema de Gestión Integral: Administrar el Sistema de Gestión de Seguridad de la Información

2. OBJETIVOS DE LA POLÍTICA

Establecer un marco estratégico de acción para la protección de la información de la Compañía y el tratamiento de datos personales, mediante la definición de directrices que permitan encaminar el manejo de los mismos en condiciones de seguridad, ciberseguridad y calidad.

3. ALCANCE DE LA POLÍTICA

La presente política tiene como alcance todos los procesos, funcionarios y partes interesadas y en general a quienes tienen acceso a la información crítica y sensible de la compañía.

4. MARCO NORMATIVO Y REGLAMENTARIO

Esta política fundamenta su enfoque metodológico en el modelo conceptual proporcionado por las Normas ISO 27001 e ISO 27032, los cuales proporcionan una base sólida para la gestión de la seguridad de la información, lo que ayuda a proteger los activos de información crítica y a mantener la confianza de las partes interesadas.

4.1. MARCO NORMATIVO

La Política de Seguridad de la Información y Ciberseguridad de LA PREVISORA S.A., busca el cumplimiento de los requerimientos regulatorios emitidos por la Superintendencia Financiera de Colombia (SFC), Ministerio de Tecnologías de la Información y las Comunicaciones y demás normas aplicables a la entidad:

- **Ley 1266 de 2008:** Reconoce y protege el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

- **Ley 1581 de 2012:** Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

- **Circular Básica Jurídica 029 de 2014 de la SFC:** Parte I – Título II – Capítulo I Canales, Medios, Seguridad y Calidad en el Manejo de Información en la Prestación de Servicios Financieros y demás requerimientos regulatorios aplicables de las circulares emitidas por la SFC.

- **Circular Externa 007 de 2018:** Imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad.

- **Resolución 500 de 2021 de MinTIC:** Establece los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

- **Resolución 746 de 2021 de MinTIC**: Crea una nueva normativa que adiciona lineamientos y estándares relacionados con los proveedores de productos y servicios de seguridad digital y con la Protección de los Datos Personales.

- **Circular Externa 008 de 2023 de la SFC:** Imparte instrucciones en materia de Sistema de Control Interno de las entidades vigiladas.

- **Carta Circular No.14 de 2024 de la SFC:** Obligaciones de las entidades vigiladas para garantizar el derecho fundamental de habeas data a los titulares de la información sobre datos financieros, crediticios, comerciales, de servicios y proveniente de terceros países.

5. DESCRIPCIÓN POLÍTICA

PREVISORA S.A., reconoce la información como un activo de vital importancia para el desarrollo de su misión y cumplimiento de los objetivos estratégicos, por lo cual establece un Sistema de Gestión en Seguridad de la Información, Ciberseguridad y de Protección de Datos Personales, que provee un proceso de mejora continua enfocado a la gestión de riesgos, donde participan y tienen responsabilidad todos los funcionarios y partes interesadas de la compañía.

Este sistema de gestión se enmarca en el desarrollo y mantenimiento de la política de Seguridad Digital de la compañía, contemplada dentro de la dimensión tres: "Gestión con valores para resultados del Modelo Integrado de Planeación y Gestión – MIPG", así como en la política del Sistema de Gestión Integral de la PREVISORA S.A, en su numeral 7:

7. *Realizar las acciones pertinentes en materia de seguridad y ciberseguridad para mantener la integridad, confidencialidad y disponibilidad de la información de la compañía*

De igual manera, se encuentra articulado el compromiso de la Alta Dirección, así como todos los colaboradores independientemente de su forma de contratación o vinculación a los objetivos para con este sistema en el objetivo número 9 del Sistema de Gestión Integral SIG, así:

9. Mitigar los riesgos de seguridad de la información mediante su adecuada gestión para preservar los activos de información que soportan la operación de la compañía.

Así mismo, el sistema de gestión propende porque la Seguridad de la Información, la Ciberseguridad y la Protección de Datos Personales sean elementos habilitadores del negocio, apoyando el cumplimiento de los objetivos y metas de la compañía. Tiene como objetivo general proteger la integridad, confidencialidad y disponibilidad de la información y de sus activos físicos y digitales.

A continuación, se listan los principios y lineamientos que consolidan la Política Integral de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales de La PREVISORA S.A.:

a. Principios para la gestión de la Seguridad de la Información, Ciberseguridad y Protección de Datos Personales

I. La PREVISORA S.A., se compromete a preservar la seguridad (confidencialidad, integridad y disponibilidad) y la calidad (efectividad, eficiencia y confiabilidad) de la información de la Compañía, protegiéndola contra amenazas internas y/o externas, mediante la implementación de controles que permiten reducir los riesgos de seguridad de la información y de ciberseguridad, a un nivel aceptable para la Compañía.

II. La PREVISORA S.A., identificará todos los recursos relacionados con el ciclo de vida de la información, los cuales son denominados activos de información. El listado de los activos de información deberá cubrir el alcance de la Política de Seguridad de la Información y Ciberseguridad aquí descrito.

III. Los Activos de Información de criticidad alta, deberán ser evaluados en términos de los riesgos de seguridad de la información y ciberseguridad. El análisis de riesgos se realizará periódicamente o de forma no programada de acuerdo con los cambios organizacionales que se den en la Compañía.

IV. Las actividades de análisis de riesgos en Seguridad de la Información y Ciberseguridad de la Compañía permitirán la definición de medidas de control a desarrollar por parte de los procesos de negocio para la mitigación de la probabilidad y/o impacto de los escenarios de riesgo identificados.

V. La PREVISORA S.A., tratará los datos personales de manera adecuada y responsable, cumpliendo a cabalidad con lo estipulado en las Leyes 1266 de 2008 y 1581 de 2012 y sus decretos reglamentarios, sin realizar algún tratamiento adicional a las finalidades autorizadas por el cliente y/o los titulares de la información.

Con el fin de afianzar el cumplimiento de estos principios, La Junta Directiva expresa su compromiso, designando recursos humanos, técnicos y financieros para tal fin.

b. Roles y responsabilidades

Las responsabilidades y funciones asociadas al Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales se encuentran especificadas en el "MN-108 Manual de Roles y Responsabilidades de Seguridad de la Información y Ciberseguridad" y en el "MN-114 Manual General para la Protección de Datos Personales". A continuación, se enumeran los roles principales junto con sus responsabilidades más relevantes:

I. **Junta Directiva:** Tiene la responsabilidad de aprobar la presente política y de hacer seguimiento al cumplimiento de la misma, así como de tomar decisiones adecuadas en materia de seguridad de la información, ciberseguridad y de protección de datos personales.

II. **Comité de auditoría**: Tiene como función de revisar y recomendar ajustes a la Política integrada de seguridad de la información, ciberseguridad y protección de datos personales, antes de ser aprobada por la Junta Directiva.

III. **Comité de Seguridad:** Tiene lugar en el comité de presidencia y entre otros, aprobará las políticas de segundo nivel y el manual de roles y responsabilidades del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, en el cual se especifican los roles, responsabilidades y funciones de todos los actores del sistema incluidos los de la unidad para la gestión del riesgo de seguridad de la información y ciberseguridad.

IV. **Oficial / Comité de Protección de Datos Personales**: Realiza la supervisión y es el encargado de hacer exigible el cumplimiento del régimen de protección de datos personales en la Compañía.

V. **Unidad de seguridad de la información y Ciberseguridad:** Encargado de realizar una gestión efectiva de la seguridad de la información y la Ciberseguridad de la compañía. Es liderada por el Gerente de Riesgos (Oficial de Seguridad de la Información) y el Gerente de Tecnología de la Información (Oficial de Seguridad Informática).

VI. **Líderes de proceso:** Son responsables de los activos de información que se identifiquen a su cargo.

VII. **Todos los funcionarios y partes interesadas de la compañía:** Conocer, aplicar y cumplir las responsabilidades que les atañen para la preservación de la seguridad de la información y la ciberseguridad de los activos de información de la compañía.

c. Procesos, procedimientos y etapas para la gestión de la Seguridad de la Información y la Ciberseguridad.

El Sistema de Gestión de Seguridad de la Información y Ciberseguridad, cuenta con procesos y procedimientos documentados, en los cuales se establecen los lineamientos para desarrollar cada una de las etapas de gestión que se identifican a continuación:

- **Prevención:** Capacidad de limitar o contener el impacto de un posible incidente de seguridad de la información o de ciberseguridad.

- **Protección y detección:** Permitir el descubrimiento oportuno de eventos e incidentes de seguridad de la información y ciberseguridad y cómo protegerse ante los mismos.

- **Respuesta y comunicación**: Desarrollar e implementar actividades para mitigar los incidentes relacionados con seguridad de la información y ciberseguridad.

- **Recuperación y aprendizaje:** Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de seguridad de la información y Ciberseguridad.

d. Cultura de Seguridad de la Información, Ciberseguridad y de Protección de Datos Personales

La PREVISORA S.A., se compromete a promover una cultura de seguridad de la información, ciberseguridad y de protección de datos personales, desarrollando actividades de difusión, capacitación y concientización, tanto al interior de la compañía como frente a usuarios, terceros y partes interesadas relevantes dentro de la política integrada.

e. Manejo de excepciones

Las excepciones a cualquiera de las directrices de esta política o sus políticas derivadas serán admitidas únicamente cuando el Oficial de Seguridad de la Información avale y divulgue su aceptación. Las excepciones a los lineamientos existentes deben estar sustentadas sobre la base de un análisis de riesgos aplicable.

f. Vigencia de la política

Esta política se encuentra inmersa en el proceso de mejora continua del Sistema Integral de Gestión de la Compañía, por tal razón se revisará cuando sea requerido, conforme los cambios organizacionales que se den en el transcurso del tiempo o en su defecto una vez cada dos años.

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE (S)	SANDRA CEDIEL B.	DAVID MARÍN VILLA	JUNTA DIRECTIVA
CARGO (S)	ESPECIALISTA GERENCIA DE RIESGOS	GERENTE DE RIESGOS (e)	JUNTA DIRECTIVA

CONTROL DE CAMBIOS	
VERSIÓN	**CAMBIOS REALIZADOS**
4	Se actualiza el documento
5	Se revisa el documento – No se generan cambios. La política es aprobada por JD en la sesión del 27-02-2023
6	Actualización y alineación con CE 008 de 2023 de la SFC y sistema de protección de datos personales. Articulación de esta política con la general del SIG y el marco MIPG. Aprobado por JD en la sesión del 30-05-2024