CIRCULAR ASUNTO: POLÍTICA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE PREVISORA S.A.			
CÓDIGO: CIR-320	**ÁREA EMISORA:** PRESIDENCIA	**FECHA:**	
VERSIÓN: 4	**CREA** ☑ **MODIFICA** ☐ **MANUAL** ☐ **NORMA** ☑ **PROCEDIMIENTO** ☐		
Documento de Uso Interno			

PARA: TODOS LOS FUNCIONARIOS Y PARTES INTERESADAS DE PREVISORA S.A

OBJETIVO: Establecer un marco estratégico de acción para la protección de la información de la Compañía, mediante la definición de directrices que permitan encaminar el manejo de la misma en condiciones de seguridad, ciberseguridad y calidad.

ALCANCE: Esta política aplica a todos los procesos de la Compañía, sus funcionarios y todas las partes interesadas que tienen acceso a la información de la compañía.

NORMA: La Política de Seguridad de la Información y Ciberseguridad de LA PREVISORA S.A., busca el cumplimiento de los requerimientos regulatorios aplicables de las circulares emitidas por la Superintendencia Financiera de Colombia (SFC) y define como base metodológica el modelo conceptual de las Normas ISO/IEC 27001 e ISO 27032.

POLÍTICA GENERAL

PREVISORA S.A., reconoce la información como un activo vital y estratégico 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 y Ciberseguridad, que provee un proceso de mejora continua con enfoque a riesgos, donde participan y tienen responsabilidad todos los funcionarios y partes interesadas de la compañía.

Este sistema de gestión propende porque la Seguridad de la Información y la Ciberseguridad sean elementos habilitadores del negocio, apoyando el cumplimiento de los objetivos y metas de la compañía y tiene como objetivo general proteger la integridad, confidencialidad y disponibilidad de la información de la entidad, así como de sus activos en el ciberespacio.

A continuación, se listan los principios y lineamientos que consolidan la Política General de Seguridad de la Información y Ciberseguridad de La PREVISORA S.A., los cuales han sido ratificados por la Junta Directiva de la entidad.

a) Principios para la gestión de la Seguridad y Calidad de la Información

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 tendientes a reducir los riesgos de seguridad de la información y ciberseguridad identificados, que afecten la información y los medios de procesamiento, llevando estos riesgos a los niveles aceptables para la Compañía.

II. La PREVISORA S.A., identificará todos los recursos relacionados con el ciclo de vida de la información, a los cuales denominará 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 de La PREVISORA S.A., deberán ser evaluados en términos de riesgos de seguridad de la información y ciberseguridad. Los análisis de riesgos se realizarán periódicamente o de forma no programada sujeto a los cambios organizacionales que se den en la Compañía.

IV. Las actividades de análisis de riesgo 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 en probabilidad y/o impacto de las situaciones de riesgo identificadas.

b) Roles y responsabilidades

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 y de ciberseguridad.

II. 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.

III. Unidad de seguridad de la información y Ciberseguridad: Debe 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).

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

V. 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 y Ciberseguridad

La PREVISORA S.A.**,** se compromete a promover una cultura de seguridad de la información y ciberseguridad desarrollando actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros relevantes dentro de la política de seguridad de la información y ciberseguridad.

e) Revisión

I. Esta política se encuentra inmersa en el proceso de mejora continua del Sistema de Gestión de Seguridad de la Información, 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.

f) Manejo de Excepciones

I. Las excepciones a cualquiera de las directrices de la Política de Seguridad General 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.