Manual de Normas Política General de Seguridad de la Información y Ciberseguridad

Gerencia de Riesgo de Negocio

Ficha Técnica del Documento			
Código:	**N-09-SC-RO-SI-03**	**Versión:**	2.0
Fecha de Emisión:	28 de Noviembre de 2018	**Fecha de Vigencia:**	10/05/2023
Proceso:	Control y Seguimiento	**Clasificación de la Información:**	De uso interno
Subproceso:	Administración Riesgo de Seguridad de Información		

CONTENIDO

1. INTRODUCCIÓN

En Porvenir la información es reconocida como uno de los activos más valiosos e importantes; la cual soporta la gestión de los procesos definidos internamente, por esta razón es necesario contar con estrategias que permitan el control y gestión efectiva de la información, preservando su confidencialidad, integridad y disponibilidad.

La Compañía cuenta con la definición de un Sistema de Gestión de Seguridad de la Información y Ciberseguridad, del cual hace parte el Manual de Políticas de Seguridad de la Información y Ciberseguridad que contiene la política general y las políticas específicas, como una declaración de las responsabilidades y conductas aceptadas para mantener la confidencialidad, integridad y disponibilidad de la información que son esenciales para la operación de la Compañía, y el desarrollo de capacidades para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, infraestructura, sistemas y aplicaciones en el ciberespacio. Igualmente contempla la definición de directrices y lineamientos relacionados con el manejo adecuado de la información para gestionar efectivamente los riesgos de seguridad de la información y ciberseguridad, afianzando de esta forma la cultura y concienciación en estos conceptos.

La Política General de Seguridad de la Información y Ciberseguridad, definida por la Alta Dirección y aprobada por la Junta Directiva, constituye el pilar principal del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, y se toma como base para la definición e implantación de controles, toma de decisiones de seguridad de la información y ciberseguridad, y para el desarrollo de las capacidades para enfrentar las crecientes amenazas cibernéticas.

2. OBJETIVO

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad de la información de la Compañía, definiendo lineamientos orientados a regular la gestión de la seguridad de la información y la ciberseguridad al interior de la Compañía.

3. ALCANCE

La Política General de Seguridad de la Información y Ciberseguridad, así como todos los documentos de apoyo al Sistema de Gestión de Seguridad de la Información y Ciberseguridad son un mandato general y aplica a:

- Todos los procesos de la Compañía.

- Todos los niveles de la Compañía, usuarios, clientes, terceros (proveedores, contratistas), entes de control y filiales que acceden interna o externamente a la información, presten servicios o tengan cualquier vínculo con los activos de información de la Compañía.
- Todos los proyectos asociados a la implementación y al uso de tecnologías de información para operar los procesos del negocio o para la prestación de los servicios de la Compañía.
- Toda información creada, procesada, almacenada, intercambiada o utilizada en el soporte de la Compañía, sin importar el medio, formato, ubicación a través de su ciclo de vida, incluyendo creación, distribución, almacenamiento y disposición final, priorizando su protección acorde a la clasificación de la misma.

4. POLÍTICA

PORVENIR S.A., compañía dedicada a contribuir al crecimiento del ahorro de sus afiliados, apoyándolos durante todas las etapas de su vida, define sus procesos y presta sus servicios de una manera amable y segura, ofreciendo altos niveles de confianza durante la administración de los recursos de sus clientes.

Para Porvenir, la información es catalogada como uno de los activos fundamentales y estratégicos para la prestación de los servicios y la toma de decisiones eficientes; por lo cual la Compañía está comprometida con el adecuado cuidado y gestión de la información propia y de los clientes mediante la adopción y aplicación de marcos regulatorios, alineado con las mejores prácticas o estándares internacionales de seguridad de la información y de ciberseguridad, encaminando sus esfuerzos en pro del mantenimiento de la Confidencialidad, Integridad, Disponibilidad y Privacidad de sus activos de información tanto On Premise como en Nube.

La Junta Directiva y la Alta Dirección mediante la aprobación de esta Política declaran su posición y compromiso con el cumplimiento de los requisitos definidos en el marco del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, aspectos en los cuales se involucra directamente la función de seguridad de la información y ciberseguridad, que tiene como propósito principal mantener un ambiente razonablemente seguro, alineado a la misión, objetivos estratégicos de Porvenir y requerimientos regulatorios aplicables, definiendo e implementando buenas prácticas que permitan minimizar posibles impactos no deseados que puedan comprometer los principios esenciales de la seguridad de la información.

5. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de Porvenir S.A., evidencia y fortalece su compromiso con el Sistema de Gestión de Seguridad de la Información y Ciberseguridad de la siguiente manera:

- Aprobación de la Política de Seguridad de la Información y Ciberseguridad.
- Proporcionando los recursos adecuados para la operación, mantenimiento y mejoramiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, al igual que los recursos necesarios para verificar de manera periódica el cumplimiento de las obligaciones y medidas adoptadas para la gestión de los riesgos de seguridad de la información y Ciberseguridad.
- Apoyando la creación, conformación y asignación de funciones del Comité de Seguridad de la Información y Ciberseguridad, y de la unidad que gestiona los riesgos de seguridad de la información y la Ciberseguridad.
- Fortaleciendo la gestión de los riesgos de seguridad de la información y de Ciberseguridad.
- Apoyando el desarrollo de competencias y capacidades de resiliencia cibernéticas en los colaboradores que realizan la gestión de los riesgos de seguridad de la información y de ciberseguridad.
- Promoviendo la cultura de seguridad de la información y ciberseguridad.
- Apoyando la divulgación de las políticas y demás lineamientos de seguridad de la información y ciberseguridad.
- Promoviendo la gestión de seguridad de la información y la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.
- Promoviendo la adopción, aplicación y apropiación de buenas prácticas de seguridad de la información y ciberseguridad con el fin de proporcionar productos y servicios seguros en el ciberespacio.
- Revisando periódicamente los indicadores para medir la eficacia y eficiencia de la gestión de seguridad de la información y la ciberseguridad.
- Promoviendo la interacción, colaboración y cooperación a nivel corporativo para el desarrollo de medidas preventivas y de respuesta ante eventos o incidentes de seguridad de la información y ciberseguridad.
- Estableciendo una estrategia de comunicación e información sobre incidentes de ciberseguridad para reporte a la SFC, autoridades competentes y al consumidor financiero.
- Colaborando con los organismos y agencias gubernamentales relevantes para la mejora de la ciberseguridad de la Compañía, el cumplimiento de la legislación vigente y contribuir a la mejora de la ciberseguridad en el ámbito nacional.

6. VIGENCIA Y ACTUALIZACIÓN DE LA POLÍTICA

La Política General de Seguridad de la Información y Ciberseguridad será revisada anualmente o cuando se identifiquen cambios en la estructura, objetivos o alguna condición que afecte la política, con el fin de asegurar que se encuentra ajustada a los requerimientos o necesidades de la Compañía. La aprobación de las actualizaciones o modificaciones se realizará por parte de la Junta Directiva previa revisión del Comité de Presidencia y del Comité de Seguridad de la Información y Ciberseguridad.

Esta política rige a partir de la fecha de publicación y lo dispuesto aquí es de obligatorio cumplimiento según alcance definido.

7. NORMATIVIDAD EXTERNA

- Circular Externa de la Superintendencia Financiera de Colombia 005 de 2019.
- Circular Externa de la Superintendencia Financiera de Colombia 007 de 2019.

Flujo Documental

Elaboró	Revisó	Aprobó
Nombre: María Gabriela Rodríguez Jiménez **Cargo:** Analista II de Seguridad de la Información y Ciberseguridad (Gobierno) **Fecha: 10/05/2023** **Nombre: Carlos Alberto Alzamora Parra** **Cargo:** Consultor Senior Innovación y Transformación Digital MO **Fecha: 10/05/2023**	**Nombre:** Marco Andres Rojas Mirquez **Cargo:** Analista III de seguridad de la Información y Ciberseguridad (Estrategia) **Fecha:**10/05/2023	**Nombre:** Diana Marcela Bonilla Perez **Cargo:** Director de Seguridad de la Información y Ciberseguridad **Fecha:** 10/05/2023 **Nombre:** Yamile Guerrero **Cargo:** Gerente de Riesgo de Negocio **Fecha:** 10/05/2023 **Nombre:** Junta Directiva **Fecha:** 10/05/2023 Aprobación Socialización

Registro de Actualización

El presente manual de normas ha sido modificado en los numerales descritos a continuación:

No.	Numeral / Título	Descripción de la Actualización	Fecha de Actualización
1.0	Todo el documento	Se crea el presente documento en reemplazo del Manual de Normas Política General de Seguridad de la Información. Se actualiza la política ampliando su alcance a Ciberseguridad, así como los compromisos de la alta dirección.	28 de Noviembre de 2018
2.0	Política	Se incluye la aplicación de nube teniendo en cuenta que ya se encuentra en estado de implementación y gestión en la compañía. Se incluye normatividad externa mencionando la C.E de SFC 005 de 2019 y la C.E de SFC 007 de 2019.	10 de mayo 2023