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

Gerencia de Riesgo de Negocio

Ficha Técnica del Documento			
Código:	**N-09-SC-RO-SI-03**	**Versión:**	5.0
Fecha de Emisión:	28 de Noviembre de 2018	**Fecha de Vigencia:**	18 jun 2025
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, disponibilidad y privacidad.

La Compañía cuenta con la definición de un Sistema de Gestión de Seguridad y Privacidad de la Información y Ciberseguridad, del cual hace parte el Manual de Políticas de Seguridad y Privacidad 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, disponibilidad y privacidad 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 y Privacidad 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 y Privacidad de la Información y Ciberseguridad, y se toma como base para la definición e implantación de controles, toma de decisiones de seguridad, la privacidad de la información y la ciberseguridad, y para el desarrollo de las capacidades para enfrentar las crecientes amenazas cibernéticas.

2. OBJETIVO

Lograr niveles adecuados de integridad, confidencialidad, disponibilidad y privacidad 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 y Privacidad de la Información y Ciberseguridad, así como todos los documentos de apoyo al Sistema de Gestión de Seguridad y Privacidad 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 recolectada, almacenada, procesada, utilizada, conservada o intercambiada en el soporte de la Compañía, sin importar el medio, formato, ubicación a través de su ciclo de vida, incluyendo distribución, eliminación y disposición final, priorizando su protección acorde a la clasificación de la misma y bajo los principios de ciclo de vida del dato.

4. POLÍTICA

4.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

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, normativos y legales, alineado con las mejores prácticas o estándares internacionales de seguridad de la información, ciberseguridad y protección de la privacidad de la información 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 derivados de un riesgo no deseado que puedan comprometer los principios esenciales de la seguridad y privacidad de la información.

4.2 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Porvenir, como entidad Responsable del tratamiento de datos personales, reafirma su compromiso con la protección de los datos de nuestros usuarios. Por ello, se implementó La Política de Tratamiento de Datos Personales de Porvenir la cual está disponible para

nuestras partes de interés en nuestro sitio web: www.porvenir.com.co. Este documento es esencial, ya que explica de manera clara cómo recopilamos, utilizamos, almacenamos y protegemos la información personal de nuestras partes interesadas. También establece los derechos que tienen en relación con sus datos, garantizando que estén informados sobre el manejo de su información y puedan ejercer sus derechos de manera efectiva.

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 y Privacidad de la Información y Ciberseguridad de la siguiente manera:

- Aprobar la Política de Seguridad de la Información y Ciberseguridad y de la Política de Tratamiento de Datos Personales.
- Proporcionar los recursos adecuados y necesarios para el desarrollo e implementación de iniciativas de Seguridad y Privacidad de la Información y Ciberseguridad para la operación, logrando así, el mantenimiento y mejoramiento del Sistema de Gestión de Seguridad y Privacidad 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 y privacidad de la información y Ciberseguridad.
- Apoyar a los cargos gerenciales para ejercer liderazgo en las áreas relacionadas con el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), que permitan promover el cumplimiento sobre lo mencionado en la norma ISO/IEC 27001:2022 y norma ISO/IEC 27701:2020.
- Promover el cumplimiento de las políticas y normas definidas en el Sistema de Gestión de Seguridad y Privacidad de la Información.
- Apoyar 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.
- Fortalecer la gestión de los riesgos de seguridad y privacidad de la información y de Ciberseguridad (pérdida de confidencialidad, disponibilidad, privacidad e integridad).
- Apoyar el desarrollo de competencias y capacidades de resiliencia cibernéticas al igual que capacidades orientadas en el tratamiento y manejo de datos personales en los colaboradores que realizan la gestión de los riesgos de seguridad y privacidad de la información y de ciberseguridad.
- Promover la cultura de seguridad y privacidad de la información y ciberseguridad.
- Apoyar la divulgación de las políticas y demás lineamientos de seguridad y privacidad de la información y ciberseguridad.

- Promover la gestión de seguridad y privacidad de la información y la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.
- Promover la adopción, aplicación y apropiación de buenas prácticas de seguridad y privacidad de la información y ciberseguridad con el fin de proporcionar productos y servicios seguros en el ciberespacio que protejan la integridad del dato.
- Revisar periódicamente la medición de los indicadores para determinar la eficacia y eficiencia de la gestión de seguridad y privacidad de la información y la ciberseguridad.
- Promover 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 y/o que tengan impacto con datos personales.
- Establecer una estrategia de comunicación e información sobre incidentes de ciberseguridad para reporte a la SFC, autoridades competentes y al consumidor financiero.
- Colaborar 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.
- Promover la mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) de acuerdo con las nuevas tecnologías y metodologías que se adquieran tanto para seguridad como privacidad de la información.

6. RESPONSABILIDADES DE LOS USUARIOS

Porvenir tiene estructuradas las funciones y responsabilidades frente al Riesgo de Seguridad y Privacidad de la Información y Ciberseguridad y su respectiva gestión, protegiendo así, los activos de información tanto críticos como no críticos para la operación del negocio, como los datos personales procesados por la Entidad de acuerdo con la Ley 1581 del 2012. A continuación, se observa el esquema de las tres líneas, considerando:

- La gestión por la línea de negocio,
- Una función de gestión de riesgos de Seguridad y Privacidad de la Información y Ciberseguridad independiente, y
- Una revisión independiente.

6.1 Primera Línea

La primera línea la constituyen la Dirección de Seguridad Informática – Comunicaciones y todos los colaboradores de Porvenir. La Política de Seguridad de la Información y Ciberseguridad reconoce a la Dirección de Seguridad Informática y demás colaboradores como responsables en primera medida de identificar, evaluar, gestionar, monitorear y reportar los riesgos e incidentes de Seguridad de la Información y Ciberseguridad

inherentes a los productos, servicios, actividades, procesos y sistemas de seguridad. Quienes conforman esta línea de defensa deben conocer sus actividades y procesos, y disponer de los recursos suficientes para realizar eficazmente sus tareas.

Así mismo, deben cumplir con las políticas, guías y procedimientos definidos por la compañía, contribuyendo a una sólida cultura de Seguridad de la Información y Ciberseguridad.

Para el cumplimiento de la primera línea sobre la privacidad de la información, consultar el Manual Interno Políticas y Procedimientos Sistema de Gestión de Privacidad de la Información.

6.2 Segunda Línea

Esta línea está conformada por la Dirección de Seguridad de la Información y Ciberseguridad, la cual establece los lineamientos en esta materia y realiza un seguimiento continuo al cumplimiento de todas las obligaciones de riesgo en Seguridad de la Información y Ciberseguridad. El director es el responsable de presentar los resultados de gestión directamente a la Alta Dirección, Comité de Riesgos, Junta Directiva o demás instancias a consideración. Debe contar con recursos suficientes para realizar eficazmente todas sus funciones y desempeñar un papel central y proactivo en el Sistema de Gestión de Seguridad de la Información y Ciberseguridad, para ello, debe estar plenamente familiarizado con las políticas y normas vigentes, sus requisitos legales y reglamentación y los riesgos de Seguridad de la Información y Ciberseguridad derivados del negocio.

Para el cumplimiento de la segunda línea sobre la privacidad de la información, consultar el Manual Interno Políticas y Procedimientos Sistema de Gestión de Privacidad de la Información.

6.3 Tercera Línea

La tercera línea juega un papel importante al evaluar de forma independiente la gestión y los controles de los riesgos de la Seguridad de la Información y Ciberseguridad, así como las políticas, estándares, guías y procedimientos de los sistemas, rindiendo cuentas al Comité de Auditoría o al que se designe. Las personas encargadas de auditorías internas que deben realizar estas revisiones deben ser competentes y estar debidamente capacitadas y no participar en el desarrollo, implementación y operación de la estructura de riesgo/control. Esta revisión puede ser realizada por el personal de auditoría o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados.

Para el cumplimiento de la tercera línea sobre la privacidad de la información, consultar el Manual Interno Políticas y Procedimientos Sistema de Gestión de Privacidad de la Información.

7. REQUISITOS APLICABLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Porvenir reconoce la importancia de proteger adecuadamente la información de amenazas que puedan afectar la continuidad del negocio, por lo anterior establece el desarrollo de actividades para la protección de los activos de información, gestión y administración de riesgos de Seguridad de la Información y ciberseguridad, protección de datos personales, cultura de seguridad y las conductas que deben adoptar todos los Colaboradores y sus subordinada, por consiguiente, todos los funcionarios temporales y proveedores que en el ejercicio de sus actividades utilicen información y servicios tecnológicos en el Porvenir y sus subordinadas deben velar por: el cumplimiento de los requisitos y pilares de la seguridad de la información y ciberseguridad, protegiendo los activos de información de la organización, preservando la confidencialidad, integridad, disponibilidad y privacidad de la información; por lo anterior, Porvenir y sus subordinadas acogen las siguientes políticas sobre las cuales se fundamenta y estructura el Sistema de Gestión de Seguridad de la Información (SGSI). Tales Políticas son expresiones de la Alta Dirección para una presentación y valoración justa y transparente de riesgos de seguridad de la información y ciberseguridad. Lo anterior permite hacer una adecuada identificación de los controles que mitigan razonablemente los riesgos identificados.

7.1 Proteger la confidencialidad, integridad, disponibilidad, privacidad y no repudio de la información

Todos los Colaboradores de Porvenir y sus subordinadas deben proteger y asegurar, la confidencialidad, integridad, disponibilidad y privacidad de la información, de tal manera que la información:

- Solo sea accedida por personal autorizado.
- Sea concisa, precisa, incidiéndose en la exactitud.
- Este disponible en el momento que sea requerida.
- Sea accedida legítimamente y utilizada para lo que se autorizó.
- Sea tratada conforme lo indique la Ley 1581 del 2012.

7.2 Adoptar y mantener una sólida cultura de Seguridad y Privacidad de la Información y Ciberseguridad

Las tres líneas deben tomar la iniciativa en el establecimiento de una sólida cultura de seguridad y privacidad de la información y ciberseguridad donde:

- La primera línea debe ser ejemplo y replicador de una sólida cultura y conciencia en Seguridad y Privacidad de la Información y Ciberseguridad, en el cumplimiento de políticas y procedimientos organizacionales definidos.

- La segunda línea debe definir y ejecutar las actividades de concienciación y cultura, que abarquen a todos los Colaboradores, sobre las políticas y procedimientos organizacionales de Seguridad y Privacidad de la Información y Ciberseguridad.
- La tercera línea debe monitorear la ejecución y el cumplimiento de cultura y concienciación de Seguridad y Privacidad de la Información y Ciberseguridad.

7.3 Implementar y Mantener un Sistema de Gestión Integral de Riesgos de Seguridad y Privacidad de la Información y Ciberseguridad

Todos los Colaboradores de Porvenir y sus subordinadas deberán utilizar un marco de control interno generalmente aceptado donde defina los elementos que se espera que estén presentes y funcionando en un sistema de control interno efectivo. Para el efecto se deberá alinear con la metodología corporativa de Administración de Riesgo Operativo – SARO (evaluación riesgo inherente, riesgo residual y mapa de calor) y con las Metodologías Corporativas de Gestión de Riesgos de Seguridad y Privacidad de la Información y Ciberseguridad.

7.4 Determinar el Apetito de Riesgo, el Nivel de Tolerancia y la Capacidad de Riesgo

La Alta Dirección, la segunda línea de Porvenir y sus subordinadas deberán determinar el Apetito de Riesgo, el nivel de tolerancia y la capacidad máxima al riesgo, considerando el efecto de la naturaleza de sus operaciones y líneas de negocio, así como los tipos y niveles de riesgo de seguridad y privacidad de la información y ciberseguridad que la compañía está dispuesta a asumir en cada uno de estos niveles. La Junta Directiva de Porvenir debe aprobar el Apetito de Riesgo, el nivel de tolerancia y la capacidad máxima al riesgo.

7.5 Establecer y mantener una evaluación de Riesgos y Oportunidades de Seguridad y Privacidad de la Información y Ciberseguridad

Porvenir y sus subordinadas deben contar con un proceso para identificar, evaluar, documentar, gestionar y mitigar los riesgos de seguridad y privacidad de la información y ciberseguridad. Este proceso se hace por lo menos una vez al año o cuando circunstancias especiales ocurran, identificando riesgos y evaluando su probabilidad e impacto, el cual debe estar alineado con las metodologías corporativas de gestión de riesgos de seguridad y privacidad de la información y ciberseguridad.

Así mismo, la segunda línea debe identificar, evaluar e implementar las oportunidades tanto internas como externas las cuales generarán una mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información y Ciberseguridad.

7.6 Supervisar la Administración del Sistema de Gestión de Seguridad y Privacidad de la Información y Ciberseguridad

La Alta Dirección y la segunda línea deben establecer, aprobar y revisar periódicamente el “Sistema de Gestión de Seguridad y Privacidad de la Información y Ciberseguridad”, Así mismo, debe supervisar la Administración para asegurarse de que las políticas, procesos y sistemas se aplican eficazmente en todos los niveles de decisión.

7.7 Establecer un proceso de mejora continua para el Sistema de Gestión de Seguridad y Privacidad de la Información y Ciberseguridad

La segunda línea debe determinar los mecanismos para la identificación de mejoras continuas del SGSPI que serán implementadas de acuerdo con el valor o impacto que generará a la compañía la aplicación de nuevas tecnologías o metodologías derivadas de buenas prácticas externas.

7.8 Gestionar el Cambio

La Alta Dirección y la segunda línea deben asegurar que haya un proceso de aprobación que evalúe plenamente los riesgos de seguridad y privacidad de la información y ciberseguridad en todos los nuevos procesos, actividades, productos, proyectos y sistemas críticos, así como que se identifiquen nuevas amenazas. Por ejemplo, cada vez que se realicen cambios sobre alguna aplicación que impacte el negocio, se lleva a un comité de cambios donde se evalúan los posibles riesgos que traería la implementación de dicho cambio.

7.9 Realizar Monitoreo y Presentar Informes

La segunda línea de Porvenir y sus subordinadas deben implementar un proceso para monitorear regularmente los perfiles de riesgo de Seguridad y Privacidad de la Información y las exposiciones a pérdidas importantes. Adicionalmente debe realizar un diagnóstico de seguridad y privacidad de la información basados en normas, estándares y marcos de referencia que respalden la gestión de seguridad de la información y ciberseguridad ISO 27000, ISO 27701 y Framework de Ciberseguridad NIST con el fin de calcular el nivel de seguridad y madurez en el que ese encuentra Porvenir y las subordinadas por medio de Indicadores Corporativos, Evolución de Riesgos y Evolución de Controles. De manera específica deberán trabajarse en este mismo sentido los riesgos de ciberseguridad.

7.10 Controlar y mitigar

La primera y segunda línea de Porvenir y las subordinadas deben tener un fuerte "ambiente de control", estructurado mediante políticas, procedimientos, estándares, sistemas, controles internos adecuados y la ponderada mitigación o compensación de riesgos. Con lo anterior, la primera línea de defensa debe contar con controles generales de accesos, privilegios, actualizaciones en los siguientes aspectos mínimos:

- Supervisión de controles de accesos físicos.
- Supervisión de controles de accesos lógicos.
- Supervisión y protección de contraseñas.
- Supervisión protección de los puertos de configuración y acceso remoto.
- Restricción de la instalación de aplicaciones por parte del usuario final.
- Asegurar que los sistemas operativos estén "parchados" con las actualizaciones o en su defecto que los controles implementados mitiguen la posibilidad de materialización de un incidente.
- Asegurar que las aplicaciones de software se actualicen regularmente.
- Restricción de los privilegios administrativos (es decir la capacidad de instalar software o cambiar los ajustes de configuración de una computadora).
- Asegurar que se realiza el correcto procesamiento del dato en todo el ciclo de vida del mismo, entre otros cumplimientos asociados a la protección de datos personales mencionados en el Manual de Normas y Políticas de Privacidad de la Información y en la Política de Tratamiento de Datos Personales.

7.11 Asegurar que el Sistema de Gestión de Seguridad y Privacidad de Información y Ciberseguridad Opera en Situaciones de Contingencia

La segunda línea o Líderes de Seguridad de la Información de Porvenir y sus subordinadas deben velar porque en los planes de continuidad del Negocio se incluyan y se implementen los controles necesarios sobre los pilares de la seguridad y la privacidad de la información y ciberseguridad.

7.12 Garantizar el Cumplimiento de la Ley Vigente Aplicable y de requerimientos de entes de control

Es obligación de las tres líneas de Porvenir y sus subordinadas dar cumplimiento a todas las normas de los reguladores vigentes y los requerimientos emitidos por los entes de control que le aplique relacionadas con Seguridad y Privacidad de la Información y Ciberseguridad.

7.13 Implementar Seguridad en Nuevas Tecnologías y Riesgos Emergentes

Es importante implementar un plan de seguridad de la información y ciberseguridad, con relación a las nuevas tecnologías. Para monitorear, desarrollar e implementar estrategias de remediación de los riesgos emergentes, donde se debe:

- Establecer políticas de seguridad sobre las tecnologías que se implementen en Porvenir y sus subordinadas.
- Adoptar procedimientos de clasificación de la información, gestión y administración de usuarios, definición de responsables y propietarios, de la información que se va a procesar en las nuevas tecnologías para determinar y aplicar los controles de seguridad de la información y ciberseguridad.
- Establecer la gestión y monitoreo de los riesgos cibernéticos y riesgos de terceros que surgen de la implementación de las nuevas tecnologías como lo son los riesgos operacionales, financieros, regulatorios, organizacionales y tecnológicos.
- Incluir en el plan de continuidad del negocio los requisitos y controles de seguridad para reanudar las operaciones orientadas en los sistemas automatizados y servicios digitales.
- Supervisar el cumplimiento del trabajo que desempeñan los sistemas automatizados, asegurando que estos sistemas se adhieran a los requerimientos regulatorios y a las políticas de la organización, en materia de seguridad.

7.14 Implementar Seguridad en nube

Es compromiso de la segunda línea establecer los lineamientos aplicables para los servicios que se encuentren expuestos a nube tanto privada como pública, y responsabilidad de la primera línea implementar y mantener la seguridad sobre estos servicios, teniendo en cuenta que, para una infraestructura de nube pública, Porvenir debe adaptarse a los criterios y prácticas de seguridad que tiene implementado el proveedor, asegurando el respaldo, acceso y privacidad de la información que allí reposa.

7.15 Modelo de Evaluación del Sistema de Gestión de Seguridad y Privacidad de la Información y Ciberseguridad

Para la identificación de riesgos y la aplicación de controles de seguridad y privacidad de la información y ciberseguridad, Porvenir y sus subordinadas adoptan y dan a conocer el modelo de evaluación de seguridad y privacidad de la información y ciberseguridad. Este modelo tiene como propósito evaluar el nivel de madurez del sistema de gestión de seguridad y privacidad de la información e identificar las oportunidades de mejora que permitan fortalecerlo, basados en los dominios y controles propuestos en la norma NTC-ISO/IEC 27001:2022, la norma NTC-ISO/IEC 27701:2020 y en el Framework de Ciberseguridad NIST.

7.16 Reportes

Con el fin de facilitar el monitoreo de cumplimiento, serán solicitados diferentes reportes de gestión que constituyan un efectivo apoyo para la administración; éstos deberán ser veraces, comprensibles, completos y oportunos. Así mismo, las subordinadas y/o proveedores deberán informar a Porvenir aquellos incidentes seguridad de la información y ciberseguridad que hayan afectado de manera significativa la confidencialidad, integridad, disponibilidad y privacidad de la información de la compañía en el momento en que estos sucedan, haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlos. Adicionalmente se deberá tener una base de datos consolidada de incidentes de seguridad de la información y ciberseguridad clasificada en tipo de incidente, impacto, afectación de pilar de seguridad de la información y plan de remediación, así como, que este reporte se encuentre protegido dada la sensibilidad de esta información.

7.17 Capacitación y Entrenamiento

Dentro del proceso de inducción de un Colaborador nuevo y al menos anualmente para la totalidad de los Colaboradores debe realizarse una capacitación y/o actualización sobre seguridad y privacidad de la información y ciberseguridad. La capacitación y entrenamiento se puede brindar en forma continua, virtual o presencial a los Colaboradores de Porvenir y sus subordinadas, con el propósito de fortalecer los conceptos y asegurar la continuidad y sostenibilidad de Sistema de Gestión de Seguridad y Privacidad de la Información y Ciberseguridad. Adicional a esto, de manera anual se realiza una capacitación en seguridad y privacidad de la información a los proveedores críticos que acceden a los activos de información.

7.18 Investigaciones y Sanciones

Porvenir y sus subordinadas reconocen que en el evento de incumplimiento de esta política y demás actividades que se deriven de ella, las personas responsables por su incumplimiento podrán ser objeto de acciones disciplinarias por parte de Porvenir de acuerdo con las políticas internas relacionadas con el manejo de Incidentes de Seguridad de la Información. Lo anterior, sin perjuicio de la eventual responsabilidad que pudiera derivarse por el incumplimiento de la normatividad aplicable a Seguridad y Privacidad de la Información y Ciberseguridad.

8. VIGENCIA Y ACTUALIZACIÓN DE LA POLÍTICA

La Política General de Seguridad y Privacidad 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.

9. NORMATIVIDAD EXTERNA

- Circular Básica Jurídica Superintendencia Financiera de Colombia (SFC) 029 de 2014 Parte I Título IV Capítulo V: Requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad.
- Circular Básica Jurídica de la Superintendencia Financiera de Colombia (SFC) 029 de 2014 Parte I Título III Capítulo I: Acceso e información al consumidor financiero.
- Circular Básica Jurídica de la Superintendencia Financiera de Colombia (SFC) 029 del 2014 Para I Título I Capítulo VI: Reglas relativas al uso de servicios de computación en la nube.
- Circular Básica Jurídica de la superintendencia Financiera de Colombia (SFC) 029 de 2014 Parte I Título II Capítulo I: Canales, medios, seguridad y calidad en el manejo de la información en la prestación de servicios financieros.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Circular Única de la Superintendencia de Industria y Comercio (SIC) Título V – Protección de Datos Personales.
- Circular Externa 006 de 2022 (SIC) Tratamiento de datos personales para fines de publicidad, marketing o prospección comercial.
- Circular Externa 001 de 2024 (SIC) Titulares de la información y entidades vigiladas por la Superintendencia de Industria y Comercio en su rol de Autoridad de Protección de Datos Personales.
- Circular Externa 002 de 2024 (SIC) Lineamientos sobre el Tratamiento de Datos personales en Sistemas de Inteligencia Artificial.
- Circular Externa 003 de 2024 (SIC) Instrucciones para los administradores societarios en relación con el Tratamiento de Datos personales.

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
3.0	Responsabilidad de los usuarios Lineamientos Generales	Se incluye el numeral 6. Responsabilidad de los usuarios, mencionando las funciones o compromisos de las tres líneas de defensa en Porvenir. Se incluye el numeral 7. Lineamientos Generales mencionando los deberes del Sistema de Gestión de Seguridad de la Información a Porvenir, sus subordinadas y las tres líneas de defensa.	22 de noviembre 2023
4.0	Todo el documento	Se modifica el documento a nivel general de acuerdo con la transición de la norma a su versión ISO 27001:2022.	Julio 2024

No.	Numeral / Título	Descripción de la Actualización	Fecha de Actualización
		1. Se modifico la Política General. 2. Se incluyen y modifican responsabilidades de la Alta Dirección. 3. Se incluyen y modifican lineamientos generales dando cumplimiento a los requisitos aplicables de la norma.	
5.0	Todo el documento 4. POLÍTICA 5. COMPROMISO DE LA ALTA DIRECCIÓN 6. RESPONSABILIDADES DE LOS USUARIOS	Se modifica el documento a nivel general de acuerdo con la implementación de la norma ISO 27701:2020, complemento de la norma ISO 27001:2022 a nivel de privacidad de la información. 4. Se incluye el apartado 4.2 POLÍTICA DE PRIVACIDAD DE LA INFORMACIÓN en la cual se menciona el documento especifico donde se encuentra alojada la política. 5. Se modifican los compromisos de la Alta Dirección de acuerdo con el enfoque en privacidad de la información. 6. Se incluye un apartado adicional para la primera, segunda y tercera línea mencionando como las tres líneas como actúan en el frente de privacidad de la información. 7. Se realizan cambios sobre todos los requisitos aplicables haciendo	Junio 2025

No.	Numeral / Título	Descripción de la Actualización	Fecha de Actualización
	7. REQUISITOS APLICABLES A SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 9. NORMATIVIDAD EXTERNA	énfasis a la privacidad de la información. 9. Se incluye la Ley 1581 aplicable a protección de datos personales, la Circular Única y Circulares Externas 006 de 2022, 001 de 2024, 002 de 2024 y 003 de 2024 de la SIC.	