TABLA DE CONTENIDO

1 INTRODUCCIÓN 2
2 OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 2
2.1 OBJETIVO GENERAL 2
2.2 OBJETIVOS ESPECÍFICOS 2
3 ALCANCE 3
4 REFERENCIAS NORMATIVAS 3
5 DIAGNÓSTICO 3
6 PLANIFICACIÓN 3
6.1 CONTEXTO 3
6.1.1 CONTEXTO EXTERNO 4
6.1.2 CONTEXTO INTERNO 4
6.1.3 PARTES INTERESADAS 5
6.2 POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 5
6.2.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES 5
6.3 ROLES Y RESPONSABILIDADES 5
6.4 ACTIVOS DE INFORMACIÓN 5
6.5 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 6
6.6 PLAN DE TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 6
6.6.1 DECLARACIÓN DE APLICABILIDAD (SOA) 6
6.7 PLAN DE TRATAMIENTO DE DATOS PERSONALES 6
6.8 RECURSOS 7
6.9 COMPETENCIA, TOMA DE CONCIENCIA Y CAPACITACIÓN 7
6.10 GESTIÓN DE SI EN SERVICIOS DIGITALES FRENTE A PROVEEDORES 7
7 EVALUACIÓN Y DESEMPEÑO 8
7.1 INDICADORES 8
7.2 AUDITORÍA INTERNA 8
7.3 REVISIÓN POR LA DIRECCIÓN 8
8 MEJORAMIENTO CONTÍNUO 8

1 INTRODUCCIÓN

Las empresas de cualquier tipo o sector se enfrentan cada vez a más riesgos procedentes de una amplia variedad de amenazas que pueden dañar de forma importante los sistemas de información y la información procesada y almacenada por ellos.

Ahora bien, debido a las situaciones derivadas de la pandemia COVID-19, se ha presentado un incremento exponencial en el acceso a la información a través de internet desde múltiples dispositivos electrónicos, el crecimiento de los servicios digitales, la utilización de medios digitales para compartir información, recuperación de datos remotos, utilización de ambientes virtuales colaborativos, entre otros, hacen que esos riesgos se incrementen.

Ante estas circunstancias y con el fin de garantizar entornos seguros, se establecen estrategias y controles adecuados que garanticen una gestión segura de los procesos del negocio dando mayor protección a la información, independientemente del medio en el que ésta se encuentre, procese, transmita, etc.

Estas estrategias y aspectos para la protección y control parten de marcos establecidos a nivel de elementos normativos que deberán ser desarrollados en las entidades del estado y de tipo asegurador y financiero para realizar una gestión y control adecuados con el fin de velar por la seguridad de la información y la gestión de la ciberseguridad.

Teniendo en cuenta lo anterior, se establece el Modelo de Seguridad y Privacidad de la Información y de Gestión de la Ciberseguridad de Previsora Seguros, cuya planificación e implementación está alineada con las necesidades y objetivos estratégicos de la compañía y a la normatividad que le aplica y se operativiza con la creación del proceso "Administrar el Sistema de Gestión de Seguridad de la Información", en adelante SGSI.

2 OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

2.1 OBJETIVO GENERAL

El objetivo general del Sistema de Gestión de Seguridad de la Información es preservar la integridad, confidencialidad y disponibilidad de la información de la Compañía y sus clientes, en cualquiera de los medios en los que se encuentre, e igualmente se pretende proteger sus activos en el ciberespacio.

2.2 OBJETIVOS ESPECÍFICOS

- Implementar un marco de seguridad integral para proteger los datos personales de nuestros clientes y nuestros activos de información críticos, asegurando el cumplimiento normativo y la continuidad del negocio.
- Identificar y gestionar los riesgos de seguridad de la información y la ciberseguridad y mantenerlos en niveles aceptables.
- Mantener un proceso de gestión de incidentes de seguridad eficaz que permita identificar, analizar y responder a incidentes. con el fin de proteger la integridad, disponibilidad y confidencialidad de nuestros datos.
- Fomentar una cultura de seguridad de la información sólida en toda la organización a través de programas de concientización y capacitación continuos, asegurando que todos los empleados comprendan y apliquen las políticas y procedimientos de seguridad de la entidad.
- Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información, seguridad digital y protección a los datos personales, conforme con las normas técnicas de la Superintendencia Financiera de Colombia, las leyes de protección de datos personales y otros requisitos legales aplicables.

3 ALCANCE

El Sistema de Gestión de Seguridad de la Información y Ciberseguridad de la Compañía y todo el esquema normativo que de él se deriva, aplica a todos los procesos de la Compañía, sus funcionarios y todas las partes interesadas que tienen acceso a la información crítica y sensible de la compañía.

Los aspectos relacionados con la protección de datos personales se rigen por el MN-114 GENERAL PARA LA PROTECCIÓN DE DATOS PERSONALES y demás normativas aplicables.

4 REFERENCIAS NORMATIVAS

Para el diseño, implementación, seguimiento y mejora del Sistema de Gestión de Seguridad de la Información y Ciberseguridad se tendrán como referencia entre otros, los siguientes documentos:

- Circular Básica Jurídica de la Superintendencia Financiera de Colombia Parte I - Instrucciones generales aplicables a las entidades vigiladas:
  - Título I Aspectos generales Capítulo. VI - Reglas relativas al uso de servicios de computación en la nube
  - Título II Capítulo. I – Canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros,
  - Título IV Deberes y responsabilidades Capítulo. V- Requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad
- Resolución 500 MinTic
- Resolución 746 MinTic
- Ley 1266 de 2008:
- Ley 1581 de 2012

El SGSI fundamenta su enfoque metodológico en el modelo conceptual proporcionado por las Normas ISO 27001, ISO 27002 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.

5 DIAGNÓSTICO

Para determinar e identificar el nivel de madurez del sistema de seguridad de la información y ciberseguridad, la Compañía realiza anualmente un autodiagnóstico utilizando el "Instrumento de Evaluación MSPI" que es una herramienta creada por el Ministerio de Tecnologías de la Información y las Comunicaciones para establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las entidades, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente "Seguridad y Privacidad de la Información".

A partir de los resultados obtenidos del autodiagnóstico, se establecen metas, planes y actividades para mantener y mejorar en cada uno de los dominios evaluados.

6 PLANIFICACIÓN

6.1 CONTEXTO

Con base en el conocimiento del contexto de la compañía, tanto interno como externo, se definen los objetivos para la gestión de la Seguridad de la Información y del Riesgo de Ciberseguridad de la entidad, el alcance del sistema, políticas y criterios para la gestión de los riesgos.

En el análisis del contexto se identifican todas las "Partes Interesadas", que podrían tener incidencia en los riesgos para La Previsora, con el fin de definir los requisitos legales, reglamentarios y las obligaciones contractuales frente al sistema. Las partes interesadas, son responsables de la salvaguarda de los activos críticos de la compañía e igualmente son responsables de evaluar los riesgos, teniendo en cuenta las amenazas que se aplican a sus activos.

Este análisis puede ayudar en la selección de los controles para contrarrestar los riesgos y reducirlos a un nivel aceptable.

6.1.1 CONTEXTO EXTERNO

Este análisis evalúa el entorno que influye y afecta el logro de los objetivos estratégicos de la organización, así como su seguridad de la información y ciberseguridad.

En esta etapa se asegura que los intereses de todas las partes interesadas sean considerados al gestionar los riesgos de seguridad de la información y ciberseguridad. Esto implica definir los parámetros dentro de los cuales se administrarán los riesgos y el alcance del proceso de gestión de seguridad en su conjunto.

Para comprender el entorno operativo de la organización y sus relaciones externas, se podrán analizar los siguientes aspectos:

- Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la compañía.
- Aspectos regulatorios o aspectos jurídicos que apliquen directa o indirectamente a la compañía
- Ciudadanos que interactúan digitalmente con la organización
- Situación financiera, económica y tecnológica
- Escenario político y social
- Impulsores clave y las tendencias que tienen impacto en los objetivos de la compañía.
- Percepciones y valores de las partes interesadas.
- Impacto ambiental de las operaciones (si aplica).
- Datos personales almacenados en las bases de datos de la compañía.

Este análisis permite a la organización comprender su entorno y tomar decisiones estratégicas informadas para proteger sus activos de información. Al monitorear continuamente a las partes interesadas y sus impactos en los riesgos, la alta gerencia alinea y mide estos riesgos con los objetivos estratégicos, evaluando su comportamiento actual y proyectado. Esto facilita la adaptación del plan estratégico para aprovechar oportunidades y mitigar riesgos emergentes.

6.1.2 CONTEXTO INTERNO

Para comprender el contexto interno de la organización y establecer una base sólida para la gestión de la seguridad de la información y ciberseguridad, se realizará un análisis exhaustivo que incluirá los siguientes aspectos

- Estructura organizacional: Gobierno corporativo, roles, responsabilidades y líneas de autoridad
- Objetivos estratégicos: Misión, visión, valores Marco normativo interno: Políticas, procesos, procedimientos y estándares vigentes
- Modelo del negocio, flujos de información y procesos de toma de decisiones y relaciones entre las diferentes áreas.
- Ambiente interno de control, normas, directrices y modelos adoptados por la organización
- Capacidades en términos de recursos (humanos, capital, sistemas, procesos, etc.)

- Cultura de la organización
- Empleados, contratistas y sus roles en la gestión de la información
- Sistemas de gestión de calidad, seguridad en el trabajo, seguridad de la información y otros sistemas relevantes.
- Activos de información: Identificación y clasificación de los activos de información (sistemas, bases de datos, etc.).

6.1.3 PARTES INTERESADAS

Dentro del sistema de gestión integral, la compañía identifica las partes interesadas que son pertinentes al mismo, para determinar sus requisitos y obligaciones, los cuales incluyen requisitos legales y reglamentarios, así como las obligaciones contractuales, incluyendo los atinentes a seguridad y ciberseguridad.

6.2 POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La política del SGSI y Gestión de la Ciberseguridad de la Compañía, se encuentra formalizada mediante la circular CIR-320 publicada en el aplicativo de gestión documental de la compañía. En ella se definen los principios y lineamientos para la gestión de la seguridad de la información y la gestión del riesgo de ciberseguridad en la entidad y es aprobada por la Junta Directiva.

6.2.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES

Complementando la política general, se han establecido políticas específicas alineadas con los estándares ISO 27001 e ISO 27002. Estas políticas, junto con los procedimientos e instructivos asociados, se adaptan continuamente a las necesidades cambiantes de la compañía, para garantizar una gestión integral de la seguridad de la información y la ciberseguridad.

Esta documentación, alojada en el sistema de gestión documental de la compañía, se actualiza de forma periódica en función de los resultados de los análisis de riesgo, auditorías y autoevaluaciones.

6.3 ROLES Y RESPONSABILIDADES

Alineado con la política de seguridad vigente, el documento "MN-108 Manual de Roles y Responsabilidades de Seguridad de la Información y Ciberseguridad", establece las responsabilidades y roles específicos de las partes involucradas en el sistema de gestión de seguridad de la información y ciberseguridad de la compañía.

De otra parte, el Reglamento del Comité de Datos Personales establece la estructura y funciones de este órgano, el cual desempeña un papel crucial en la supervisión de la gestión de los datos personales.

6.4 ACTIVOS DE INFORMACIÓN

La compañía ha definido un marco de trabajo para la gestión de activos de información, basado en un proceso de identificación y clasificación que permite evaluar el valor y la criticidad de cada activo. Esta clasificación, alineada con los principios de confidencialidad, integridad y disponibilidad, sirve de base para la implementación de las medidas de seguridad necesarias.

Los líderes de cada proceso son responsables de mantener actualizado el inventario de activos, asegurando así una gestión continua y efectiva de la seguridad de la información.

6.5 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La compañía ha implementado una metodología formalizada en el MN-188 MANUAL DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN para la gestión de riesgos de seguridad de la información y ciberseguridad, centrada en la protección de activos de información críticos. Esta metodología permite:

- Identificación de riesgos: Detecta amenazas específicas que puedan comprometer la confidencialidad, integridad, disponibilidad de la información y la continuidad operativa de la entidad.
- Valoración de riesgos: Define criterios para valorar el impacto de la materialización de los riesgos y la probabilidad de su ocurrencia.
- Definición de niveles de riesgo: Establece umbrales de tolerancia al riesgo, permitiendo priorizar las acciones a tomar.
- Priorización de riesgos: Ordena los riesgos según su criticidad, facilitando la asignación de recursos para su tratamiento

La Junta Directiva ha aprobado esta metodología, asegurando su alineación con los objetivos estratégicos de la compañía.

6.6 PLAN DE TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Una vez se han identificado los riesgos de seguridad de la información y de ciberseguridad la entidad definirá sobre aquellos que permanezcan ubicados en niveles de riesgo extremo o alto las opciones de tratamiento (plan de tratamiento o plan de acción) para evitarlos y reducir su consecuencia, probabilidad o establecer la forma de soportar las pérdidas que éstos generen

Estos planes se enfocarán en prevenir incidentes, reducir su impacto y establecer mecanismos para responder de manera efectiva en caso de materializarse.

6.6.1 DECLARACIÓN DE APLICABILIDAD (SOA)

La compañía elabora la Declaración de Aplicabilidad o Statement of Applicability (SOA), que es el documento que lista los objetivos y controles que se van a implementar en la Compañía, así como las justificaciones de aquellos controles que no van a ser implementados.

Este documento dinámico, se actualiza regularmente para adaptarse a las necesidades cambiantes de la organización y a las nuevas amenazas.

6.7 PLAN DE TRATAMIENTO DE DATOS PERSONALES

El plan de tratamiento de datos personales comprende las directrices y procedimientos establecidos en el Manual General para la Protección de Datos Personales y la Política de Tratamiento de Información diseñados para gestionar y controlar cómo se recopilan, almacenan, procesan y utilizan los datos personales dentro de la entidad. El propósito principal de este plan es garantizar que los datos personales sean manejados de manera legal, ética y segura, y que se cumplan todas las regulaciones de protección de datos aplicables a la compañía.

De otra parte, la gestión de riesgos de datos personales incluye una serie de procedimientos y medidas destinados a identificar, evaluar, mitigar y supervisar los riesgos relacionados con la recopilación, procesamiento y almacenamiento de información personal en una organización. Su objetivo principal es propender por la seguridad y la privacidad de los datos personales y, garantiza el cumplimiento de las regulaciones de protección de datos y minimiza la probabilidad de incidentes de seguridad o infracciones de privacidad.

Con base en la evaluación de riesgos, se implementan medidas de seguridad y controles para reducir la probabilidad de ocurrencia de riesgos y minimizar su impacto en caso de que ocurran. Así mismo, se desarrolla el plan de respuesta a incidentes mediante el cual se establecen procedimientos para responder de manera efectiva en caso de que ocurra una violación de datos o un incidente de seguridad.

6.8 RECURSOS

La compañía determina y proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información, lo cual se evidencia en el presupuesto anual asignado en los rubros de seguridad informática y demás rubros asignados a las diferentes áreas para la implementación o ejecución de controles que apoyen la seguridad de la información y la ciberseguridad.

6.9 COMPETENCIA, TOMA DE CONCIENCIA Y CAPACITACIÓN

Para fomentar una cultura de seguridad de la información, la compañía implementa un programa de capacitación integral que incluye:

- Inducción: Curso virtual obligatorio para nuevos empleados y charlas en el proceso de incorporación.
- Reinducción anual: Actualización de conocimientos para todos los empleados como parte del plan de formación.
- Comunicación continua: Envío de mensajes de sensibilización y campañas específicas según las necesidades.
- Capacitación especializada: Cursos sobre manejo de datos personales.
- Actividades interactivas: Webinars, charlas y simulacros para reforzar el aprendizaje.

6.10 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN SERVICIOS DIGITALES FRENTE A PROVEEDORES

La creciente dependencia de servicios digitales y la proliferación de datos sensibles han elevado la importancia de una gestión rigurosa de la seguridad de la información y la ciberseguridad, en las relaciones con proveedores. Previsora S.A. reconoce este imperativo y ha implementado un marco de trabajo integral para garantizar la confidencialidad, integridad y disponibilidad de los activos de información cuando estos son procesados por terceros.

Para asegurar una gestión efectiva de la seguridad de la información en servicios digitales prestados por terceros, Previsora S.A. ha implementado un marco de seguridad para sus proveedores, estableciendo dos políticas fundamentales: la Política de Gestión de Proveedores, desde el área de gestión contractual y la Política para las Relaciones con los Proveedores, bajo el ámbito de seguridad de la información.

Este marco incluye la evaluación de los requisitos de seguridad exigidos a nuestros proveedores, cláusulas contractuales, aspectos relativos a la ciberseguridad, auditorías regulares, definición de acuerdos de nivel de servicio (SLA) y procedimientos para gestión de incidentes. El objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información, incluso cuando es procesada por terceros.

DOCUMENTO DE USO INTERNO

7 EVALUACIÓN Y DESEMPEÑO

7.1 INDICADORES

La compañía establece indicadores para evaluar el desempeño y eficacia del SGSI. Las hojas de vida de los indicadores se encuentran publicados en la caracterización del proceso y la medición queda registrada en la herramienta que la compañía designe para tal fin.

7.2 AUDITORÍA INTERNA

La oficina de control interno de la entidad es la encargada de efectuar auditorías internas para verificar el estado del sistema de seguridad de la información, de acuerdo con el plan anual de auditorías aprobado por la alta dirección.

7.3 REVISIÓN POR LA DIRECCIÓN

De forma semestral, se elabora un informe de la gestión de seguridad de la información (SGSI) y ciberseguridad, el cual es presentado al Comité de Seguridad de la Información y a la Junta Directiva. Este informe proporciona una visión del estado actual del SGSI.

Adicionalmente, durante la revisión anual del Sistema de Gestión Integral, se presenta un análisis específico del SGSI, asegurando su alineación con los objetivos estratégicos de la organización

8 MEJORAMIENTO CONTÍNUO

De acuerdo con los resultados obtenidos de la fase de evaluación de desempeño se determinan e implementan las acciones oportunas para mitigar las debilidades identificadas los cuales son tratadas de acuerdo con el Proceso de Mejora Continua y son documentadas en los planes de mejoramiento de la compañía.

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE (S)	Sandra Cediel Bravo	Sandra Cediel Bravo	David Ricardo Marín Villa
CARGO (S)	Especialista G. Riesgos	Especialista G. Riesgos	Gerente de Riesgos.

CONTROL DE CAMBIOS	
VERSIÓN	CAMBIO REALIZADO
1	Se crea el documento
2	Se actualiza el documento alineando e incluyendo lineamientos de privacidad y datos personales
3	Se revisa y actualiza el documento