## PORTADA

## A) HISTORIAL DE CAMBIOS

| VERSIÓN | FECHA | JUSTIFICACIÓN DE LA MODIFICACIÓN |
|---|---|---|
| 1 | 25/01/2019 | Lanzamiento del plan |
| 2 | 30/06/2020 | Se actualiza todo el documento, a fin de lograr una cobertura total de acuerdo al contenido de las guías del Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio de las Tecnologías y las Comunicaciones – MINTIC, de forma que contribuya al establecimiento del SGSI |
| 3 | 03/12/2021 | Se finaliza el "plan para la adopción del modelo de seguridad y privacidad de la información MSPI" y se da inicio a este nuevo enfoque para la gestión de los instrumentos adoptados para la seguridad y privacidad de la información, ciberseguridad, datos personales y continuidad de negocio.<br><br>Se cambia nombre por el de "Plan para sistema de gestión de seguridad de la información - SGSI"<br><br>Se redefinen objetivos, alcance e introducción. Se agregan definiciones. Cambia la tabla de contenido. Los cambios se encuentran en letra cursiva en el documento. |

## B) REVISIONES Y APROBACIONES DEL DOCUMENTO

| ELABORÓ | REVISÓ | APROBÓ |
|---|---|---|
| Nombre: Jesús Goyes Alvarado | Nombre: Germán Armando Correa Amado | Nombre: Francisco Álvaro Ramírez Rivera |
| Cargo: Contratista Asesor Planeación y Sistemas | Cargo: Jefe Oficina Asesora de Planeación y Sistemas | Cargo: Director General |
| Fecha: 16/11/2021 | Fecha: 02/12/2021 | Fecha:03/12/2021 |

| REVISÓ | REVISÓ | REVISÓ |
|---|---|---|
| Nombre: Oscar Herrera Isaza | Nombre: Zulli Yazmin Rosas Becerra | Nombre: Carolina Tobar Sierra |
| Cargo: Contratista Asesor de Calidad | Cargo: Contratista unidad de riesgo operativo URO | Cargo: Profesional Especializado Oficina Asesora de Planeación y Sistemas |
| Fecha: 01/12/2021 | Fecha: 29/11/2021 | Fecha: 24/11/2021 |

## C) LISTA DE DISTRIBUCIÓN

| N° | NOMBRE Y CARGO |
|---|---|
| 1 | Jefe Oficina Asesora de Planeación y Sistemas |
| 2 | Profesional Oficina Asesora de Planeación y Sistemas |
| 3 | Profesional Especializado Oficina Asesora de Planeación y Sistemas |
| 4 | Profesional Universitario Oficina Asesora de Planeación y Sistemas |
| 5 | Técnico Operativo Oficina Asesora de Planeación y Sistemas |

TABLA DE CONTENIDO

## 1. INTRODUCCION

*A través del Decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente transversal de seguridad y privacidad de la información, como parte integral de la estrategia de Gobierno en Línea – GEL iniciando en la versión 1 en el año 2010 hasta la versión 4 de 2015.*

*Para agosto de año 2018 la estrategia GEL evoluciona en su versión 5 convirtiéndose en política de Gobierno Digital. A la fech, el Manual de implementación de dicha política se encuentra en la versión 7 de abril de 2019, cuyo objetivo consiste en: "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital"*

*La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, se lleva a cabo a partir de una serie de guías en cada una de las fases, que pone a disposición el Ministerio de las Tecnologías y las Comunicaciones – MINTIC. Su adopción debe ser acorde a las necesidades y objetivos, requisitos de seguridad, procesos misionales, el tamaño y estructura de Fondo de Previsión Social del Congreso de la República - Fonprecon*

*Con la adopción del MSPI, resultan una serie de instrumentos como planes, procedimientos, manuales, formatos y demás que, en conjunto deben ser gestionados desde el contexto de un Sistema de Gestión de Seguridad de la Información - SGSI conducente a la preservación de la confidencialidad, integridad y disponibilidad de la información.*

*El SGSI agrupa y gestiona los esfuerzos humanos, técnicos administrativos y tecnológicos para una adecuada gestión de riesgos, seguridad y privacidad de la información, ciberseguridad, datos personales y continuidad de negocio.*

## 2. OBJETIVOS

- *Trazar un sistema de gestión de seguridad de la información – SGSI, que integre los instrumentos existentes de seguridad de la información, ciberseguridad, MSPI, seguridad de los datos personales y continuidad de negocio.*
- *Realizar seguimiento y mejora continua a los componentes del SGSI*
- *Contribuir al objetivo estratégico denominado* ***Consolidar el sistema de seguridad de la información***

## 3. ALCANCE

*Gestión y mejora continúa en el contexto de la seguridad y privacidad, ciberseguridad, datos personales y continuidad de negocio.*

## 4. MARCO DE REFERENCIA

- Decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, que define el componente de seguridad y privacidad de la información, como parte integral de la política de Gobierno Digital
- Decreto 1008 de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital
- Guía técnica ISO/IEC 27001: Requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información – SGSI dentro del contexto de la organización.
- Guía técnica ISO/IEC 27032: conjunto de buenas prácticas para la ciberseguridad.
- Ley 1581 de 2012 y sus decretos reglamentarios: protección de datos personales.
- Políticas seguridad y privacidad de la información de Fonprecon.
- Política para el tratamiento de datos personales de Fonprecon.

- Política para la continuidad de negocio de Fonprecon
- Circulares de la Superintendencia Financiera de Colombia:
  - *Circular Externa 007 de 2018 que imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad.*
  - *Circular Externa 005 de 2019 que imparte instrucciones relacionadas con el uso de servicios de computación en la nube*
  - *Circular Externa 033 de 2020 que imparte instrucciones relacionadas con la Taxonomía Única de Incidentes Cibernéticos – TUIC, el formato para el reporte de métricas de seguridad de la información y ciberseguridad y el protocolo de etiquetado para el intercambio de información Traffic Light Protocol, TLP*

## 5. DEFINICIONES

***Sistema de Gestión de Seguridad de la Información SGSI****: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.*

***Bases de datos manuales:*** *Son los archivos cuya información se encuentra organizada y almacenada de manera física.*

***Bases de datos automatizadas:*** *aquellas que se almacenan y administran con la ayuda de herramientas informáticas.*

***Dato personal:*** *Cuando hablamos de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos.*

***Dato público:*** *Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio ya su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.*

***Datos sensibles:*** *Son aquellos que afectan la intimidad del titular o pueden dar lugar a que lo discriminen, es decir, aquellos que revelan su origen racial o étnico, su orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos, entre otros.*

***Dato semiprivado:*** *Son los datos que no tienen naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo al titular sino a cierto sector o a la sociedad en general. Los datos financieros y crediticios de la actividad comercial o de servicios, son algunos ejemplos.*

***Dato privado:*** *Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular. Los gustos o preferencias de las personas, por ejemplo, corresponden a un dato privado.*

**Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

**Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información que genere, obtenga, adquiera, transforme o controle.

**Archivo**: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia.

**Amenazas**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

**Ciberseguridad**: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

**Ciberespacio**: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

**Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

**Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

**Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3)

**Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información –SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

**Información Pública Clasificada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

**Información Pública Reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

**Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

**Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Fuente:

https://www.mintic.gov.co/gestionti/615/articles5482_Modelo_de_Seguridad_Privacidad.pdf

## 6. POLÍTICAS.

### *6.1. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.*

*Tomado del documento denominado "Políticas de seguridad y privacidad de la información"*

- *FONPRECON ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información SGSI, derivado de la adopción del modelo de seguridad y privacidad de la información MSPI del MINTIC, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.*
- *Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas por la Entidad y aceptadas con carácter de cumplimiento mandatorio por cada uno de los empleados, contratistas o terceros.*
- *FONPRECON mantendrá actualizado el inventario de activos, como uno de los insumos fundamentales a la hora de identificar riesgos y diseño de controles.*
- *FONPRECON protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de su actividad institucional.*
- *FONPRECON protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos, reputacionales o legales debido a un uso incorrecto de POLITICAS CODIGO: POL-DEI-005 DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 5 Página 15 de 34 Fecha de aprobación: 13/11/2020. Para ello se identificarán los riesgos y aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.*
- *FONPRECON protegerá su información de las amenazas originadas por parte del personal que intervenga en su administración, manejo o custodia.*
- *FONPRECON protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.*
- *FONPRECON controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.*

- *FONPRECON implementará mecanismos de control de acceso a la información, sistemas y recursos de red.*
- *FONPRECON intervendrá para que la seguridad sea parte integral del ciclo de vida de los sistemas de información, así como de la información en medio físico clasificada dentro del inventario de activos.*
- *FONPRECON ejecutará una mejora efectiva de su modelo de seguridad, para enfrentar, mitigar o eliminar las debilidades asociadas con los sistemas de información.*
- *FONPRECON garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en la identificación de riesgos, aplicación de controles y en el impacto que pueden generar los eventos.*
- *FONPRECON garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales vigentes en materia de seguridad y privacidad de la información.*

### *6.2. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES.*

*Tomado del documento denominado "Política para el tratamiento de datos personales"*

*El Fondo de Previsión Social del Congreso dará tratamiento a los datos personales que genere, adquiera, distribuya, almacene o suprima, en su condición de administradora de Régimen de Prima Media con Prestación Definida, con sujeción total a la ley y jurisprudencia vigente, garantizando los derechos de todos y cada uno de sus usuarios y de la ciudadanía, junto con los intereses de los titulares de la información que repose en sus archivos y bases de datos.*

### 6.2.1. SEGURIDAD DE LOS DATOS PERSONALES.

Los datos personales se almacenarán en bases de datos automatizadas y manuales, frente a lo cual, El Fondo de Previsión Social del Congreso se compromete a adoptar las medidas administrativas, humanas y técnicas necesarias para su custodia, conservación, transporte, acceso, divulgación o comunicación, trazabilidad, auditoria y demás aspectos que se consideren necesarios, tanto para la información digital que se apoya en componentes tecnológicos como para la información en físico almacenada y custodiada en bodegas y que contienen datos personales.

### *6.3. POLÍTICA DE CONTINUIDAD DE NEGOCIO.*

Tomado del documento denominado "*Plan de continuidad de negocio*".

El Fondo de Previsión Social del Congreso de la República – FONPRECON, en procura de garantizar la prestación de los servicios como Administradora del régimen pensional de prima media con prestación definida, garantizará la continuidad de sus procesos de negocio y operación con base en la identificación de procesos y procedimientos priorizados, tratamiento de riesgos, seguridad y bienestar de usuarios y servidores, con la disposición y uso de los recursos humanos, logísticos y técnicos necesarios, para superar eventos adversos que pudieran afectar la operación, vida y seguridad de las personas, consultando con sus grupos de interés y ciudadanía en general

## 7. COMPONENTES DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION - SGSI.

El SGSI se compone de instrumentos diversos como políticas, planes, formatos e instancias específicas de seguridad como la unidad de riesgo operativo y el comité

estratégico de continuidad de negocio. Todos estos instrumentos se documentan en el anexo *Catálogo de componentes SGSI.xlsx*

## 8. INDICADORES

| ***INDICADORES*** | | | |
|---|---|---|---|
| ***Definición*** | ***Relación matemática*** | ***Meta*** | ***Frecuencia*** |
| *Eficiencia en el tratamiento de incidentes relacionados con la seguridad de la información.* | *(Número de incidentes cerrados/ Número total de incidentes) x 100* | *100%* | *Trimestral* |
| *Efectividad de plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad* | *(Número total de temáticas abordadas/ Número total de temáticas planeadas) x 100* | *100%* | *Trimestral* |
| *Impacto de los ataques informáticos* | *Cantidad de ataques informáticos que interrumpieron la prestación de algunos de los servicios que la entidad ofrece a los ciudadanos o internamente* | *0* | *Trimestral* |
| *Pruebas y ejercicios de continuidad de negocio* | *(Pruebas desarrolladas / Pruebas programadas) * 100* | *100%* | *Anual* |
| *Tiempo máximo de Inactividad durante una interrupción frente al RPO adoptado por la Entidad* | *Tiempo de interrupción / RPO establecido* | *< = 12 horas* | *Anual* |
| *Disponibilidad de la operación de los servicios de TI, en un total de 720 horas esperadas en el mes* | *(1 - (TOTAL HORAS OPERACIÓN CAIDA / 720) ) * 100* | *100%* | *Trimestral* |

## 9. METRICAS.

*Se abordan las métricas contempladas en el formato 408 de la circular externa 033 de 2020 expedida por la Superintendencia Financiera de Colombia y que se relacionan en el documento excel "F.0000-164 Formato 408 - Fuente de datos.xlsx"; cuyo objetivo es "recopilar información para el cálculo de métricas e indicadores de seguridad de la información y ciberseguridad con el fin de hacer seguimiento a la gestión del riesgo de las entidades vigiladas" las mismas métricas que son transmitidas a la Delegatura para Riesgo Operacional y Ciberseguridad de dicha Entidad con periodicidad trimestral.*

## 10. ACTIVIDADES PERIODICAS

*Las siguientes son las actividades generales que soportan la etapa de Evaluación del Desempeño del SGSI:*

| ***Actividad*** | ***Responsable*** |
|---|---|
| *Gestión de riesgos y controles* | *Unidad de Riesgo Operativo* |
| *Medición de los indicadores SGSI* | *OAPS* |
| *Actualizar los planes y procedimientos del SGSI* | *OAPS* |
| *Análisis de indicadores* | *Calidad* |
| *Reuniones del comité estratégico de continuidad de negocio* | *Unidad de Riesgo Operativo* |
| *Pruebas y ejercicios de continuidad de negocio* | *OAPS Y LIDERES DE PROCESO* |
| *Pruebas y ejercicios de recuperación de desastres tecnológicos - DRP* | *OAPS* |
| *Sesiones de capacitación y sensibilización* | *OAPS* |
| *Análisis del nivel de madurez del SGSI* | *OAPS* |

## 11. EVALUACIÓN DEL DESEMPEÑO DEL SGSI.

| ***Objetivo*** | ***Revisar la efectividad del SGSI*** |
|---|---|
| *Alcance* | *Controles de seguridad y medidas establecidas en el marco de tratamiento de riesgos de seguridad* |
| *Descripción* | *La efectividad del MSPI incluye el cumplimiento de las políticas y objetivos del SGSI, y la revisión de los controles de seguridad* |
| *Entradas* | • *Políticas y objetivos del SGSI*<br>• *Resultados de análisis anteriores*<br>• *Documentación de incidentes*<br>• *Indicadores*<br>• *Análisis del nivel de madurez mediante instrumento del MSPI* |
| *Salidas* | *Informe de resultados* |
| *Actividades* | • *Identificar la política y objetivos*<br>• *Análisis de métricas*<br>• *Análisis de indicadores*<br>• *Análisis de efectividad de controles diseñados en el mapa de riesgos*<br>• *Análisis de logs* |
| *Frecuencia* | *Anual* |
| *Mejora continua* | *Aplicar las mejoras en los componentes, de acuerdo con los resultados* |



## 12. FORMATOS Y ANEXOS.

- *F.0000-164 Formato 408 - Fuente de datos.xlsx*
- *Catálogo normatividad SGSI.xlsx.*
- *Estrategias de continuidad de negocio.xlsx*
- *Catálogo de activos de información.xlsx*

- *Catálogo de componentes SGSI.xlsx*
- *Catálogo de bases de datos personales RNBD - SIC.xlsx*