El emprendimiento es de todos

Minhacienda

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020-2022

Enero de 2021

Plan de Seguridad y Privacidad de la Información 2020-2022

Equipo Directivo Fondo Adaptación:

Edgar Ortiz Pabón
Gerente

Aníbal José Pérez García
Subgerente de Gestión Del Riesgo

Andrés Parra Beltrán
Subgerente de Estructuración

Rafael Abuchaibe López
Subgerente de Proyectos

Iliana Margarita Garzón
Subgerente de Regiones

Diana Patricia Bernal
Secretaria General

Alejandro Venegas Mendoza
Jefe Oficina Asesora de Planeación y Cumplimiento

Equipo Técnico:

Jorge William Alzate Sánchez
Asesor I Líder Equipo de Trabajo Tecnología de la Información

.

Plan de Seguridad y Privacidad de la Información 2020-2022

Control de Cambios

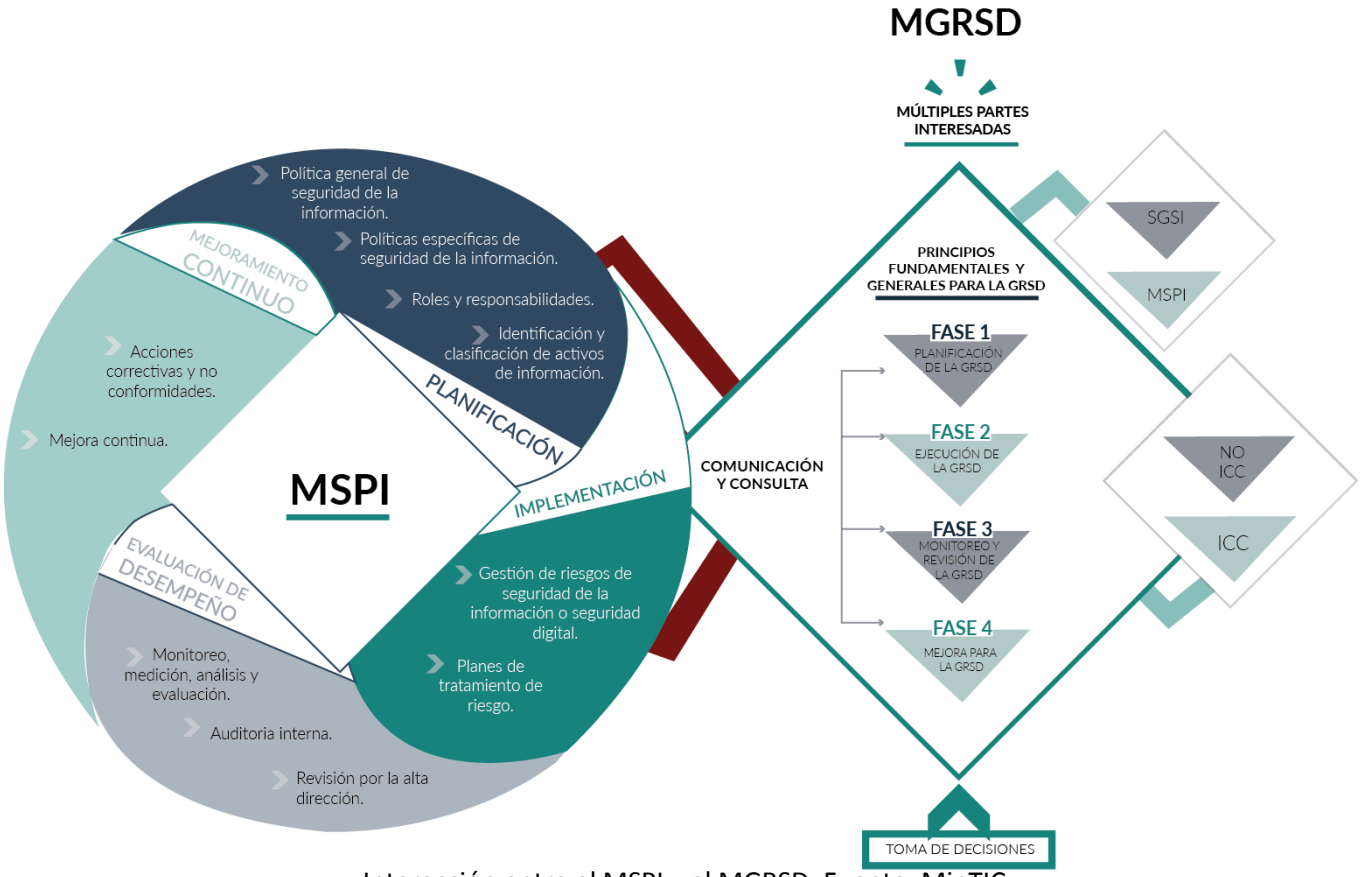
Versión	Fecha	Descripción
1	2020/01/31	Documento Inicial
2	2021/01/20	Ajustes del Plan de acuerdo al cumplimiento del 2020

Plan de Seguridad y Privacidad de la Información 2020-2022

Contenido

1. Alcance

El Plan de Seguridad y Privacidad de la Información se basa en el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI), ambos del Ministerio de las TIC como órgano regulador en la materia. Existe una interacción entre estos dos modelos que se puede ver en la siguiente imagen:



Interacción entre el MSPI y el MGRSD. Fuente: MinTIC.

El Modelo de Seguridad y Privacidad de la Información (MSPI) en su etapa de implementación, contempla las actividades de gestión y tratamiento del riesgo de seguridad digital y el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD), abarca el monitoreo, revisión y mejora para las actividades propias de la gestión de riesgos de seguridad digital.

El alcance en el Plan de Seguridad y Privacidad de la Información abarca la planificación, la implementación y la evaluación del desempeño del MSPI, así como la planificación, la ejecución, el monitoreo, revisión y mejora de todas las fases del MGRSD.

Es importante mencionar que la Entidad tiene una Política de Seguridad de la Información desde el año 2014 y que ha venido siendo actualizada cada año. Esta política puede ser consultada en el siguiente vínculo: https://drive.google.com/file/d/1mjSBJmXB7m7AEjwCLvXPOFAqTdl2qNMz/view?usp=sharing

2. Objetivos

- Establecer una ruta para la correcta planeación y ejecución de un modelo de seguridad y privacidad de la información en la Entidad.
- Formalizar una estrategia de gestión de riesgos de seguridad digital en todos los procesos de la Entidad.
- Promover el uso de mejores prácticas de seguridad de la información en todo nivel dentro y fuera de la Entidad con todas las partes interesadas.
- Establecer un Sistema de Gestión en Seguridad de la Información en la Entidad, que conlleve a las actividades del ciclo Deming de la en el Planear (P), Hacer (H), Verificar (V) y Actuar (A); de cualquier sistema de Gestión.
- Velar por cumplimiento normativo dado por el Gobierno a través del Ministerio de las TIC, con respecto a la Seguridad y Privacidad de la Información en todas las entidades del Estado del orden Nacional y Territorial.

3. Lineamientos para su Implementación

El Comité Institucional de Gestión y Desempeño (CIGD), dará las directrices para la implementación del Modelo de Seguridad y Privacidad de la

Información y del Modelo de Gestión de Riesgos de Seguridad y Privacidad de la Información. El CIGD debe articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de los Modelos. Así mismo se designa como representante por la Alta Dirección ante el Sistema de Gestión de Seguridad de la Información al jefe de la Oficina Asesora de Planeación y Cumplimiento y como responsable de la seguridad de la información de la entidad al líder del Equipo de Trabajo de Tecnología de la Información, quien a su vez se apoyará en expertos técnicos para la implementación, puesta en marcha, mantenimiento, supervisión y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

4. Marco Normativo

MARCO LEGAL

- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional” .
- Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Ley 962 de 2005. “Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;”
- Ley 1150 de 2007. “Seguridad de la información electrónica en contratación en línea”.
- Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.
- Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.
- Decreto 886 de 2014. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- Decreto 1083 de 2015. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad Digital.

REQUISITOS TÉCNICOS

- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Modelo Nacional de Gestión de Riesgos de Seguridad Digital – MINTIC.
- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad.

5. Modelo de Seguridad y Privacidad de la Información - MSPI

El Modelo de Seguridad y Privacidad de la Información (MSPI) desarrollado por MINTIC, contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información. En la siguiente figura se presenta el ciclo de operación:

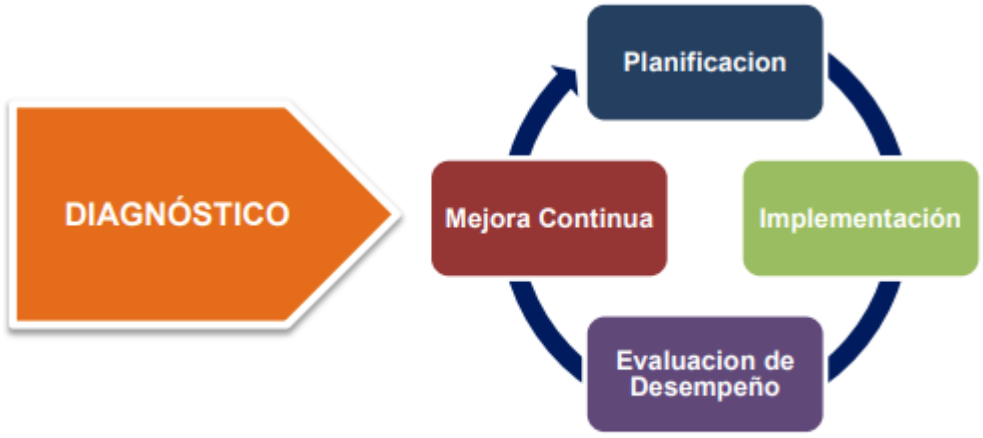


Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

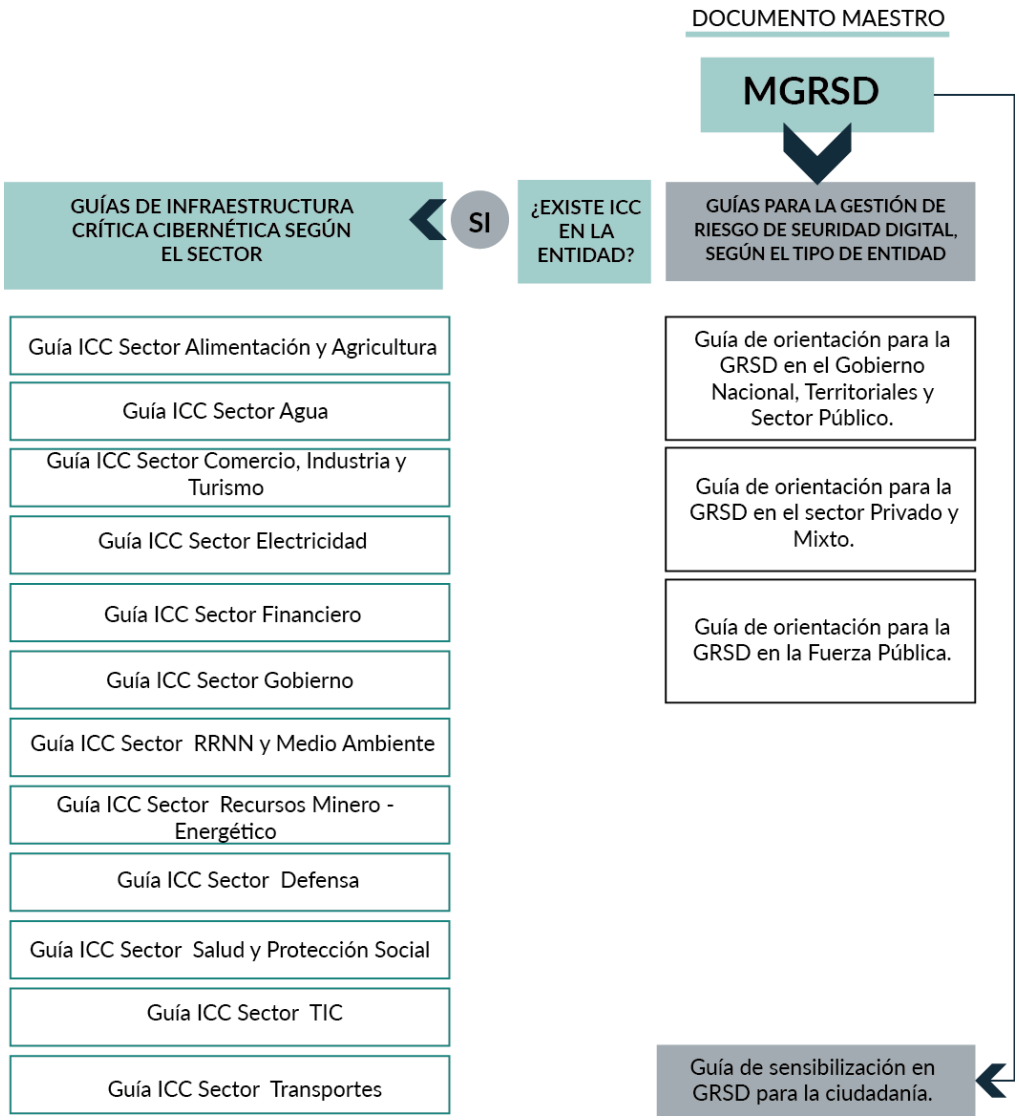
Fuente: MINTIC

El MSPI propone unas metas, resultados e instrumentos que deben ser ejecutados de acuerdo a unos lineamientos y guías que propone el Ministerio de las TIC, basado en las mejores prácticas en la materia. Este modelo conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindado confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

6. Modelo Nacional de Gestión de Riesgos de Seguridad Digital - MGRSD

Este modelo fue desarrollado por MINTIC, para dar cumplimiento a la política nacional de seguridad establecida en el documento CONPES 3854 del 11 de abril de 2015. El modelo está orientado a incrementar la conciencia ciudadana y las capacidades del Gobierno y de las empresas en general para identificar, analizar, evaluar y tratar los riesgos de seguridad digital.

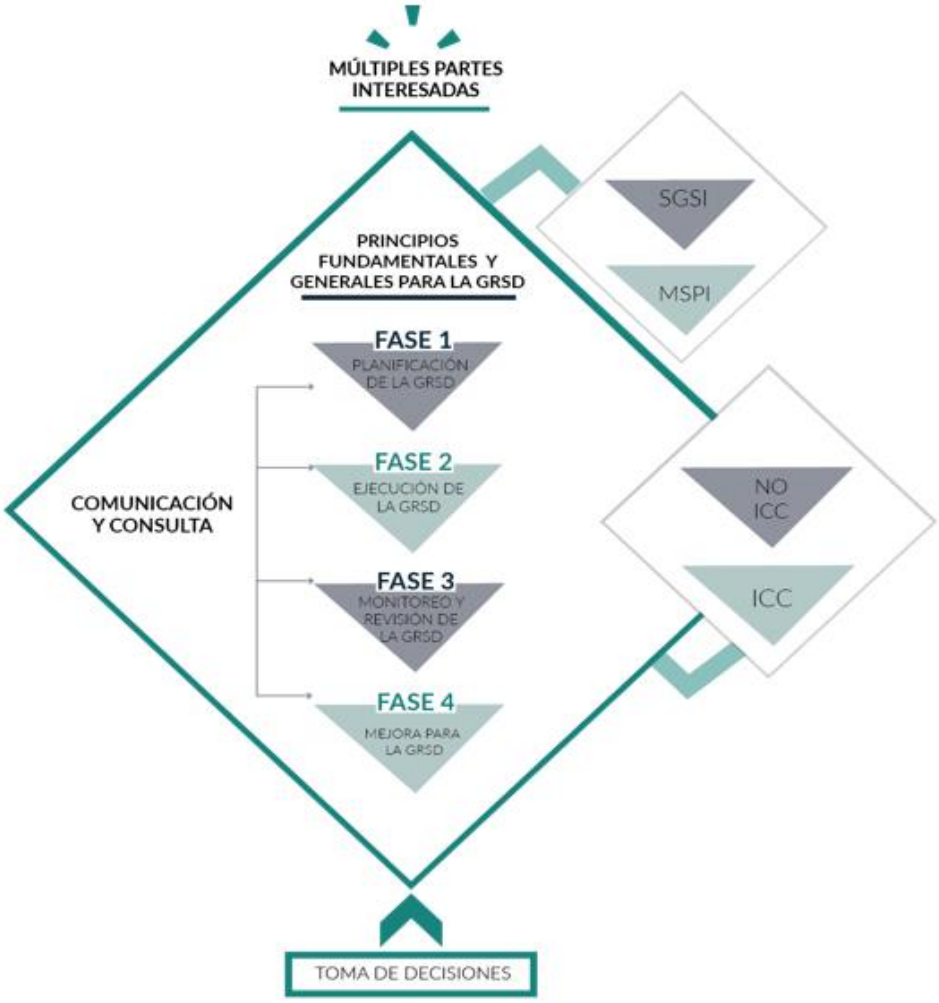
El MGRSD está estructurado como lo indica la siguiente imagen:



Fuente: MINTIC

En este modelo también se presentan unas guías para la gestión del riesgo de seguridad digital según el tipo de sector. (Gobierno nacional, territoriales y sector público; sector privado y mixto; sector fuerza pública y ciudadanía en general).

Así mismo el marco conceptual del modelo propone las siguientes fases:



Fuente: MINTIC

- Planificación de la GRSD: Consiste en la definición de contextos, variables para posterior análisis y evaluación de riesgos y en general todos los aspectos que se desarrollarán en los demás componentes.
- Ejecución de la GRSD: Consiste en el desarrollo de las actividades para el análisis y evaluación de los riesgos de seguridad digital, se identifican aspectos inherentes y residuales de los mismos, así como la definición del tratamiento de los riesgos en el marco de la seguridad de la información y particularmente en las ICC.
- Monitoreo y Revisión de la GRSD: Consiste en la permanente evaluación que permita asegurar que dicha gestión se está llevando a cabo bajo los aspectos y lineamientos definidos por cualquier entidad para sus riesgos de seguridad digital. Se desprenden aspectos de reporte y aseguramiento

del seguimiento de todos los planes de tratamiento que se derivan de su aplicación.

- Mejora de la GRSD: Componente que tiene una orientación para establecer los mecanismos que permitan alcanzar un mayor grado de madurez de la GRSD en cualquier entidad. El mejoramiento continuo se estará dando de forma progresiva en la medida que se cumplan con los objetivos de la GRSD así como la definición y aplicación modelos de evaluación de riesgos de seguridad digital con una orientación menos subjetiva y basada en modelos matemáticos que brinden mayor exactitud en la medición de las variables de impacto de los riesgos de seguridad digital sobre los activos de información y las ICC identificadas.

7. Política y Lineamientos de Gestión del Riesgo en el Fondo Adaptación

La política y lineamientos de gestión del riesgo en el Fondo Adaptación integran un proceso de gestión del riesgo de manera transversal en toda la gestión de la entidad, en sus políticas de operación y en general en la cultura organizacional. Incluye además los planteamientos legales y reglamentarios referidos a la gestión del riesgo de seguridad digital, de acuerdo al Anexo 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas. En el siguiente vínculo se puede consultar la política:

https://drive.google.com/file/d/15RjZBzZPUgHOwGUlr2DqCIfa7ZlbX746/view?usp=sharing

8. Actividades del Plan de Seguridad y Privacidad de la Información y del Plan de Tratamiento de Riesgos

De acuerdo con los modelos anteriormente descritos y la política y lineamientos de gestión del riesgo del Fondo Adaptación, se proponen las siguientes

actividades del plan de seguridad y privacidad de la información y de tratamiento del riesgo de seguridad digital:

Etapa	Actividad	Fecha Inicio	Fecha Fin	Estado
Diagnóstico	Análisis de resultados del FURAG 2019	20-jul-2020	24-jul-2020	Ejecutado
	Análisis de entregables del MSPI y su cumplimiento	20-jul-2020	24-jul-2020	Ejecutado
	Análisis de las políticas de SPI y seguridad digital en la entidad	28-jul-2020	31-jul-2020	Ejecutado
	Análisis del mapa de procesos e identificación de aspectos de seguridad de la información	28-jul-2020	31-jul-2020	Ejecutado
	Análisis de auditorías externas en seguridad de la información	28-jul-2020	31-jul-2020	Ejecutado
	Análisis de activos de información y la documentación en la entidad	28-jul-2020	07-Ago-2020	Ejecutado
	Análisis de la gestión de riesgos en seguridad de la información o seguridad digital y el estado en la entidad	28-jul-2020	07-Ago-2020	Ejecutado
Planeación	Elaboración, presentación y aprobación de las	04-Ago-2020	29-Ago-2020	En ejecución

	políticas de seguridad y privacidad de la información			
	Elaboración, presentación y aprobación de los procedimientos de seguridad y privacidad de la información	25-Ago-2020	30-Sep-2020	En ejecución
	Ajuste en la documentación institucional existente en la gestión de activos de información	01-Sep-2020	26-Sep-2020	Ejecutado
	Presentación, aprobación y oficialización de instrumentos de activos de información	29-Sep-2020	30-Sep-2020	Ejecutado
	Incorporación de políticas y lineamientos de gestión de riesgos de seguridad digital en la política institucional de riesgos	15-Sep-2020	10-Oct-2020	Ejecutado
	Identificación de activos de información relevantes/críticos como objeto de trabajo en la gestión de riesgos de SD	15-Sep-2020	10-Oct-2020	Ejecutado

	Identificación, análisis y evaluación de riesgos de seguridad digital y/o seguridad de la información	01-Oct-2020	31-Oct-2020	Ejecutado
	Aceptación y aprobación de riesgos de SD/SPI identificados	01-Feb-2021	15-Feb-2021	Sin Iniciar
	Elaboración del Plan de Tratamiento de Riesgos de SD/SPI	01-Feb-2021	28-Feb-2021	Sin Iniciar
	Aceptación y aprobación del Plan de Tratamiento de Riesgos	01-Mar-2021	15-Mar-2021	Sin Iniciar
	Seguimiento al estado de plan de tratamiento de riesgos identificados y verificación de evidencias	01-Mar-2021	30-Abr-2021	Sin Iniciar
	Evaluación de riesgos residuales	01-May-2021	15-May-2021	Sin Iniciar
	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	16-May-2021	31-May-2021	Sin Iniciar
	Revisión y mejoramiento del procedimiento de	15-Dic-2020	31-Dic-2020	Ejecutado

	gestión de incidentes			
	Publicación y socialización del procedimiento de gestión de incidentes	15-Feb-2021	28-Feb-2021	Sin Iniciar
	Elaboración de la matriz de contacto con las autoridades y establecer contacto	15-Dic-2020	31-Dic-2020	Ejecutado
	Elaborar, publicar y socializar el plan de gestión de cultura organizacional en la apropiación del SGSI	01-Dic-2020	28-Feb-2021	En ejecución
	Implementar estrategias del plan de gestión de cultura en la apropiación del SGSI	01-Dic-2020	30-Nov-2021	En ejecución
	Analizar los instrumentos de medición del plan de cultura en apropiación en el SGSI	01-Dic-2021	31-Dic-2021	Sin Iniciar
	Crear la matriz de verificación de requisitos legales de SPI y evidenciar su cumplimiento	17-Nov-2020	21-Nov-2020	Ejecutado
	Formular, presentar, aprobar y oficializar los	22-Dic-2020	31-Dic-2020	En ejecución

	indicadores del SGSI			
	Apoyar en la elaboración de la política de tratamiento de datos personales y el diseño del procedimiento para el registro de datos personales ante la SIC.	08-Dic-2020	31-Dic-2020	Ejecutado
	Elaborar el plan de diagnóstico para la transición de IPV4 a IPV6.	01-Mar-2021	31-Mar-2021	Sin Iniciar
Ejecución	Elaborar, aprobar y socializar la estrategia de planificación y control operacional	01-Abr-2021	30-Sep-2021	Sin Iniciar
	Informe de ejecución del Plan de tratamiento de riesgos	01-Oct-2021	15-Oct-2021	Sin Iniciar
Monitoreo, revisión y reporte de la GRSD	Auditorías Internas y/o externas	15-Oct-2021	15-Nov-2021	Sin Iniciar
	Medición del desempeño	01-Nov-2021	15-Nov-2021	Sin Iniciar
	Reporte con los indicadores de gestión de seguridad y privacidad de la información y de la gestión del riesgo de seguridad digital	15-Nov-2021	30-Nov-2021	Sin Iniciar

9. Presupuesto

El Plan de Seguridad y Privacidad de la Información, así como el Plan de Tratamiento de Riesgos en Seguridad Digital, se financian con el presupuesto del Proyecto de Fortalecimiento de la Capacidad Institucional en la Gestión de Información, código BPIN 2019011000266 del DNP.