



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2022

TABLA DE CONTENIDO

<u>1.</u>	<u>INTRODUCCIÓN</u>	<u>3</u>
<u>2.</u>	<u>OBJETIVO DEL DOCUMENTO</u>	<u>3</u>
<u>2.1.</u>	<u>OBJETIVOS ESPECÍFICOS</u>	<u>3</u>
<u>3.</u>	<u>ALCANCE DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y CONTINUIDAD DEL NEGOCIO</u>	<u>4</u>
<u>4.</u>	<u>ANTECEDENTES</u>	<u>4</u>
<u>5.</u>	<u>MARCO NORMATIVO.....</u>	<u>5</u>
<u>6.</u>	<u>PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, PROTECCIÓN DE DATOS PERSONALES Y CONTINUIDAD DEL NEGOCIO</u>	<u>6</u>
<u>6.1.</u>	<u>IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD (II FASE)</u>	<u>9</u>
<u>7.</u>	<u>MAPA DE RUTA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....</u>	<u>11</u>
<u>8.</u>	<u>SEGUIMIENTO Y CONTROL</u>	<u>16</u>
<u>9.</u>	<u>ANEXOS.....</u>	<u>16</u>

1. INTRODUCCIÓN

Este documento tiene como fin presentar un plan de acción para el establecimiento, implementación, operación, monitoreo, revisión y mejora continua del Sistema Integrado de Gestión de Seguridad de la Información, Protección de Datos Personales y Continuidad del Negocio (SIGSI-PDP-CN) en el que el SGC se encuentra trabajando.

Esto demuestra que la entidad se encuentra comprometida con la seguridad y privacidad de la información, la protección de datos personales y la continuidad de los procesos del negocio, y de los servicios tecnológicos, asignando los recursos necesarios para garantizar que los procesos de la entidad se encuentren incluidos en el alcance de dichos sistemas, permitiéndole dar cumplimiento a sus objetivos estratégicos y enfocar las acciones del sistema integrado en términos de la gestión efectiva del riesgo.

2. OBJETIVO DEL DOCUMENTO

Definir un Plan de Seguridad y Privacidad de la Información que fortalezca el SIGSI-PDP- CN del Servicio Geológico Colombiano, acorde a los requerimientos del modelo de seguridad de la estrategia de la política de gobierno digital, protección de datos personales, requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes.

2.1. OBJETIVOS ESPECÍFICOS

- Definir las acciones que den continuidad al proceso que se ha venido desarrollando la entidad en la implementación del Sistema Integrado de Gestión de Seguridad de la Información, Protección de Datos Personales y Continuidad del Negocio.
- Fortalecer la implementación del Sistema Integrado de Gestión de Seguridad de la Información, Protección de Datos Personales y Continuidad del Negocio de la entidad, verificando los requerimientos establecidos en el modelo de seguridad de la estrategia de la Política de Gobierno Digital.
- Establecer lineamientos que permitan continuar con la gestión de la seguridad de la información al interior de la entidad.
- Presentar el plan estratégico para el establecimiento, implementación, operación, monitoreo, revisión y mejora continua del Sistema Integrado de Gestión de Seguridad de la Información, Protección de Datos Personales y Continuidad del Negocio en el SGC.

3. ALCANCE DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y CONTINUIDAD DEL NEGOCIO

El Plan de Seguridad y Privacidad de la Información considera los controles de la norma NTC/ISO 27001:2013, las disposiciones de la ley de protección de datos personales, la metodología de gestión de riesgos del Departamento Administrativo de la Función Pública, los procesos del SGC y los lineamientos del Modelo de Seguridad y Privacidad de la Información -MSPI de la Estrategia de Gobierno Digital GD con el fin de determinar la estrategia de implementación de los controles de seguridad de la información requeridos para el SGC.

4. ANTECEDENTES

El Servicio Geológico Colombiano como organismo generador y administrador de información geocientífica, debe garantizar durante todo el ciclo de gestión de la información, que se tengan los mecanismos de seguridad necesarios y adecuados para proteger sus activos de amenazas a los que la Entidad pueda verse expuesta.

La postura de seguridad de la información del SGC le ha permitido construir una estrategia de gestión del ciclo de vida de las vulnerabilidades en donde se hace la detección, remediación y afinamiento con un esquema de priorización de riesgo basado en la criticidad de los activos, producto de la matriz de análisis de riesgo; por otra parte se implementan estrategias de defensa en profundidad tales como la adopción de estándares de aseguramiento de plataforma tecnológica, disposición de controles a lo largo de toda la cadena de gestión del ciclo de vida de la información, de igual manera una clara orientación a la gestión del riesgo como eje central del SIGSI-PDP-CN.

En comunión con lo anterior, el SGC implementa los planes de tratamiento de riesgo diseñados con anterioridad y establece unos indicadores de gestión que permiten la administración y operación de los controles (productos o servicios) técnicos aplicados para mitigación de riesgos en el marco de la mejora continua.

Desde el año 2014 el SGC se encuentra gestionando acciones relacionadas con la seguridad de la información, con aliados estratégicos como la Universidad de los Andes y el personal de la entidad se han venido desarrollando actividades como:

- Diagnóstico del estado de seguridad de la entidad, a través de un ejercicio de Arquitectura empresarial.
- Diagnóstico de cumplimiento del MSPI
- Diagnóstico, Planeación e Implementación del SIGSI-PDP-CN
- Operación y mantenimiento de herramientas de seguridad informática que se

enmarcan en los diferentes planes de tratamiento de riesgos

- Elaboración, divulgación y adopción de políticas, procedimientos y estándares del SIGSI-PDP-CN.

En 2021 se realizó una tarea importante de actualización de la matriz de riesgo (activos.) así como también la implementación del sistema de Gestión de la Continuidad del Negocio lo que permitió concretar la estrategia de defensa en profundidad y los planes de seguridad organizacional para proteger los activos de la Entidad.

Esto demuestra que la entidad está comprometida con la seguridad de la información, protección de datos personales y continuidad del negocio, asignando los recursos necesarios para asegurar que los procesos de la Entidad se encuentren incluidos en el alcance del sistema, permitiéndole a la entidad dar cumplimiento a sus objetivos estratégicos, alineados con las fases de Arquitectura Empresarial acorde al trabajo que ha venido desarrollando la Entidad.

5. MARCO NORMATIVO

Conforme con lo establecido en la normatividad vigente el Servicio Geológico Colombiano - SSGC, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación de la Política General de Seguridad de la información, Protección de Datos Personales y Continuidad del Negocio de los Servicios de TI en la Entidad:

- Constitución Política de Colombia. Artículos 15, 209 y 269.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- CONPES 3854 de 2016. Política Nacional de Seguridad Digital.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 2106 de 2019. Establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.
- MRAE - MinTIC 2021.
- ISO 27001, ISO 22301.

6. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, PROTECCIÓN DE DATOS PERSONALES Y CONTINUIDAD DEL NEGOCIO

De acuerdo con el Modelo de Seguridad y Privacidad de la Información de la política de Gobierno Digital, se contempla el siguiente ciclo de operación que contiene (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información. El Servicio Geológico Colombiano cuenta con un Sistema Integrado SIGSI-PDP-CN, por tanto, el ciclo de operación se ha adoptado para dicho sistema en conjunto, es decir: gestión de la seguridad de la información, protección de datos personales y continuidad del negocio.

Ilustración 1. Ciclo de operación Modelo de Seguridad y Privacidad de la Información



- **Fase Diagnóstico:** Permite identificar el estado actual de la Entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, protección de datos personales y continuidad del negocio. Esta fase se encuentra ejecutada en un 100%.
- **Fase Planificación (Planear):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos. Esta fase se encuentra ejecutada en un 100%.
- **Fase Implementación (Hacer):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones (planes de tratamiento de riesgo) para lograr mejoras planteadas. Esta fase se encuentra ejecutada así:
 - Gestión de seguridad de la Información: 82% ejecutada
 - Protección de datos personales: 100% ejecutada
 - Continuidad del Negocio: 100% ejecutada
- **Fase Evaluación de desempeño (Verificar):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas. Esta fase se encuentra ejecutada así:
 - Gestión de seguridad de la Información: 62% ejecutada
 - Protección de datos personales: 50% ejecutada
 - Continuidad del Negocio: 35% ejecutada
- **Fase Mejora Continua (Actuar):** Se analizan los resultados de las acciones

implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones. Estafase se ejecuta de manera constante con el uso y apropiación del SIGSI-PDP-CN

Además de lo anterior, se ha venido desarrollando durante todo el año 2020 las siguientes actividades:

- Renovación de soluciones de seguridad informática:
 - Protección avanzada de EndPoint
 - SIEM
 - Control de acceso a la red (NAC)
- Adquisición de nuevas soluciones de seguridad informática
 - Solución de Orquestación, Automatización y Respuesta en seguridad informática (SOAR)
 - Solución de gestión del ciclo de vida de vulnerabilidades en plataforma tecnológica
 - Solución de gestión del ciclo de vida de vulnerabilidades en aplicaciones web (DAST)
 - Solución de gestión del ciclo de vida de vulnerabilidades en aplicaciones web (SAST)
 - Appliance de propósito específico IPS
- Afinamiento e implementación de mejores prácticas en seguridad informática paraproductos/servicios existentes:
 - Imperva
 - FAM
 - WAF
 - DAM
 - Splunk (SIEM)
 - McAfee
 - CEB
 - EDR
 - IPS
 - ForeScout
 - NAC
- Adopción de estándares de configuración segura de servidores y estaciones de trabajo (*hardening*)
- Adopción de mejores prácticas en cuanto a:
 - Higiene del Directorio Activo
 - Configuración de estaciones de trabajo altamente fortificadas como *pivot*

deautenticación a servidores críticos (PAW)

- Adopción e implementación del marco de referencia CIS-20
- Diseño, revisión y creación de políticas, procedimientos y estándares en el marco del SIGSI-PDP-CN.
- Implementación de Planes de tratamiento de riesgo.
- Integración y participación en el proyecto sectorial de Gobierno, Riesgo y Cumplimiento (GRC) liderado por el Ministerio de Minas y Energía

6.1. IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD (II FASE)

Para la implementación del SIGSI-PDP-CN, el Servicio Geológico Colombiano realizó inmensos esfuerzos que permitieron avanzar en todos los frentes del sistema integrado tal y como se evidencia en el numeral 5. Para dar continuidad a la fase de implementación (hacer), fase de evaluación de desempeño (verificar) y fase de mejora continua (actuar) se han diseñado los siguientes proyectos:

1. Organización y estructuración del grupo de seguridad de la información:
 - Iniciativa orientada a estructurar un equipo de trabajo que pueda afrontar los inmensos desafíos que representa el ciclo PHVA del SIGSI-PDP-CN, pretendiendo dar forma a las responsabilidades y roles de aplicación en cuanto a cada subsistema, así como también hacer efectiva la gestión del riesgo al interior del SGC.
 - Mitiga 127 riesgos altos y 163 riesgos medios
2. Programa de capacitación y concientización del SIGSI-PDP-CN para equipo de trabajo (profundización) y usuarios con ejercicios prácticos y conceptos de *gamification*
 - Iniciativa orientada a establecer un programa de concientización maduro, sostenible y repetible en el tiempo que no solo se enfoque en los usuarios del SIGSI-PDP-CN sino que también involucre esquemas de capacitación de medio y alto nivel para el equipo de trabajo de seguridad de la información
 - Mitiga 182 riesgos altos y 177 riesgos medios
3. Gobierno efectivo del SIGSI-PDP-CN
 - Iniciativa enmarcada en el ciclo PHVA del SIGSI-PDP-CN y que permitirá avanzar sustancialmente en la adopción efectiva del sistema integrado, dará cumplimiento a los requerimientos normativos y apoyará decididamente la estrategia de gestión de riesgos.
 - Mitiga 146 riesgos altos y 402 riesgos medios

4. Implementación, mejora y fortalecimiento de soluciones de seguridad informática y ciberseguridad
 - Iniciativa que, a través de personas, productos y servicios, se alinea con la estrategia de defensa en profundidad y que permite el aseguramiento de la plataforma tecnológica del SGC.
 - Mitiga 700 riesgos altos y 611 riesgos medios

7. MAPA DE RUTA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Todos los proyectos serán responsabilidad de la DGI en cabeza del Oficial de Seguridad de la Información del SGC

PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	FECHA	
				INICIO	FIN
Organización y estructuración del grupo de seguridad de la información	Diseño de la estructura organizacional	Avance del proyecto	<ul style="list-style-type: none"> Documento con análisis de requerimientos y necesidades a satisfacer en términos de la gestión del SIGSI-PDP-CN Estructura organizacional del grupo de seguridad de la información 	Enero 2021	Abril 2022
	Construcción de matriz de roles y responsabilidades	Avance del proyecto	<ul style="list-style-type: none"> Matriz de roles y responsabilidades elaborada 	Enero 2022	Junio 2022
Programa de capacitación y concientización del SIGSI-PDP-CN	Implementación del programa de capacitación y concientización	Avance del proyecto	<ul style="list-style-type: none"> Adquisición de piezas multimediales Despliegue y ejecución del programa de capacitación y concientización en SI 	Febrero 2022	Diciembre 2022
Gobierno efectivo del SIGSI-PDP-CN	Adopción de Archer como plataforma GRC	Avance del proyecto	<ul style="list-style-type: none"> Actualización de la matriz de riesgos Cargue de la matriz de riesgos en la plataforma Archer Automatización de flujos de trabajo en Archer 	Febrero 2021	Mayo 2022

PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	FECHA	
				INICIO	FIN
	Estandarización a través de políticas y procedimientos	Avance de proyecto	<ul style="list-style-type: none"> Políticas actualizadas Nuevas políticas creadas Procedimientos actualizados Nuevos procedimientos creados 	Febrero 2022	Diciembre 2022
	Implementación de indicadores	Avance de proyecto	<ul style="list-style-type: none"> Definición de indicadores de gestión del Sistema Integrado Implementación y automatización de los indicadores de gestión del Sistema Integrado 	Febrero 2022	Diciembre 2022
	Implementación de planes de tratamiento de riesgo (PTR)	Planes de tratamiento implementados	<ul style="list-style-type: none"> Actualización de planes de tratamiento de riesgo (matriz de riesgo) Priorización de implementación de PTR Implementación de PTR 	Febrero 2022	Diciembre 2022
	Actualización de inventario y RNBD	Avance de proyecto	<ul style="list-style-type: none"> Inventario de bases de datos que contiene información personal actualizado Registro de la actualización en el RNBD 	Febrero 2022	Diciembre 2022
	Actualización de documentación del sistema de protección de datos personales	Avance de proyecto	<ul style="list-style-type: none"> Documentación actualizada de requerirse en caso de que salga nueva normatividad sobre este tema 	Febrero 2022	Diciembre 2022

Implementación, mejora y fortalecimiento de soluciones de seguridad informática y ciberseguridad	Renovación y actualización de PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN plataforma GigaMon e Imperva (DAM), adquisición de una solución Cloud WAF y adquisición de una solución de monitoreo, auditoría y control de repositorios de archivos	Avance de proyecto	<ul style="list-style-type: none"> • Documento con requerimientos técnicos para adquisición de productos y servicios • Adquisición de solución de seguridad informática • Despliegue e implementación del producto adquirido, integración de políticas y validación de funcionamiento de acuerdo con lo adquirido 	Febrero 2022	Diciembre 2022
	Adquisición de una solución de Gestión de Identidad	Avance de proyecto	<ul style="list-style-type: none"> • Documento con requerimientos técnicos para adquisición de productos y servicios • Adquisición de solución de seguridad informática • Despliegue e implementación del producto adquirido, integración de políticas y validación de funcionamiento de acuerdo con lo adquirido 	Actualmente no se cuenta con presupuesto para la adquisición de esta solución	
	Adquisición de una solución de Prevención de Fuga de Información	Avance de proyecto	<ul style="list-style-type: none"> • Documento con requerimientos técnicos para adquisición de productos y servicios • Adquisición de solución de seguridad informática • Despliegue e implementación del producto adquirido, integración de políticas y validación de funcionamiento de acuerdo con lo adquirido 	Actualmente no se cuenta con presupuesto para la adquisición de esta solución	

<p>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p> <p>Aseguramiento de plataformas</p>	<p>Porcentaje de servidores asegurados</p>	<ul style="list-style-type: none"> • Implementación de <i>guide lines</i> de Microsoft para realizar el proceso de aseguramiento de servidores • Implementación de estándares <i>CIS Benchmark</i> para realizar el proceso de aseguramiento de servidores Linux y dispositivos activos de red 	<p>Febrero 2022</p>	<p>Diciembre 2022</p>
<p>Gestión del ciclo de vida de vulnerabilidades</p>	<p>Porcentaje de vulnerabilidades gestionadas</p>	<ul style="list-style-type: none"> • Gestión de vulnerabilidades en plataforma(servidores, estaciones de trabajo, dispositivos activos de red) a través de InsightVM® • Gestión de vulnerabilidades en aplicacionesweb a través de InsightAppSec® • Gestión de vulnerabilidades en código fuente de software desarrollado <i>in-house</i> a través de SonarQube® 	<p>Febrero 2022</p>	<p>Diciembre 2022</p>

PROYECTO	ACTIVIDAD	META /INDICADO R	PRODUCTO /EVIDENCIA	FECHA	
				INICIO	FIN
	Orquestación, automatización y respuesta a incidentes de seguridad informática	Porcentaje de incidentes gestionados	<ul style="list-style-type: none"> Automatización de casos de uso de gestión de incidentes a través de SOAR a través de INCman® Implementación de casos de uso de recolección, normalización, correlación, visualización, alertamiento y automatización de <i>logs</i> (registros) en plataforma tecnológica enfocados a seguridad informática a través de Splunk® 	Febrero 2022	Diciembre 2022
	Seguridad de la red	Avance de proyecto	<ul style="list-style-type: none"> Rediseño e implementación del esquema de protección del perímetro de red con el <i>appliance</i> IPS de McAfee. Aplicación de políticas de control de acceso a la red a través de la implementación efectiva del <i>appliance</i> NAC de Forescout® Diseño y proyección de implementación (2022) de un esquema efectivo de microsegmentación en la red corporativa del SGC 	Febrero 2022	Diciembre 2022

8. SEGUIMIENTO Y CONTROL

El seguimiento y monitoreo a la ejecución de las actividades establecidas para los planes/proyectos del plan de seguridad y privacidad de la información, se realizará a través del Plan de Acción y de las herramientas definidas en el Sistema de Gestión Institucional del SGC, se determinará la periodicidad en Cronograma de Seguimiento a los Planes definidos en el Decreto 612 de 2018.

9. ANEXOS

Las evidencias de los productos desarrollados durante el período 2019 – 2020 bajo el SIGSI-PDP-CN y el modelo de seguridad y privacidad de la información de MinTIC está almacenada en el repositorio institucional dado el volumen y peso de los documentos.

- Informe Técnico Vulnerabilidades Geológico
- SGC - Informe Análisis Gap ISO 22301
- Informe de Análisis de Brechas de SGSI
- Diagnóstico Protección Datos Personales Responsabilidad Demostrada
- Informe Técnico EH Geológico
- Instrumento Evaluación MSPI Geológico
- Plan de Sensibilización y Capacitación
- Contexto Organizacional
- Manual del Sistema SGSI
- Política del Sistema de Seguridad de la Información, Protección de datos Personales y Continuidad de Negocio
- Matriz DOFA
- Activos de Información SGC
- Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información
- Declaración de Aplicabilidad SGC
- Manual de Políticas específicas de Seguridad de Información
- Procedimientos y estándares de seguridad de la información
- Informe BIA SGC
- Análisis de Riesgos SGC
- Estrategias de continuidad
- Plan de Continuidad
- Manual de crisis
- Plan de Recuperación de Desastres
- PRR - Red Sismológica (Falla Datacenter Principal)
- PRR - Red Sismológica (Falla Internet)
- PRR - Red Sismológica (Falla Servidor Principal)
- Verificación de la implementación del MSPI

- Plan de reporte de incidentes y resultados de pruebas técnicas
- Plan de mejora continua MSPI v1.0