PLAN DE SEGURIDAD Y PRIVACIDAD DELA INFORMACIÓN

2023

TABLA DE CONTENIDO

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 (SIG-SI-PDP-CN) en el que el Servicio Geológico Colombiano (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 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 y la ciberseguridad.

2. Objetivo del documento

Definir un Plan de Seguridad y Privacidad de la Información que fortalezca el SIG-SI-PDP-CN del SGC, acorde a los requerimientos del modelo de seguridad y 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 en 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 y 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 Política de Gobierno Digital 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 implementación de la Arquitectura de Defensa en Profundidad en la Entidad en la cual se evidencian iniciativas tales como la adopción de estándares de aseguramiento de plataforma tecnológica (*hardening*), 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 y disposición de controles a lo largo de toda la cadena de gestión del ciclo de vida de la información; y una clara orientación a la gestión del riesgo como eje central del SIGSI-PDP-CN le permiten a la Entidad mitigar los diferentes riesgos y responder de manera proactiva a los desafíos de ciberseguridad presentes hoy en día.

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 2013 el SGC inició un proceso de cumplimiento y apego al marco regulatorio y a las diferentes disposiciones que en materia de seguridad de la información ha generado el gobierno central, en tal virtud se han desarrollado actividades tales 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.
- Gestión eficiente del riesgo con el fin de fijar la postura de seguridad y la implementación de la arquitectura de defensa en profundidad.

En el año 2021 se realizó una tarea importante de actualización de la matriz de riesgo y 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 dar cumplimiento a sus objetivos estratégicos, alineados con las fases de Arquitectura Empresarial y con la misión de proveer los servicios de Integridad, Confidencialidad y Disponibilidad de la Información.

5. Marco regulatorio

Conforme con lo establecido en la normatividad vigente el SGC, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del Sistema Integrado 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 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
- 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 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.
- CONPES 3995 de 2020. Política nacional de confianza y seguridad digital.

- Resolución MinTIC 1519 del 2020 - Condiciones mínimas técnicas y de seguridad digital (anexo 3)
- Resolución 500 de 2021 Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- Directiva presidencial 03 de 2021 - Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos
- Decreto 338 de 2022. Por el cual se adiciona el Titulo 21 a la Parte 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"
- Resolución 746 de 2022 por la cual se fortalece el MSPI y se definen lineamientos adicionales a los establecidos.
- 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 SIG-SI-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.

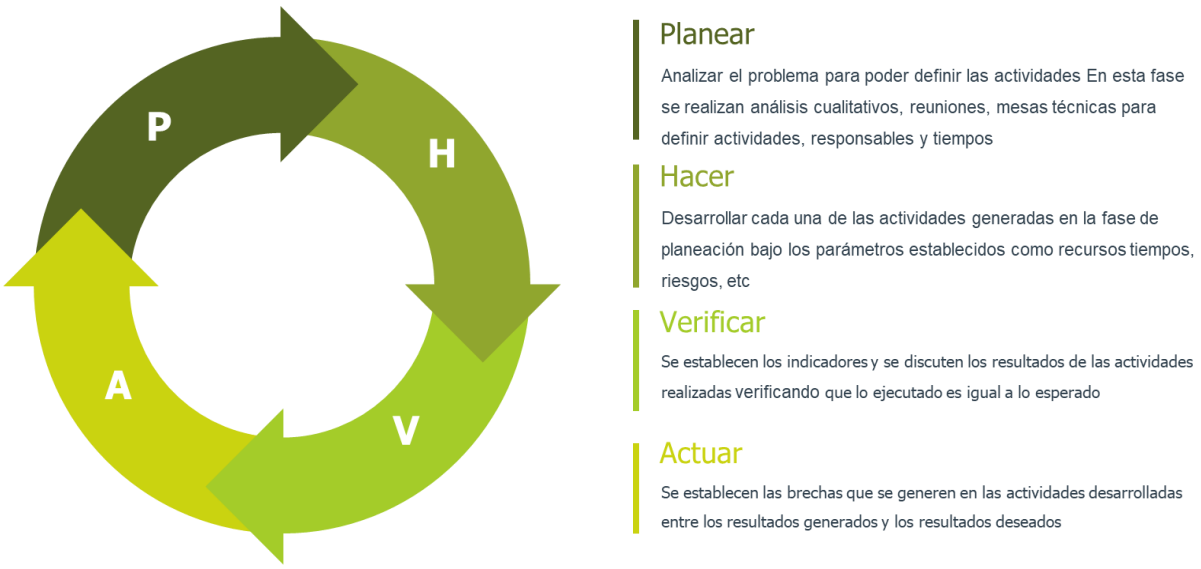

Ilustración 1. Ciclo de operación Modelo de Seguridad y Privacidad de la Información (elaboración propia 2022)

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: 100% 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: 72% ejecutada
    - Protección de datos personales: 70% ejecutada
    - Continuidad del Negocio: 65% 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. Esta fase se ejecuta de manera constante con el uso y apropiación del SIG-SI-PDP-CN

Además de lo anterior, se han desarrollado las siguientes actividades en relación con los planes estratégicos de años anteriores:

- Renovación y/o adquisición de controles de seguridad informática:
    - Protección avanzada de Endpoint
    - SIEM
    - Control de acceso a la red (NAC)
    - 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)
    - Sistema de Prevención de Intrusos (IPS)
- Mejora continua de los controles implementados a través de la implementación de mejores prácticas en seguridad informática y en concordancia con las lecciones aprendidas de los incidentes de seguridad atendidos así como también de la documentación técnica disponible a través de portales de fabricantes y de investigadores reconocidos. Los controles implementados son:
    - Imperva
        - WAF
        - DAM/DBF

        - CloudWAF
    - Splunk (SIEM)
    - Trellix
        - CEB
        - EDR
        - IPS
    - ForeScout (NAC)
    - Rapid7
        - InsightAppSec (DAST)
        - InsightVM
    - SonarQube Enterprise (SAST)
    - Varonis
        - DatAdvantage
        - Data Classification Policy
        - Data Classification Framework
        - DatAlert Suite
- 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 equipos activos de red con base en la documentación del fabricante
- Diseño, revisión y creación de políticas, procedimientos y estándares en el marco del SIG-SI-PDP-CN.
- Implementación de Planes de tratamiento de riesgo.

6.1. Implementación del Sistema de Gestión de Seguridad (II Fase)

Para la implementación del SIG-SI-PDP-CN, el Servicio Geológico Colombiano realizó 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. Fortalecimiento de las capacidades estratégicas de seguridad de la información. Iniciativa orientada al fortalecimiento de la capacidad estratégica de la Entidad para mitigar los diferentes riesgos de ciberseguridad, pretende servir de base documental y estratégica para la toma de decisiones y el mantenimiento eficiente del SIG-SI-PDP-CN.
2. Programa de capacitación y concientización del SIGSI-PDP-CN para equipo de trabajo (profundización) y usuarios con ejercicios prácticos y conceptos de gamificación. 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
3. Gobierno efectivo del SIG-SI-PDP-CN. Iniciativa enmarcada en el ciclo PHVA del SIG-SI-PDP-CN y que permitirá avanzar sustancialmente en la adopción efectiva del Sistema, dará

cumplimiento a los requerimientos normativos y apoyará decididamente la estrategia de gestión de riesgos.

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 Arquitectura de defensa en profundidad y que permite el aseguramiento de la plataforma tecnológica del SGC.

7. Mapa de ruta del Plan de Seguridad y Privacidad de la Información

PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	FECHA	
				INICIO	FIN
Fortalecimiento de las capacidades estratégicas de seguridad de la información	Revisión y monitoreo de la matriz de roles y responsabilidades del equipo	Avance del proyecto	Matriz de roles y responsabilidades actualizada	Enero 2023	Diciembre 2023
	Oficialización del Sistema integrado de gestión SIG-SI-PDP-CN	Avance del proyecto	100% de la documentación del sistema Oficializada	Enero 2023	Diciembre 2023
	Monitoreo y seguimiento al Sistema Integrado a través del cumplimiento de indicadores clave	Avance del proyecto	• Indicadores estratégicos definidos y monitoreados • Indicadores tácticos/operativos definidos y monitoreados	Enero 2023	Diciembre 2023
	Ajuste constante a la documentación del Sistema y validación de cumplimiento de políticas, procedimientos y estándares.	Avance del proyecto	• Cumplimiento del 100% de las políticas • Cumplimiento del 100% de los procedimientos • Cumplimiento del 100% de los estándares • Ajuste de todas las políticas, procedimientos y estándares	Enero 2023	Diciembre 2023
	Revisión y seguimiento a la implementación de la arquitectura de defensa en profundidad y sus artefactos.	Avance del proyecto	• Artefactos de Arquitectura • Arquitectura de defensa en profundidad actualizada e implementada • Arquitectura de segmentación de tráfico perimetral (DMZ)	Enero 2023	Diciembre 2023

PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	FECHA	
				INICIO	FIN
			implementada • Arquitectura de segmentación de red implementada		
Programa de capacitacióny concientización del SIGSI-PDP-CN	Implementación del programa de capacitación yconcientización	Avance del proyecto	• Adquisición de piezas multimediales • Adquisición de plataforma de sensibilización y concientización • Despliegue y ejecución del programa decapacitación y concientización en SI	Enero 2023	Diciembre 2023
Gobierno efectivo del SI-GSI-PDP-CN	Actualización del inventario de activos y análisis de riesgo a través de la plataforma Gestión, Riesgo y Cumplimiento - GRC	Avance del proyecto	• Inventario de activos actualizado • Plataforma Gestión, Riesgo y Cumplimiento - GRC actualizada y en uso	Enero 2023	Diciembre 2023
	Estandarización a través de políticas y procedimientos	Avance del proyecto	Creación de políticas, procedimientos y estándares requeridos en la Operación	Enero 2023	Diciembre 2023
	Implementación de indicadores operativos de cada control	Avance del proyecto	• Indicadores operativos definidos • Indicadores operativos monitoreados • Automatización de la medición de los indicadores operativos	Enero 2023	Diciembre 2023
	Implementación de planes de tratamiento de riesgo (PTR)	Avance del proyecto	Implementación de los PTR definidos en el SIG-SI-PDP-CN	Enero 2023	Diciembre 2023

PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	FECHA	
				INICIO	FIN
	Actualización de inventario y Registro Nacional de Base de Datos - RNBD y del Sistema de protección de datos personales	Avance del proyecto	• Inventario de bases de datos actualizado • Documentación del Sistema de protección de datos personales actualizado	Enero 2023	Diciembre 2023
Implementación, mejora y fortalecimiento de soluciones de seguridad informática y ciberseguridad	Renovación y actualización de la solución de protección del Dato (Imperva DAM/DBF + WAF + CloudWAF + GigaMon + Varonis)	Avance del proyecto	• Documento con requerimientos técnicos para renovación de productos y servicios • Renovación de solución de seguridad informática • Despliegue e implementación del producto renovado, integración de políticas y validación de funcionamiento de acuerdo con lo renovado	Enero 2023	Diciembre 2023
	Migrar las capacidades de adquisición, monitoreo, auditoría, correlación, orquestación y automatización de la solución Splunk a un modelo MDR (Managed Detection and Response) basado en la combinación de SoC (Security Operation Center) con CSVD (Centro de Seguridad y Vigilancia Digital) con una disponibilidad de 7x24x365.	Avance del proyecto			
	Renovación de la solución de seguridad en punto final (EDR) con protección perimetral IPS	Avance del proyecto			
	Renovación de la Plataforma de gestión del ciclo de vida de vulnerabilidades técnicas (SAST +	Avance del proyecto			

PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	FECHA	
				INICIO	FIN
	DAST + Plataforma)				
	Adquisición de una solución de gestión de identidad	Avance del proyecto	• Estudio del mercado y del sector para validar la opción que mejor se adecua a las necesidades de la Entidad. • Documento con requerimientos técnicos para la adquisición de productos y servicios • Adquisición de la solución de seguridad informática. • Despliegue e implementación del producto adquirido, integración de políticas y validación de funcionamiento de acuerdo con lo adquirido	Abril 2023	Diciembre 2023
	Adquisición de una solución de prevención de fuga de información (DLP)	Avance del proyecto			
	Adquisición de una solución de monitoreo y alertamiento automatizado de superficie de ataque	Avance del proyecto			
	Adquisición de una solución de parcheo virtual de sistema operativo	Avance del proyecto			
	Adquisición de una solución tecnológica que permita implementar el plan de capacitación y concientización del SIGSI-PDP-CN para equipo de trabajo (profundización) y usuarios con ejercicios prácticos y conceptos de gamificación	Avance del proyecto			

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 2021 – 2022 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
- Informe de análisis de brechas de SGSI
- Diagnóstico protección datos personales responsabilidad demostrada
- Instrumento evaluación MSPI – SGC
- 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
- Manual de políticas específicas del Sistema
- Matriz DOFA
- Inventario de activos de información SGC
- Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información
- Declaración de aplicabilidad SGC
- Procedimientos y estándares de seguridad de la información
- Informe BIA SGC
- Análisis de riesgos SGC
- Estrategias de continuidad
- Plan de continuidad