POLITICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Diagnóstico y Planificación del Modelo de Seguridad y Privacidad de la Información, para los procesos misionales y de apoyo del Servicio Geológico Colombiano.

CONTROL DE CAMBIOS

Fecha de actualización	Versión	Creado Por:	Aprobado Por:

1/08/2018	1.0	Jhon García – Andrea Neira	DGI
19/01/2019	2.0	Jhon García – Andrea Neira	Comité de Gestión y Desempeño Institucional

1. INTRODUCCIÓN

El Servicio Geológico Colombiano tiene la necesidad de diseñar, establecer, implementar, operar y mantener un Sistema de Gestión Integrado que contemple los aspectos de Seguridad y Privacidad de la información basada en ISO27001:2013 y la ley 1581, así como los aspectos de Continuidad del Negocio basados en ISO22301:2012.
Debido a lo anterior, este documento tiene como fin establecer la Política del Sistema de Gestión Integrado de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio para el SGC.

2. OBJETIVO GENERAL

Definir la política del Sistema de Gestión Integrado de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio para el SGC, con el fin de establecer los lineamientos requeridos por los estándares ISO27001:2013, ISO22301:2012, y la ley 1581 del 2012 y de esta manera garantizar su cumplimiento.

2.1. Objetivos Específicos

- Establecer las responsabilidades y deberes de la alta dirección, funcionarios, contratistas y usuarios en general con el Sistema de Gestión de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio.
- Garantizar la asignación de recursos administrativos y financieros necesarios para alcanzar y mantener los objetivos del Sistema de Gestión de Seguridad de la Información, Protección de Datos Personales Y Continuidad de Negocio.
- Establecer los lineamientos mínimos necesarios para dar cumplimiento a los estándares que conforman el Sistema de Gestión Integrado.

3. POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PROTECCIÓN DE DATOS PERSONALES Y CONTINUIDAD DE NEGOCIO

El Servicio Geológico Colombiano como Instituto de Ciencia y Tecnología, en cumplimiento de sus funciones y entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con el establecimiento, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio, como mecanismo para identificar y mitigar los riesgos asociados a la generación e integración de conocimientos, el levantamiento, compilación, validación, almacenamiento y suministro de información geocientífica, en el ejercicio de sus deberes con el Estado y los ciudadanos, enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

El conocimiento geocientífico es la base para el progreso social y económico del país, por lo tanto, los datos y la información generada en las etapas de investigación y desarrollo de los productos misionales, se almacenan de forma integrada en los fondos documentales y repositorios institucionales, asegurando su confiabilidad para suministrarla a nuestros usuarios. El Sistema de Gestión de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio establece los mecanismos para proteger, recuperar y conservar la información física y digital en el tiempo, asegurando su integridad, confidencialidad, disponibilidad, interacción y usabilidad, consolidando la cultura de seguridad de la información y protección de la propiedad intelectual del Servicio Geológico Colombiano.

Esta política aplica a la Entidad según lo establecido en el alcance del sistema a: activos y contenedores de información gestionados por todos los procesos, así como a todos los funcionarios, contratistas, proveedores y la ciudadanía en general que generen, accedan o utilicen información de la Entidad, con el fin de garantizar su confidencialidad, integridad y disponibilidad. Esto teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del sistema integrado estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información, protección de datos personales y continuidad del negocio.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información, protección de datos personales y continuidad del negocio.
- Fortalecer la cultura de seguridad de la información, protección de datos personales y continuidad del negocio en los funcionarios, terceros, aprendices, practicantes y clientes del SGC.
- Garantizar la continuidad del negocio frente a incidentes.

Por lo anterior, se definen los siguientes roles: Oficial de Seguridad de la Información, Oficial de Protección de Datos Personales y Oficial de Continuidad, al igual que los equipos de trabajo comités de: Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio y Crisis. Estos roles deben encontrase libre de conflicto de intereses por ende deben depender de la Alta Dirección del SGC, con el fin de monitorear y dar cumplimiento a las políticas establecidas en Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio.

Cabe destacar que el SGC, cuenta con el comité Institucional de Gestión y Desempeño (resolución 093 de 2018), el cual se compromete a desarrollar las funciones dependiendo del Rol que se requiera según las necesidades, es decir deberá hacer las veces de los Comités mencionados anteriormente.

De igual manera el Servicio Geológico Colombiano se compromete con lo siguiente:

- El SGC deberá asegurar que las políticas y los objetivos del Sistema de Gestión de Seguridad de la Información, Protección de Datos Personales Y Continuidad de Negocio sean adecuados al propósito de la institución.
- El SGC dispondrá los recursos administrativos y financieros necesarios para alcanzar y mantener los objetivos del Sistema de Gestión de Seguridad de la Información, Protección de Datos Personales Y Continuidad de Negocio.
- El SGC protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- El SGC gestionará los riesgos Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio acorde con la metodología de gestión de riesgos aprobada.
- El SGC protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- El SGC controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- El SGC implementará control de acceso a la información, sistemas y recursos de red.
- El SGC garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- El SGC garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- El SGC garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- El SGC deberá velar por el cumplimiento de los requisitos legales o reglamentarios y las obligaciones contractuales en materia de Seguridad de la Información, Protección de Datos Personales Y Continuidad de Negocio, que le apliquen a la institución, para esto se han definido los siguientes documentos como pilares del Sistema de Gestión de Seguridad de la Información, Protección de Datos Personales Y Continuidad de Negocio, los cuales también

deben ser cumplidos por funcionarios, contratistas y usuarios en general del sistema:

- ✓ **Manual del Sistema de Gestión de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio:** Documento mediante el cual se documenta el establecimiento del sistema.
- ✓ **Manual de Políticas de Seguridad de la Información:** Manual de políticas que pretende dar cumplimiento a los objetivos de control y controles establecidos en los 14 dominios del Anexo A de la ISO 27001, con el fin de garantizar buenas prácticas en seguridad de la información en el SGC.
- ✓ **Plan de Continuidad de Negocio:** Es un plan que le permite al SGC recuperarse y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.
- ✓ **Manual de Protección de Datos Personales:** Este manual le permite al SGC dar cumplimiento a la ley 1581 del 2012, en la que se establecen disposiciones para la protección de datos personales.

- La Política de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio, debe ser revisada, por los comités establecidos en el sistema de gestión al menos una vez al año, y/o cuando ocurran cambios significativos en la entidad, garantizando su evolución y cumplimiento, con el fin de lograr la mejora continua del Sistema de Gestión de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio.
- La alta dirección garantiza que el personal del SGC relacionado directamente con el establecimiento, implementación y mejora continua del Sistema Integrado de Gestión de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio, cuente con las competencias, formación y capacitación necesarias para ejercer las funciones y responsabilidades establecidas en dicho sistema, con el fin de asegurar el cumplimiento de sus objetivos.

Por otra parte, los usuarios de información del SGC se comprometen a:

- Toda persona que tenga acceso a información institucional del SGC, debe mantenerla en estricta confidencialidad y no deberá compartirla ni modificarla sin la debida autorización.
- Los usuarios deben acceder exclusivamente a la información a la que tienen permisos y que es necesaria para cumplir sus funciones.
- Los usuarios tienen la obligación de reportar los incidentes que afecten la Seguridad de la Información, la Protección de Datos Personales y la Continuidad del Negocio de acuerdo a los procedimientos y los canales establecidos en el Sistema Gestión de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio.

- Los funcionarios, contratistas, proveedores y público en general del SGC deben conocer, cumplir y divulgar, ésta y todas las políticas y buenas prácticas de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio.
- Las Políticas de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio son de aplicación obligatoria para todos los funcionarios, contratistas y proveedores del SGC, así como a cualquier persona que tenga acceso a la información de carácter institucional independientemente del área en la que se encuentren y sin importar las características de las tareas que desempeñen.
- Es de carácter obligatorio la implementación de las Políticas de Seguridad de la Información, Protección de Datos Personales y Continuidad de Negocio, en cada una de las direcciones, así como el cumplimiento de dichas políticas por funcionarios, contratistas, pasantes y proveedores.

4. ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, PROTECCIÓN DE DATOS PERSONALES Y CONTINUIDAD DE NEGOCIO

El comité Institucional de Gestión y Desempeño está integrado por:

1. Director General
2. Secretario General
3. Jefe de la Oficina Asesora Jurídica
4. Director de Geociencias Básicas
5. Director de Recursos Minerales
6. Director de Hidrocarburos
7. Director de Geoamenazas
8. Director de Gestión de Información
9. Director de Asuntos Nucleares
10. Director de Laboratorios
11. Coordinador del Grupo de Trabajo de Planeación

Dicho comité tendrá las funciones relacionadas a continuación y que son requeridos por el sistema:

4.1. Seguridad de la Información

4.1.1 Funciones del comité de gestión y desempeño institucional sobre Seguridad de la información

El comité de Seguridad de la Información determina las estrategias para el desarrollo del Sistema de Gestión de Seguridad de la Información, garantizando que se cumplan los lineamientos establecidos y los objetivos establecidos. Sus funciones son:

- Decide la asignación de los recursos necesarios para el cumplimiento de las metas establecidas del SGSI.
- El comité deberá realizar un proceso continuo de revisión de las políticas de seguridad de la Información con el fin de mantenerlas actualizadas, vigentes, operativas para asegurar su permanencia y nivel de eficacia.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de la información del SGC frente a posibles amenazas, sean internas o externas.
- Aprobar iniciativas para incrementar la seguridad de la información.
- Estudiar y conceptuar los casos especiales de seguridad presentados en la institución, para recomendar las acciones pertinentes y apoyar la toma de decisiones.
- Revisar los diagnósticos del estado de seguridad de la información.
- Acompañar e impulsar el desarrollo de proyectos de seguridad.
- Aprobar el uso de metodologías y procesos específicos para la seguridad de la Información.
- Realizar revisiones periódicas o cuando ocurran cambios significativos del SGSI.
- Promover la difusión y sensibilización de la seguridad de la información en el SGC.

4.1.2 Responsabilidades del Oficial de Seguridad de la información

El Oficial de Seguridad de la Información tendrá asignadas las siguientes responsabilidades:

- Responsable de establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información del SGC.
- Verifica que el Sistema de Gestión de Seguridad de la Información cuente con los procedimientos, formatos y herramientas necesarias para su correcta implementación dentro del SGC.
- Coordina la realización de un análisis de riesgos de seguridad de la información en cada una de las áreas del SGC, el cual debe llevarse a cabo

como mínimo una vez al año, para determinar el grado de exposición a las amenazas relacionadas con los activos de información.
- Difunde y controla la aplicación e implementación de las políticas de Seguridad de la Información con el fin de garantizar su cumplimiento.
- Prepara el plan de formación y sensibilización para la seguridad de la información
- Mantiene el inventario de activos de la Información actualizado.
- Evalúa los riesgos de las actividades subcontratadas
- Controla la efectividad de las medidas adoptadas.

4.2. Protección De Datos Personales

4.2.1 Funciones del comité de gestión y desempeño institucional sobre la Protección de Datos Personales

El Comité con las funciones sobre la Protección de Datos Personales determina las estrategias para el cumplimiento de la ley 1581 de 2012, garantizando que se cumplan las disposiciones allí establecidas. Sus funciones son:

- Realizar un proceso continuo de revisión de las políticas de Protección de Datos Personales, con el fin de mantenerlas actualizadas y operativas para asegurar su eficacia.
- Analizar las iniciativas para incrementar la protección de los datos personales.
- Estudiar y conceptuar los casos especiales en materia de Protección de Datos Personales, con el fin de recomendar las acciones pertinentes.
- Revisar el diagnóstico del estado de Privacidad de la Información de SGC.
- Acompañar e Impulsar el desarrollo de Proyectos de Privacidad de la Información, solicitando la aprobación del Presupuesto necesario.
- Escalar la aprobación de metodologías y Políticas de Privacidad de la Información cuando sea necesario.
- Evaluar y aprobar los planes de tratamiento establecidos para prevenir la materialización de los riesgos identificados en materia de Protección de Datos Personales.
- Promover la difusión y sensibilización en Privacidad de la Información.

4.2.2 Responsabilidades del Oficial de Protección de Datos Personales

- Proteger los datos personales y dar trámite a las solicitudes de los Titulares de los datos personales para el ejercicio de los derechos que se consagran en la ley 1581 de 2012.
- Servir de coordinador con las demás áreas de la organización para asegurar una implementación transversal del cumplimiento de la ley 1581 de 2012.
- Mantener un inventario de las bases de datos personales en poder del SGC y clasificarlas según su contenido.
- Registrar las bases de datos del SGC en el Registro Nacional de Bases de Datos, en cuanto corresponda, y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la Superintendencia de Industria y Comercio (“SIC”).
- Implementar en los contratos que celebre el SGC, disposiciones que aseguren el cumplimiento de la ley 1581 de 2012.
- Velar porque se capacite periódicamente en temas de protección de datos personales al personal del SGC, para generar una cultura de protección de datos dentro de la institución. Esto incluirá realizar sesiones de sensibilización y medir la participación y calificar el desempeño de los asistentes.
- Integrar las políticas de datos personales dentro de las actividades de las demás áreas de la institución.
- Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de las Políticas y Procedimientos en materia de Protección de Datos Personales.
- Coordina la realización de un análisis de riesgos anual de Protección de datos Personales de cada una de las áreas.
- Proponer un Plan de Sensibilización anual en materia de Protección de Datos Personales para el SGC.

4.3. Continuidad del Negocio

4.3.1 Funciones del comité de gestión y desempeño institucional sobre Continuidad/Crisis

- Obtener y proteger el presupuesto para la sostenibilidad del BCP, garantizando la sostenibilidad de este.
- Garantizar que el personal que tenga la responsabilidad del Plan de Continuidad de Negocio esté capacitado y entrenado, teniendo claro su rol y sus responsabilidades.
- Revisar y Aprobar el BCP, por lo menos una vez al año.
- Revisar que las pruebas BCP sean integrales teniendo en cuenta el Plan de Emergencias, el Plan de Recuperación de Desastres (DRP) y la gestión adecuada de Crisis.
- Identificar la categoría del desastre, según el informe entregado por el equipo de respuesta a emergencias y el equipo de evaluación de daños y recuperación de instalaciones.
- Definir si se requieren equipos de apoyo según la situación presentada.

- Tomar la decisión de activar el Plan de Continuidad del Negocio y/o el Plan de Recuperación de Desastres.
- Definir las acciones a seguir para recuperar la infraestructura física (sede, muebles y enseres) y la tecnológica, estableciendo la necesidad de reemplazarla o de recuperarla dependiendo del reporte de daños que entregue el equipo de evaluación de daños y recuperación de instalaciones, buscando siempre la mejor opción costo / beneficio.
- Autorizar la publicación de comunicaciones sobre la crisis y manejo de la misma a interesados.
- Coordinar la emisión de comunicados con los voceros autorizados.
- Hacer seguimiento a los procedimientos y a las actividades involucradas en las fases de respuesta y de restauración del Plan de Continuidad del Negocio.

4.3.2 Responsabilidades del Oficial de Continuidad

- Actualizar la información de contacto de los miembros del comité de crisis.
- Actualizar la información de contacto de clientes, proveedores, e interesados críticos.
- Mantener actualizado el Plan de Continuidad del Negocio y sus anexos correspondientes.
- Asegurar que existe y funciona un procedimiento de control de cambios al plan de continuidad del negocio.
- Estimar el presupuesto anual de mantenimiento del plan de continuidad del negocio.
- Estimar el presupuesto anual de capacitación requerida en continuidad del negocio.
- Convocar o disolver el Comité de Crisis.
- Gobernar la secuencia de recuperación de los procesos de negocio.
- Actuar como enlace entre los diferentes equipos que hacen parte del Plan de Continuidad del Negocio y el Comité de Crisis.
- Controlar la ejecución del Plan de Continuidad del Negocio, detectar desvíos y comunicarlos al Comité de Crisis para realizar los ajustes necesarios en función de los inconvenientes, problemas y errores hallados durante la ejecución del mismo.
- Informar de lo sucedido a Proveedores, Contratistas, Aseguradoras y demás fuentes externas previa autorización del Comité de Crisis.