SERVICIO GEOLÓGICO COLOMBIANO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y CONTINUIDAD DEL NEGOCIO

2020

SERVICIO GEOLÓGICO COLOMBIANO	**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y CONTINUIDAD DEL NEGOCIO**

TABLA DE CONTENIDO

SERVICIO GEOLÓGICO COLOMBIANO	**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y CONTINUIDAD DEL NEGOCIO**

1. INTRODUCCIÓN

Este documento tiene como fin presentar un plan de acción para el establecimiento, implementación, operación, monitoreo, revisión y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información 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 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 a la entidad dar cumplimiento a sus objetivos estratégicos.

2. OBJETIVO DEL DOCUMENTO

Definir un Plan de Seguridad y Privacidad de la Información que fortalezca el Sistema de Gestión de Seguridad y Privacidad de la Información del Servicio Geológico Colombiano, acorde a los requerimientos del modelo de seguridad de la estrategia de la política de gobierno digital, los 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 de Gestión de Seguridad y Privacidad de la Información.
- Fortalecer la implementación del Sistema de Gestión de Seguridad de la Información 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 de Gestión de Seguridad y Privacidad de la Información y del Sistema de Gestión de Continuidad de Negocio en el SGC.

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

El Plan de Seguridad y Privacidad de la Información considera los controles de la norma NTC/ISO 27001:2013, el análisis de riesgos realizado, 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 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 entidad ha venido identificando las vulnerabilidades, amenazas y riesgos latentes, de manera que sea posible construir estrategias de protección e implementar acciones para proteger los activos, tratar y disminuir las amenazas, contener y mitigar los riesgos.

Con el desarrollo del proyecto de arquitectura empresarial se realiza un análisis de los riesgos de los activos de información. A través de una serie de talleres, reuniones de concertación y de indagación se identifican los activos críticos, se construye el perfil de amenazas latentes para los activos del SGC, se identifican las vulnerabilidades organizacionales y de la infraestructura que afectan a los activos o que soportan a los activos y finalmente se desarrolla la estrategia y los planes de seguridad organizacional para proteger los activos de la organización.

Acorde a lo anterior el SGC ha venido desarrollando diferentes estrategias e implementando herramientas de seguridad informática que le permitan el aseguramiento de los activos de información con los que actualmente cuenta la entidad, como resultado del desarrollo de proyectos y las investigaciones realizadas.

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.
- Análisis de vulnerabilidades sobre los procesos misionales de la entidad 2018.
- Análisis de riesgos y plan de tratamiento sobre la información de Aero geofísica.
- Adquisición de herramientas de seguridad informática.

- Elaboración y divulgación de políticas para el buen uso de los servicios tecnológicos con los que cuenta la entidad.

Complementando el trabajo desarrollado, en el año 2018 la entidad conforma el Sistema de Gestión de Seguridad de la Información de acuerdo con los lineamientos de MinTIC, bajo el Modelo de Seguridad y Privacidad de la Información, se desarrollaron las dos primeras etapas del ciclo PHVA (diagnóstico y planeación) con el apoyo de una consultoría IT Security S.A, a continuación se relacionan las fases y entregables de las etapas gestionadas.

Tabla 1. Fases y entregables de las etapas gestionadas.

FASE	NO	ENTREGABLE
Fase 1. Gerencia de Proyectos	1	Project Charter
	2	Plan de Comunicaciones del Proyecto
	3	Plan de Calidad
	4	Matriz de Riesgo del Proyecto
	5	Gestión de Cambio y Análisis de Cambio
	6	Registro de Interesados
Fase 2. Diagnóstico	7	Informe de análisis de brechas ISO 27001
	8	Informe de análisis de brechas ISO 22301
	9	Instrumento de evaluación MSPI diligenciado
	10	Informe de cumplimiento de protección de datos personales
	11	Informe técnico y gerencial del análisis de vulnerabilidades
	12	Informe técnico y gerencial del hacking ético
	13	Plan de sensibilización y capacitación
	14	Informe de análisis del contexto

FASE	NO	ENTREGABLE
Fase 3. Planificación o planeación	15	Documento de alcance del sistema de gestión de seguridad, privacidad, protección de datos personales y continuidad de negocio
	16	Documento de integración con otros sistemas de gestión (calidad, seguridad y salud en el trabajo, medio ambiente, entre otros)
	17	Documento de liderazgo del sistema de gestión (compromiso, roles y responsabilidades)
	18	Política general del sistema de gestión
	19	Plan de comunicaciones del sistema de gestión
	20	Análisis DOFA del sistema de gestión
	21	Plan de acción para la implementación del MPSI
Fase 4. Sensibilización y capacitación	22	Contenidos y piezas elaboradas
	23	Capacitación y sensibilización al comité de seguridad (composición del comité, funciones, responsabilidades, entre otros)
	24	Capacitación para los responsables del sistema de gestión
	25	Socialización a nivel institucional de las políticas y principales controles del sistema de gestión
Fase 5. Activos de información y bases de datos personales	26	Metodología de levantamiento de activos de información y bases de datos
	27	Inventario de activos de información para los 8 procesos misionales y los 7 procesos de apoyo

FASE	NO	ENTREGABLE
	28	Inventario de bases de datos personales para los 8 procesos misionales y los 7 procesos de apoyo
Fase 6. Gestión de riesgos	29	Metodología de gestión de riesgos
	30	Informe de análisis de riesgos (incluye riesgos inherentes, presentes y esperados) para los 8 procesos misionales y los 7 procesos de apoyo
	31	Plan de tratamiento de riesgos
	32	Declaración de aplicabilidad (SOA)
	33	Plan de ruta de proyectos a implementar (incluye recursos, alcance, costos, tiempos y estrategia de cumplimiento sugerida)
Fase 7. Modelo de seguridad y privacidad de la Información	34	Documentación, revisión y/o actualización de los objetivos de seguridad
	35	Indicadores del sistema de gestión
	36	Documentación, revisión y/o actualización de políticas, procesos y procedimientos del sistema
	37	Documento con la definición de recursos y competencias
	38	Informe de diagnóstico de transición hacia IPv6 (situación actual de la infraestructura de comunicaciones, plan de acción de migración de IPv4 a IPv6, recomendaciones)
	39	Estrategias de cierre de brechas para la transición hacia IPv6
	40	Documentación para cumplimiento de responsabilidad demostrada

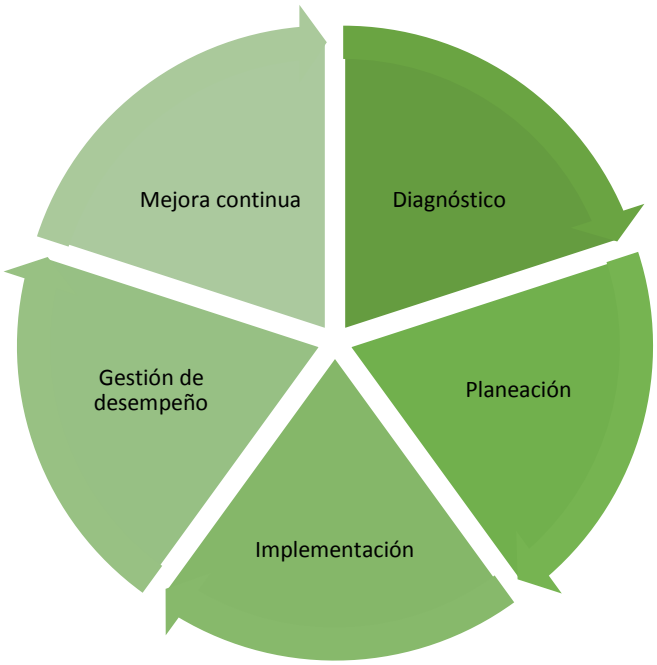
FASE	NO	ENTREGABLE
Fase 8. Responsabilidad Demostrada	41	Plan de ruta de proyectos para cierre de brechas
Fase 9. Plan de continuidad del negocio y plan de recuperación de desastres	42	Documentación de contexto, liderazgo, planeación y soporte
	43	Manual de gestión de continuidad del negocio
	44	Análisis de impacto al negocio (BIA)
	45	Análisis de riesgos de continuidad (Escenarios de desastre)
	46	Estrategia de continuidad del negocio
	47	Plan de crisis
	48	Plan de continuidad del negocio general para la organización (no incluye pases específicos que deberán desarrollar en un proyecto de implementación posterior)
	49	Desarrollo o actualización de un plan de recuperación de desastres para una aplicación crítica
Fase 10. Evaluación de desempeño de la implementación del MSPI	50	Metodología de verificación de la implementación del MSPI
	51	Métricas e indicadores de gestión de desempeño del MSPI
	52	Metodología para la definición de riesgos, amenazas y vulnerabilidad junto a sus probabilidades de aparición o explotación y su impacto
Fase 11. Plan de mejora continua del MSPI	53	Plan de reporte de incidentes y resultados de pruebas técnicas
	54	Plan de mejoramiento continuo del MSPI

Esto demuestra que la entidad está comprometida con la seguridad y privacidad de la información, la continuidad de los procesos del negocio, y de los servicios tecnológicos, 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 AE acorde al trabajo que ha venido desarrollando la entidad.

5. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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.

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



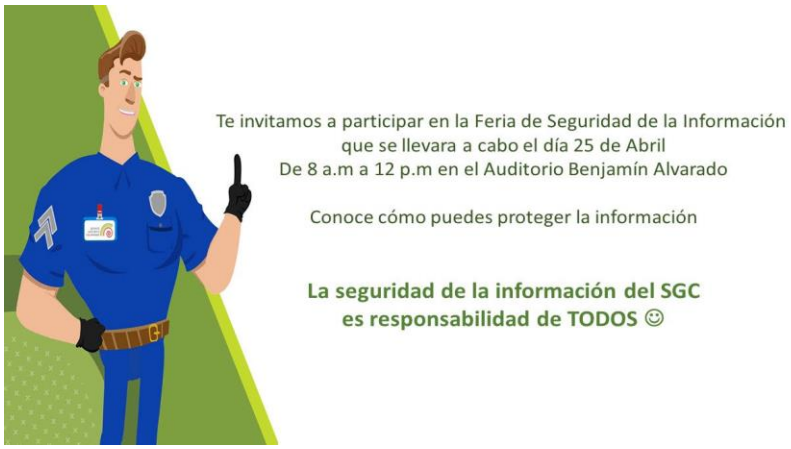
- Fase Diagnóstico: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información

- 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.
- Fase Implementación (Hacer): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- 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.
- 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.

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

- Se renueva una solución informática que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de los mismos.
- Inclusión de la política general de Seguridad de la información en el sistema de gestión Isolución.
- Revisión en proceso del manual de políticas y procedimientos del SGSI para subirlos al sistema de gestión de Isolución
- Se renueva la adquisición de un sistema SIEM (información de seguridad y gestión de eventos), tecnología capaz de detectar rápidamente, responder y neutralizar las amenazas informáticas. Su objetivo principal es el de proporcionar una visión global de la seguridad de las tecnologías de la información.
- Feria de seguridad de la información en donde se trataron temas de fishing, contraseñas robustas y tips de seguridad.

Ilustración 2. Campañas de sensibilización



Sesiones de sensibilización sobre el uso del repositorio institucional en todas las Direcciones Técnicas y sus Grupos de Trabajo, en el cual se abordaron los temas que se detallan a continuación:

- Políticas relacionadas con la Custodia y Protección de la Información,
- Responsabilidades de los Funcionarios Públicos,
- Procedimiento de Almacenamiento,
- Tipos de permisos Otorgados,
- Organización del Repositorio.
- Aclaración a los usuarios que los equipos de cómputo no se les hace backup, razón por la cual se ven expuestos a pérdidas de información.

Las reuniones fueron precedidas por Jhon Jairo García, Andrea Neira B., Diego Barragán, William J. Clavijo B.

A continuación, se relacionan las dependencias y sus grupos de trabajos que han sido citados a las reuniones de sensibilización hasta la fecha:

Tabla 2. Reuniones de sensibilización realizadas.

Fecha reunión	Dependencia	Grupo de trabajo	No. asistentes	Asistentes DGI
Febrero 14 de 2019	Secretaria General	Servicios Administrativos	10	2
Febrero 15 de 2019	Geociencias Básicas	Tectónica/Geociencias Básica	4	3
Febrero 20 de 2019	Dirección General	Oficina de Control Interno	8	5
Marzo 05 de 2019	Geoamenazas	MMasa/Geoamenazas/Geored/RNSC	4	4
Marzo 07 de 2019	Secretaria General	Unidad de Recursos Financieros	11	4
Marzo 21 de 2019	Secretaria General	Talento Humano / Liquidación de Nómina y Seguridad Social	13	3
Marzo 21 de 2019	Geoamenazas	Movimiento en Masa	22	3
Marzo 22 de 2019	Geoamenazas	Red Sismológica Nacional de Colombia	25	3
Marzo 27 de 2019	Geoamenazas	Red Sismológica Nacional de Colombia /Sismología	16	3

Fecha reunión	Dependencia	Grupo de trabajo	No. asistentes	Asistentes DGI
Marzo 29 de 2019	Secretaría General	Contratos y Convenios	14	3
Abril 29 de 2019	Geociencias Básicas	Cartografía e Investigación Geológica y Geomorfológica	7	4
Mayo 06 de 2019	Geociencias Básicas	Tectónica	10	3
Mayo 30 de 2019	Geociencias Básicas	Exploración de Aguas Subterráneas	12	3
Junio 06 de 2019	Asuntos Nucleares	Investigaciones y Aplicaciones Nucleares y Geocronológicas/ Licenciamiento y Control	4	3
Junio 12 de 2019	Secretaría General	Planeación	11	2
Julio 23 de 2019	Dirección General	Participación Ciudadana y Comunicaciones	5	3
Agosto 09 de 2019	Gestión de Información	EPIS	23	4
Agosto 09 de 2019		BIP	2	

Fecha reunión	Dependencia	Grupo de trabajo	No. asistentes	Asistentes DGI
Agosto 09 de 2019		Litoteca Facatativá	3	
Agosto 12 de 2019	Recursos Minerales	Investigación y Exploración de Recursos Minerales Metálicos	2	2
Agosto 20 de 2019	Recursos Minerales	Investigación y Exploración de Recursos Minerales Energéticos	8	2
Agosto 21 de 2019	Geociencias Básicas	Geología de Volcanes	7	3
Agosto 26 de 2019	Dirección General	Oficina Asesora Jurídica	4	4
Agosto 26 de 2019	Secretaria General	Control Interno Disciplinario	1	
Agosto 26 de 2019		Contratos y Convenios	2	
Agosto 26 de 2019		Asesoría Secretaría General	1	
Agosto 28 de 2019	Gestión de Información	Biblioteca	9	2

Todas las reuniones han sido acordadas con el director técnico o coordinador de grupo. En las reuniones en la mayoría de los usuarios han despejado muchas dudas, se han configurado los

repositorios en los PCs de usuarios que no los tenían configurados y les fueron asignados los respectivos permisos para que hagan el adecuado uso de los mismos, esto a su vez ha generado confianza en el uso del repositorio institucional.

Dando cumplimiento al modelo como se describió en los antecedentes las entidad cuenta con la fase diagnóstico y planificación gestionados, en el 2019 la entidad a adelantado gestión en la fase de implementación que contempla la implementación de los planes de tratamiento de riesgos, fase que se desarrolla y describe en el documento plan de tratamiento de riesgos y en paralelo la implementación del plan de continuidad del negocio descrito a continuación en el numeral 5.1.

5.1. IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD (I FASE)

El DRP y la continuidad de servicios tecnológicos tienen prácticamente el mismo alcance, buscando que en caso de desastre los sistemas de información de la Entidad mantenga un nivel de servicio mínimo. Este alcance no es suficiente para la Entidad, entendiendo que el solo mantener los servicios de TI no permite que los servicios que presta la Entidad a la ciudadanía y a otras Entidades puedan ser prestados de manera adecuada en caso de una catástrofe, pues existen muchos procesos donde los funcionarios que no pertenecen a tecnología analizan, confirman, procesas y escalan información. Un DRP o continuidad de servicios tecnológicos debe ir orquestado o cobijado por un plan de continuidad de negocio o un sistema de continuidad de negocio, tal como se definió con los resultados del BIA y los demás resultados de la fase de Diagnóstico y Planeación del sistema integrado de gestión de seguridad de la información, protección de datos personales y continuidad de negocio adelantado en el 2018.

Para lo anterior se contratará una consultoría para la actualización, implementación y puesta en funcionamiento del Plan de Recuperación de Desastres Tecnológicos en el marco de la Fase I del proyecto de Diagnóstico y Planeación del modelo de seguridad y privacidad de la información (MSPI) del Servicio Geológico Colombiano, alineado a la planeación de la entidad y su arquitectura empresarial.

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

ASPECTO A MEDIR	CATEGORÍA	PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	RESPONSABLE	FECHA	
							INICIO	FIN
Efectividad	Continuidad del Negocio	Implementación del Sistema de Gestión de Seguridad (I Fase)	Gerencia de proyectos	Avance del proyecto	- Cronograma del proyecto - Project Charter - Plan de comunicaciones - Plan de calidad del proyecto - Riesgos del proyecto - Documento de impacto y manejo de cambios	DGI	Enero 2020	Diciembre 2020
			Definición del Plan de Recuperación de Desastres	Avance del proyecto	A partir del BIA con el que cuenta la entidad elaborar, revisar, actualizar o ajustar, los documentos mínimos necesarios para el establecimiento de la continuidad del negocio en el SGC	DGI	Enero 2020	Diciembre 2020

ASPECTO A MEDIR	CATEGORÍA	PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	RESPONSABLE	FECHA	
							INICIO	FIN
					bajo la norma ISO 22301 y los requerimientos del MinTIC			
			Procedimientos de recuperación (basados en el BIA y los tiempos del mismo como el RPO y RTO)	Avance del proyecto	• Construcción de los procedimientos de recuperación de procesos según lo contemplado en el análisis de impacto al negocio (BIA) que tiene la entidad. (Cubriendo todos los procedimientos que se requieran en las áreas contempladas en el plan y los escenarios aprobados). • Construcción de los procedimientos de recuperación de servicios y sistemas tecnológicos según lo contemplado en el análisis de impacto al	DGI	Enero 2020	Diciembre 2020

ASPECTO A MEDIR	CATEGORÍA	PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	RESPONSABLE	FECHA	
							INICIO	FIN
					negocio (BIA) actualizado de la entidad.			
			Plan de capacitación y Sensibilización	Avance del proyecto	• Diseño, desarrollo y ejecución del plan de capacitación y sensibilización en recuperación de desastres a toda la Entidad, respetando el manual de imagen de la Entidad. Este debe contener al menos: o Curso virtual con contenidos animados con al menos 3 módulos con evaluación de entendimiento. o Al menos 12 Piezas digitales relacionadas. o Charlas de capacitación a los diferentes comités	DGI	Enero 2020	Diciembre 2020

ASPECTO A MEDIR	CATEGORÍA	PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	RESPONSABLE	FECHA	
							INICIO	FIN
					relacionados con la continuidad de negocio, comité de crisis, de recuperación de desastres y todos los que se relacionan dentro de los planes de continuidad. o Talleres didácticos planteados dentro del cronograma de proyecto.			
			Gestión de Indicadores del plan de recuperación de desastres	Avance del proyecto	• Definir los indicadores de recuperación de desastres, alineados al MSPI, las definiciones del MinTIC y la arquitectura empresarial de la Entidad.	DGI	Enero 2020	Diciembre 2020
			Prueba del Plan de	Avance del proyecto	• Formular el plan de pruebas anual al	DGI	Enero 2020	Diciembre 2020

ASPECTO A MEDIR	CATEGORÍA	PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	RESPONSABLE	FECHA	
							INICIO	FIN
			Recuperación de Desastres		Plan de Recuperación de Desastres. • Realizar las capacitaciones a los involucrados en cada una de las pruebas planeadas del plan de recuperación de desastres. • Realizar las pruebas con el acompañamiento de la Entidad a las diferentes pruebas planeadas dentro del proyecto, llevando el registro de tiempos y otras métricas dentro de las pruebas de recuperación de desastres para los procesos de			

ASPECTO A MEDIR	CATEGORÍA	PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	RESPONSABLE	FECHA	
							INICIO	FIN
					Dirección de Geo Amenazas Red sismológica nacional de Colombia y Secretaria General – Gestión de Comisiones, emitiendo Informe de cada prueba a fin de validar los tiempos del RTO y RPO establecidos, los indicadores definidos y en general los diferentes aspectos relacionados con el control y seguimiento del plan de recuperación de desastres.			
			Comité de Continuidad y Crisis	Avance del proyecto	• Con el apoyo de la entidad definir el comité de continuidad y crisis incluyendo la Revisión y	DGI	Enero 2020	Diciembre 2020

ASPECTO A MEDIR	CATEGORÍA	PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	RESPONSABLE	FECHA	
							INICIO	FIN
					actualización de roles y responsabilidades de la entidad y partes interesadas hacia el plan de recuperación de desastres. • Participación en los diferentes comités definidos para el plan de recuperación de desastres, como lo puede ser el comité de continuidad, el comité de crisis, etc			
			Diagnóstico orientado a la construcción del plan de continuidad del negocio		• Elaboración del diagnóstico del Plan de Continuidad de Negocio para todos los procesos de la entidad incluyendo los observatorios vulcanológicos y sismológicos.	DGI	Enero 2020	Diciembre 2020

ASPECTO A MEDIR	CATEGORÍA	PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	RESPONSABLE	FECHA	
							INICIO	FIN
					• El proveedor deberá ejecutar un análisis para Medir el nivel de madurez del SGC en el cumplimiento de las cláusulas y controles definidos por el estándar ISO 22301:2012, conforme a los avances de la implementación del Sistema de Gestión de Continuidad del Negocio (el cual es parte del sistema integrado de gestión de seguridad de la información, protección de datos personales y continuidad de negocio). • Medición del Nivel de Madurez			

ASPECTO A MEDIR	CATEGORÍA	PROYECTO	ACTIVIDAD	META /INDICADOR	PRODUCTO /EVIDENCIA	RESPONSABLE	FECHA	
							INICIO	FIN
					(tipo GAP) del Sistema de Gestión de Continuidad del Negocio y DRP, bajo la ISO 22301 y los requerimientos del MinTIC			
			Revisión de la Dirección del Plan de Recuperación de Desastres	Avance del proyecto	Acompañamiento en la presentación y aprobación gerencial del sistema de gestión, el cual es parte del sistema integrado de gestión de seguridad de la información y protección de datos personales.	DGI	Enero 2020	Diciembre 2020

7. 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.

8. ANEXOS

Las evidencias de los productos desarrollados durante el período 2018 – 2019 bajo el modelo de seguridad y privacidad de la información de MinTIC esta 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
- 15 procedimientos 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

Versión	Fecha de aprobación	Descripción	Responsable
1	27/01/2020	Aprobación Plan de Seguridad y Privacidad de la Información.	DT Gestión de Información