UNGRD
Unidad Nacional para la Gestión del Riesgo de Desastres

Sistema Nacional de Gestión del Riesgo de Desastres

Sistema Integrado de Planeación y Gestión de la UNGRD certificado en:

ISO 9001:2015 Certificado No. SG-2015001782-A

ISO 14001:2015 Certificado No. SG-2019001056-B

ISO 45001:2018 Certificado No. SG-2019001056-F

Plan de seguridad y privacidad de la información

28/01/2022

Grupo de Tecnologías de la Información

El futuro es de todos

Presidencia de la República

Tabla de contenido

1. OBJETIVO

Describir las actividades del Plan de Seguridad y Privacidad de la Información con las cuales se busca desarrollar, verificar y aplicar la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI en la Unidad Nacional para la Gestión del Riesgo de Desastres – UNGRD, de acuerdo con los requerimientos establecidos en la norma ISO 27001 y la Política de Seguridad Digital.

2. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información se aplica al proceso de Gestión de Tecnologías de la Información en sus líneas de sistemas de información e Infraestructura tecnológica de la Unidad Nacional para la Gestión del Riesgo de Desastres, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información – SGSI.

3. TERMINOS Y DEFINICIONES

Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.
Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

4. POLITICA DE SEGURIDAD

Propender por el aseguramiento de la confidencialidad, integridad y disponibilidad de la información en la Entidad y sus partes interesadas a través de la gestión de riesgos de seguridad de la información; así como confirmar el cumplimiento de los objetivos y metas para garantizar la Seguridad de la Información.

Cumplir con los requisitos legales y de otra índole aplicable a la UNGRD con relación al cuidado del medio ambiente, a la Seguridad y Salud en el Trabajo y Seguridad de la Información de acuerdo a la normatividad legal vigente.

Mejorar continuamente el desempeño del Sistema Integrado de Planeación y Gestión SIPLAG, por medio del establecimiento, implementación y seguimiento de Políticas, Planes y Programas, para contribuir a la seguridad, el bienestar, la calidad de vida de las personas, el cuidado del medio ambiente y la Seguridad de la Información, así como en la gestión de riesgos, la prevención de la contaminación o cualquier aspecto prioritario.

5. OBJETIVOS DEL SGSI

- Asegurar la preservación de la confidencialidad, integridad y disponibilidad de la información, de acuerdo a las políticas, procedimientos y demás documentación de la UNGRD para la gestión del SGSI.

- Minimizar los riesgos de seguridad de la información a los que pueda estar expuesta la UNGRD y aquella información que sea de interés de sus partes interesadas.

- Generar y divulgar una cultura sobre seguridad de la información a los funcionarios públicos, contratistas, comunidad, proveedores y demás partes interesadas de la UNGRD.

- Desarrollar una cultura de desarrollo, maduración y mejoramiento continuo al interior de la UNGRD de los aspectos relacionados con seguridad de la información, con la participación de los funcionarios y contratistas de la Entidad.

6. ALCANCE DEL SGSI

El Sistema de Gestión de Seguridad de la Información de la Unidad Nacional para la Gestión del Riesgo de Desastres — UNGRD, comprende el proceso de Gestión de Tecnologías de la Información.

7. COMITÉ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Mediante la Resolución 445 de 2018 (que derogó la Resolución 1568 de 2016), por la cual se actualiza el Sistema Integrado de Planeación y Gestión SIPLAG de la Unidad Nacional para la Gestión del Riesgo de Desastres. A partir de esta actualización, se crea el Comité Institucional de Gestión y Desempeño que es la máxima instancia encargada de orientar la implementación y operación del Sistema Integrado de Planeación y Gestión, y sustituye los demás comités que tienen relación con el Modelo Integrado de Planeación y Gestión.

El Comité de Gestión y Desempeño está conformado por los siguientes funcionarios:

1. El Secretario General o su delegado quien lo presidirá.
2. El Jefe de la Oficina Asesora de Planeación e Información.
3. El Jefe de la Oficina Asesora Jurídica.
4. El Jefe de la Oficina Asesora de Comunicaciones.
5. El Coordinador del Grupo de Gestión Contractual.
6. El Coordinador del Grupo de Talento Humano.
7. El Coordinador del Grupo de Apoyo Administrativo.
8. El Coordinador del Grupo de Apoyo Financiero y Contable.
9. El Coordinador del Grupo de Cooperación Internacional.
10. El Jefe de la Oficina de Control Interno, quien tendrá derecho a voz, pero no voto.

Dentro de las funciones del Comité de Gestión y Desempeño, las siguientes se encuentran relacionadas con seguridad digital y de la información, así como con el MIPG donde se encuentran las políticas de Gobierno Digital y Seguridad Digital:

- Aprobar y hacer seguimiento, por lo menos una vez cada tres meses, a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión MIPG.

- Proponer al Comité Sectorial de Gestión y el Desempeño Institucional, inician/as que contribuyan al mejoramiento en la implementación y operación del Modelo Integrado de Planeación y Gestión.

- Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.

8. PLAN DE IMPLEMENTACION

	Tema	Actividad	Responsable	FECHA
1	Sensibilización y divulgación	Presentar el SGSI en las jornadas de inducción y reinducción que adelante la entidad	Grupo de tecnologías de la información	Mensual con los funcionarios y contratistas que ingresan en el periodo a la Entidad.
		Realizar charla sobre Ataques de ciberseguridad y cómo cuidar la información de la UNGRD, orientada a funcionarios y contratistas		Primer semestre de 2022
		Realizar charla sobre Prácticas en Seguridad de la Información, orientada a funcionarios y contratistas		Segundo semestre de 2022
		Envío de piezas gráficas con tips y políticas de seguridad de la información		Trimestral durante la vigencia 2022
		Realizar ejercicio de Ingeniería social *(Phishing y mailing)*		Segundo semestre de 2022
2	Medición y seguimiento	Realizar medición y seguimiento a los indicadores del SGSI	Grupo de tecnologías de la información	Semestral
3	Auditorias	Realizar las auditorías internas, evaluaciones y seguimientos al Sistema de Gestión de Seguridad de la Información y presentar los informes respectivos.	Grupo de tecnologías de la información Oficina de Control Interno	Auditoría interna (Febrero 2022) Auditaría de certificación (Abril 2022)
4	Activos de información	Actualizar el inventario y valoración de activos de información con los diferentes procesos de la UNGRD.	Todos los procesos de la entidad	Octubre – Noviembre de 2022
5	Riesgos de seguridad de la información	Identificar y valorar los riesgos de seguridad de la información, según la política de tratamiento de riesgos de la entidad.	Todos los procesos de la entidad	Noviembre – Diciembre de 2022

9. DOCUMENTOS DE REFERENCIA

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de abril 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 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- 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 y se dictan otras disposiciones.
- FR-1603-SIS-01-Envío De Equipos De Cómputo Electrónico A Bodega-Formato Donde Se Describe El Equipo, Marca, Placa O Serie Y Observaciones. Firma Quien Envía Y Quien Recibe.
- FR-1603-SIS-02-Formato De Planeación De Pruebas Del Procedimiento De Continuidad De La Seguir-Formato De Planeación De Pruebas Del Procedimiento De Continuidad De La Seguridad De La Información
- FR-1603-SIS-03-Formato De Solicitud De Cambio/ Evaluación De Nuevos Proyectos De Tecnología D-Formato De Solicitud De Cambio/ Evaluación De Nuevos Proyectos De Tecnología De La Información
- FR-1603-SIS-04-Matriz De Gestión De Incidentes De Seguridad De La Información-Matriz De Gestión De Incidentes De Seguridad De La Información
- FR-1603-SIS-05-Formato De Documentación De Pruebas Del Procedimiento De Continuidad De La Seguridad de la Información
- PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Versión 3.0 Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC)
- M-1101-GTI-03 MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION - UNGRD
- Plan de Sensibilización SI – UNGRD
- Plan de Tratamiento de Riesgos de Seguridad y privacidad de la Información –UNGRD

10. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del cambio
28/01/2022	1	Elaboración del plan

Elaborado por: Sylvia Ribero Corzo / GTI

Revisó y aprobó: Carolina Jiménez Zapata / GTI