



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:



Plan de Seguridad y Privacidad de la Información

21 // 01 // 2019

Oficina Asesora de Planeación e Información //



El futuro
es de todos

Presidencia
de la República

Plan de Seguridad y Privacidad de la Información

Formato de documento

Título:	Plan de Seguridad y Privacidad de la Información				
Fecha de Aprobación:	25/01/2019				
Palabras claves:	Seguridad de la Información, tecnología , información, comunicaciones, infraestructura, aplicaciones, marco de referencia, arquitectura empresarial, PETI, UNGRD				
Formato:	PDF	Lenguaje:	Español		
Dependencia:	Oficina Asesora de Planeación e Información				
Código:		Versión:	1.0	Estado:	
Categoría:	Planes				
Autor(es):	Carolina Jiménez Zapata Luz Paula Contreras Murcia				
Revisó:	Luz Paula Contreras Murcia Javier Edgardo Soto Argel Luis Javier Barrera Naicipa				
Aprobó:	Juan José Neira Santacruz				
Ubicación:	Oficina Asesora de Planeación e Información				

Contenido

1. Objetivo.
2. Alcance.
3. Términos y Definiciones
4. Política de Seguridad de la Información de la UNGRD.
5. Objetivos del Sistema de Gestión de Seguridad de la Información.
6. Alcance del Sistema de Gestión de Seguridad de la Información.
7. Comité de Seguridad y Privacidad de la Información.
8. Planes Desarrollados de Seguridad y Privacidad de la Información.
9. Actividades de Seguridad y Privacidad de la Información.
10. Marco Legal.
11. Documentos Asociados.

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.

2. Alcance

El alcance del Plan de Seguridad y Privacidad de la Información se aplica al proceso de Gestión de Sistemas de Información y al Subproceso de 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. Términos y Definiciones

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. Política 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.

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 Sistemas de Información y el subproceso de Infraestructura Tecnológica.

7. Comité de Seguridad y Privacidad de la Información

Mediante Resolución 1568 del 28 de diciembre de 2016, se integró al Comité Institucional del Sistema Integrado de Planeación y Gestión, las funciones del Comité de Seguridad de la Información.

El Comité SIPLAG se encontraba integrado por los funcionarios:

- a. El Representante de la Alta Dirección, quien lo presidirá.
- b. El funcionario designado por el Representante de la Alta Dirección como líder del Sistema Integrado de Planeación y Gestión.
- c. Un funcionario de la Dirección General.
- d. Un funcionario de la Secretaría General.
- e. Un funcionario de la Subdirección General.
- f. Un funcionario de la Oficina Asesora Jurídica.
- g. Un funcionario de la Oficina Asesora de Comunicaciones.
- h. Un funcionario de la Oficina de Control Interno.
- i. Un funcionario de la Oficina Asesora de Planeación e Información.
- j. Un funcionario de la Subdirección para el Conocimiento del Riesgo.
- k. Un funcionario de la Subdirección para la Reducción del Riesgo.
- l. Un funcionario de la Subdirección para el Manejo de Desastres
- m. Un funcionario del Grupo de Contratación.
- n. Un funcionario del Grupo de Talento Humano.
- o. Un funcionario del Grupo de Apoyo Administrativo.
- p. Un funcionario del Grupo de Apoyo Financiero y Contable.
- q. Un funcionario del Grupo de Cooperación Internacional.

El comité Institucional del Sistema Integrado de Planeación y Gestión, sin perjuicio de las funciones y obligaciones que sean contempladas en normas específicas, desarrollará las siguientes actividades:

- a. Liderar, coordinar y facilitar la implementación, mejoramiento continuo y sostenibilidad del Sistema Integrado de Planeación y Gestión, con respecto a cada uno de los sistemas que lo conforman.
- b. Aprobar el plan de trabajo de cada sistema que hace parte del Sistema Integrado de Planeación y Gestión.
- c. Verificar la ejecución de los planes de trabajo del desarrollo, implementación y mejoramiento continuo del Sistema Integrado de Planeación y Gestión.
- d. Evaluar los productos resultantes del desarrollo, implementación y mejoramiento continuo del Sistema Integrado de Planeación y Gestión.

- e. Recomendar las acciones de mejora continua que surjan como resultado de la evaluación del Sistema Integrado de Planeación y Gestión a partir de las evaluaciones e informes presentados por la Oficina de Control Interno.
- f. Apoyar y divulgar a alto nivel el Sistema de Gestión de Seguridad de la Información- SGSI.
- g. Tomar decisiones estratégicas para el Sistema de Gestión de Seguridad de la Información- SGSI.
- h. Estudiar los cambios propuestos para el Modelo de Seguridad de la Información.
- i. Presentar propuestas para la adopción de medidas relacionadas con el mejoramiento del Sistema de Gestión de Seguridad de la Información- SGSI.
- j. Permitir la aprobación de políticas, acciones y controles a ser implementadas por la UNGRD para fortalecer su estado en seguridad de la información.
- k. Generar confianza y proteger adecuadamente la información de la UNGRD.
- l. Promover la difusión y apoyo a la seguridad de la información dentro de la entidad y a las campañas de sensibilización en temas de seguridad de la información.
- m. Velar por el cumplimiento de las políticas del Sistema de Gestión de Seguridad de la Información- SGSI n. Reportar a la Alta Dirección las oportunidades de mejora frente al Sistema de Gestión de Seguridad de la Información- SGSI."

Dicha resolución fue derogada en el año 2018, por medio de la Resolución 445, 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.

4	Definición del nuevo alcance del SGSI	Continuar con la vinculación de los procesos de la UNGRD al SGSI	Paula Contreras Carolina Jiménez Luis Javier Barrera Javier Soto	4/03/2019	31/12/2019
---	---------------------------------------	--	---	-----------	------------

10. Marco Legal

- 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.

11. Documentos Asociados

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- M-1603-SIS-04 Manual del Sistema de Gestión de Seguridad de la Información.
- M-1603-SIS-03_3 Manual de Políticas de Seguridad de la Información.
- RG-1603-SIS-17 Formato Matriz de Riesgos SGSI UNGRD Infraestructura.
- RG-1300-GSI-12 Formato Matriz de Riesgos SGSI UNGRD Aplicaciones.