



SGI-PL-011

**Política de
Gobierno Digital y
Seguridad Digital
29/11/2024**



CONTENIDO

INTRODUCCIÓN	3
OBJETIVO	4
ALCANCE.....	4
DEFINICIONES	5
MARCO NORMATIVO	6
DESCRIPCIÓN DE LA POLÍTICA	7
ROLES Y RESPONSABILIDADES	8
DIAGNOSTICO / AUTODIAGNÓSTICO.....	11
SEGUIMIENTO	17
DOCUMENTOS RELACIONADOS	17
BIBLIOGRAFÍA.....	17
HISTORIAL DE CAMBIOS	18



INTRODUCCIÓN

El Modelo integrado de Planeación y Gestión – MIPG – es el marco de referencia diseñado por el Gobierno Nacional para que las entidades públicas planeen, ejecuten y hagan seguimiento a su gestión de cara a la ciudadanía. Bajo este concepto, MIPG tiene como propósito mejorar la capacidad del Estado en su relación con la ciudadanía, incrementando su confianza en las entidades y en los servidores públicos, logrando mejores niveles de gobernabilidad y legitimidad del aparato público y generando resultados con valores a partir de una mejor coordinación interinstitucional, compromiso del servidor público, mayor presencia en el territorio y mejor aprovechamiento y difusión de información confiable y oportuna, y de esta manera permitir que las organizaciones, cumplan con los objetivos para las cuales fueron creadas y enfoquen toda su actividad en la producción de resultados que garanticen los derechos y resuelvan las necesidades de los ciudadanos.

La dimensión No. 3 Gestión con valor para resultados, tiene como propósito permitirle a la entidad realizar las actividades que la conduzcan a lograr los resultados propuestos y a materializar las decisiones plasmadas en su planeación institucional, en el marco de los valores del servicio público.

En este caso la política de Gobierno Digital de MIPG busca impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio.

En cuanto a la Política de Seguridad Digital busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia. Lo



anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

Esta política contiene los lineamientos establecidos por la alta dirección y fue aprobada por el comité de gestión y desempeño en la sesión del día 29 de noviembre de 2024.

OBJETIVO

Fortalecer y promover el uso y aprovechamiento de las tecnologías de la información en el Instituto de Hidrología, Meteorología y Estudios Ambientales (Ideam), convirtiéndolas en un pilar fundamental de su transformación digital. Este objetivo estratégico buscará no solo fomentar la transparencia y el acceso a la información, sino también mejorar la calidad de los servicios públicos digitales y garantizar un acceso inclusivo.

ALCANCE

A nivel nacional, la entidad que lidera esta política generando los lineamientos, directrices e instrucciones formulados para su implementación es Ministerio de Tecnologías de la Información y Comunicaciones. En el Ideam, el proceso que lidera la aplicación de los lineamientos dados por la Función Pública es el proceso de Gestión de Tecnologías de información y comunicaciones, estos lineamientos serán aplicados en los demás procesos del Instituto.

Esta Política aplica a todos los procesos establecidos en la entidad en el marco del Modelo Integrado de Planeación y Gestión – MIPG.

BREVIATURAS

Ideam: Instituto de Hidrología, Meteorología y Estudios Ambientales

MIPG: Modelo integrado de Planeación y Gestión

DAFP: Departamento Administrativo de la Función Pública

ITA: Índice de Transparencia y Acceso a la Información



DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: Los activos de información son el resultado de la construcción de un inventario y clasificación de los activos que posee la entidad de acuerdo con la Política General de Seguridad y Privacidad de la información, la cual determina que activos posee la entidad, cómo deben ser utilizados, así como los roles y responsabilidades que tienen los funcionarios sobre los mismos.

Arquitectura empresarial – AE: Es una práctica estratégica que consiste en analizar integralmente las entidades desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su situación actual y establecer la transformación necesaria. El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión de la entidad.

Dato: Representación simbólica ya sea numérica o alfanumérica, cuyo valor está listo para ser procesado por una computadora y ser presentado en formato de información.

Políticas: Directrices que codifican los principios y la intención de la dirección en normas fundamentales que rigen la creación, adquisición, integridad, seguridad, calidad y uso de los datos y la información.

Política de TI: Es una directriz u orientación que tiene el propósito de establecer pautas para lograr los objetivos propuestos en la Estrategia de TI. Las políticas son usadas para dirigir las decisiones, para asegurar la consistencia y el apropiado desarrollo e implementación de los procesos, estándares, roles, actividades y servicios de TI.

Riesgo Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.



Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital.

Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

MARCO NORMATIVO

- Ley 1955 de 2019 art. 147 y 148
- Decreto 2106 de 2019 art. 8 -17
- Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2)
- Directiva presidencial 02 de 2019 - Simplificación de la interacción digital entre los ciudadanos y el Estado
- Ley 1712 de 2014 - Transparencia y Acceso a la Información Pública
- Decreto 415 de 2016 (Compilado en el Título 35, parte 2, libro 2 del Decreto No. 1083 de 2015) - Lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones
- Decreto 1413 de 2017 (Título 17, parte 2, libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
- Decreto 1078 de 2015 - Reglamenta la prestación de los Servicios Ciudadanos Digitales
- Decreto 767 de 2022- Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Decreto 088 de 2022- "Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 y 6 de la Ley 2052 de 2020, estableciendo los conceptos,



lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea”

- DECRETO 767 DE 2022 “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”

DESCRIPCIÓN DE LA POLÍTICA

La Política de Gobierno Digital en conjunto con la de seguridad son la política del Gobierno Nacional que propende por la transformación digital pública. Con esta política pública se busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública y el Estado en general, a través del uso y aprovechamiento de las TIC. Hace parte del Modelo Integrado de Planeación y Gestión - MIPG y se integra con las políticas de Gestión y Desempeño Institucional.

- **Gobernanza:** Este elemento se basa el relacionamiento entre el orden nacional y territorial, y el nivel central y descentralizado. Asimismo, involucra a los grupos de interés en la toma de decisiones, la definición de los focos estratégicos de acción y la distribución de los recursos disponibles.
- **Innovación Pública Digital:** La Política de Gobierno Digital propenderá por la generación de valor público a través de la introducción de soluciones novedosas y creativas que hagan uso de las TIC y de metodologías de innovación, para resolver problemáticas públicas desde una perspectiva centrada en los ciudadanos.
- **Habilitadores:** Corresponde a las capacidades que les permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital.

Se mantienen los tres habilitadores de la actual Política de Gobierno Digital: Arquitectura, Seguridad y privacidad de la información, y Servicios ciudadanos digitales.

Se adiciona el habilitador "Cultura y Apropiación", el cual busca desarrollar las capacidades de los sujetos obligados y los Grupos de Interés, requeridas para el acceso, uso y aprovechamiento de las TIC.

- **Líneas de acción:** Son las acciones orientadas a desarrollar servicios y procesos inteligentes, tomar decisiones basadas en datos y consolidar un Estado abierto, con el fin de articular las Iniciativas Dinamizadoras de la Política de Gobierno Digital. Estas Líneas de Acción se materializarán en las sedes electrónicas de cada uno de los sujetos obligados, siguiendo los estándares señalados para tal fin.
- **Iniciativas dinamizadoras:** Las iniciativas dinamizadoras comprenden los Proyectos de Transformación Digital y las Estrategias de Ciudades y Territorios Inteligentes, que materializan las Líneas de acción y permiten dar cumplimiento al objetivo de la Política.

ROLES Y RESPONSABILIDADES

Tabla 1 Roles y responsabilidades

Instancia y/dependencia	Rol
MINTIC	Líder de la política de Gobierno Digital. Es el Ministerio de Tecnologías de la Información y las Comunicaciones, quién a través de la Dirección de Gobierno Digital, se encarga de emitir las normas, manuales, guías y la metodología de seguimiento y evaluación para la implementación de la política de Gobierno Digital, en las entidades públicas del orden nacional y territorial. De igual manera, a través de la Dirección de Gobierno Digital se desarrollan diferentes iniciativas y

Instancia y/dependencia	Rol
	proyectos que buscan apalancar la implementación de la política en las entidades públicas.
REPRESENTANTE LEGAL	Responsable de coordinar, hacer seguimiento y verificación de la implementación de la Política de Gobierno Digital. Como responsables de la política de Gobierno Digital, deben garantizar el desarrollo integral de la política al interior de sus entidades, entendiendo que esta es un eje transversal y apalancador de su gestión interna, que apoya el desarrollo de las políticas de gestión y desempeño institucional.
COMITÉS INSTITUCIONALES DE GESTIÓN Y DESEMPEÑO	La principal función de este comité es orientar la implementación y operación de todas las políticas del Modelo Integrado de Planeación y Gestión - MIPG (entre las que se encuentra Gobierno Digital); debe articular todos los esfuerzos institucionales, recursos, metodologías y estrategias para el desarrollo de las políticas del MIPG y en esta medida, lograr que Gobierno Digital se desarrolle articuladamente con las demás políticas en el marco del sistema de gestión de la entidad.

Instancia y/dependencia	Rol
DIRECTORES, SUBDIRECTORES, JEFES DE OFICINAS, ETC	Las demás áreas serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia. En este sentido, áreas o dependencias afines a los siguientes temas también son responsables en la implementación de la política de Gobierno Digital, dada su transversalidad en la gestión de la entidad: planeación, secretaría general, servicio al ciudadano, participación ciudadana, comunicaciones o prensa, desarrollo organizacional, talento humano, archivo y gestión documental.
OFICINA DE INFORMATICA	Realizar la implementación de la política de seguridad digital y Gobierno digital
OFICINA ASESORA DE PLANEACIÓN	Realizar el seguimiento a la implementación de la política.
OFICINA DE CONTROL INTERNO	Realizar control y evaluación a la implementación de la política
GRUPO DE SERVICIO AL CIUDADANO	Elaborar estadísticas sobre el uso y la aceptación de los servicios digitales ofrecidos por el Instituto a través de sus canales de comunicación oficiales.
GRUPO DE ADMINISTRACIÓN Y DESARROLLO DEL TALENTO HUMANO	Incluir en el Plan Institucional de Capacitaciones anualmente la formación constante para los funcionarios y contratistas en los temas de:

Instancia y/dependencia	Rol
	- Gobierno digital - Seguridad y Privacidad de la Información.

Fuente: Propia 2024

DIAGNOSTICO / AUTODIAGNÓSTICO

Como parte del proceso de medición del Índice de Desempeño Institucional – IDI del 2023, esta política presentó unos resultados bajos por lo cual se deben realizar acciones específicas respecto con el fin de tener una mejora continua.

Por ello se llevó a cabo el ejercicio de autodiagnóstico de la política y se aplicó la herramienta definida por el Departamento Administrativo de la Función Pública – DAFP, obteniéndose el siguiente resultado:

Ilustración 1 Resultados autodiagnóstico

Política	2022	2023
POL01: Gestión estratégica del talento humano	94,53	91,22
POL02: Integridad	66,95	84,55
POL03: Planeación institucional	88,99	90,61
POL04: Gestión presupuestal y eficiencia del gasto público	72,00	69,33
POL05: Compras y contratación pública	95,12	100,00
POL06: Fortalecimiento organizacional y simplificación de procesos	98,18	92,97
POL07: Gobierno digital	69,55	74,45
POL08: Seguridad digital	70,00	63,22
POL09: Defensa jurídica	100,00	100,00
POL11: Servicio al ciudadano	71,76	73,21
POL12: Racionalización de trámites	40,30	48,00
POL13: Participación ciudadana en la gestión pública	74,30	75,73
POL14: Seguimiento y evaluación del desempeño institucional	69,30	87,13
POL15: Transparencia, acceso a la información y lucha contra la corrupción	74,73	81,33
POL16: Gestión documental	86,90	94,94
POL17: Gestión información estadística	72,76	85,78
POL18: Gestión del conocimiento	49,00	74,08
POL19: Control interno	65,63	86,18

Fuente: Función Pública 2024

POLÍTICA 7	i11.Gobernanza	i12.Innovación	i13.Arquitectura	i14.Seguridad y	i15.Servicios	i16.Cultura y	i17.Servicios y	i18.Estado	i19.Decisiones	i20.Proyectos	i21.Estrategias
Gobierno Digital	Pública Digital	a	Privacidad de la	Ciudadanos	Digitales	apropiación	Procesos	abierto	basadas en	de	de Ciudades y
			información				Inteligentes		datos	Transformación	Territorios
										Digital	Inteligentes
	74,5	44,4	70,8	65,9	58,3	91,3	42,9	85,9	97,1	66,7	

Ilustración 2 Resultados autodiagnóstico

POLÍTICA 8	i22.Asignación	i23.Implementación	i24.Despliegue
Seguridad Digital	de Recursos	de Lineamientos de Política	de Controles
	63,2	37,0	75,0
			66,7

Fuente: Función Pública 2024

IMPLEMENTACIÓN

Con base en el resultado obtenido. La entidad priorizará las siguientes acciones para conforme a las recomendaciones realizadas por la Función pública en agosto del 2024:

GOBIERNO DIGITAL

Tabla 2 Recomendaciones de la política de Gobierno Digital

	RECOMEDACIÓN	TEMA
1	Analizar los incidentes de seguridad digital (Ciberseguridad) que se presentaron y tomar las medidas necesarias para evitar que se vuelvan a presentar	SEGURIDAD
2	Capacitar a servidores y contratistas de la entidad en temáticas de la Política de Gobierno Digital tales como Gobernanza, Innovación Pública Digital, Seguridad y Privacidad de la Información, Arquitectura TI, Cultura y Apropiación, Servicios Ciudadanos Digitales, Decisiones basadas en datos, Estado abierto, servicios y procesos inteligentes, Proyectos de transformación digital y Estrategias de Ciudades y Territorios Inteligentes.	USO Y APROPIACIÓN

	RECOMEDACIÓN	TEMA
3	Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información (MSPI) de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.	SEGURIDAD
4	Desarrollar conjuntos de datos abiertos estratégicos de la entidad en procesos de cocreación o consulta pública.	DATOS ABIERTOS
5	Determinar el alcance de los proyecto con componentes de TI en su entidad, así como la priorización de actividades asociadas a cada uno.	PETI
6	Documentar las lecciones aprendidas de los proyectos con componentes de TI implementados y realizar la respectiva comunicación a los interesados	USO Y APROPIACIÓN
7	Elaborar un diagnóstico de seguridad y privacidad de la información para la entidad a través de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI). Posteriormente, presentar y lograr la aprobación del diagnóstico en el Comité de Gestión y Desempeño Institucional.	SEGURIDAD
8	Establecer instancias/dependencias de toma de decisiones sobre la implementación de la Política de Gobierno Digital en la entidad, tales como el Comité de Gestión y Desempeño Institucional, la Oficina de Tecnologías de Información, la Oficina de Planeación, entre otras.	GOBIERNO
9	Establecer una metodología para la gestión de proyectos con componentes de TI.	PETI
10	Formular, aprobar, implementar y actualizar mediante un proceso de mejora continua la política de seguridad y privacidad de la información de la entidad.	SEGURIDAD

	RECOMEDACIÓN	TEMA
11	Identificar, aprobar, implementar un proceso de valoración y actualizar mediante un proceso de mejora continua los riesgos de seguridad y privacidad de la información de la entidad.	SEGURIDAD
12	Implementar el criterio de accesibilidad web 'CC1. Alternativa de texto para elementos no textuales' en la sede electrónica de la entidad, acorde con el anexo 1 de la Resolución 1519 de 2020.	PÁGINA WEB
13	Implementar el criterio de accesibilidad web 'CC26. Enlaces adecuados' en la sede electrónica de la entidad, acorde con el anexo 1 de la Resolución 1519 de 2020.	PÁGINA WEB
14	Implementar el criterio de accesibilidad web 'CC28. Manejo de error' en la sede electrónica de la entidad, acorde con el anexo 1 de la Resolución 1519 de 2020.	PÁGINA WEB
15	Implementar el criterio de accesibilidad web 'CC29. Imágenes de texto' en la sede electrónica de la entidad, acorde con el anexo 1 de la Resolución 1519 de 2020.	PÁGINA WEB
16	Implementar el criterio de accesibilidad web 'CC30. Objetos programados' en la sede electrónica de la entidad, acorde con el anexo 1 de la Resolución 1519 de 2020.	PÁGINA WEB
17	Implementar el criterio de accesibilidad web 'CC31. Desde una letra hasta un elemento complejo utilizable' en la sede electrónica de la entidad, acorde con el anexo 1 de la Resolución 1519 de 2020.	PÁGINA WEB
18	Implementar el criterio de accesibilidad web 'CC32. Manejable por teclado' en la sede electrónica de la entidad, acorde con el anexo 1 de la Resolución 1519 de 2020.	PÁGINA WEB
19	Implementar el criterio de accesibilidad web 'CC4. Textos e imágenes ampliados y en tamaños adecuados' en la sede	PÁGINA WEB

	RECOMEDACIÓN	TEMA
	electrónica de la entidad, acorde con el anexo 1 de la Resolución 1519 de 2020.	
20	Implementar la hoja de ruta definida en el Plan Estratégico de Tecnologías de la Información (PETI).	PETI
21	Incluir a grupos de valor e interés como la ciudadanía, sociedad civil, academia, sector privado, entre otros, en ejercicios de participación para la toma de decisiones sobre la implementación de la Política de Gobierno Digital en la entidad.	PARTICIPACIÓN
22	Integrar el proceso de Arquitectura Empresarial al Sistema de Gestión de Calidad de la entidad.	CALIDAD
23	Integrar el proceso de gestión de proyectos con componentes de TI con el Sistema de Gestión de Calidad de la entidad.	CALIDAD
24	Publicar en la sección transparencia y acceso a la información pública del portal web información actualizada sobre calendario de actividades	PÁGINA WEB
25	Realizar análisis de vulnerabilidades de seguridad a los activos de información en su infraestructura On Premise	SEGURIDAD
26	Realizar ejercicios de consulta o toma de decisiones con los grupos de interés de la entidad haciendo uso de medios digitales.	PARTICIPACIÓN
27	Realizar seguimiento a través de indicadores de eficiencia y eficacia a la ejecución de proyectos con componentes de TI en la entidad.	PETI
28	Usar medios digitales de la entidad como la sede electrónica, redes sociales, espacios virtuales de participación (juntas comunales, cabildos, consejos, foros, talleres, mesas informativas, mesas consultivas, mesas resolutivas o de decisión), entre otros, para interactuar con grupos de valor e	PARTICIPACIÓN

	RECOMEDACIÓN	TEMA
	interés como ciudadanía, sociedad civil, academia, sector privado y sector público.	

SEGURIDAD DIGITAL

Tabla 3 Recomendaciones de la política de Seguridad Digital

N	RECOMEDACIÓN	TEMA
1	Designar un área o responsable de la seguridad digital.	SEGURIDAD
2	Elaborar un diagnóstico de seguridad y privacidad de la información para la entidad a través de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI). Posteriormente, presentar y lograr la aprobación del diagnóstico en el Comité de Gestión y Desempeño Institucional.	SEGURIDAD
3	Garantizar el soporte a la infraestructura tecnológica de la entidad (plataformas, licencias, servicios y sistemas de información)	SEGURIDAD
4	Identificar, aprobar, implementar un proceso de valoración y actualizar mediante un proceso de mejora continua los riesgos de seguridad y privacidad de la información de la entidad.	SEGURIDAD
5	Realizar un ejercicio de análisis de vulnerabilidades y Assessment de Seguridad.	SEGURIDAD



SEGUIMIENTO

Para conocer el avance de la política en el Instituto, se aplicará al inicio de cada vigencia, la herramienta de autodiagnóstico diseñado por el Departamento Administrativo de la Función Pública – DAFP y adoptada por el Ideam, así como el formulario de autodiagnóstico ITA, y como resultado de este autodiagnósticos se formularán las acciones de mejora o cierres de brechas necesarios y una vez sean entregados por resultados del Índice de Desempeño Institucional, estas acciones se articularán ajustándolas o incluyendo nuevas acciones de mejora.

El seguimiento a estas acciones se adelantará de manera trimestral, por parte del líder de la política y los procesos involucrados, entregando los resultados del seguimiento junto con sus evidencias a la Oficina Asesora de Planeación para su consolidación y análisis.

EVALUACIÓN

Anualmente, el avance y la efectividad del Modelo Integrado de Planeación y Gestión MIPG, y cada una de sus políticas, incluida la política de gobierno digital, se mide en el Índice de Desempeño Institucional – IDI, que recopila la información a través del Formulario Único de Reporte y Avance de Gestión - FURAG o mediante la metodología o herramienta definidas por el Departamento Administrativo de la Función Pública o la entidad del gobierno competente. A partir de las mediciones de FURAG, se articulará con las acciones de mejora o cierre de brechas originadas por el autodiagnóstico, ajustando las actividades si fuera necesario o adicionando nuevas acciones para el mejoramiento en la implementación de la política.

DOCUMENTOS RELACIONADOS

No aplica

BIBLIOGRAFÍA

- Manual Operativo del Modelo Integrado de Planeación y Gestión 2023 V.5 - Departamento Administrativo de la Función Pública.

- Portal web del Departamento Administrativo de la Función

Pública: <https://www.funcionpublica.gov.co/web/mipg/como-opera-mipg>

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
01	29/11/2024	Creación del Documento