Unidad de Planeación
Minero Energética

UPME - UNIDAD DE PLANEACIÓN MINERO ENERGÉTICA - 30 años

Proyecto de

# POLÍTICAS DE GOBIERNO DE DATOS

y Gestión de información del Sector Minero Energético

Abril 2025

CIO SECTORIAL
CHIEF INFORMATION OFFICER

UPME
Av Calle 26 # 69D – 91 Torre 1 – Piso 9
Bogotá – Colombia
Tel.: +57 6012220601
upme.gov.co

**UNIDAD DE PLANEACIÓN MINERO ENERGÉTICA - UPME**

CARLOS ADRIÁN CORREA FLÓREZ
*Director General*

**AUTORES**

JOHANNA STELLA CASTELLANOS
*Subdirectora Gestión de la Información*

*Equipo Subdirección Gestión de la Información*

JOHN ÁVILA ARIAS
MARLET GARCÍA PÁEZ
ARMANDO BOSSIO RAMOS
FABIÁN GARZÓN GARCÍA

*Diagramación y diseño*

OLGA LUCÍA ROJAS SOLÓRZANO
JUAN MANUEL ZUÑIGA BOLAÑOS

República de Colombia Ministerio de Minas y Energía
**Abril 2025**

# CONTENIDO

Contenido

# Índice de tablas



# Índice de figuras

# Introducción

# Introducción

El gobierno de datos es un proceso estructurado que permite administrar la disponibilidad, calidad, integridad y seguridad de la información en una organización. Según IBM (2024), el gobierno de datos se define como el conjunto de políticas, procedimientos y estándares diseñados para asegurar que la información sea precisa, confiable y protegida, garantizando su accesibilidad y utilidad para la toma de decisiones estratégicas.

La Unidad de Planeación Minero-Energética (UPME), en su rol de Chief Information Officer (CIO) sectorial, tiene la responsabilidad de liderar la estrategia de gobernanza de datos del sector. De acuerdo con la Resolución 40199 de 2021 y el Decreto 2121 de 2023, la UPME presenta este documento con el propósito de establecer lineamientos y políticas para la administración y gestión de los datos en las entidades del sector. Su objetivo principal es orientar a las organizaciones en la implementación, mantenimiento y mejora de programas de gobierno de datos que garanticen la calidad, seguridad y disponibilidad de la información, avanzando en la madurez de la gestión de los datos y priorizando la correcta administración de los datos maestros según los flujos de información en los distintos procesos institucionales.

El objetivo de este documento es proporcionar una hoja de ruta clara para que las entidades del sector minero energético, incluyendo el Ministerio de Minas y Energía y sus entidades adscritas y vinculadas, implementen políticas de gobierno de datos alineadas con las particularidades del sector. No obstante, se reconoce la autonomía de cada entidad para adaptar e implementar estos lineamientos de acuerdo con su estructura, prioridades y nivel de madurez institucional, respetando sus dinámicas organizacionales internas y sus capacidades técnicas y operativas.

A diferencia de las Guías de Gobierno de Datos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), que establecen principios generales aplicables a todas las entidades públicas, este documento está diseñado específicamente para las necesidades y particularidades del sector minero energético. Mientras que las guías del MinTIC proveen un marco de referencia sobre aspectos como arquitectura empresarial, interoperabilidad y gestión del riesgo aplicables al sector público en general, este documento se

enfoca en la implementación operativa y sectorializada de un modelo de gobierno de datos dentro de las entidades del sector, alineando las políticas con las dinámicas propias de los procesos y sistemas de información sectoriales.

El presente documento se fundamenta en lineamientos internacionales y nacionales reconocidos. Según el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en su guía G.INF.06 - Guía Técnica de Información - Gobierno de Datos, la gobernanza de datos debe estar alineada con principios de arquitectura empresarial, interoperabilidad y gestión del riesgo para garantizar su efectividad y sostenibilidad. Asimismo, se tienen en cuenta las mejores prácticas establecidas en el *DAMA-DMBOK*, que enfatiza la necesidad de contar con estructuras organizativas claras y metodologías robustas para la administración de datos. En la sección de lineamientos de este documento, se explicita que las políticas propuestas se basan en estos marcos de referencia y estándares, buscando una implementación coherente con el ecosistema digital estatal y con el ciclo de vida de los datos en las entidades del sector.

Posteriormente, el documento aborda los lineamientos y políticas de gobierno de datos, estableciendo principios fundamentales para la administración, uso y seguridad de la información. De acuerdo con el Manual de Gobierno de Datos de la Función Pública, estos lineamientos incluyen aspectos como la seguridad de la información, interoperabilidad, calidad de datos y gestión del acceso y circulación de la información, con el fin de asegurar la aplicación de estándares adecuados que faciliten el aprovechamiento de los datos en el sector.

Finalmente, se desarrolla la política de gestión de la continuidad para el gobierno de datos, que define estrategias y mecanismos orientados a garantizar la continuidad del ecosistema de información. El objetivo general de este documento es establecer e implantar lineamientos y políticas para la administración y gestión de los diferentes componentes de información en las entidades del sector minero energético, en el marco de la arquitectura empresarial de gobierno de datos. Con ello, se busca garantizar la calidad y oportunidad de los datos, facilitando la toma de decisiones basadas en evidencia y contribuyendo a la modernización del sector.

Para cumplir con este propósito, se establecen los siguientes objetivos específicos. Primero, se busca fomentar una cultura de gestión y calidad de

datos, promoviendo el uso estratégico de la información dentro de las entidades del sector. Segundo, se pretende garantizar la gestión de la información bajo estándares de calidad, asegurando que sea confiable y apta para el análisis y procesamiento. Además, se trabajará en la identificación y clasificación de los componentes de información y sus flujos dentro de cada entidad, permitiendo su administración estructurada y eficiente. Asimismo, se busca garantizar la homologación de la información en los distintos sistemas de información, evitando inconsistencias y redundancias que puedan comprometer su integridad. Finalmente, se establecerán medidas para asegurar la disponibilidad, seguridad y privacidad de los datos, en cumplimiento con la normativa vigente y las mejores prácticas en protección de la información.

La estructura de este documento se divide en tres apartados, abordando el gobierno de datos desde una perspectiva general hasta aspectos más específicos. En primer lugar, se establecen los roles del gobierno de datos, determinando las funciones y responsabilidades de los actores involucrados en la gestión de la información. Según el Manual de Gobierno de Datos de Función Pública (2021), la gobernanza de datos debe basarse en una distribución clara de responsabilidades a través de tres niveles: estratégico, táctico y operacional. En esta sección se incluyen además los roles de acceso a los datos, garantizando un modelo de gestión seguro y eficiente.

A través de la implementación de este modelo de gobierno de datos, el sector minero energético fortalecerá su capacidad para administrar la información como un activo estratégico, asegurando su calidad, seguridad y uso eficiente en la toma de decisiones y en la optimización de la gestión pública.

# 1. Roles
## del Gobierno de Datos

# 1. Roles del Gobierno de Datos

El gobierno de datos en el sector minero energético requiere una clara definición de roles, autoridades y responsabilidades que garanticen la gestión, protección y aprovechamiento estratégico de la información sectorial. Esta sección establece la estructura organizativa para la administración de los datos en el sector, asignando funciones específicas a cada actor involucrado en el ciclo de vida de la información.

En la primera subsección, Roles, autoridad y responsabilidad, se describen las funciones y competencias de los actores responsables del gobierno de datos, asegurando una gestión alineada con los principios de transparencia, eficiencia y seguridad de la información. Posteriormente, en la subsección Roles de acceso a los datos, se establecen los niveles de acceso y los perfiles de usuario, garantizando que la manipulación de la información sectorial se realice conforme a criterios de confidencialidad, integridad y disponibilidad.

## 1.1 Roles, autoridad y responsabilidad

La estructura organizacional es un componente fundamental para la implementación y sostenibilidad del gobierno de datos en el sector minero energético. Una estructura clara y bien definida permite distribuir responsabilidades de manera efectiva tanto en la toma de decisiones estratégicas como en la ejecución operativa de las políticas de gestión de datos.

Si bien la estructura de gobierno de datos puede variar entre entidades, siguiendo los lineamientos de Función Pública sobre gobernanza de la información en entidades estatales se pueden identificar tres niveles principales: i) el nivel estratégico es el encargado de definir la visión y los lineamientos generales para la gobernanza de datos, asegurando su alineación con las políticas sectoriales y nacionales. En este nivel participan los órganos directivos y de alto nivel de decisión, que garantizan el cumplimiento de los principios de transparencia, seguridad y eficiencia en la gestión de datos, ii) el **nivel táctico** es el encargado de traducir las directrices estratégicas en acciones concretas, coordinando la gestión de datos entre diferentes áreas y

actores involucrados. Este nivel garantiza la implementación de estándares, procedimientos y herramientas para una administración eficiente de la información, y; iii) el **nivel operativo** es el responsable de la implementación y administración diaria de los procesos de gestión de datos. Aquí se incluyen los roles encargados de la recopilación, almacenamiento, procesamiento y seguridad de la información, asegurando su integridad y disponibilidad.

En la **figura 1**, se muestran los roles asociados al gobierno de datos y gestión de la información que pueden existir dentro de una entidad, aunque su distribución y denominación pueden variar según la estructura y necesidades específicas de cada organización.

**Roles para el gobierno de datos**

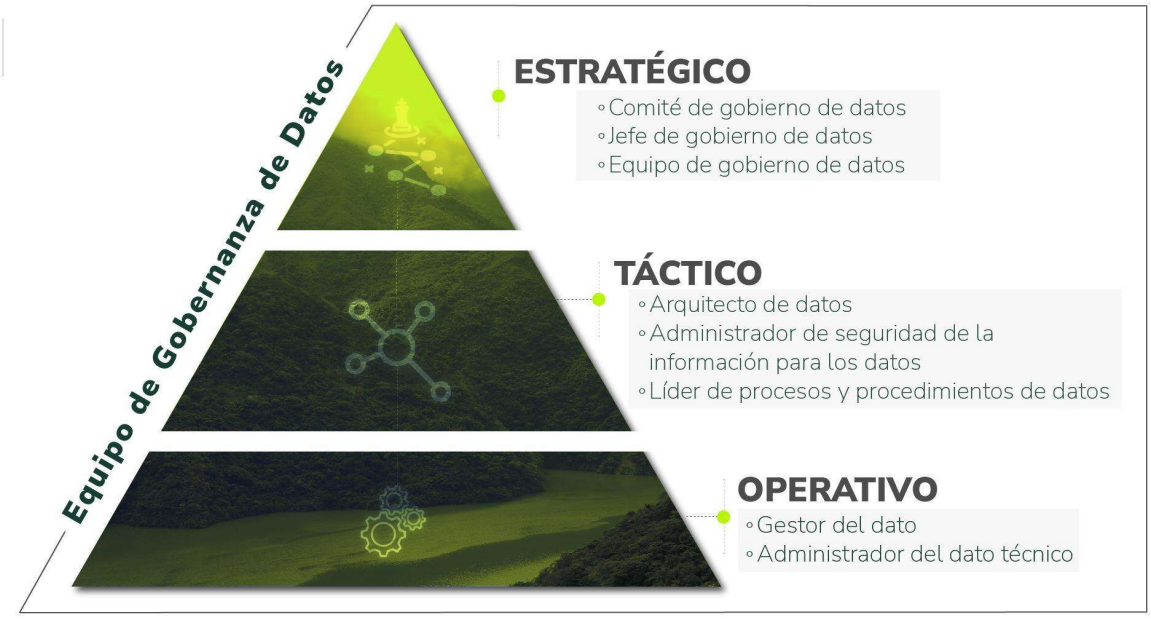


*Figura 1. Roles para el gobierno de datos. Elaboración propia.*

En este modelo general, las dependencias y áreas responsables, como las unidades de tecnología de la información y las dependencias de gestión de datos, desempeñan un papel clave, asegurando tanto el soporte tecnológico como la administración eficiente de la información sectorial.

### Nivel estratégico

El nivel estratégico del gobierno de datos está compuesto por los actores encargados de definir la visión, principios y lineamientos generales para la gestión y aprovechamiento de la información. Su función principal es garantizar

que el gobierno de datos esté alineado con las políticas nacionales y sectoriales, promoviendo su uso como un activo estratégico para la toma de decisiones, la eficiencia operativa y la transparencia en la gestión pública.

En este nivel participan las instancias de mayor jerarquía dentro de la estructura organizacional, responsables de formular y aprobar las políticas de datos, supervisar su implementación y asegurar el cumplimiento de la normativa vigente. Como se observa en la Figura 1, estos roles desempeñan funciones de liderazgo y articulación, facilitando la cooperación interinstitucional y el desarrollo de estrategias de gobernanza que permitan una gestión de datos eficiente, segura y sostenible.

Como parte de la estructura organizativa del nivel estratégico en el gobierno de datos, el Comité de Gobierno de Datos es la instancia encargada de definir las políticas y lineamientos estratégicos que orientan la gestión de datos en el sector minero energético. Su función principal es garantizar que la gobernanza de datos esté alineada con las políticas nacionales y sectoriales, promoviendo su uso eficiente, seguro y transparente en la toma de decisiones.

Este comité actúa como un órgano de coordinación y supervisión, asegurando que la recolección, almacenamiento, procesamiento y uso de los datos cumplan con los principios de calidad, accesibilidad e interoperabilidad. Además, define estándares, revisa el plan operativo del programa de gobierno de datos y asigna responsabilidades dentro del ecosistema de datos, tal como se especifica en la **Tabla 1.**

La formalización de un órgano de gobernanza implica su reconocimiento oficial dentro de la estructura organizativa de una entidad, estableciendo sus funciones, responsabilidades y mecanismos de operación. La formalización de un consejo de gobierno proporciona supervisión del programa de gobierno de datos, tomando decisiones a nivel estratégico, se encargan de la aprobación de políticas y de asignación de los recursos necesarios para su cumplimiento.

**Rol consejo de Gobierno**

| Rol | Comité de gobierno de datos |
|---|---|
| Actor | Unidades de tecnología de la información y las dependencias de gestión de datos |
| Responsabilidades | 1. Definir políticas o lineamientos estratégicos en el programa del gobierno de datos.<br>2. Gestionar los recursos necesarios para el cumplimiento de las estrategias que se planteen.<br>3. Revisar y aprobar el plan operativo del programa de gobierno de datos<br>4. Establecer, en caso de requerirse, el nivel de participación de las dependencias involucradas en la atención de la necesidad del usuario.<br>5. Definir, en caso de requerirse, la dependencia responsable (única) para cada fuente de información<br>6. Designación de roles y responsabilidades para el gobierno de datos<br>7. Definir, conjuntamente con el productor, la periodicidad de la información |
| Nivel Decisorio | Estratégico |
| Cargo Servidor | Director General (presidente, ministro..) Subdirectores, Directores, Vicepresidentes y/o Jefes de Oficinas misionales |

*Tabla 1. Rol consejo de gobierno*
*Fuente: Elaboración propia con base en DAFP (2021)*

En adición, el jefe de gobierno de datos es la figura responsable de coordinar y liderar la implementación de las políticas y estrategias de gestión de datos dentro del sector minero energético. Este rol es fundamental para garantizar la ejecución efectiva del programa de gobierno de datos, supervisando el cumplimiento de los lineamientos establecidos por el Comité de Gobierno de Datos y asegurando su alineación con la normativa vigente **(Ver tabla 2).**

El jefe de gobierno de datos y su equipo desempeñan un papel central dentro del ecosistema de datos, actuando como el principal articulador entre el Comité de gobierno de datos y los actores operativos encargados de la gestión y administración de la información. Su liderazgo es esencial para asegurar que las estrategias definidas a nivel estratégico se implementen correctamente a nivel operativo, fomentando el uso de los datos como un activo estratégico para la toma de decisiones.

Por otro lado, la Subdirección de Información juega un papel clave en la coordinación de la gestión de datos dentro de la entidad, participando activamente en el equipo de gobierno de datos. Sus responsabilidades incluyen la centralización de la información estadística, el apoyo en el análisis de datos y la asistencia técnica a las diferentes dependencias bajo un enfoque estadístico, asegurando la calidad y utilidad de la información para el sector.

**Rol jefe y equipo de gobierno**

| Rol | Jefe de gobierno de datos y equipo de Gobierno de Datos |
|---|---|
| Actor | 1. Oficina de Tecnologías de la información<br>2. Dirección/ subdirección/vicepresidencia/dependencia /(la que aplique dentro de la unidad organizacional) de gestión de información |
| Responsabilidades | 1. Coordina el proceso del gobierno de datos<br>2. Convoca y lidera sesiones de comité de gobierno de datos<br>3. Realiza un seguimiento de las métricas<br>4. Gestiona las comunicaciones internas<br>5. Realizar evaluaciones periódicas al programa en materia de políticas dispuestas, calidad de datos, riesgos de privacidad, entre otros<br>6. Desarrollar estrategias de gobernanza y su plan de implementación<br>7. Determinar las estrategias más adecuadas de divulgación o socialización de las decisiones tomadas en todo lo |

| | |
|---|---|
| | relacionado a gobierno de datos. |
| Nivel Decisorio | Estratégico |
| Cargo Servidor | Director/ subdirector/vicepresidente/directivo /(del área que aplique dentro de la unidad organizacional) de la gestión de información<br>Jefe de la OTI |

*Tabla 2. Rol jefe y equipo de gobierno*
*Fuente: Elaboración propia con base en DAFP (2021)*

## Nivel táctico

El nivel táctico del gobierno de datos actúa como un puente entre la visión estratégica y la ejecución operativa de las políticas de gestión de datos en el sector minero energético. Su función principal es traducir las directrices y lineamientos definidos en el nivel estratégico en acciones concretas, asegurando su implementación efectiva dentro de las entidades del sector.

Este nivel está compuesto por actores responsables de coordinar y supervisar la aplicación de estándares, procedimientos y herramientas necesarias para garantizar la calidad, seguridad e interoperabilidad de los datos. Además, en este nivel se promueve el uso adecuado de la información, facilitando su disponibilidad y acceso para la toma de decisiones basada en evidencia.

Roles con conocimiento del negocio, con capacidades técnicas y habilidades analíticas e informáticas conforman este segundo nivel, deben tener una constante comunicación con el nivel estratégico y operativo para la toma de decisiones tácticas para una gestión adecuada de la información en el ciclo de vida del dato.

Como parte del nivel táctico del gobierno de datos, el Arquitecto de Datos desempeña un rol fundamental en la implementación de los lineamientos estratégicos definidos en el nivel superior. Su principal responsabilidad es diseñar y estructurar la arquitectura de datos dentro de la entidad, asegurando su integración, seguridad y alineación con los objetivos organizacionales. Este rol actúa como el enlace técnico entre la estrategia de datos y su ejecución

operativa, facilitando la estandarización y la interoperabilidad de los sistemas de información.

El Arquitecto de Datos se encarga de definir la estructura, organización y flujo de los datos dentro de la entidad, garantizando que los modelos de información sean eficientes, escalables y alineados con las necesidades del sector. Como se detalla en la **Tabla 3**. Este profesional desempeña funciones clave relacionadas con la integración de datos y el desarrollo de modelos que permitan su aprovechamiento empresarial.

**Rol consejo de Gobierno**

| Rol | Arquitecto de datos |
|---|---|
| Actor | Subdirección de tecnologías de la información<br>Dirección/ subdirección/vicepresidencia/dependencia /(la que aplique dentro de la unidad organizacional) de gestión de información |
| Responsabilidades | 1. Arquitectura de datos y la integración de los mismos<br>2. desarrollo, mantenimiento y aprovechamiento del modelo de datos empresarial. |
| Nivel Decisorio | Táctico |
| Cargo Servidor | Administrador de base de datos |

*Tabla 3. Rol Arquitecto de datos*
*Fuente: Elaboración propia con base en DAFP (2021)*

Así mismo, el Administrador de Seguridad de la Información para los Datos desempeña un rol esencial en la protección y resguardo de la información dentro de la entidad. Su función principal es garantizar que los datos sean gestionados bajo criterios de seguridad, confidencialidad, integridad y disponibilidad, alineándose con las políticas establecidas en el nivel estratégico y con las regulaciones vigentes en materia de seguridad de la información.

Este rol es crucial para mitigar riesgos asociados al manejo de datos sensibles, prevenir vulnerabilidades y fortalecer la capacidad institucional para garantizar

la protección de la información en los diferentes sistemas de la organización. Como se detalla en la Tabla 4. Este profesional define los requerimientos mínimos de seguridad y supervisa su implementación en los sistemas de información de la entidad.

**Rol administrador de datos en seguridad de la información**

| Rol | Administrador de seguridad de la información para los datos |
|---|---|
| Actor | Oficina de Tecnologías de la información |
| Responsabilidades | 1. Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información.<br>2. Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano.<br>3. Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora<br>4. Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados.<br>5. Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.<br>6. Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI. |
| Nivel Decisorio | Estratégico |
| Cargo Servidor | Jefe de la OTI |

*Tabla 4. Rol Administrador de datos en seguridad de la información*
*Fuente: Elaboración propia con base en DAFP (2021)*

Por otro lado, el Líder de Procesos y Procedimientos de Datos cumple un papel fundamental en la estandarización y articulación de los procesos relacionados con la gestión de la información dentro del sector. Su principal responsabilidad es garantizar que los procedimientos implementados en las entidades del sector sean coherentes con los lineamientos estratégicos y que permitan una administración eficiente y estructurada de los datos.

Este rol actúa como un facilitador dentro del ecosistema de datos, asegurando que las dependencias involucradas en la gestión de información cuenten con directrices claras y responsables designados para su implementación. Como se detalla en la Tabla 5. Su labor es clave para la adecuada integración de los procesos de datos en el funcionamiento operativo de la entidad.

**Rol líder de procesos y procedimientos**

| Rol | Líder de procesos y procedimientos de datos |
|---|---|
| Actor | Direcciones Técnicas |
| Responsabilidades | 1. apoyar la articulación de los procesos y procedimientos con la gestión de información y el gobierno de datos<br>2. Designar los responsables temáticos por dependencia para implementación y seguimiento al gobierno de datos |
| Nivel Decisorio | Táctico |
| Cargo Servidor | Directores técnicos |

*Tabla 5. Rol líder de procesos y procedimientos*
*Fuente: Elaboración propia con base en DAFP (2021)*

## Nivel operacional

El nivel operacional del gobierno de datos está conformado por los actores responsables de la ejecución y administración diaria de los procesos de gestión de datos dentro de la entidad. Su función principal es asegurar que la información sea recolectada, procesada, almacenada y utilizada de manera

eficiente, conforme a los lineamientos estratégicos y tácticos definidos en los niveles superiores.

Este nivel es vital para el desarrollo del programa de gobierno de datos, ya que en él participan tanto el gestor del dato como su administrador funcional, quienes son responsables de garantizar la calidad de la información. Estos actores deben tener un conocimiento profundo de los procesos que intervienen en la generación, administración y uso de los datos, asegurando su integridad y disponibilidad para la toma de decisiones.

El nivel operacional está conformado por representantes de las dependencias que producen información y que, en el marco del protocolo de gobierno de datos, asumen el rol de productores de información. Como se observa en la **Figura 1**, los roles dentro de este nivel tienen una función técnica y operativa clave en la implementación de los lineamientos establecidos en los niveles estratégicos y tácticos.

**Rol gestor del dato**

| Rol | Gestor del dato |
|---|---|
| Actor | Direcciones Técnicas |
| Responsabilidades | 1. Producir información estadística de calidad para satisfacer las necesidades del usuario.<br>2. Propender por el mejoramiento continuo de la información estadística que produce.<br>3. Reportar hallazgos al administrador de gobierno de datos<br>4. Definir el flujo de datos en los procesos y los sistemas de información<br>5. Comunicar y promover el valor de la información.<br>6. Monitorear y hacer cumplir las políticas y prácticas de datos en su dependencia. |
| Nivel Decisorio | Operacional |
| Cargo Servidor | Directores técnicos<br>Analista de datos dependencia |

*Tabla 6. Rol gestor del dato*
*Fuente: Elaboración propia con base en DAFP (2021)*

Así mismo, el Gestor del Dato es el responsable de la generación y administración de información dentro de su dependencia, garantizando que los datos sean precisos, confiables y útiles para la toma de decisiones. Su labor es clave para asegurar la calidad y trazabilidad de los datos, en cumplimiento con los lineamientos definidos en los niveles estratégicos y tácticos.

Para el desarrollo de sus funciones, el Gestor del Dato cuenta con el apoyo de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), encargada de la administración del componente tecnológico del sistema de información que centraliza los datos gestionados. Asimismo, recibe apoyo temático de la dependencia técnica, lo que permite que su gestión esté alineada con los objetivos y necesidades sectoriales.

Como se detalla en la **Tabla 6**. Este actor es responsable de producir y mejorar continuamente la información estadística, reportar hallazgos clave y garantizar que los flujos de datos dentro de los sistemas de información sean eficientes y alineados con las políticas del gobierno de datos.

**Rol administrador del dato técnico**

| Rol | Administrador del dato técnico |
|---|---|
| Actor | Oficina de Tecnologías de la información<br>Subdirección de gestión de información |
| Responsabilidades | 1. Aplicar las políticas y lineamientos de gobierno de datos a los sistemas de información<br>2. Apoyar en la definición y ajuste de problemas de datos y alternativas de solución.<br>3. Apoyar en la definición de políticas y estándares de gestión de datos.<br>4. Apoyar a comprender las necesidades de información.<br>5. Participar en el modelado y la arquitectura de datos.<br>6. Apoyar en las definiciones y requisitos de calidad de los datos |
| Nivel Decisorio | Operacional |

| | |
|---|---|
| Cargo Servidor | Jefe Oficina Tecnologías de la Información<br>Administrador del sistema de información |

*Tabla 7. Administrador del dato técnico*
*Fuente: Elaboración propia con base en DAFP (2021)*

Por otra parte, el Administrador del Dato Técnico es el responsable de garantizar la correcta aplicación de los lineamientos de gobernanza de datos en los sistemas de información de la entidad. Su labor es fundamental para asegurar la coherencia, integridad y calidad de los datos en el entorno tecnológico, facilitando su correcta estructuración y disponibilidad para la toma de decisiones.

Este rol se enfoca en la implementación técnica de las políticas de datos, brindando soporte en la definición de estándares y en la solución de problemas relacionados con la gestión de la información. Además, trabaja en estrecha colaboración con el Gestor del Dato, asegurando que la información administrada cumpla con los requerimientos establecidos en los niveles estratégicos y tácticos. Como se detalla en la T**abla 7**, este actor desempeña funciones clave en la gestión y modelado de datos, apoyando la definición de políticas y requisitos de calidad.

## 1.2 Roles de acceso a los datos

El acceso a los datos dentro del sector minero energético debe garantizar un equilibrio entre disponibilidad, seguridad y cumplimiento normativo, asegurando que la información sea utilizada de manera adecuada por los diferentes actores dentro del ecosistema de gobierno de datos. Para ello, cada uno de los sistemas de información de la entidad cuenta con roles y permisos de acceso previamente identificados, definidos por los usuarios funcionales y técnicos, en concordancia con la matriz de roles y responsabilidades, el manual de usuario y el manual técnico correspondiente.

Dado que el gobierno de datos en las entidades del sector minero energético se soporta en estos sistemas de información, los roles de acceso serán los

mismos que ya se encuentran establecidos. No obstante, para la consulta y acceso a los datos maestros identificados en el software o aplicativo definido por la entidad, se adoptan tres roles específicos:

- Propietario: Rol asignado al usuario funcional o responsable del dato a gobernar. Tiene acceso sin restricciones para la consulta de la información.
- Administrador: Rol asignado al equipo de gobierno de datos de Función Pública. Posee permisos de consulta y modificación sin ningún tipo de restricción.
- Consulta: Rol que permite el acceso a la información para todos los usuarios de la entidad. Su configuración puede ajustarse según las necesidades específicas de cada usuario.

Estos roles aseguran que el acceso y uso de los datos dentro de la entidad se realicen conforme a las políticas de gobernanza establecidas, minimizando riesgos y promoviendo el uso eficiente de la información en la toma de decisiones.

# 2. Lineamientos y Políticas de Gobierno de Datos Para la seguridad de la información

# 2. Lineamientos y políticas del gobierno de datos para la seguridad de la información

En el marco del fortalecimiento de la gestión de la información en el sector minero energético, es fundamental establecer lineamientos y políticas claras que orienten el gobierno de datos. Estos lineamientos buscan garantizar la calidad, seguridad, disponibilidad y uso eficiente de los datos, alineándose con las directrices nacionales y sectoriales establecidas.

A nivel nacional, el Decreto 1389 de 2022 establece los lineamientos generales para la gobernanza en la infraestructura de datos y crea el Modelo de Gobernanza de la Infraestructura de Datos. Este decreto busca articular acciones entre el sector público, privado, la academia y la sociedad civil, generando un escenario de confianza y seguridad para el uso y reutilización de los datos.

Específicamente para el sector minero energético, el Ministerio de Minas y Energía adoptó los lineamientos del Modelo de Gobierno de Tecnologías de la Información y del Modelo de Gobierno de Datos mediante la Resolución 40199 de 2021. Este modelo establece una estructura de gobernanza que incluye la Comisión Estratégica de TI y de Datos del sector, el Líder de la Gestión Estratégica de la Información y la Unidad de Planeación Minero-Energética (UPME), con el objetivo de alinear los macroprocesos, procesos y planes sectoriales en materia de tecnologías de la información y datos.

Además, la Política de Gobierno Digital promueve el desarrollo económico y social del país impulsado por datos, considerándolos como infraestructura y activos estratégicos. Esta política enfatiza la necesidad de mecanismos de gobernanza que faciliten el acceso, intercambio, reutilización y explotación de los datos, fomentando decisiones basadas en información de calidad.

En este contexto, la Unidad de Planeación Minero-Energética (UPME), designada como el CIO sectorial, tiene la responsabilidad de liderar la implementación de estas políticas y lineamientos, asegurando una gestión eficiente y segura de los datos en el sector. La UPME, a través de su Oficina de Gestión de la Información, coordina las acciones necesarias para garantizar que los datos se gestionan como activos estratégicos, apoyando la toma de decisiones y contribuyendo al cumplimiento de los objetivos sectoriales.

La implementación de estos lineamientos y políticas de gobierno de datos en el sector minero energético busca no solo cumplir con las normativas establecidas, sino también potenciar el uso de la información como un recurso clave para la innovación, eficiencia y competitividad del sector.

En cumplimiento de los principios legales identificados en las normas aplicables al tratamiento de datos personales y la Política de Gobierno Digital, se hace necesario consolidar un marco normativo robusto que garantice la seguridad de la información en la entidad. En este sentido, los lineamientos presentados a continuación se basan en el *Manual de Gobierno de Datos* del Departamento Administrativo de la Función Pública (DAFP, 2021), el cual establece principios y controles orientados a la preservación de la privacidad, confidencialidad, integridad y disponibilidad de los datos personales en el marco de la arquitectura de seguridad digital institucional. Sin desconocer la importancia de otros principios relevantes, se detallan los principios fundamentales aplicables al gobierno de datos, acompañados de los controles específicos que permiten su implementación efectiva dentro de las entidades del sector minero energético.

## 2.1 Principios y controles de seguridad para el tratamiento de datos personales

### 2.1.1 Principio de veracidad o calidad

Los datos personales sujetos a tratamiento deben ser veraces, completos, exactos, actualizados, comprobables y comprensibles. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

**Tratamiento de datos personales**

Control: Política de tratamientos de datos personales

En cumplimiento de la ley 1581 de 2012, la entidad cuenta con una política de protección de datos personales, garantizando a los titulares de los datos personales el ejercicio de su derecho de hábeas data. *(Ver: Política de tratamiento de datos personales.)*

**Uso aceptable de los activos de información**

Control: lineamientos de gestión de activos de información en Función Pública.

Todos los servidores públicos, contratistas y pasantes de la entidad deben aplicar los controles de seguridad de la información establecidos, garantizando la confidencialidad, integridad, disponibilidad de los activos de información institucionales.

Los propietarios de estos activos son responsables de su uso y protección, ya sea en custodia física o electrónica, e informarán a sus superiores sobre cualquier incidente de seguridad, como uso indebido, alteración o divulgación no autorizada.

**Gestión de cambios sobre los activos de información**

Control: Procedimiento de control de cambios.

Los cambios en la infraestructura tecnológica y servicios de información deben seguir los procedimientos definidos por las dependencias y áreas responsables, asegurando una transición controlada y segura.

### 2.1.2 Principio de acceso y circulación restringida

El tratamiento de datos personales está sujeto a los límites derivados de su naturaleza, de las disposiciones legales y de la Constitución. Por lo tanto, sólo podrán ser tratados por personas autorizadas por el titular o por quienes la ley faculte expresamente.

**Restricciones de acceso a la información**

Control: Lineamientos para el control de acceso a la información

• La Oficina de Tecnologías de la Información y las Comunicaciones es la responsable de implementar controles de acceso a los servicios de información e infraestructura tecnológica. Es responsabilidad de los dueños de los servicios de información restringir el acceso a los servidores públicos, pasantes y contratistas de acuerdo con las funciones y/o actividades a realizar.

• Las áreas responsables de la administración de los sistemas de información, aplicaciones y portales con el apoyo de la Oficina de Tecnologías de la Información y las Comunicaciones son responsables de mantener actualizados los privilegios de acceso a los sistemas de información de sus usuarios.

### 2.1.3 Principio de seguridad

La información sujeta a Tratamiento por el responsable del tratamiento o encargado del tratamiento, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

**Modelo de seguridad y privacidad de la información institucional**

Control: Política institucional de la seguridad de la información.

En su condición de Entidad cabeza del Sector responsable de la formulación de las políticas generales de Administración Pública, en especial de materias relacionadas con el Empleo Público, Organización Administrativa, Control Interno y Racionalización de Trámites, el Departamento Administrativo de la Función Pública, está comprometido con preservar la confidencialidad, Integridad, disponibilidad y veracidad de sus activos de información, reduciendo los riesgos de seguridad digital a través del mejoramiento continuo de los controles en sus procesos, planes y proyectos, el cumplimiento de la normatividad vigente, la aplicación de lineamientos de la Política de Gobierno Digital y la adopción de buenas prácticas de seguridad de la información que contribuyan al logro de los objetivos institucionales y faciliten el aprovechamiento de las tecnologías de la información y las Comunicaciones para que la entidad constantemente sea más proactiva e innovadora.

### 2.1.4 Principio de confidencialidad

todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de esta.

Aplicando el principio nueve de OEA sobre tratamiento de datos personales sensibles la Entidad acepta que: algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos. En ese sentido el DAFP aplica la normatividad vigente en Colombia sobre la protección de datos personales.

### Clasificación de la información

Control: lineamiento de gestión de activos de información

- La clasificación e inventario de la información se realiza bajo el procedimiento de calificación de información.
- Se identifican riesgos de seguridad digital en activos de información clasificados como reservados o confidenciales.
- La información calificada como datos abiertos es evaluada para su publicación en datos.gov.co.
- La calificación de la información debe ser considerada antes de autorizar el acceso a los activos de información institucionales.

**Lineamientos para la transferencia e intercambio de información**

Control: acuerdos de confidencialidad

- La entidad establece **acuerdos de confidencialidad** con terceros que manipulen información reservada.
- El **Grupo de Gestión Contractual** acompaña a las áreas para incluir acuerdos de confidencialidad en los contratos o convenios que lo requieran.

## 2.2 Principios de seguridad para el tratamiento de información pública

Todos los grupos de valor tienen derecho a conocer la información que reposa en las instituciones públicas con las limitaciones que la constitución o la ley impongan. Por ello, la entidad adopta políticas, procesos y procedimientos que garantizan el acceso a la información con integridad y disponibilidad.

### 2.2.1 Principios claves en el acceso a la información publica

- **Principio de Máxima Publicidad**: Toda la información bajo control de un sujeto obligado es **pública por defecto**, salvo disposiciones legales que indiquen lo contrario. *(Ley 1712 de 2014).*
- **Principio de Transparencia**: Se presume que toda información en poder del Estado es pública. Las entidades tienen el deber de **facilitar su acceso** en los términos más amplios posibles. *(Ley 1712 de 2014).*
- **Principio de Buena Fe**: Toda actuación en el cumplimiento del acceso a la información pública se hará con **honestidad, lealtad y sin dolo**.

Control: lineamiento de gestión de activos de información

- La información calificada como **datos abiertos** es evaluada antes de su publicación.
- Se verifica la **clasificación y reserva** antes de autorizar el acceso a información pública.

## 2.3 Principios de seguridad para la interoperabilidad

Como lo establece el manual del marco de interoperabilidad de MINTIC, la interoperabilidad busca facilitar el acceso a los grupos de valor de los servicios ciudadanos digitales de las entidades del Estado de manera completa, adecuada, minimizando los pasos y evitando el desplazamiento del ciudadano a diversas entidades para obtener la información necesaria de una entidad y acceder así a sus derechos y obligaciones con el Estado, pero este valor agregado obliga a la implementación de servicios y controles de seguridad que garanticen al ciudadano que la información que consulta o los servicios que demanda protegen sus derechos fundamentales, contemplan principios y controles de seguridad y privacidad, y sobre todo, son confiables.

### 2.3.1 Seguridad, protección y preservación de la Información

Deberán aplicarse medidas y controle que aseguren, protejan, preserven y mantengan la privacidad de la información susceptible de interoperar generando un entorno seguro y de confianza que permita transmitir a los ciudadanos una sensación de seguridad, donde se vela por sus intereses y se cuida la privacidad de la información y se respeta plenamente la normativa aplicable cada vez que interactúan con el Estado.

Aquellos datos que pertenezcan a ciudadanos y cuya pérdida y/o alteración pueda significar algún tipo de inconveniente para ellos con el Estado, deberán ser especialmente protegidos evitando el uso no autorizado y garantizando su integridad, disponibilidad y resguardo. Los ciudadanos y empresas tendrán el derecho a conocer, actualizar y rectificar la información que hayan recogido las entidades, así como demás derechos, libertades o garantías relacionadas con la recolección, tratamiento y circulación de datos personales. En términos de preservación de la información para las consultas históricas de los servicios de intercambio de información, las entidades deberán considerar el almacenamiento de históricos de los datos y ofrecer servicios interoperables para que se pueda acceder a la información compartida o intercambiada durante un período de tiempo determinado.

Las entidades deben aplicar controles de seguridad para proteger la información en procesos de **intercambio de datos con el Estado**, asegurando:

- **Privacidad y confidencialidad** de los datos transmitidos.
- **Integridad y disponibilidad** de la información.
- **Resguardo y trazabilidad** de los datos intercambiados.

Control: Lineamientos de Seguridad para Intercambio de Información

- Se adoptan los **"Lineamientos de seguridad para la transferencia o transmisión de datos personales"**, disponibles en el **Sistema Integrado de Planeación y Gestión** de la entidad.

### 2.3.2 Neutralidad tecnológica y adaptabilidad

El desarrollo de servicios de intercambio de información se deberá orientar en la atención de las necesidades manifiestas de los ciudadanos y empresas; por lo tanto, la construcción de estos servicios deberá orientarse por la funcionalidad y no por la tecnología que ofrezca una herramienta o proveedor en particular. Las decisiones de tecnología, durante el desarrollo de un servicio de intercambio de información, deberán guiarse por el uso de especificaciones que faciliten su interconexión con el mayor número de sistemas que conforman el ecosistema de soluciones con el que interoperan. Los servicios de intercambio de información no deberán exigir, por parte de las entidades, ninguna tecnología exclusiva o limitada al ámbito de un proveedor o plataforma, así mismo, las entidades públicas deben dar acceso a sus servicios de intercambio de información con independencia de cualquier tecnología o producto concreto y permitir su reutilización.

Control: lineamientos de seguridad para intercambio de información

- Con el fin de adoptar lineamientos que se deben aplicar al momento de realizar intercambios de información con otras entidades con el fin de habilitar el cumplimiento de obligaciones misionales y, facilitar la prestación de servicios o mejorar la entrega de valor, la entidad adopta el documento de "Lineamientos de seguridad para el intercambio, transferencia o transmisión de datos personales". Disponible en el sistema integrado de planeación y gestión de la entidad.

# 3. Bibliografía

# 3. Bibliografía

Beach, B. (2009). *The DAMA Guide to The Data Management Body of Knowledge*. DAMA International.

Departamento Administrativo de la Función Pública. (2021). *Manual de Gobierno de Datos*. https://www.funcionpublica.gov.co/documents/34645357/0/2021-12-15_Manual_gobierno_datos_v1.pdf

Departamento Administrativo de la Función Pública. (2021). *Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG) - Versión 4*. https://www.funcionpublica.gov.co/documents/28587410/38054865/Manual+Operativo+del+Modelo+Integrado+de+Planeaci%C3%B3n+y+Gesti%C3%B3n+MIPG+-+Versi%C3%B3n+4+-+Marzo+2021.pdf

Departamento Nacional de Planeación. (2018). *Documento CONPES 3920 - Política Nacional para la Explotación de Datos (Big Data) y la Inteligencia Artificial en Colombia*.

IBM. (2024). *Data Governance: Overview & Best Practices*. https://www.ibm.com/es-es/topics/data-governance

International Organization for Standardization. (2005). *ISO 27001:2005 - Information Security Management Systems Requirements*.

International Organization for Standardization. (2018). *ISO 8000 - Data Quality*. http://iso8000.es/normas-iso-8000

Ministerio de Minas y Energía. (2021). *Resolución 40199 de 2021*. https://gestornormativo.creg.gov.co/gestor/entorno/docs/resolucion_minminas_40199_2021.htm

Ministerio de Tecnologías de la Información y las Comunicaciones. (2019). *Guía del Dominio de Información G.IN.01*.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2019). *Guía Técnica de Información - Administración del Dato Maestro G.INF.02*.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2019). *Guía Técnica de Información - Gobierno del Dato G.INF.06*.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). *Política de Gobierno Digital*. https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/

Ministerio de Tecnologías de la Información y las Comunicaciones. (2023). *Guía de Gestión de Riesgos – Gobierno Digital*. https://gobiernodigital.mintic.gov.co/692/articles-150516_G7_Gestion_Riesgos.pdf

Presidencia de la República. (2000). *Directiva Presidencial 02 de 2000*. https://intranet.secretariajuridica.gov.co/node/2233

Presidencia de la República. (2023). *Decreto 2121 de 2023*. https://www.secretariasenado.gov.co/senado/basedoc/decreto_2121_2023.html