MODELO DE GOBERNANZA DE DATOS

Plataforma de Analítica de Datos del Observatorio de Salud

Dirección Territorial de Salud de Caldas

Centro de Bioinformática y Biología Computacional de Colombia – BIOS

Agosto de 2026

www.bios.co
Centro de Bioinformática y Biología Computacional de Colombia - Bios
Manizales - Caldas Colombia
Tel: +57 312 630 7973

Contenido

1. Introducción 3
2. Roles, responsabilidades y gobernanza organizativa 3
2.1 Propietario del dato 3
2.2 Responsable funcional 4
2.3 Responsable técnico o custodio 4
2.4 Usuarios de datos 4
3. Contexto y gestión de las fuentes de datos 4
4. Calidad, esquemas y validación de datos 6
4.1 Dimensiones de calidad 6
4.2 Principios para la gestión de calidad 6
4.3 Responsabilidad sobre la calidad 7
5. Centralización y gestión de activos de datos 7
5.1 Fuentes originales y datos derivados 8
6. Linaje de datos y procedencia 8
6.1 Información mínima de procedencia 8
7. Gobernanza de metadatos y documentación 8
7.2 Diccionario de datos 8
8. Seguridad, privacidad y cumplimiento 8
8.2 Acceso 9

www.bios.co
Centro de Bioinformática y Biología Computacional de Colombia - Bios
Manizales - Caldas Colombia
Tel: +57 312 630 7973

1. Introducción

En el contexto de la gestión institucional de información, los datos constituyen un activo fundamental para el desarrollo de las funciones del Observatorio, la generación de conocimiento y el apoyo a la toma de decisiones. En consecuencia, su adecuada administración requiere establecer criterios comunes que permitan asegurar que la información sea confiable, comprensible, trazable, protegida y utilizada de acuerdo con las finalidades autorizadas.

El presente Modelo de Gobernanza de Datos establece el marco mediante el cual se definen los principios, responsabilidades, autoridades y mecanismos de decisión asociados con la gestión de los datos del Observatorio.

La gobernanza de datos no se limita a la administración tecnológica de las fuentes de información. Comprende la definición de responsabilidades sobre los datos, los criterios para determinar su calidad, clasificación y uso, las condiciones para su acceso y compartición, la gestión de sus metadatos y trazabilidad, así como los mecanismos para supervisar su adecuado tratamiento durante todo su ciclo de vida.

El modelo tiene como finalidad proporcionar un marco común para la toma de decisiones relacionadas con los datos, promoviendo una gestión coordinada entre las áreas responsables de la información, los equipos técnicos y las demás partes que intervengan en su utilización.

El alcance del modelo comprende el ciclo de vida de los datos, desde su identificación, generación o recepción, hasta su utilización, transformación, publicación, conservación y disposición, de acuerdo con las condiciones establecidas para cada fuente.

El presente modelo deberá aplicarse de manera articulada con las políticas institucionales, instrumentos jurídicos, lineamientos de seguridad de la información y demás disposiciones que resulten aplicables.

2. Roles, responsabilidades y gobernanza organizativa

La gobernanza efectiva de los datos requiere establecer de manera explícita quién tiene autoridad para tomar decisiones sobre la información, quién es responsable de su gestión funcional y quién proporciona los medios tecnológicos necesarios para su administración.

Los roles definidos en este modelo deberán entenderse como responsabilidades de gobierno y gestión, independientemente de la estructura organizacional específica de la entidad. Una misma persona podrá desempeñar más de un rol cuando las características de la organización lo permitan, siempre que se mantenga una adecuada separación de responsabilidades y no se comprometa la independencia de las decisiones.

2.1 Propietario del dato

El propietario del dato es el área o responsable institucional que tiene autoridad funcional sobre una fuente o conjunto de datos.

Sus responsabilidades comprenden:

www.bios.co Centro de Bioinformática y Biología Computacional de Colombia - Bios Manizales - Caldas Colombia
Tel: +57 312 630 7973

- Autorizar o validar las condiciones de acceso.
- Establecer restricciones de uso.
- Validar modificaciones que puedan afectar el significado de la información.
- Validar la clasificación de la información.
- Determinar las condiciones bajo las cuales la información puede compartirse o publicarse.

2.2 Responsable funcional

Es la persona que posee conocimiento sobre el significado, contexto y utilización de los datos.

Sus responsabilidades comprenden:

- Definir y validar el significado de las variables.
- Resolver dudas relacionadas con la interpretación de la información.
- Participar en la definición de reglas de calidad.
- Validar inconsistencias que tengan impacto funcional.
- Apoyar la identificación de cambios en las fuentes.

2.3 Responsable técnico o custodio

Es el responsable de proporcionar y mantener los mecanismos tecnológicos necesarios para la administración de los datos.

Sus responsabilidades comprenden:

- Administrar los repositorios y mecanismos tecnológicos.
- Mantener los mecanismos de disponibilidad y respaldo.
- Facilitar la trazabilidad técnica.
- Mantener los registros técnicos definidos.

2.4 Usuarios de datos

Los usuarios podrán consultar, analizar o utilizar información de acuerdo con las autorizaciones correspondientes.

Todo usuario será responsable de utilizar los datos exclusivamente para las finalidades autorizadas y de cumplir las condiciones de seguridad, confidencialidad y uso establecidas.

3. Contexto y gestión de las fuentes de datos

La gobernanza de datos requiere que cada fuente de información pueda ser comprendida dentro de su contexto de origen, finalidad y utilización.

Antes de incorporar una fuente al ecosistema de información del Observatorio, deberá identificarse la información necesaria para establecer su procedencia, propósito, características y condiciones de uso.

Who — ¿Quién?

Identificación de la entidad, área o sistema responsable de generar o suministrar la información.

Deberá identificarse, cuando corresponda:

- Entidad de origen.
- Área responsable.
- Propietario del dato.

What — ¿Qué?

Identificación de la naturaleza y características de la información.

Se deberá establecer, entre otros aspectos:

- Tipo de información.
- Estructura.
- Principales variables.
- Unidad de análisis.
- Periodo cubierto.
- Existencia de datos personales o sensibles.

Where — ¿Dónde?

Identificación del origen y ubicación de la información.

Deberá conocerse, cuando corresponda:

- Sistema de origen.
- Repositorio.
- Fuente primaria.

When — ¿Cuándo?

Identificación de la temporalidad de la información.

Se deberá establecer:

- Fecha de generación.
- Fecha de recepción.
- Periodo de referencia.
- Frecuencia de actualización.

Why — ¿Por qué?

Identificación de la finalidad que justifica la utilización de la información. Este criterio permitirá evitar el uso o recopilación de información que no sea necesaria para los objetivos acordados.

How — ¿Cómo?

Identificación de la forma en que se genera, recibe, transforma o entrega la información.

Se documentará, cuando corresponda: Procesos de transformación relevantes y dependencias conocidas.

Result — ¿Cuál es el resultado?

Identificación de los productos de información que se generan a partir de la fuente.

La caracterización de las fuentes deberá permitir establecer una base común para las posteriores decisiones de clasificación, calidad, acceso, trazabilidad y uso.

4. Calidad, esquemas y validación de datos

La calidad de los datos constituye un componente fundamental de la gobernanza, dado que las decisiones institucionales y los productos derivados dependen de la confiabilidad de la información utilizada.

El modelo establece que la calidad debe ser gestionada desde la fuente y durante las diferentes etapas del ciclo de vida de los datos.

La gobernanza deberá definir los criterios bajo los cuales una fuente se considera adecuada para una determinada finalidad, así como los responsables de evaluar y aceptar su calidad.

4.1 Dimensiones de calidad

Como mínimo, se considerarán las siguientes dimensiones:

- **Completitud:** grado en que se dispone de la información requerida.
- **Validez:** cumplimiento de los formatos, dominios y reglas establecidos.
- **Consistencia:** ausencia de contradicciones entre registros o fuentes relacionadas.
- **Unicidad:** ausencia de duplicidades no justificadas.
- **Exactitud:** correspondencia con la fuente oficial o realidad de referencia, cuando pueda verificarse.
- **Oportunidad:** disponibilidad dentro del periodo establecido.
- **Integridad:** conservación de las relaciones y características necesarias.
- **Trazabilidad:** capacidad de identificar el origen y las transformaciones aplicadas.

4.2 Principios para la gestión de calidad

Las decisiones de calidad deberán distinguir entre:

- Datos inválidos.
- Datos incompletos.

- Datos inconsistentes.
- Valores atípicos.
- Errores de registro.
- Cambios legítimos en el comportamiento de la información.

Un valor atípico no deberá considerarse automáticamente un error. Antes de excluir o modificar un registro deberá determinarse si representa una situación válida dentro del contexto de la fuente.

Las reglas de tratamiento que puedan modificar el significado de los datos deberán ser definidas o validadas por el responsable funcional correspondiente.

4.3 Responsabilidad sobre la calidad

La responsabilidad sobre la definición del significado y criterios de aceptación de los datos corresponderá al propietario y responsable funcional de la fuente.

Los equipos técnicos serán responsables de implementar los mecanismos necesarios para aplicar y verificar las reglas definidas.

De esta manera, la calidad será una responsabilidad compartida, pero con una clara diferenciación entre:

decisión funcional → implementación técnica → seguimiento y evidencia.

5. Centralización y gestión de activos de datos

La gobernanza deberá promover una visión unificada de los activos de información utilizados por el Observatorio, evitando la existencia de fuentes sin responsable, sin clasificación o sin documentación suficiente.

La centralización deberá entenderse como la capacidad institucional para identificar y controlar los activos de datos, independientemente de que estos se encuentren físicamente distribuidos entre diferentes sistemas o repositorios.

Cada activo deberá contar, como mínimo, con:

- Identificador.
- Nombre.
- Descripción.
- Fuente de origen.
- Finalidad.
- Periodicidad.
- Estado.
- Restricciones.
- Productos asociados.

5.1 Fuentes originales y datos derivados

Deberá diferenciarse entre:

Datos originales: información recibida directamente de la fuente de origen.

Datos derivados: información que ha sido transformada, agregada, integrada, calculada o enriquecida a partir de una o más fuentes.

Esta diferenciación permitirá establecer responsabilidades y garantizar que los productos derivados puedan relacionarse con las fuentes que les dieron origen.

6. Linaje de datos y procedencia

El linaje constituye un elemento esencial de la gobernanza, debido a que permite comprender la relación entre el origen de la información y los productos generados a partir de ella.

6.1 Información mínima de procedencia

El linaje deberá permitir identificar, cuando sea aplicable:

- Fuente de origen.
- Fecha de recepción o generación.
- Transformaciones relevantes.
- Versión de los datos.
- Producto derivado.
- Dependencias existentes.

7. Gobernanza de metadatos y documentación

Los metadatos constituyen un componente esencial para garantizar que los datos puedan ser comprendidos, utilizados y administrados de manera consistente.

Cada fuente deberá contar con un conjunto mínimo de información descriptiva que permita conocer su significado, origen, responsables y condiciones de utilización.

7.2 Diccionario de datos

El diccionario de datos deberá permitir comprender el significado de las variables y establecer criterios comunes para su interpretación.

8. Seguridad, privacidad y cumplimiento

La seguridad y privacidad forman parte de la gobernanza de los datos y deberán incorporarse en las decisiones relacionadas con su acceso, tratamiento, almacenamiento, intercambio y publicación.

La protección de los datos deberá ser proporcional a su nivel de sensibilidad, criticidad y riesgo.

8.2 Acceso

El acceso deberá regirse por los principios de:

- Mínimo privilegio.
- Necesidad de conocer.
- Responsabilidad individual.
- Trazabilidad.