GESTIÓN BÁSICA DE DATOS EN ORGANIZACIONES

GUÍA PRÁCTICA

datagéner

La presente guía práctica tiene como objetivo ofrecer un panorama básico de elementos y buenas prácticas para una gestión responsable de datos en una organización, con énfasis en la **gobernanza**, la **privacidad**, la seguridad y la confidencialidad.

Su propósito es apoyar a organizaciones en la construcción de procesos sencillos y efectivos que protejan a las personas y fortalezcan su misión social.

Equipo

Coordinación General
Mailén García

Redacción de contenidos
Facundo Benítez Piloni

Año: octubre 2025

DataGénero. Observatorio de datos con perspectiva de Género
datagenero.org | info@datagenero.org

CONTENIDOS

1. Introducción a la gestión de datos 4

2. Conceptos básicos de la gestión de datos 4

Datos, información y conocimiento 4

Datos estructurados y no estructurados 6

3. Gobernanza de los datos 7

Principios 7

Pasos iniciales para gestionar datos 7

Roles y responsabilidades 9

4. Ciclo de vida de los datos 9

Recolección 10

Procesamiento 11

Uso y reutilización 11

Almacenamiento 12

Cesión, transferencia o intercambio 13

Eliminación o archivado definitivo 13

1. INTRODUCCIÓN A LA GESTIÓN DE DATOS

En nuestro día a día, manejamos grandes volúmenes de datos e información para el cumplimiento de los deberes y funciones cotidianas de nuestras organizaciones. No obstante, muchas veces, no tomamos los recaudos necesarios para su administración, organización y gestión responsable. Al igual que otros recursos (humanos, físicos, mobiliarios o financieros), **los datos deben ser considerados un activo estratégico más de nuestra organización que requieren atención y protección**. De aquí, la importancia de la **gestión** y el **gobierno de datos**.

El gobierno de los datos se puede definir como el **conjunto de políticas, procedimientos, lineamientos y prácticas que regulan cómo se acceden, manejan y almacenan los datos en una organización**.

En otras palabras, es la práctica o área de conocimiento que se especializa en la gobernanza y gestión de los datos a lo largo de todo su ciclo de vida, desde que lo capturamos en el origen, lo procesamos, usamos y almacenamos.

2. CONCEPTOS BÁSICOS DE LA GESTIÓN DE DATOS

La gestión de datos se entiende mejor si distinguimos algunas nociones fundamentales.

2.1 Datos, información y conocimiento

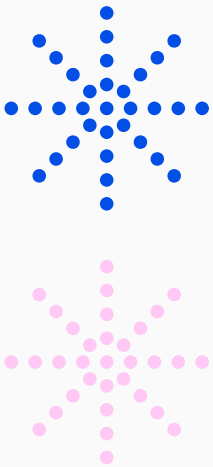
Al gestionar datos, conviene empezar con una distinción central: datos, información y conocimiento. ¿Son sinónimos? ¿Significan lo mismo? ¿A qué nos referimos cuando hablamos de datos?

Datos: En general, los datos son **elementos crudos, sin procesar, símbolos que describen hechos, condiciones, valores o situaciones**. Un dato puede ser una letra, un número o cualquier símbolo que representa una cantidad, una medida, una palabra o una descripción. Los datos son el nivel más básico de la materia prima que se recoge a través de la observación o medición.

EJEMPLO

El número “50” escrito en una hoja no significa nada por sí solo.

Información: La información surge cuando **los datos se organizan y adquieren contexto para ser comprensibles y útiles**. La información se construye a partir del procesamiento, transformación y análisis de los datos que funcionan como materia prima y donde se los dota de relevancia y utilidad.
La información surge cuando los datos se organizan o se procesan. La transformación de datos en información implica añadir contexto, categorización, cálculos, correcciones, o comparaciones.
La información tiene una relevancia aplicada y puede responder a preguntas básicas como: quién, qué, cuándo y dónde.



EJEMPLO

***"50 personas participaron en el taller de alfabetización digital"*, convierte el dato en información útil.**

Conocimiento: Surge cuando la información se interpreta y se usa para tomar decisiones o generar aprendizajes. En otras palabras, refiere al conjunto de información comprensible y útil que se ha integrado con experiencias, reglas, ideas, condiciones y proyecciones. Implica comprensión, contexto y perspectiva. El conocimiento permite a las personas realizar predicciones, tomar decisiones y explicar causas.

EJEMPLO

***"La mayoría de las personas beneficiarias prefieren talleres presenciales en lugar de talleres digitales"* se trata de un conocimiento que orienta la estrategia de la organización.**

2.2 Datos estructurados y no estructurados

Datos estructurados

Los datos estructurados son todos aquellos que se almacenan en formatos tabulares, como hojas de cálculo o bases de datos, donde existen columnas para identificar campos o variables y filas para cada uno de los registros.
Ejemplos: listados de participantes con nombre, edad y teléfono; listado de inscripciones a cursos; registros contables; inventarios de recursos. Estos datos son más fáciles de procesar y analizar, incluso con herramientas básicas como Excel o Google Sheets.

Datos no estructurados

Son aquellos que no siguen un formato fijo y suelen estar en documentos, correos electrónicos, fotografías, audios o videos. Por ejemplo: grabaciones de entrevistas con beneficiarios, fotografías de actividades, informes narrativos. Son valiosos porque capturan contexto, historias y percepciones, pero requieren más cuidado en su almacenamiento y clasificación.

2.3 Datos personales y sensibles

Los **datos personales** son todos aquellos que permiten identificar a una persona, directa o indirectamente, por uno o varios elementos característicos de su identidad física, fisiológica, genética, biométrica, psíquica, económica, cultural, social o de cualquier otro tipo. Ejemplos: nombre completo, correo electrónico, número de teléfono, domicilio, salario, profesión, IP de conexión, entre otros.

Por su parte, los **datos sensibles constituyen una categoría especial de datos personales** y refieren a aquellos que reflejan datos que **permiten conocer aspectos de las personas como su origen étnico, las creencias o convicciones religiosas, filosóficas y morales, su afiliación sindical u opiniones políticas, los datos relativos a la salud, discapacidad, los datos vinculados a la preferencia u orientación sexual y los datos genéticos o biométricos, entre otros.**

IMPORTANTE

En la *Guía Práctica - Tratamiento de Datos Personales y Sensibles* se profundiza con mayor detalle acerca de los principios, lineamientos y buenas prácticas vinculadas al tratamiento de los datos personales por parte de las organizaciones.

3. GOBERNANZA DE LOS DATOS

La **gobernanza de datos** es el conjunto de reglas, procesos y roles que aseguran que los datos en una organización sea gestionada de manera responsable, coherente y segura.
Para una organización de la sociedad civil, la gobernanza no significa tener sistemas complejos o costosos, sino establecer prácticas, lineamientos y procesos claros que garanticen:

- Cumplimiento legal en materia de privacidad y protección de datos.
- Eficiencia interna al saber quién es responsable de cada tarea.
- Protección de las personas más vulnerables.

3.1 Principios

- **Datos como activos:** los programas de gobierno de datos entienden que los datos son activos estratégicos que deben ser cuidados, administrados y gobernados para la organización.

- **Responsabilidad compartida:** todos los miembros de la organización deben cuidar los datos, aunque existan responsables designados.

- **Transparencia:** las comunidades y personas que forman parte de la organización deben saber cómo y para qué se usan sus datos.

- **Proporcionalidad:** sólo recolectar y utilizar los datos que sean necesarios para cumplir los fines de la organización.

- **Seguridad y privacidad:** garantizar que los datos estén protegidos en todo momento.

- **Ética:** nunca usar datos de manera que pueda dañar, discriminar o poner en riesgo a las personas.

3.2 Pasos iniciales para gestionar datos

A continuación, te acercamos una serie de buenas prácticas para empezar un programa básico de gobierno de datos en tu organización:

a) Mapear los datos con los que trabajamos

Mapear y hacer un inventario (catálogo) de los conjuntos de datos que maneja la organización. En este diagnóstico, se recomienda:

- Listar qué datos se recolectan
- Identificar qué tipos o categorías de datos son y cuál es su fuente de origen, es decir, de dónde provienen (formulario de inscripción, registro administrativo interno, etc.).
- Averiguar dónde se guardan (carpetas físicas, hojas de Excel, correos electrónicos, Google Drive, etc.).
- Preguntar quién tiene acceso a cada activo de información.
- Conocer cada cuánto se actualizan los datos.

b) Definir responsabilidades sobre nuestros datos

La definición de roles y responsabilidades claras es importante. Establecer quién decide, quién custodia y quién usa los datos, evitando duplicidades, negligencias o accesos indebidos es un aspecto central en toda estrategia de gestión de datos. En este punto, se sugiere:

- Designar a una persona responsable de datos, aunque sea de manera parcial (ejemplo: coordinador administrativo o de proyectos)
- Establecer reglas claras sobre quién puede ver o modificar cierta información y documentarlas.
- Comunicar esas reglas al equipo.

c) Generar políticas y procesos internos

Avanzar en el diseño e implementación de **políticas, procesos, estándares o protocolos para la gestión de los datos de la organización** es un paso relevante para consolidarnos como organizaciones.
Es importante contar con documentación interna clara y fácil de entender que faciliten la continuidad de los proyectos, el traspaso de responsabilidades y la eficiencia en el uso de la información. Sobre este punto, se aconseja:

- Redactar un documento corto (2–4 páginas) que incluya:
  1. Qué datos se recolectan y por qué.
  2. Cómo se almacenan y durante cuánto tiempo.
  3. Cómo se eliminan o archivan.
- Compartir esta política con el equipo.

d) Aplicar medidas básicas de seguridad de datos
La seguridad digital es un primer escudo contra riesgos y amenazas digitales. Aunque parezca técnico, con simples cambios se puede proteger mejor la información.

- **Cambiar y fortalecer contraseñas** (mínimo 12 caracteres, mezcla de letras, números y símbolos)
- Activar la **autenticación en dos pasos** en cuentas de correo y nubes.
- Realizar **copias de seguridad en un lugar seguro** (ejemplo: disco externo cifrado o nube confiable)
- Evitar usar **dispositivos personales** sin protección para guardar información sensible como así también el uso de servicios de mensajería instantánea.

e) Promover una cultura de datos en la organización
Fomentar una **cultura organizacional basada e impulsada por los datos** a través de diferentes capacitaciones, jornadas, charlas o encuentros de reflexión y sensibilización. Se recomienda:

- Organizar breves talleres internos sobre:
  - Identificación de datos personales y sensibles.
  - Cómo detectar correos fraudulentos (phishing).
  - Cómo guardar y compartir información de forma segura en la organización.

- Enviar las políticas, estándares y consejos para la gestión diaria de datos por parte de los diferentes equipos y personas dentro de la organización.

Estos pasos no requieren grandes recursos ni tecnología compleja, **sino voluntad organizativa y constancia**. Con pequeñas acciones, las organizaciones pueden dar un salto significativo hacia una gestión de datos más responsable y segura.

3.3 Roles y responsabilidades

La gobernanza de los datos requiere definir **quién hace qué dentro de la organización**. Según el tamaño y recursos, una organización puede asignar diferentes roles en distintas personas en materia de gestión de datos.

Responsable de datos

- Coordina las políticas de protección y uso de la información.
- Autoriza accesos a bases de datos.
- Supervisa la aplicación de protocolos en cada etapa del ciclo de vida.

Usuarios autorizados o consumidores de datos

- Miembros del equipo que acceden a la información para actividades específicas.
- Deben seguir las reglas establecidas y proteger la confidencialidad.

Comité de Gestión de Datos

- Evalúa riesgos, actualiza lineamientos y capacita a los equipos.
- Revisa casos de incidentes o incumplimientos.
- Establece políticas y procedimientos para la gestión de datos.

4. CICLO DE VIDA DE LOS DATOS

El ciclo de vida de los datos describe todas las etapas por las que pasa la el dato desde el momento en que se genera o se recolecta hasta que deja de ser necesario y se elimina de forma segura. Comprender este ciclo ayuda a las organizaciones a tener control sobre la información y a garantizar un manejo responsable en cada fase.
En otras palabras, como ciclo de vida del dato entendemos todas las etapas que atraviesa el dato desde su creación o captura hasta su destrucción o archivado definitivo,

pasando por su almacenamiento, uso/reutilización, intercambio y/o publicación.
El ciclo de vida de los datos no es lineal, sino un proceso continuo de revisión y mejora. Una organización responsable debe establecer reglas claras para cada etapa y asegura que todo el personal las conozca.

A continuación, repasemos las buenas prácticas y lineamientos recomendados para la gestión responsable de los dato en cada una de las fases de ciclo de vida.

4.1 Recolección

Refiere al momento en que la organización obtiene, recopila y captura los datos necesarios para el cumplimiento de sus misiones y objetivos institucionales como así también el desarrollo de sus proyectos e iniciativas.

La captura de datos puede hacerse a través de formularios en papel o digitales, entrevistas, formularios de inscripción, registros de asistencia, encuestas en línea, entre otros.

Buenas prácticas para la recolección:

- Recolectar sólo los datos estrictamente necesarios para cumplir los fines del proyecto, iniciativa o misión institucional (principio de minimización).

- Informar claramente a las personas por qué se solicitan los datos, cómo se usarán, durante cuánto tiempo se conservarán y con quién podrían compartirse.
- Obtener consentimiento informado, usando un lenguaje sencillo y accesible.
- Evitar la duplicación de formularios y registros innecesarios.
- En recolecciones digitales, asegurar que las plataformas tengan medidas de seguridad (formularios con cifrado, almacenamiento confiable).
- Toda recolección debe estar respaldada por un **documento interno** que especifique los fines, responsables y duración de conservación.

EJEMPLO

Una organización lleva a cabo un proyecto de alfabetización. Para recolectar datos para brindar un taller, si se requiere contactar a las personas participantes, se justifica pedir nombre y número telefónico, pero no estado civil o DNI, que no son relevantes.

4.2 Procesamiento

Es el momento en que la información se procesan, limpian y preparan los datos antes de ser utilizados para un **f**in específico. Muchas veces, los archivos, bases o registros de datos contienen datos de baja calidad que requieren de la implementación de técnicas de saneo, limpieza y transformación.

Buenas prácticas para el procesamiento:

- Usar formatos homogéneos (ejemplo: todas las fechas en el mismo formato, todos los teléfonos con código de área).
- Depurar datos erróneos, duplicados o incompletos.
- Establecer estándares para asegurar la calidad de los datos (evitar errores que puedan distorsionar informes o diagnósticos)
- Aplicar reglas de calidad de datos desde del diseño.
- Limitar el procesamiento a personal autorizado y, si es posible, realizarlo en dispositivos institucionales, no personales.
- Aplicar anonimización o seudonimización cuando se trate de información sensible.
- Documentar cada procedimiento de procesamiento (qué se hizo, cuándo y quién lo hizo).

EJEMPLO

Ejemplo. Una organización que atiende casos de violencia de género puede procesar sus registros eliminando nombres y reemplazandolos por códigos numéricos antes de analizarlos.

4.3 Uso y reutilización

Refiere al uso, tratamiento y aplicación específica de los datos para cumplir la misión de la organización. Es la etapa en que los datos se aplican a actividades institucionales: informes, seguimiento de beneficiarios, planeación de proyectos o evaluación de impacto. También incluye la reutilización de datos para nuevos propósitos.

Buenas prácticas para el uso y la reutilización:

- Usar los datos únicamente para los fines que fueron informados en la etapa de recolección.
- Controlar accesos: cada usuario debe ver solo lo que necesita.
- Evitar usos secundarios no autorizados, como emplear bases de datos de beneficiarios para fines de recaudación sin consentimiento.
- Aplicar anonimización cuando la identidad no sea relevante (ejemplo: usar porcentajes agregados en informes públicos).
- Toda reutilización debe documentarse y estar alineada con los valores éticos de la organización.
- En caso de querer usar datos con un fin distinto, debe obtenerse un consentimiento adicional.

EJEMPLO

Un informe mensual puede mostrar cuántas personas fueron atendidas por género y edad, pero no incluir nombres ni datos de contacto que permitan identificar personas.

4.4 Almacenamiento

Implica las medidas de guardado y resguardo de los datos de forma organizada y segura, ya sea en archivos físicos (carpetas, cajas) o digitales (bases de datos, nubes) durante el tiempo que sea necesario para la operación o cumplimiento legal.

Buenas prácticas para el almacenamiento:

- Clasificar datos en categorías: públicos, confidenciales, sensibles.
- Establecer medidas de seguridad proporcionales: contraseñas fuertes, cifrado de archivos, candados físicos en gabinetes.
- Hacer copias de seguridad periódicas en entornos seguros.
- Revisar y actualizar los sistemas de almacenamiento con regularidad.
- Definir tiempos de conservación (retención) según criterios legales y organizativos.
- Evitar que datos sensibles se almacenen en dispositivos personales.

- Nombrar un responsable en la organización encargado del almacenamiento y la custodia de la información.

EJEMPLO

En una organización que brinda asistencia a mujeres víctimas de violencia de género, los registros donde se guardan sus datos personales y sensibles o las causas judiciales deben estar protegidos con medidas de seguridad, como por ejemplo, contraseñas fuertes, doble factor de autenticación y control de accesos diferenciado.

4.5 Cesión, transferencia o intercambio

A veces es necesario compartir datos con otros actores tanto internos como externos (terceros) de la organización para una finalidad determinada.

Buenas prácticas:

- Compartir solo la información estrictamente necesaria evitando el envío de información personal o sensible de las personas en caso de no ser necesario.
- Elaborar y firmar acuerdos de confidencialidad para el tratamiento de la información
- Anonimizar información cuando sea posible y verificar que el receptor cumpla con estándares adecuados de seguridad.
- Enviar la información por medios seguros (archivos cifrados, plataformas con control de acceso). Evitar el envío y manipulación de bases de datos por servicios de mensajería instantánea (ej. Whatsapp, Telegram, etc.).
- Registrar cada transferencia: qué datos se compartieron, con quién, por qué y bajo qué condiciones.

EJEMPLO

En una rendición de cuentas se solicita evidencia del impacto: se comparte una base de datos con estadísticas agregadas, pero no se entregan nombres ni contactos de los beneficiarios de un programa de becas.

4.6 Eliminación o archivado definitivo

Refiere a la fase en la que los datos dejan de ser necesarios o cumplen con el tiempo legal de retención, por lo que deben eliminarse de forma segura o conservarse únicamente con fines históricos o legales. Los datos no deben guardarse indefinidamente: cada organización debe definir cuánto tiempo es necesario conservarlos.

Buenas prácticas para eliminación o archivado:

- Establecer políticas claras de retención y eliminación.
- Usar métodos seguros de borrado:
  - Físico: trituración de papel, borrado térmico.
  - Digital: software de eliminación definitiva, no solo “enviar a la papelera”.
- Archivar de manera controlada los datos que tengan valor histórico, con condiciones seguras de custodia.
- Documentar qué se elimina y qué se archiva.
- Evitar conservar información indefinidamente sin propósito definido.
- Comunicar a los beneficiarios, si corresponde, que sus datos han sido eliminados.

EJEMPLO

Una base de datos de participantes de un taller de 2016 que ya no tiene vigencia operativa ni legal debe eliminarse de forma segura para liberar espacio y proteger la privacidad.