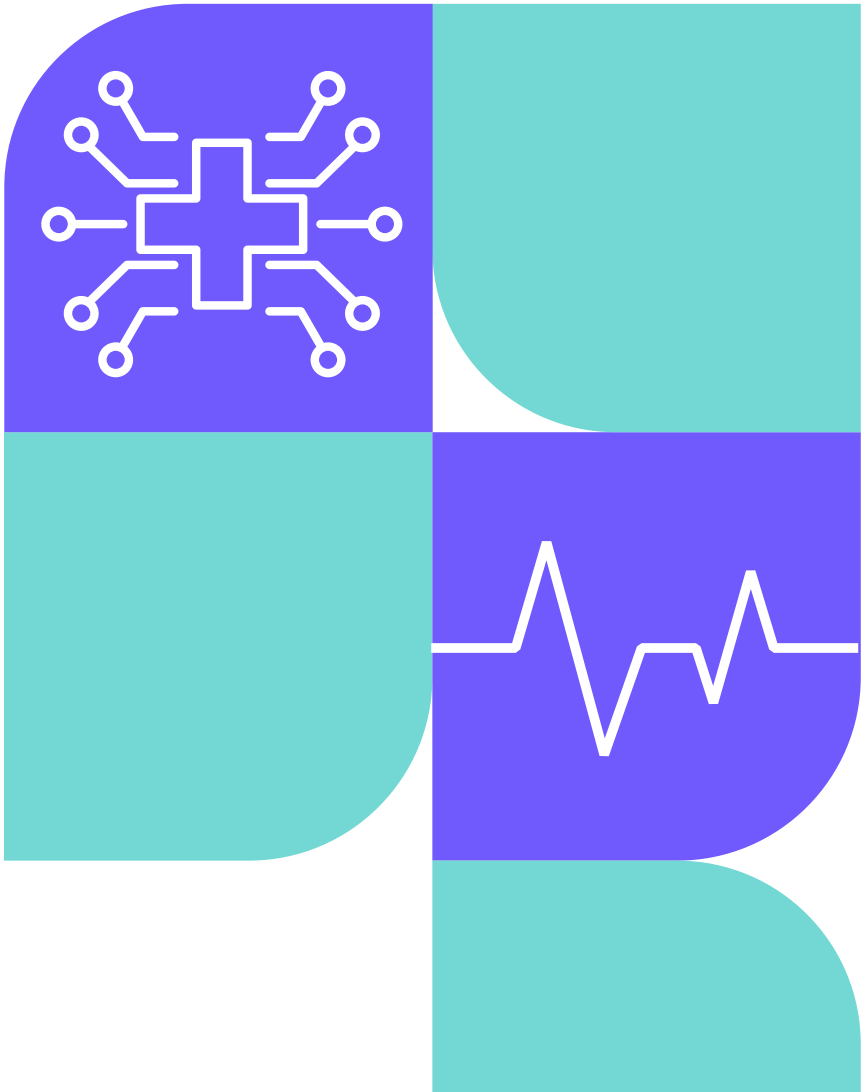
GUÍA DE BUENAS PRÁCTICAS EN GOBERNANZA DE DATOS EN SALUD

Centro Nacional en Sistemas de Información en Salud - Fundación Movimiento Salud



ÍNDICE

Estructura de esta guía

La presente guía es un documento de acompañamiento al **Documento Marco de Gobernanza de Datos en Salud: Definiciones, Recomendaciones y Buenas Prácticas** para su Implementación en Instituciones Prestadoras de Salud. En dicho trabajo encontrará un marco teórico y conceptual detallado, un resumen del marco legal de la gobernanza de datos en salud en Chile y un glosario de conceptos técnicos.
Por su parte, esta guía está dirigida a tomadores de decisiones y encargados de implementación de gobierno de datos en instituciones y organizaciones de salud[1], presentando un conjunto de recomendaciones prácticas y procedimientos a seguir. En este sentido, no busca ser un resumen del documento marco ya citado, sino más bien un complemento. De ahí la denominación de "documento de acompañamiento".
Ambos trabajos son el resultado tanto de una revisión bibliográfica, como de un proceso de discusión y validación que se desarrolló a partir de un taller presencial con representantes de organizaciones de pacientes, servicios de atención primaria, hospitales, clínicas privadas, proveedores de dispositivos médicos, académicos, comunicadores de la ciencia, expertos en análisis de datos y representantes de instituciones públicas de nivel central, tanto autónomas como de gobierno. Sus intervenciones y aportes fueron clave para desarrollar la versión final de esta guía.

Teniendo esto en cuenta, el presente documento se estructura en tres secciones:

¿Qué es una Gobernanza de datos?
En la primera sección se presenta la definición y **el proceso completo de establecimiento de un sistema de gobernanza de datos**, con información necesaria para implementarlo al interior de su institución. El objetivo es dar una visión general de todo el proceso, lo que permitirá más claridad para comprender las siguientes secciones.

¿Qué conceptos debo saber para implementar una Gobernanza de datos?
La segunda sección incluye **un breve glosario**, que resume la terminología técnica que se necesita para comprender la literatura especializada sobre gobernanza, tanto en esta guía como en la documentación de profundización.

¿Cómo implementar una Gobernanza de datos?
La tercera y última sección presenta un **modelo de implementación gradual**, poniendo énfasis en la Gobernanza de datos **como un proceso y no una meta**. Cada institución parte de un "nivel de madurez" determinado, desde el cual proponemos aspirar a un nivel de implementación. La tercera sección, además, cierra con una recomendación de lecturas de profundización que busca ser una herramienta de trabajo, más que una lista de referencias.

[1] Se usarán los términos "organización" e "institución" de manera intercambiable. Sepa que la presente guía es aplicable tanto a instituciones públicas como privadas, en todo nivel del sistema.

1. ¿Qué es una Gobernanza de datos?

La Gobernanza de datos no es un objeto, ni mucho menos un mero protocolo: **es una actividad continua que permite establecer un sistema que contiene un conjunto de normas, procesos y responsabilidades que aseguran que los datos de una organización sean precisos, seguros y bien administrados**. Su objetivo es definir cómo se recopilan, almacenan, usan y protegen los datos, garantizando que cumplan con regulaciones y sean confiables para la toma de decisiones y los usos definidos por la organización. Una vez establecido el sistema, se debe mantener, evaluar y escalar.

Etapa	Preguntas clave	Acciones
Diagnóstico inicial	¿Qué datos tengo en custodia? ¿Cómo están almacenados? ¿Existe algún esquema para ordenarlos?	Levantar información sobre los datos y esquemas de datos
Planificación	¿Cuáles son mis obligaciones de procesamiento de datos? ¿Cuáles son mis objetivos?	Discutir qué objetivos tendrá el sistema
Cuerpos de gobernanza	¿Cuento con los recursos humanos necesarios? ¿Cómo distribuir las responsabilidades en términos de jornada laboral y formación de competencias?	Establecer el Comité de Gobernanza de Datos
Responsabilidades y cuerpos de gobernanza adicionales	¿Qué prestaciones tiene que tener mi sistema para cumplir con la legislación vigente?	Establecer cuerpos de gobernanza adicionales
Procedimientos	¿Qué procedimientos debo estandarizar para cumplir con las prestaciones?	Delinear protocolos y procedimientos por escrito

Tabla 1: Etapas de implementación en formato lineal.

Con el fin de facilitar la comprensión, estas etapas se presentan de manera lineal. Sin embargo, en la práctica algunos procesos ocurren en paralelo, como se puede apreciar en la tabla 2:

Establecimiento de sistema de gobernanza de datos			
Diagnóstico inicial	Planificación	Servicios	Procedimientos
	Conformación primer cuerpo de gobernanza	Establecimiento de cuerpos adicionales de gobernanza	

Tabla 2: Etapas de implementación en formato paralelo

A continuación, se abordan las principales características de las etapas de implementación.

1.1 El diagnóstico inicial

Todas las organizaciones que generan, almacenan, utilizan, comparten, archivan y eliminan datos reciben de la denominación de "Institución Responsable" (Ley 19.628). A todos los procesos que involucran los datos, por su parte, se les llama "Ciclo de Vida del Dato". Toda acción de este ciclo se denomina "tratamiento". El diagnóstico inicial es, entonces, una línea de base sobre la situación del tratamiento de los datos: ¿qué datos tiene su institución? ¿Cómo están almacenados? ¿Se encuentran en pendrives en las oficinas o en discos duros externos? ¿Quizás en alguna aplicación de mensajería instantánea (Whatsapp, Telegram u otra)?

En terminología técnica, el "esquema" de datos se denomina "catálogo de datos" y se refiere a la forma en que son registrados, almacenados y ordenados. Por ejemplo, si usted quiere conocer la cantidad de pacientes con enfermedades infecciosas, puede tener una base de datos que liste el nombre de la patología, pero también puede tener una base de datos con una columna que especifique "tipo" y liste: crónica, infecciosa, trauma, entre otras. En el primer caso, es posible para un profesional imputar el tipo de enfermedad usando el nombre, pero ¿es eficiente? Por su parte, todas las bases que listan patologías, ¿cuentan con una columna de "tipo"? El catálogo de datos busca generar una estructura estandarizada y eficiente para todas las necesidades de su institución.

Para este diagnóstico es importante considerar todas las fuentes de datos de interés. Las más comunes en instituciones prestadoras de salud son:

- Fichas clínicas.
- Datos generados por equipos (dispositivos) médicos de imágenes, sistemas de información de laboratorios, entre otros.
- Datos administrativos (cobranza, presupuestos, entre otras).
- Datos sobre personal médico y no médico que trabaja en la organización.
- "Meta datos", que corresponden a datos sobre los datos mismos, como la hora de registro o la frecuencia de actualización de un dato.

También existen otras fuentes específicas para cada organización.

1.2 La planificación

La fase de planificación busca responder a seis preguntas fundamentales:

1. ¿Qué es lo que **queremos y tenemos** que hacer con los datos que generamos como institución? Estos serán nuestros propósitos.
2. ¿A qué personas (o grupos de personas) tenemos que darle acceso a los datos para cumplir nuestros propósitos?
3. ¿Qué nivel de confianza tenemos en estos grupos de personas a los cuales tenemos que darles acceso a los datos para cumplir nuestros propósitos?
4. ¿Cómo almacenamos los datos según nuestros propósitos, el nivel de acceso que tenemos que dar y el nivel de confianza que tenemos en el acceso que se hará de los datos?
5. ¿Qué riesgo representan nuestros datos para las personas o grupos sobre los cuales esos datos fueron generados?
6. ¿Qué riesgo representa el análisis de nuestros datos para las personas o grupos sobre los cuales esos datos fueron generados?

Esta discusión se debe generar entre tomadores de decisiones al interior de su institución, con representación de profesionales involucrados en la generación de datos (ver punto 1.1).

Para evitar generar una confusión sobre la relación existente entre “objetivos” y “obligaciones”, para efectos del sistema definiremos que son lo mismo. La ley obliga a las instituciones de salud a cumplir una serie de requisitos de reporte de datos, pero también su institución puede plantearse objetivos de acuerdo a su funcionamiento. Dichos objetivos pueden requerir (o no) una habilitación legal. Ahora bien, sin importar si son de carácter obligatorio o voluntario, en la fase de planificación se deben fijar con claridad.

Respecto de las preguntas (2) y (3), recuerde no sólo pensar en otras instituciones, sino también en usuarios, investigadores, colaboradores de negocio u otros; fundamentalmente, toda persona natural o jurídica a la cual usted comparta datos. Cuando hablamos de **confianza** no nos referimos a una propiedad interpersonal, sino más bien a una evaluación del nivel de riesgo. ¿Es su colaborador una entidad nacional o internacional? ¿Conoce sus prácticas de seguridad? ¿Existe un contrato que regule el tratamiento de los datos que la contraparte hará una vez los reciba?

La pregunta número (4) versa específicamente sobre la arquitectura de datos (ver punto 1.1). Mientras que las preguntas (5) y (6) guardan relación específicamente con consideraciones de seguridad y control estadístico de los datos. Para estas preguntas se recomienda contar con la participación, ya sea permanente o en calidad de consultor, de un profesional de arquitectura de datos y ciberseguridad.

1.3 Cuerpos de gobernanza

Como explica DAMA-International, "la gobernanza de datos se enfoca en cómo las decisiones se toman con relación a los datos y en cómo se espera que las personas y los procesos se comporten, en relación con los mismos" (Henderson et al., 2017; p. 67-68). La toma de decisiones estratégicas se genera al interior de un "cuerpo de gobernanza". **Este es un grupo de personas que tiene un conjunto de responsabilidades**. Su nombramiento es de vital importancia para establecer, por una parte, la cadena de responsabilidades y, por otra, los procesos de respuesta ante un incidente de vulneración de datos, auditoría, entre otros.

La cantidad exacta y los nombres específicos de cuerpos de gobernanza son una recomendación de la Data Management Association (DAMA), sin embargo no buscan ser taxativos.

El primer cuerpo de gobernanza a conformar es el **Comité de Gobernanza de Datos (Comité GD)**, el cual estará integrado por actores que cumplan tres criterios:

- Actores con capacidad de decisión al interior de la organización.
- Actores con control sobre el presupuesto al interior de la organización.
- Actores con conocimiento del estado de la producción y arquitectura de datos de la organización (ver punto 1.1).

Estos requisitos no son individuales, sino grupales, es decir, la suma de individuos seleccionados debe cumplir estos tres criterios. Otras consideraciones quedan a discreción de cada institución. El Comité GD se encarga de destinar recursos, tanto monetarios como humanos a la construcción del sistema; no supervisa el funcionamiento cotidiano del sistema, pero sí debe convenir para generar cambios importantes a nivel de políticas de gobernanza de datos al interior de la institución.

Una vez establecido el Comité de GD se conformarán los **cuerpos de gobernanza adicionales**, cuyos números y especificidad se determinan por en el siguiente punto, (1.4).

1.4 Responsabilidades y cuerpos de gobernanza adicionales

Responsabilidades
La Ley 19.623 —modificada por la Ley 21.719— de Protección de Datos Personales entrará en vigencia en diciembre de 2026 y establecerá una serie de derechos para los titulares de los datos, así como obligaciones para todas las instituciones que sean responsables del tratamiento de datos. Para el sector salud esto es especialmente importante, puesto que reciben la denominación de datos sensibles, teniendo una atención especial en la legislación.

Las **responsabilidades** son aquellos aspectos que la institución responsable debe cumplir en cuanto al tratamiento de datos se refiere.

Por su parte, los servicios son las prestaciones que el sistema ofrecerá a sus usuarios. Los servicios están naturalmente vinculados con las responsabilidades, pero no necesariamente terminan en éstas. Las responsabilidades básicas y específicas a la Gobernanza de datos son:

Responsabilidad	Definición
Comunicarse con titulares y otras organizaciones	Responder a las solicitudes de las personas naturales, individuales, que son titulares de los datos, así como a solicitudes de otras organizaciones. Desde diciembre de 2026 los titulares tendrán derecho a: 1. solicitar sus datos, 2. solicitar rectificaciones, 3. suspensión del tratamiento (con limitaciones), y 4. portabilidad.
Mantener la seguridad de los datos	1. Mantener el secreto mediante pseudo anonimización y anonimización, 2. mantener la integridad de los datos, 3. garantizar que se encuentren disponibles, y 4. que los sistemas tengan resiliencia a interrupciones de servicio.
Generar documentación	1. Mantener catálogo de documentación tanto sobre el sistema de gobernanza (de cara al usuario) como sobre los protocolos y procedimientos (de cara a los miembros de la organización).
Vigilar y reportar vulneraciones	1. Detectar fallas en la seguridad, 2. analizar el daño, y 3. reportar el incidente para la toma de medidas. El reporte tanto de fallas como de intentos de acceso (frustrados) será obligatorio a contar de diciembre de 2026.
Tratar los datos	1. Procesamiento mismo de los datos, las labores de seudo anonimización, anonimización, análisis estadístico, cruces, entre otros.

Tabla 3: Resumen de principales responsabilidades de un sistema de Gobernanza de datos

Para una revisión más detallada sobre seguridad en la gestión de datos, sugerimos consultar la "Guía Introductoria de Buenas Prácticas de Privacidad y Seguridad de Datos en Salud" desarrollada por CENS (ver al final, en Lecturas de Profundización Recomendadas).
Naturalmente existirán otras tareas específicas a su institución. Lo fundamental en esta etapa es tener claridad sobre todas las responsabilidades del sistema.

Cuerpos de gobernanza adicionales

En este punto, se deben establecer **cuerpos de gobernanza adicionales**. Como adelantamos, es complejo comprender esto como un proceso lineal, pero en términos generales **estos van aparejados a un conjunto de responsabilidades**. De esta forma, la cantidad y especificidad de cada cuerpo de gobernanza adicional guardará relación con la cantidad y complejidad de las responsabilidades, encargándose de:

1. Supervisar que se cumpla la responsabilidad,
2. Tomar decisiones sobre qué hacer cuando no se está cumpliendo una responsabilidad, y
3. Actuar en caso de un incidente, tomando medidas de mitigación, reparación o recuperación.

Ya mencionamos que los nombres y tipos de cuerpos de gobernanza son recomendación de DAMA International, pero no son taxativos. A continuación, se describen los cuerpos de gobernanza más comunes:

1. **Consejo de GD:** es el cuerpo de gobernanza que supervisa el funcionamiento cotidiano del sistema, administra la implementación de las políticas, se encarga de escalar problemas según sea necesario y desarrolla métricas de medición de logros del sistema.

   Recomendación: conformarlo con agentes con capacidad de decisión al interior de la organización.

2. **Oficina de GD:** coordina la relación entre titular y responsable de los datos, estableciendo políticas de comunicación y atención de solicitudes. Una buena y pronta comunicación es la diferencia entre un manejo exitoso de crisis y un escándalo e infracción a la ley de Protección de DatosPersonales.

   Recomendación: conformarlo con al menos un representante del Consejo GD con capacidad de decisión, en conjunto con profesionales que tengan contacto con usuarios, investigadores y todo agente externo a la organización.

3. **Equipos responsables o "albaceas" de datos:** del inglés "steward", se define como una persona que administra algo (los datos) en nombre de alguien más (el titular). Su rol es supervisar que el tratamiento se haga bajo altos estándares de calidad, tal como lo establece la norma ISO/IEC 25012, así como de la protección efectiva de los derechos de los titulares.

   Recomendación: componerlo, según sea el caso, de representantes de los intereses de los titulares y analistas de datos. Este es el cuerpo de gobernanza con mayor presencia de especialistas en el tratamiento efectivo de datos.

4. **Servicios de Tecnologías de la Información**: también abreviado como "servicios TI", se refiere a la división que administra los recursos de soporte físico (hardware), así como el despliegue de soluciones de software al interior de la organización.

5. **Servicio de Administración de Datos:** compuesto por expertos en la administración de los datos, se encarga de la construcción, operación y mantención de las bases de datos, así como de la auditoría de procesos de seguridad y control estadístico. También se encarga de garantizar el acceso y seguridad de las bases de datos. El servicio de administración, no obstante, no realiza el procesamiento mismo de los datos, sino su preparación, ordenamiento y sistematización para el procesamiento.

Un error común en la conformación de los cuerpos de gobernanza es depositar las responsabilidades en el personal encargado de tecnologías de la información, dada su vinculación con las tecnologías de seguridad informática. Otra confusión surge de mezclar los roles del Servicio de Tecnologías de la Información con el Servicio de Administración de Datos. Si bien la escasez de recursos es un desafío de instituciones y organizaciones, recomendamos evitar esta mezcla de funciones. La implementación puede ser gradual y de acuerdo a las necesidades de su organización. No es "obligatorio" contar con cinco cuerpos de gobernanza, pero sí es necesario que las responsabilidades del sistema sean abordadas por el cuerpo de gobernanza adecuado. A medida que aumentan las responsabilidades, recomendamos escalar los cuerpos de gobernanza de su institución.

1.5 Procedimientos

Por último, tenemos los procedimientos. En este caso se entienden como la relación que tendrán entre sí los cuerpos de gobernanza en el cumplimiento de sus responsabilidades, así como los protocolos a tomar de acuerdo a una ocurrencia. En términos simples, los procedimientos responden a dos preguntas: ¿quién hace X? y ¿qué hacer en caso de Y?
La lista de procedimientos tiene relación con la cantidad de servicios y cuerpos de gobernanza de su institución. Puede ser muy simple o muy compleja. A continuación, se presenta una lista de recomendaciones —basada en un sistema básico— que cumple con las responsabilidades y servicios fundamentales.

Responsabilidad	Procedimientos básicos de GD
Comunicarse con los titulares	Protocolo de comunicaciones que debe cubrir el reporte a la Agencia de Protección de Datos[2] y a los titulares.
Mantener la seguridad de los datos	Protocolos de seguridad tanto a nivel de administración de datos como de usuarios.
Generar documentación	Protocolo de documentación. DAMA International recomienda al menos un glosario de términos GD y un repositorio online de documentación para todos los miembros de su organización.
Vigilancia y Reporte de Vulneración	Procedimiento de reporte de incidentes y una estructura que defina claramente a quién se reporta y cómo escalan los incidentes. Los incidentes menores pueden ser manejados por el equipo de seguridad, mientras los incidentes mayores deben ser escalados a instancias de toma de decisiones.
Tratamiento de los datos	Protocolos de tratamiento que definan: ¿qué tratamientos están permitidos? ¿Qué tratamientos se hacen al interior y cuáles se deben externalizar?

Tabla 4: Resumen de procedimientos básicos de un sistema de Gobernanza de datos

[2] Se usarán los términos “organización” e “institución” de manera intercambiable. Sepa que la presente guía es aplicable tanto a instituciones públicas como privadas, en todo nivel del sistema.

2. ¿Qué conceptos debe conocer para implementar una Gobernanza de datos en salud?

A continuación, detallamos los conceptos básicos de Gobernanza de datos.

Agregación de datos: se refiere a un método simple de anonimización en donde se agrupan casos individuales bajo categorías más grandes, eliminando las fuentes individuales de datos. La agregación sólo cuenta como anonimización si no permite la reidentificación. De lo contrario, es una técnica de pseudo anonimización.

Anonimización: se refiere al procedimiento por el cual se eliminan todos los datos de una base que permitan la identificación o reidentificación de un sujeto dentro de un conjunto de datos, incluso haciendo uso de datos externos a la misma base. La técnica de anonimización más común es la "agregación de datos", pero existen otras.

Calidad del dato: de acuerdo a lo establecido en la ISO 25012, se define como el grado en que los datos satisfacen los requisitos definidos por la organización a la que pertenece el producto. En términos operativos se caracteriza por el cumplimiento de un conjunto de propiedades de los datos.

a. **El dato es "completo":** cuando representa la realidad de la que busca dar cuenta; en otras palabras, efectivamente recogemos las variables que nos permiten entender lo que buscamos entender con los datos. Por ejemplo, ¿podemos realmente saber el estado de los tiempos de espera con una base de datos que no considere tiempo desde reserva de hora hasta momento de atención? La completitud muchas veces es un ideal que no se logra, pero se busca conseguirlo en un grado razonable.
b. **El dato es "único":** cuando la base no tiene datos redundantes que refieran a la misma cosa.
c. **El dato es "válido":** cuando se encuentran estandarizados (registrados de una manera acordada previamente) y siguen una estructura que se ajusta a las necesidades de la organización u institución. Esto se refiere al formateo de los datos y es uno de los criterios más ignorados en la gestión de los mismos. El concepto también considera "metadatos" (los datos del dato), como por ejemplo, la hora de registro, la cantidad de cambios y actualizaciones, el tiempo desde la última actualización, entre otros. El marco de gestión de datos de Transformación Digital llama a esto "catálogo de datos" y es un punto de evaluación importante a la hora de implementar un sistema de gobernanza.
d. **El dato es "preciso":** cuando el dato es fiel a su fuente, es decir, es preciso en lo que busca reportar. Cuando un mismo dato es reportado por distintas fuentes, se debe escoger un "estándar de verdad" o de fidelidad para evaluar este criterio.
e. **El dato es "consistente":** cuando al ser contrastado con distintas fuentes o con otros datos, mantiene su lógica. Esto es similar a la precisión y se refiere a que, por ejemplo, un dato no es consistente si indica que hay más personas con una determinada patología que el total de personas realmente atendidas en un servicio.
f. **El dato es "actualizado":** esto en referencia a un marco temporal específico. Algunos datos se requieren en tiempo real, otros pueden tener una temporalidad más larga. Lo importante es tener claro el marco temporal necesario y pertinente para evaluar este criterio.

Control administrativo: se refiere a la cadena de responsabilidades a lo largo del ciclo de vida de los datos en una institución u organización. El control administrativo se compone de cuerpos de gobernanza y cumple responsabilidades.

Control estadístico: se refiere al conjunto de técnicas para la administración correcta de los datos, desde los insumos tecnológicos, las técnicas de catalogación de datos y el aseguramiento de la calidad de los mismos, hasta las medidas de seguridad tomadas para protegerlos. El control estadístico también guarda relación con la protección contra procesos de reidentificación (ver entrada "procesos de reidentificación").

Datos sensibles: categoría especial de datos definida en la ley 19.628. Se trata de aquellos datos que representan un mayor riesgo para la privacidad o la honra de las personas. Los datos de salud son de tipo sensible y tienen ciertas particularidades en la ley.

Gobernanza de datos: sistema de planificación, control administrativo y control estadístico de datos sensibles o "Información de Salud Protegida", ejecutada por una institución responsable, que permite mantener altos estándares de privacidad para los titulares, mientras que asegura utilidad para el seguimiento individual, epidemiológico, la administración hospitalaria, la toma de decisiones en materia de salud pública, la investigación u cualquier otro propósito establecido tanto en la legislación, como por la Institución Responsable en cuestión.

Institución mandante: aquella a la cual se encarga el tratamiento de datos, bajo un contrato de servicios. Las responsabilidades de la institución mandante se traspasan desde la institución responsable, siendo ambas corresponsables. La institución mandante no puede hacer ningún otro uso de los datos más que los permitidos por la institución responsable.

Institución responsable: aquella que se dedica al tratamiento de datos y es custodia responsable de la seguridad, privacidad y calidad de los datos.

Principio de privacidad: se refiere al derecho que las personas tienen a la privacidad y la honra. También a la realidad que la producción de datos sobre las personas puede representar un peligro para su privacidad o su honra. Por ejemplo, un diagnóstico podría impedir de manera arbitraria que una persona obtenga un trabajo, si este es conocido por un potencial empleador.

Principio de utilidad: se refiere al uso que se puede dar a los datos en distintas materias. La utilidad puede ser para generar decisiones de política pública basadas en la evidencia o para avanzar la investigación científica, así como tomar decisiones de negocios, pero también pueden existir utilidades no deseadas como la estafa o la discriminación.

Procesos de reidentificación: se refiere a procedimientos que se pueden hacer usando datos de una base, en conjunto con datos externos para volver a identificar a un individuo dentro de una base. Los procesos de reidentificación más comunes son:

a. **Individualizar (singling out):** es cuando un dato permite identificar a un sujeto, por ejemplo, si en una base de datos de altura existe sólo una persona que mide 3 metros, evidentemente será muy fácil saber quién es. Esto vuelve ciertos conjuntos de datos imposibles de anonimizar, especialmente cuando son conjuntos muy pequeños y con campos muy dispares. Otro ejemplo, si tenemos una base de datos con 20 casos que contempla registros de edad, y cada persona tiene una edad distinta, será muy fácil de reidentificar a todas las personas, aunque hayamos realizado procesos de pseudo anonimización a la base. Por eso hay que preguntarse: ¿es posible anonimizar realmente esta base de datos?

b. **Conexión (linkability):** refiere a la información en un conjunto de datos que puede ser conectada con otra base para reidentificar personas. Por ejemplo: usando datos extraídos de LinkedIn que permitan conocer nombre y lugar de trabajo de una persona, cruzados con una base de datos de gestión de personas de una empresa que hayan sido pasados por procesos de pseudo anonimización. Otro ejemplo, quizás menos intuitivo, es el uso de llaves de descifrado. El cifrado de datos es una forma de pseudo anonimización, porque la llave para abrir el cifrado es un "dato externo a la base" que permite reidentificar a una persona.

c. **Inferencia (inference):** es cuando se puede inferir una conexión entre dos campos en un mismo conjunto de datos para reidentificar a una persona, por ejemplo, conectar salario y antigüedad en una base de datos de empleados.

Existen otros procesos de reidentificación y estos varían según el tipo de datos con los que se esté trabajando.

Pseudo anonimización: procedimientos por los cuales se eliminan de una base de datos los elementos que permiten identificar a un sujeto dentro de la misma, como el RUT, el nombre completo, o la dirección, sin hacer uso de datos externos a la misma base. Se le denomina pseudo, puesto que es posible reidentificar a un sujeto usando datos externos. Es común confundir a la pseudo anonimización con la anonimización. Para más detalles, ver "procesos de reidentificación".

Titular: aquella persona que es dueña de los datos. Es quien da el consentimiento para que los datos se levanten en primer lugar y es el sujeto de derecho sobre los mismos. La ley no faculta a instituciones (personas jurídicas o no naturales) a ser titulares.

Tratamiento de datos: se refiere a todas las operaciones que se pueden hacer con los datos, tanto automáticas como manuales, realizadas por una analista o una máquina. Esto incluye el uso de modelos de inteligencia artificial, el análisis manual y el análisis que terceros hagan con la información.

3. ¿Cómo implementar una Gobernanza de datos?

El modelo de implementación gradual.

Es importante **recordar que la gobernanza es un proceso y no una meta**. Su evaluación no se da tanto por "objetivos cumplidos" sino por "grado de madurez". Este concepto de madurez está definido como el grado de preparación que tiene una institución para desarrollar una tarea, en este caso: gobernar sus datos. Se determina por una serie de aspectos tanto internos como externos, algunos bajo el control de las organizaciones y otros fuera de él.

En el proceso de discusión que llevó a la estructura final de esta guía, se puso énfasis en que la aplicabilidad de la misma está basada en comprender que las instituciones tendrán distintos contextos y distintas capacidades: ¿cómo hablamos de implementar un cuerpo de gobernanza para responder a problemas de seguridad cuando no contamos con equipos conectados a internet y en buen estado? Teniendo en cuenta esta premisa, proponemos un modelo de gradualidad que se basa en una revisión simple del grado de madurez de su institución u organización.

La tabla de la siguiente página no busca ser una herramienta de diagnóstico de su institución, ni menos una medición de su nivel de madurez. Más bien, busca entregar una orientación sobre las preguntas y pasos a seguir que debe considerar para avanzar el proceso gradual de la implementación de su Gobernanza de datos.

Etapa	Preguntas clave	Acciones
Bajo: No hay condiciones tecnológicas adecuadas de ningún tipo. No se cuenta con personal capacitado contratado al menos a media jornada. Los datos están almacenados de forma poco segura.	¿Qué datos produzco? ¿Cómo se encuentran almacenados estos datos? ¿Tengo algún esquema para ordenar mis datos?	• Resolver problemas más graves en el almacenamiento como uso de: Whastapp, correos personales y pendrives. • Crear un protocolo de destrucción periódica de registros impresos (si aplica). • Centralizar los datos en un repositorio general. • Avanzar en la implementación de capacidades tecnológicas mínimas. Se recomienda, al menos, una ubicación física/virtual segura para los datos (servidor local o servicio seguro en la nube) y la contratación de un profesional de datos a media jornada.
Medio: Existe un departamento de TI a jornada completa con recursos tecnológicos adecuados. Los datos se encuentran almacenados en una ubicación física o virtual con seguridad mínima.	¿Qué mandatos y propósitos tengo para mis datos? ¿Cómo me posiciono en la gradiente de privacidad/utilidad?	• Establecer el Comité de Gobernanza de Datos, compuesto por directivos de su institución u organización. • Llevar a cabo la fase de planificación. • Determinar qué servicios de datos se ofrecerán. • Determinar las responsabilidades que se deben cubrir.
Alto: Existe un documento interno de Gobernanza de datos donde se establecen las bases del modelo. Hay claridad de las responsabilidades y servicios que se ofrecerán. Hay recursos, ya sea para formar, o captar talento con las competencias necesarias.	¿Cómo distribuyo las responsabilidades en términos de jornada laboral y formación de competencias?	• Establecer cuerpos de gobernanza adicionales (ver primera sección n A.4). • Capacitar a personas de la organización o captar talentos ya formados en las materias relevantes para el modelo. • Consolidar Servicios de Administración de Datos. Establecer una arquitectura o catálogo de datos. • Establecer procesos como tiempos de respuesta, cadena de crisis, procesos de estandarización en registro, entre otros.

Tabla 5: Modelo de implementación gradual de la Gobernanza de datos

Lecturas de profundización recomendadas

La presente selección es más amplia que las referencias bibliográficas usadas en la construcción de esta guía, por tanto es una una lista de recomendaciones para los distintos temas tratados:

- Bailie, J. (2020). Big data, differential privacy and national statistical organisations. Statistical Journal of the IAOS, 36(4), 1067–1074. **https://doi.org/10.3233/SJI-200685**

- Centro Nacional en Sistemas de Información en Salud (2024). Guía Introductoria de Buenas Prácticas de Privacidad y Seguridad de Datos en Salud. **https://cens.cl/guia-introductoria-de-buenas-practicas-de-privacidad-y-seguridad-de-datos-en-salud/**

- Henderson, D., Earley, S., & Data Administration Management Association (Eds.). (2017). DAMA-DMBOK: Data management body of knowledge (Second edition). Technics Publications. Apartado 1.3.2 Data Governance Organization (págs..73 a 79)

- Oktaviana, S., Handayani, P. W., & Hidayanto, A. N. (2024). Health organization challenges in health data governance implementation: A systematic review. Journal of Infrastructure, Policy and Development, 8(6), Article 6. **https://doi.org/10.24294/jipd.v8i6.3892**

- Ritchie, F. (2021). Microdata access and privacy: What have we learned over twenty years? Journal of Privacy and Confidentiality, 11(1), Article 1. **https://doi.org/10.29012/jpc.766**

- Green, E., & Ritchie, F. (2023). The present and future of the Five Safes framework. Journal of Privacy and Confidentiality, 13(2), Article 2. **https://doi.org/10.29012/jpc.831**

- Ritchie, F., & Whittard, D. (2024). Using the Five Safes to structure economic evaluations of data governance. Data & Policy, 6, e16. **https://doi.org/10.1017/dap.2024.12**

CENS
CENTRO NACIONAL EN SISTEMAS DE INFORMACIÓN EN SALUD

MOVEMENT HEALTH