TRABAJANDO PARA USTED

Políticas y Lineamientos Institucionales de Gobernanza de Datos en JUNJI

JUNJI
Ministerio de Educación

Gobierno de Chile

TRABAJANDO PARA USTED

Contenido

I. Resumen Ejecutivo 3
II. Introducción 4
III. Curva de Madurez en JUNJI 6
IV. Fundamentos y Referencias 8
V. Objetivos del Documento 13
VI. Principios Rectores de la Gobernanza de Datos 14
VII. Lineamientos Generales por Ámbitos Priorizados de Gobernanza de Datos 16
VIII. Estructura Organizacional para la Gobernanza de Datos 23
IX. Instrumentos de Apoyo 31
X. Plan de Implementación por Fases 34
XI. Indicadores y Métricas de Seguimiento 37
XII. Monitoreo y Mejora Continua 41
XIII. Consideraciones Finales 45
XIV. Anexo 1: Matriz de Conexión entre Políticas TI y ámbitos de Gobernanza de Datos 46

I. Resumen Ejecutivo

La Junta Nacional de Jardines Infantiles (JUNJI), en su rol de garante del derecho a la educación parvularia en Chile, gestiona información que constituye un activo estratégico y sensible: datos de niños, niñas, familias, funcionarios y establecimientos educativos, que deben resguardarse, gestionarse y aprovecharse bajo criterios de legalidad, ética, calidad y valor público.

El diagnóstico institucional de 2024 situó a JUNJI en una etapa "inactiva" de madurez en gobernanza de datos, evidenciando ausencia de estructuras formales, baja trazabilidad y riesgos en la calidad y seguridad de la información. Ante este escenario se formula el presente documento de Políticas y Lineamientos Institucionales de Gobernanza de Datos en JUNJI.

El documento adopta un enfoque progresivo basado en el marco internacional DAMA-DMBOK, priorizando cuatro ámbitos por su impacto estratégico, viabilidad técnica y urgencia institucional: **Gobierno de Datos** (marco rector, roles y toma de decisiones), **Seguridad de los Datos** (protección, control de acceso y respuesta a incidentes), **Calidad de los Datos** (precisión, completitud y confiabilidad) y **Documentos y Contenido** (gestión documental y trazabilidad).

Su implementación se articula mediante principios rectores alineados con la normativa nacional vigente y con estándares internacionales en gestión de datos y seguridad de la información; una estructura organizacional bajo modelo federado, donde cada área es responsable de sus datos con coordinación central; instrumentos de apoyo específicos por ámbito; e indicadores de seguimiento de la madurez institucional.

El despliegue se estructura en cuatro fases:

- **Fase 0 (2024):** Diagnóstico institucional y marco metodológico, documentado en el Informe de Gobernanza de Datos JUNJI (2024). Completada.
- **Fase I (2025–2026):** Diseño y preparación — elaboración normativa, conformación del Comité de Gobernanza de Datos, coordinación con TI e inventario inicial de la información institucional. Incluye los instrumentos exigidos por la Ley N°21.719, cuyo plazo está determinado por su entrada en plena vigencia el 1 de diciembre de 2026.
- **Fase II (2027):** Piloto acotado al dominio Gestión de Párvulos (GesparvuWeb y SIMM) y ajuste de instrumentos según los aprendizajes obtenidos.
- **Fase III (2028):** Implementación ampliada — monitoreo del avance, capacitación progresiva y consolidación del modelo.

Este plazo constituye el compromiso más exigente de la hoja de ruta: por tratarse de datos de niños y niñas —categoría sujeta a protección reforzada—, los instrumentos asociados son de máxima criticidad en la Fase I.

Este documento es un instrumento evolutivo que se ajustará conforme JUNJI avance en su curva de madurez, contribuyendo a fortalecer una cultura basada en datos y garantizar el uso responsable, seguro y estratégico de la información al servicio de la primera infancia.

II. Introducción

La Junta Nacional de Jardines Infantiles (JUNJI) tiene presencia en todo Chile y un rol central en la garantía de los derechos de la primera infancia. En el ejercicio de sus funciones gestiona diariamente grandes volúmenes de información sobre niños, niñas, familias, establecimientos educativos, funcionarios y procesos educativos — información que, por su naturaleza, exige un tratamiento particularmente riguroso.

Los datos que administra JUNJI no son meros registros administrativos: son la base para la toma de decisiones, la planificación de políticas, la rendición de cuentas y para garantizar una educación inicial de calidad. Su creciente complejidad y sensibilidad exigen nuevas capacidades institucionales para su gestión, protección y uso ético. Este desafío se inscribe en un contexto país favorable: Chile alcanzó en 2025 la décima posición en el Índice de Gobierno Digital de la OCDE (puntaje 0,79)[1], posicionándose entre los países miembros con mayor progreso relativo en transformación digital y gobernanza de datos.

Durante 2024, JUNJI desarrolló un diagnóstico institucional en gobernanza de datos, documentado en el *Informe de Gobernanza de Datos JUNJI (2024)*[2], en ejercicio de las funciones conferidas a la Sección de Gobernanza de Datos por el Artículo 66 de la Resolución Exenta N°408/2026[3], que aprueba la estructura orgánica vigente de la Junta Nacional de Jardines Infantiles. Dicho diagnóstico constituye el punto de partida de este documento. Sus principales hallazgos evidenciaron un estado de madurez "inactivo", con las siguientes debilidades:

- *Ausencia de estructuras formales de gobernanza de datos*.
- *Escasa articulación entre áreas usuarias de datos y equipos técnicos*.
- *Baja trazabilidad de la información a lo largo de su ciclo de vida*.
- *Riesgos crecientes en la calidad, seguridad y consistencia de los datos*.
- *Documentación dispersa y desconectada de una visión estratégica institucional*.

A partir de este diagnóstico, JUNJI adoptó el marco DAMA-DMBOK como referencia metodológica, por su reconocimiento internacional, su adaptabilidad al sector público y su compatibilidad con los estándares que orientan la gestión de datos del Estado chileno. El documento prioriza cuatro ámbitos de alto impacto: **Gobierno de Datos**, **Seguridad de los Datos**, **Calidad de los Datos**, **Documentos y Contenido**, seleccionados por su relevancia estratégica y por la viabilidad de implementación en la etapa actual de madurez institucional.

Este enfoque se articula con el marco normativo nacional vigente — en particular la reforma a la Ley N°19.628 introducida por la Ley N°21.719 sobre Protección de Datos Personales, con entrada en vigencia

[1] OCDE (2026). *Digital Government Index and Open, Useful and Re-usable Data Index 2025 Results*. OECD Public Governance Policy Papers. Disponible en: https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/02/digital-government-index-and-open-useful-and-re-usable-data-index_dbe102ed/6347ec74-en.pdf

[2] Informe de Gobernanza de Datos JUNJI (2024). Documento técnico elaborado por la Sección de Gobernanza de Datos del Departamento de Planificación, correspondiente a la Fase 0 del plan de implementación. Constituye un antecedente de trabajo cuyos hallazgos fundamentan el presente instrumento; no forma parte del acto administrativo que lo aprueba ni de su articulado. La actualización de la línea base de madurez que en él se establece se realizará mediante el instrumento de autoevaluación previsto en el Capítulo IX.

[3] Resolución Exenta N°408, de fecha 09 de marzo de 2026, que aprueba la estructura orgánica interna de la Junta Nacional de Jardines Infantiles.

plena el 1 de diciembre de 2026. Esta normativa establece obligaciones generales para el tratamiento de todos los datos personales que administra JUNJI — incluidos los de las y los funcionarios que se desempeñan en la institución — y obligaciones reforzadas para el tratamiento de los datos de niños y niñas. Se complementa con estándares internacionales como ISO/IEC 27001:2023 y las recomendaciones de organismos como OCDE, CEPAL y BID sobre gobernanza de datos en el sector público. El detalle de estas referencias se desarrolla en el Capítulo IV.

Sobre esta base metodológica y normativa, el presente documento constituye la propuesta formal de políticas y lineamientos que permitirá a JUNJI transitar desde la actual etapa inactiva hacia una etapa reactiva de madurez en el corto plazo, y avanzar progresivamente hacia una etapa proactiva en el mediano plazo, según la ruta de implementación por fases que se detalla en el Capítulo X.

Este documento se enmarca, además, en los compromisos institucionales del Plan Estratégico JUNJI 2023-2026, particularmente en su Eje 5 "Modernización Institucional" y su Objetivo Estratégico 5.2[4], que busca fortalecer el proceso de toma de decisiones en todos los niveles de la institución mediante información confiable, oportuna y que aporte a una visión institucional integral. La gobernanza de datos constituye la condición habilitante para el cumplimiento de dicho objetivo.

El documento se concibe como un instrumento evolutivo: esta primera versión aborda los ámbitos priorizados para iniciar el tránsito, y se ampliará en versiones futuras hacia las restantes Áreas de Conocimiento del marco DAMA-DMBOK —Arquitectura de Datos; Modelamiento y Diseño de Datos; Almacenamiento y Operaciones de Datos; Integración e Interoperabilidad de Datos; Datos Maestros y de Referencia; Metadatos; y Data Warehousing e Inteligencia de Negocios— conforme se fortalezca la madurez institucional. La oportunidad y secuencia de su incorporación serán resueltas por el Comité de Gobernanza de Datos, sobre la base de criterios de viabilidad técnica, capacidad operativa y prioridad normativa, y quedarán registradas en el Plan Plurianual de Gobernanza de Datos.

[4] Junta Nacional de Jardines Infantiles (2023). *Plan Estratégico JUNJI 2023-2026*, Eje 5 "Modernización Institucional", Objetivo Estratégico 5.2.

III. Curva de Madurez en JUNJI

La curva de madurez en gobernanza de datos es un marco estratégico que evalúa la capacidad de una organización para gestionar sus datos, evolucionando desde un estado inicial sin prácticas formales hasta uno optimizado, en el que la gestión del dato se integra a la cultura institucional y genera valor de manera continua. JUNJI adopta para estos efectos una escala de madurez propia, elaborada sobre la base de modelos progresivos de amplio uso en la disciplina y adaptada a la realidad institucional[5].

Este modelo de madurez es útil porque permite:

- Identificar el punto de partida institucional (línea base).
- Establecer metas realistas de avance.
- Priorizar esfuerzos según brechas identificadas.
- Comunicar avances a la alta dirección y partes interesadas.

La escala de madurez adoptada por JUNJI contempla cinco etapas progresivas:

Etapa	Características
0. Inactiva	No existen prácticas formales de gestión de datos. Desconocimiento del valor de los datos. Gestión fragmentada y reactiva ante problemas.
1. Reactiva	Se reconoce la necesidad de gestionar los datos. Se establecen políticas iniciales, roles básicos y se comienza a documentar. Las acciones responden a problemas identificados.
2. Proactiva	Existen procesos estandarizados y roles definidos. Se implementan controles de calidad y seguridad. La gestión de datos se integra a los procesos institucionales.
3. Gestionada	Se miden indicadores de desempeño. Existe mejora continua basada en métricas. Los datos se gestionan como activos estratégicos con gobernanza formal.
4. Optimizada	La gobernanza de datos está integrada a la cultura organizacional. Se genera valor público a partir de los datos. Innovación y anticipación de necesidades.

Esta propuesta se enfoca en asegurar el tránsito desde la etapa Inactiva (Nivel 0) hacia la etapa Reactiva (Nivel 1), y sentar las bases para avanzar hacia la etapa Proactiva (Nivel 2). Los niveles Gestionada y Optimizada son horizontes de largo plazo, cuya materialización requerirá versiones futuras del modelo de gobernanza institucional de datos.

[5] La escala de madurez adoptada por JUNJI constituye una adaptación institucional elaborada sobre la base de la curva de madurez en gestión de datos difundida por SDG Group (2023), que distingue cuatro estados —inactivo, reactivo, proactivo y optimizado— caracterizados según las dimensiones de personas, procesos y tecnología. La adaptación incorpora un quinto estado intermedio, denominado "Gestionada", en coherencia con los niveles progresivos de madurez que contempla el marco DAMA-DMBOK, y amplía las dimensiones de caracterización a gobernanza, procesos, personas, tecnología y documentación, conforme al diagnóstico institucional realizado en 2024. Fuente de referencia: SDG Group (2023). *Curva de madurez en data analytics: navegando por las etapas del desarrollo*. Disponible en: https://www.sdggroup.com/es-es/insights/blog/curva-de-madurez-segun-data-analytics

El diagnóstico realizado en 2024 (Fase 0 del plan de implementación) situó a JUNJI en la etapa inactiva (nivel 0) de madurez en gobernanza de datos. Esta clasificación se fundamenta en las siguientes evidencias:

Dimensión	Situación identificada
Gobernanza	Falta de estructuras, comités o instancias institucionales vinculadas a la gestión de datos.
Procesos	Ausencia de lineamientos comunes para la gestión de datos. No hay procesos estandarizados de recolección, almacenamiento ni análisis.
Personas	No existen roles específicos para la gestión de datos (Data Owner, Data Steward). Baja consciencia institucional sobre el valor de los datos.
Tecnología	Sistemas no integrados (islas de información). Herramientas insuficientes para gestionar el volumen y complejidad de los datos.
Documentación	Información dispersa y desconectada de una visión estratégica. Sin catálogo ni diccionario de datos institucional.

Esta propuesta busca que JUNJI avance desde la etapa inactiva hacia la **etapa reactiva (nivel 1)**, en la cual la institución comienza a establecer políticas, definir responsabilidades, organizar información y promover una cultura inicial de datos.

Este tránsito implica:

- Institucionalizar un marco de políticas y lineamientos transversales a la organización.
- Activar una estructura mínima de gobernanza: Comité de Gobernanza de Datos, Propietarios de Datos (Data Owner) y Administradores de Datos (Data Steward).
- Priorizar ámbitos estratégicos: Gobierno de Datos, Seguridad de los Datos, Calidad de los Datos, y Documentos y Contenido.
- Coordinar esfuerzos técnicos (TI) con los equipos de gestión, bajo un modelo federado.
- Establecer indicadores de seguimiento para monitorear el avance.

Este avance permitirá a JUNJI sentar las bases para construir una **cultura organizacional basada en datos**, primera condición para sostener las etapas más avanzadas del modelo de madurez a las que la institución aspira en el largo plazo.

Figura 1. Hoja de ruta de la gobernanza de datos en JUNJI — proyección de madurez y fases de implementación.

El presente documento compromete metas de avance hasta el Nivel 2 (Proactiva). Los Niveles 3 (Gestionada) y 4 (Optimizada) se declaran como horizonte institucional de largo plazo y no llevan metas asociadas en esta versión, por cuanto su materialización requiere capacidades que exceden el alcance de las fases aquí definidas.

La aplicación operativa de esta escala se realizará mediante el instrumento de autoevaluación de madurez en gobernanza de datos previsto en el Capítulo IX, cuyo desarrollo está contemplado para la Fase II.

IV. Fundamentos y Referencias

La construcción de esta propuesta no parte de cero. Se sustenta en marcos de referencia internacionales ampliamente reconocidos, en la legislación chilena vigente y en la evidencia comparada de organismos multilaterales. Estos fundamentos orientan tanto el enfoque metodológico adoptado como los contenidos técnicos y operativos del documento.

A continuación, se presentan los tres pilares que dan soporte a esta propuesta: el **marco DAMA-DMBOK** como referente metodológico, la **normativa nacional e internacional** aplicable, y las recomendaciones de **organismos internacionales con experiencia en gobernanza de datos** para el sector público.

4.1. Enfoque DAMA-DMBOK

El modelo de referencia DAMA-DMBOK constituye la base conceptual de esta propuesta[6]. Este marco reconoce once áreas fundamentales para la gestión de datos, con el "Gobierno de Datos" como función central y habilitante. Desde allí se desprenden ámbitos como calidad de los datos, seguridad, arquitectura, documentos y contenido, entre otros.

JUNJI ha optado por una implementación gradual, comenzando con cuatro de estas áreas priorizadas: Gobierno de Datos, Seguridad de los Datos, Calidad de los Datos y Documentos y Contenido. Este enfoque permite alinear los esfuerzos institucionales con buenas prácticas reconocidas, sin sobrecargar las capacidades actuales ni generar estructuras difíciles de sostener. El cumplimiento normativo y el ciclo de vida de los datos, que no constituyen Áreas de Conocimiento independientes

[6] DAMA International (2017). DAMA-DMBOK: Data Management Body of Knowledge, 2ª edición

en el DAMA-DMBOK sino conceptos transversales a todo el marco, se abordan de manera cruzada dentro de los cuatro ámbitos priorizados, según el mapeo detallado en el Capítulo VII.

La elección de DAMA-DMBOK como marco de referencia responde a su reconocimiento internacional, su adaptabilidad a distintos contextos organizacionales y su compatibilidad con los estándares normativos que se describen a continuación. Adicionalmente, el Estado de Chile ha adoptado oficialmente el marco DAMA como base para el Marco de Referencia de Gestión de Datos del Estado (MGDE), lo que valida la elección metodológica de JUNJI y facilita su alineación con las directrices nacionales de gestión de datos.

4.2. Normativa nacional e internacional

Además del marco metodológico, la propuesta responde al contexto normativo chileno, que en los últimos años ha fortalecido significativamente las exigencias en materia de transparencia, protección de datos y ciberseguridad. Las siguientes normativas establecen obligaciones directas para instituciones públicas como JUNJI:

Normativa nacional. El siguiente conjunto de leyes constituye el marco vinculante para el tratamiento de datos e información pública por parte de JUNJI:

- *Ley N°20.285 sobre Acceso a la Información Pública*: Consagra el principio de transparencia y establece obligaciones de publicación, resguardo y entrega de datos.

- *Ley N°21.180 sobre Transformación Digital del Estado*: establece la obligatoriedad de tramitar los procedimientos administrativos a través de medios electrónicos e incorpora, en el artículo 16 bis de la Ley N°19.880, el principio de interoperabilidad, conforme al cual los medios electrónicos deben ser capaces de interactuar y operar entre sí al interior de la Administración del Estado mediante estándares abiertos. De este principio se deriva la regla de "solo una vez": los órganos del Estado no pueden requerir a las personas datos que ya obran en poder de otro órgano público. Su aplicación es gradual, conforme a las fases establecidas en el Decreto con Fuerza de Ley N°1 de 2020 del Ministerio Secretaría General de la Presidencia, y no podrá extenderse para ningún órgano de la Administración del Estado más allá del 31 de diciembre de 2027, según el artículo segundo transitorio sustituido por la Ley N°21.464. La fase aplicable a JUNJI es coordinada por la Coordinación de Transformación Digital institucional en su relación con la Secretaría de Gobierno Digital.

- *Ley N°21.658 que crea la Secretaría de Gobierno Digital*: establece la coordinación, asesoría y apoyo intersectorial en el uso estratégico de tecnologías digitales, datos e información pública para mejorar la gestión de los órganos de la Administración del Estado.

- *Ley N°21.663 Marco sobre Ciberseguridad: Establece la Agencia Nacional de Ciberseguridad (ANCI) e impone deberes de gestión de riesgos, adopción de medidas de resguardo y reporte de incidentes al CSIRT Nacional. La ley distingue dos categorías: los*

prestadores de servicios esenciales —calidad que corresponde a los órganos de la Administración del Estado por definición legal— y los operadores de importancia vital, calificación que efectúa el Director Nacional de la ANCI mediante resolución fundada, conforme al artículo 5° de la ley y al procedimiento del Decreto Supremo N°285 de 2024 del Ministerio del Interior y Seguridad Pública. JUNJI fue calificada como operador de importancia vital mediante Resolución Exenta N°87 de 2025 de la ANCI, correspondiente al primer proceso de calificación, quedando por tanto sujeta a los deberes reforzados que establece la ley para dicha categoría. Su cumplimiento es conducido por la Sección de Tecnologías de la Información, en el marco del Sistema de Gestión de Seguridad de la Información institucional, y se articula con el presente modelo conforme al Capítulo VIII[7].

- *Ley N°21.719 sobre Protección de Datos Personales (en vigencia plena el 1 de diciembre de 2026): Reforma íntegramente la Ley N°19.628 de 1999 sobre Protección de la Vida Privada, alineando a Chile con estándares internacionales como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Crea la Agencia de Protección de Datos Personales (APDP) como autoridad autónoma con potestades fiscalizadoras y sancionatorias, establece los derechos ARCO-P (acceso, rectificación, cancelación, oposición y portabilidad), categorías especiales de protección para datos de niños, niñas y adolescentes, y sanciones de hasta 20.000 UTM. En el caso de JUNJI, estas obligaciones reforzadas aplican al tratamiento de datos de niños y niñas (0 a 4 años), mientras que las obligaciones generales de la ley aplican a todos los datos personales que administra la institución, incluidos los de las y los funcionarios.*

  Adicionalmente, la ley contempla cuatro disposiciones que estructuran el diseño institucional de la gobernanza de datos: el ***artículo 44****, que consagra la responsabilidad administrativa personal del jefe superior del órgano público por las infracciones cometidas por el organismo, con multas agravadas tratándose de datos sensibles como los que administra JUNJI; el* ***artículo 49****, que regula el modelo de prevención de infracciones como instrumento voluntario cuya adopción constituye atenuante de responsabilidad; el* ***artículo 50****, que regula la figura del* ***Delegado(a) de Protección de Datos (DPO)****, cuya designación es voluntaria pero constituye elemento constitutivo del referido modelo; y el* ***artículo quinto transitorio****, que restringe, para los órganos públicos, que el eventual delegado recaiga en un funcionario de la dotación vigente. El desarrollo institucional de estas disposiciones se aborda en el Capítulo VIII.*

  La ley refuerza asimismo la dimensión de coordinación interinstitucional: el ***artículo 21*** *somete el tratamiento de datos por parte de los órganos públicos al principio de coordinación, exigiendo alcanzar un alto grado de interoperabilidad y coherencia, de modo de evitar contradicciones en la información almacenada y la reiteración de requerimientos de información o documentos a los titulares; y el* ***artículo 22*** *habilita la comunicación o cesión de datos personales entre organismos públicos para el cumplimiento de sus funciones, evitando la duplicidad de trámites, estableciendo además*

[7] Resolución Exenta N°87, de 16 de diciembre de 2025, de la Agencia Nacional de Ciberseguridad, que aprueba la nómina de operadores de importancia vital correspondiente al primer proceso de calificación. Publicada en el Diario Oficial N°44.326-B, de 17 de diciembre de 2025.

el deber de informar mensualmente en el sitio web institucional los convenios de cesión o transferencia de datos suscritos, obligación sujeta a fiscalización de la Agencia.

Estándares internacionales. Complementan la normativa nacional al establecer buenas prácticas técnicas ampliamente reconocidas:

- *Norma ISO/IEC 27001:2023*: Norma técnica internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI).

Instrumentos de política pública nacional. Estos instrumentos orientan operativamente la implementación de la gestión de datos en el sector público chileno y ofrecen a JUNJI un marco de referencia concreto para el diseño de sus lineamientos internos:

- *Marco de Referencia de Gestión de Datos del Estado (MGDE)*: Guía técnica publicada por la Secretaría de Gobierno Digital que adapta el modelo DAMA-DMBOK a la realidad del servicio público chileno, complementándolo con dimensiones específicas como datos abiertos, aspectos legales y normativos. Orienta a los órganos de la Administración del Estado en la adopción de buenas prácticas de gestión de datos.

- *Estrategia de Datos de la Administración del Estado*: Establece lineamientos y una hoja de ruta para que el Estado avance hacia una gestión de datos estratégica, con foco en la generación de valor público. Propone la conformación del Consejo Estratégico de Datos y una gobernanza nacional de datos.

- *Sistema de Transformación Digital (STD)*: Incorporado al Programa de Mejoramiento de la Gestión (PMG) desde 2025, busca instalar progresivamente los principios y estándares de gobierno digital en las instituciones públicas. Uno de sus componentes centrales corresponde a la gestión de datos, alineado con las directrices del MGDE, lo que hace que el avance de JUNJI en gobernanza de datos contribuya directamente al cumplimiento del STD-PMG institucional.

En conjunto, estas normativas configuran un marco vinculante que obliga a JUNJI a gestionar sus datos con criterios de transparencia, protección de datos personales, seguridad y responsabilidad. La propuesta aquí presentada busca precisamente dar cumplimiento a estas exigencias, articulándolas con las buenas prácticas del marco DAMA-DMBOK.

4.3. Recomendaciones internacionales

Complementariamente al marco normativo, resulta relevante considerar las recomendaciones de organismos internacionales que han estudiado la implementación de gobernanza de datos en el sector público, particularmente en contextos latinoamericanos similares al chileno.

Los tres organismos que se citan a continuación aportan miradas complementarias sobre gobernanza de datos: la OCDE define estándares de política pública, la CEPAL orienta la implementación adaptada

al contexto latinoamericano, y el BID entrega experiencia operativa desde proyectos concretos financiados en la región.

- *OCDE (Organización para la Cooperación y el Desarrollo Económicos):* Organismo internacional que reúne a países de ingreso medio-alto y alto para definir estándares y buenas prácticas de política pública. En materia de gobernanza de datos, enfatiza que los datos deben tratarse como infraestructura estratégica del Estado, recomendando avanzar hacia políticas institucionales formales, responsables identificados y una gobernanza clara del ciclo de vida de los datos. Chile alcanzó en 2025 el décimo lugar en el Índice de Gobierno Digital de la OCDE (puntaje 0,79)[8] y figura entre los países miembros con mayor progreso relativo en esta edición, lo que valida la dirección adoptada por instituciones como JUNJI.

- *CEPAL (Comisión Económica para América Latina y el Caribe):* Organismo técnico de Naciones Unidas con sede en Santiago, especializado en investigación y análisis de desarrollo económico y social para la región. Su aporte a la gobernanza de datos se enfoca en cómo avanzar con capacidades institucionales limitadas: recomienda modelos de implementación gradual, priorizar ámbitos críticos (calidad, seguridad y gobernanza), y trabajar con pilotos y coordinación entre áreas usuarias y equipos técnicos.[9]

- *BID (Banco Interamericano de Desarrollo):* Banco multilateral de desarrollo con foco en América Latina y el Caribe, cuya experiencia proviene de proyectos concretos de modernización del Estado financiados en la región. Destaca la necesidad de estructurar la operación mediante roles claramente definidos: propietarios de datos (Data Owner, del lado de la institución) y equipos técnicos (custodios de infraestructura), articulados bajo un modelo federado y transversal.

Estas recomendaciones validan el enfoque adoptado por JUNJI: una implementación gradual, focalizada en ámbitos críticos, con roles claramente definidos y bajo un modelo federado que articula las áreas de gestión[10] con los equipos técnicos. La convergencia de las recomendaciones internacionales fundamenta el enfoque metodológico y organizacional que se desarrolla en los capítulos siguientes.

[8] OCDE (2026). *Digital Government Index and Open, Useful and Re-usable Data Index 2025 Results*. OECD Public Governance Policy Papers. Disponible en: https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/02/digital-government-index-and-open-useful-and-re-usable-data-index_dbe102ed/6347ec74-en.pdf

[9] CEPAL (2022). *Agenda Digital de América Latina y el Caribe (eLAC2022)*. Comisión Económica para América Latina y el Caribe.

[10] Las expresiones "área de gestión" y "dominio de datos" empleadas en este documento corresponden a lo que el marco DAMA-DMBOK denomina business area y business domain, y "valor público" a lo que dicho marco denomina business value. La equivalencia se consigna para preservar la trazabilidad metodológica con el marco de referencia adoptado.

V. Objetivos del Documento

A partir del diagnóstico institucional y los fundamentos expuestos, este capítulo formaliza los objetivos que orientan la presente propuesta. Estos objetivos permitirán guiar la implementación, evaluar los avances y asegurar la alineación de los esfuerzos con las prioridades estratégicas de JUNJI, sirviendo de referencia para el Comité de Gobernanza de Datos, Equipo Coordinador y las áreas de gestión propietarias de dominios institucionales.

Objetivo General

Establecer un marco institucional de principios, lineamientos y responsabilidades que permita a JUNJI avanzar hacia una gobernanza de datos sólida, abordando de forma priorizada los ámbitos de Gobierno de Datos, Seguridad de los Datos, Calidad de los Datos, y Documentos y Contenido, en concordancia con el marco DAMA-DMBOK, la normativa nacional vigente y los estándares internacionales.

Objetivos Específicos

1. Definir los principios rectores que orientarán la gestión de datos a nivel institucional.
2. Definir los ámbitos estratégicos de gobernanza de datos priorizados en esta primera versión del modelo institucional.
3. Establecer lineamientos específicos para cada uno de los ámbitos priorizados.
4. Definir la estructura organizacional para la gobernanza de datos, incluyendo los roles, funciones y responsabilidades de los actores involucrados bajo un modelo federado.
5. Establecer instrumentos de apoyo específicos por cada ámbito priorizado, que operacionalicen los lineamientos definidos.
6. Establecer indicadores de seguimiento que permitan monitorear el avance y la madurez institucional en gobernanza de datos.
7. Asegurar el cumplimiento del marco normativo vigente en materia de transparencia, protección de datos personales, ciberseguridad y transformación digital del Estado.
8. Definir una ruta de implementación gradual, estructurada en fases, que permita avanzar de manera sostenible según la capacidad operativa de la institución.
9. Impulsar el desarrollo de una cultura organizacional orientada a la gestión ética, segura y estratégica de los datos, mediante acciones de capacitación y sensibilización institucional.

VI. Principios Rectores de la Gobernanza de Datos

Los principios rectores constituyen el fundamento normativo y ético sobre el cual se estructura la gobernanza de datos en JUNJI. Orientan la toma de decisiones, definen prioridades y guían el comportamiento institucional a lo largo del ciclo de vida de los datos.

Los once principios que se presentan a continuación han sido definidos en coherencia con el marco DAMA-DMBOK, la normativa nacional vigente (Leyes 20.285, 21.719, 21.663, 21.180 y 21.658) y los principios de buen gobierno público. Se organizan en tres dimensiones: principios de cumplimiento normativo, principios de gestión de datos y principios de cultura y valor institucional.

Principios de cumplimiento normativo:

1. **Legalidad:** Asegurar que el tratamiento de los datos se realice conforme al marco normativo vigente, resguardando los derechos fundamentales de las personas.

2. **Transparencia**: Garantizar el acceso y conocimiento público sobre los datos disponibles, sus fuentes y su propósito, promoviendo la rendición de cuentas.

3. **Seguridad y protección**: Garantizar la confidencialidad, integridad y disponibilidad de los datos, con especial resguardo de las categorías especiales de protección establecidas por la Ley 21.719, en particular los datos de niños y niñas administrados por JUNJI.

4. **Proporcionalidad y minimización**: Recopilar y tratar únicamente los datos que sean estrictamente necesarios para cumplir con la finalidad declarada, conforme al principio de minimización establecido en la Ley 21.719. Este principio es especialmente relevante en JUNJI dado el tratamiento de datos de niños, niñas y sus familias.

Principios de gestión de datos:

5. **Calidad**: Asegurar que los datos sean completos, consistentes, actualizados, precisos y pertinentes para su uso institucional.

6. **Accesibilidad y usabilidad**: Asegurar que los datos estén disponibles internamente en formatos útiles y oportunos para quienes los requieren dentro de la institución, favoreciendo la toma de decisiones informadas.

7. **Interoperabilidad**: Facilitar el intercambio seguro, estandarizado y formalizado de datos entre las distintas unidades de JUNJI y con otros organismos del Estado, en cumplimiento del principio de interoperabilidad y de la regla de "solo una vez" que consagra la Ley N°21.180, y del principio de

coordinación establecido en el artículo 21 de la Ley N°21.719. Su aplicación supone evitar que se requiera a las personas, a los jardines infantiles o a las unidades internas información que ya obra en poder de la institución o de otro órgano del Estado, y que todo intercambio interinstitucional se sustente en convenios formales con condiciones de uso, acceso y seguridad definidas. Este principio es clave para la articulación con MINEDUC y otros organismos con los que JUNJI intercambia información, y se operacionaliza mediante los instrumentos del ámbito Gobierno de Datos definidos en el Capítulo VII.

8. **Responsabilidad compartida**: Reconocer que la gobernanza de datos requiere la participación coordinada de distintas unidades, tanto técnicas como sustantivas, bajo un modelo federado que se materializa en la estructura organizacional definida en el Capítulo VIII.

Principios de cultura y valor institucional:

9. **Ética en el uso de los datos**: Establecer una cultura organizacional que valore el uso ético de la información, evitando distorsiones, manipulaciones o usos indebidos.

10. **Valor público**: Orientar la gestión de datos hacia la generación de beneficios concretos para la ciudadanía, la mejora de políticas públicas y el fortalecimiento de la gestión institucional.

11. **Mejora continua**: Impulsar procesos de evaluación, retroalimentación y ajuste permanente de las prácticas de gobernanza de datos.

Estos principios deberán ser interiorizados por todas las unidades de JUNJI, integrándose tanto en los procesos estratégicos como en los operativos y de apoyo. Su aplicación práctica se traduce en los lineamientos específicos por ámbito priorizado que se desarrollan en el Capítulo VII, y se sostiene mediante los instrumentos de apoyo (Capítulo IX) y los indicadores de seguimiento (Capítulo XI) que permiten monitorear su cumplimiento.

El Comité de Gobernanza de Datos velará por la difusión, cumplimiento y revisión periódica de estos principios, asegurando su vigencia y pertinencia a lo largo del tiempo.

VII. Lineamientos Generales por Ámbitos Priorizados de Gobernanza de Datos

En concordancia con los principios rectores definidos en el capítulo anterior, JUNJI ha optado por una implementación progresiva y realista del modelo DAMA-DMBOK, priorizando cuatro ámbitos fundamentales para su contexto institucional: Gobierno de Datos, Seguridad de los Datos, Calidad de los Datos y Documentos y Contenido.

Estos ámbitos fueron seleccionados considerando su impacto estratégico, viabilidad técnica, riesgos actuales y alineación con la normativa nacional e internacional. Para cada uno se presenta una definición, los objetivos específicos que se persiguen y los instrumentos sugeridos para su implementación.

7.1. Gobierno de Datos

Corresponde al marco rector que establece la autoridad, las estructuras y la toma de decisiones sobre los datos en la organización. Implica definir políticas, roles, procesos y mecanismos de control que aseguren una gestión coherente y coordinada de los activos de datos. Este ámbito es el eje articulador de toda la gobernanza, ya que habilita y sostiene a los demás.

Objetivos específicos:

- Establecer un Comité de Gobernanza de Datos con representantes de unidades clave.
- Asignar roles institucionales como responsables de datos (Data Owner), administradores (Data Steward), custodios técnicos y usuarios, conforme al modelo federado.
- Elaborar lineamientos y procedimientos institucionales sobre gestión de datos.
- Mantener un **Registro de Actividades de Tratamiento** (RAT) que documente de manera actualizada las actividades institucionales que involucran datos personales — sus finalidades, categorías de datos, destinatarios, plazos de conservación y medidas de seguridad aplicadas —, conforme a las obligaciones establecidas por la Ley N°21.719.
- Formalizar el intercambio interinstitucional de datos, identificando los flujos que JUNJI mantiene con otros órganos del Estado, asegurando que cada intercambio cuente con un instrumento formal que defina finalidad, condiciones de acceso y medidas de seguridad, y evitando la duplicidad de requerimientos de información a las unidades internas, a los jardines infantiles y a las familias, en aplicación del principio de interoperabilidad establecido en el Capítulo VI.
- Adoptar una mirada de proceso sobre el ciclo de vida del dato, asegurando la trazabilidad de extremo a extremo de los datos institucionales a través de las distintas áreas que intervienen en su creación, uso, actualización y conservación. Este enfoque constituye un criterio complementario para delimitar dominios y responsabilidades, y no sustituye el modelo federado definido en el Capítulo VIII ni implica la redefinición de los dominios ya establecidos para el pilotaje.

Instrumentos sugeridos:

- Modelo federado de gobernanza.
- Catálogo de Datos Institucional: inventario estructurado de los activos de datos que administra JUNJI, indicando su dominio, área propietaria, sistema de origen y nivel de sensibilidad.
- Glosario institucional de datos: definición estandarizada de términos técnicos y conceptos utilizados en la gobernanza de datos.
- Catálogo de roles y responsabilidades.
- Registro de Actividades de Tratamiento (RAT): planilla institucional que documenta las actividades de tratamiento de datos personales, sus finalidades, categorías de datos, destinatarios, plazos de conservación y medidas de seguridad, conforme a la Ley N°21.719.
- Mapa institucional de flujos de datos interinstitucionales: instrumento que identifica y documenta los intercambios de datos que JUNJI sostiene con otros órganos del Estado —MINEDUC, JUNAEB, Servicio de Registro Civil e Identificación, Subsecretaría de Educación Parvularia, entre otros—, señalando para cada flujo el dominio de datos involucrado, la finalidad, la periodicidad, el sistema de origen y el instrumento formal que lo respalda. Permite detectar duplicidades de requerimiento y vacíos de formalización.
- Catálogo de convenios de intercambio de datos: registro consolidado y actualizado de los convenios vigentes de cesión, transferencia o comunicación de datos personales suscritos con organismos públicos y entidades privadas. Constituye el insumo directo para dar cumplimiento al deber de publicación mensual establecido en el artículo 22 de la Ley N°21.719, y se articula con el Registro de Actividades de Tratamiento.
- Protocolo de intercambio interinstitucional de datos: instrumento que define los requisitos mínimos que debe cumplir toda solicitud de datos proveniente de otro órgano del Estado o dirigida a él —verificación de base de licitud, principio de minimización, canal de transmisión, resguardos aplicables a datos de niños y niñas, y registro de la operación—. Se articula con la Política de Protección de Datos Personales y con el lineamiento de protección ante intercambio interinstitucional definido para los datos de párvulos.

El gobierno de datos actúa como columna vertebral de la gobernanza. Sin embargo, su operación requiere que los datos estén resguardados, lo que nos lleva al siguiente ámbito.

7.2. Seguridad de los Datos

Se refiere a las políticas, controles y prácticas que protegen los datos contra accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas. Considera tanto medidas técnicas como organizacionales, y responde directamente a las exigencias de la Ley 21.663 de Ciberseguridad y la Ley 21.719 de Protección de Datos Personales.

Objetivos específicos:

- Proteger la confidencialidad, integridad y disponibilidad de los datos.
- Cumplir con las normativas de ciberseguridad (Ley N°21.663) y de protección de datos personales (Ley N°21.719), considerando que JUNJI se encuentra sujeta a obligaciones reforzadas en ambos cuerpos legales: por su condición de operador de importancia vital en materia de ciberseguridad, y por el tratamiento de datos de niños y niñas en materia de protección de datos personales.
- Elaborar el Protocolo institucional de Gestión de Incidentes de Seguridad de la Información, que defina la actuación coordinada ante incidentes críticos, incluyendo la notificación de vulneraciones de seguridad a la Agencia de Protección de Datos Personales y a los titulares afectados o sus representantes conforme a la Ley N°21.719, y el reporte a la Agencia Nacional de Ciberseguridad (ANCI) conforme a la Ley N°21.663, en los términos exigibles a los operadores de importancia vital. Este protocolo complementa el Procedimiento de Gestión de Incidentes existente (JUNJI_A.16.1, V1.4), enfocándose en las dimensiones institucionales, decisionales y de comunicación externa que el procedimiento operativo no cubre.

Instrumentos sugeridos:

- Política de Seguridad de la Información.
- Política de Protección de Datos Personales: instrumento normativo específico que aterriza las obligaciones de la Ley N°21.719 en materia de licitud del tratamiento, consentimiento informado, minimización, derechos de titulares y protección reforzada de datos de niños y niñas. Complementa la Política General de Seguridad de la Información, la cual, por su base ISO/IEC 27001, no cubre las obligaciones específicas de protección de datos personales.
- Procedimiento de respaldo y recuperación.
- Registro de brechas y eventos de seguridad, con trazabilidad de las notificaciones efectuadas a la APDP, a la ANCI y a los titulares o sus representantes. Este registro constituye un anexo operativo del Protocolo de Gestión de Incidentes que se elaborará en Fase I.
- Procedimiento para la atención de derechos ARCO-P: mecanismo formal para responder a solicitudes de acceso, rectificación, cancelación, oposición y portabilidad de datos personales, conforme a los plazos y requisitos establecidos por la Ley N°21.719.

La seguridad protege los datos, pero su utilidad depende también de que estos sean confiables. Por ello, el siguiente ámbito aborda la calidad de los datos.

7.3. Calidad de los Datos

Comprende el conjunto de prácticas destinadas a asegurar que los datos sean precisos, completos, consistentes, actualizados y adecuados para sus fines de uso. La calidad es un factor clave para la confianza en la toma de decisiones, para el cumplimiento de las obligaciones de transparencia establecidas en la Ley 20.285 y para garantizar que los datos de párvulos y familias sean confiables y sirvan efectivamente a la mejora de la educación parvularia.

Objetivos específicos:

- Definir dimensiones de calidad prioritarias (completitud, consistencia, exactitud, oportunidad y unicidad) y establecer estándares mínimos aplicables a los datos institucionales.
- Establecer controles y métricas de validación que aseguren la confiabilidad de los datos utilizados en la toma de decisiones.
- Integrar mecanismos de monitoreo de calidad en los sistemas institucionales, considerando también los procesos de rectificación de datos personales establecidos por la Ley N°21.719.

Instrumentos sugeridos:

- Fichas técnicas de datos.
- Indicadores de calidad por dimensión (completitud, consistencia, oportunidad, etc.).
- Tableros de monitoreo de calidad.

Los datos de calidad deben además estar debidamente documentados y organizados. El último ámbito priorizado aborda precisamente la gestión de documentos y contenido.

7.4. Documentos y Contenido

Hace referencia a la gestión estructurada de los documentos físicos y digitales que contienen información institucional relevante. Incluye la organización, resguardo, trazabilidad y acceso controlado a dichos contenidos. Este ámbito es fundamental para preservar el conocimiento institucional y constituye la base operativa para el cumplimiento de las obligaciones de transparencia establecidas en la Ley N°20.285 sobre Acceso a la Información Pública.

Objetivos específicos:

- Sistematizar la gestión documental institucional mediante criterios uniformes de clasificación, resguardo y acceso.

- Asegurar la integridad, disponibilidad y trazabilidad de los documentos institucionales relevantes.
- Establecer mecanismos de clasificación y acceso controlado a la información, alineados con las obligaciones de transparencia y protección de datos personales.

Instrumentos sugeridos:

- Políticas de gestión documental.
- Mapa de activos documentales.
- Clasificador institucional de documentos.
- Tabla de Retención Documental: instrumento que establece los plazos de conservación, transferencia y eliminación de los documentos institucionales, según su valor administrativo, legal e histórico.

Los cuatro ámbitos priorizados operan de forma articulada y transversal. Sin embargo, dado que JUNJI gestiona datos sensibles de primera infancia, se requieren consideraciones específicas que atraviesan estos cuatro ámbitos y que se detallan a continuación.

Consideraciones Especiales: Tratamiento de Datos de Primera Infancia

Dado que JUNJI gestiona información de niños, niñas y sus familias, resulta indispensable establecer consideraciones específicas para el tratamiento de estos datos. La Ley N°21.719 sobre Protección de Datos Personales establece categorías especiales de protección para datos de niños, niñas y adolescentes, exigiendo medidas reforzadas de resguardo que van más allá de las obligaciones generales. En el caso particular de JUNJI, cuya población objetivo corresponde a niños y niñas de 0 a 4 años, estas obligaciones reforzadas se aplican íntegramente al tratamiento de todos los datos de párvulos y sus familias.

Los lineamientos específicos para el tratamiento de datos de primera infancia en JUNJI son:

- *Principio del interés superior del niño/a*: Todo tratamiento de datos de párvulos debe orientarse a su bienestar integral, priorizando su protección por sobre cualquier otro interés institucional o administrativo. Este principio, consagrado en la Convención sobre los Derechos del Niño (ratificada por Chile en 1990) y reforzado por la Ley N°21.430 sobre Garantías y Protección Integral de los Derechos de la Niñez y Adolescencia (2022), constituye un mandato transversal para toda actuación institucional que involucre a niños y niñas.

- *Minimización reforzada*: Solo se recopilarán datos de párvulos y sus familias que sean estrictamente necesarios para el cumplimiento de las funciones institucionales de JUNJI. Se evitará la recopilación de datos excesivos o no pertinentes, en cumplimiento del principio de proporcionalidad de la Ley 21.719.

- *Consentimiento informado*: El tratamiento de datos personales de niños y niñas requerirá consentimiento informado del padre, madre o representante legal, conforme a lo establecido en la Ley 21.719. Se deberá informar de manera clara y accesible sobre la finalidad, alcance y plazo de tratamiento de los datos.

- *Anonimización y seudonimización*: Los datos de párvulos utilizados para fines estadísticos, de planificación o investigación deberán ser anonimizados o seudonimizados, eliminando toda posibilidad de identificación individual. Esta práctica se aplicará especialmente en reportes, informes de gestión y bases de datos compartidas con otros organismos.

- *Acceso restringido y diferenciado*: Los datos de niños, niñas y familias tendrán niveles de acceso diferenciados según el rol y la necesidad funcional. Solo el personal con responsabilidad directa podrá acceder a datos identificables, y todo acceso quedará registrado para garantizar trazabilidad.

- *Retención limitada*: Los datos de párvulos se conservarán únicamente por el tiempo necesario para cumplir la finalidad declarada, o por el plazo que establezca la normativa vigente. Una vez cumplido el plazo, se procederá a la eliminación segura o anonimización definitiva de los datos.

- *Protección ante intercambio interinstitucional*: Cuando JUNJI comparta datos de párvulos con MINEDUC u otros organismos del Estado, se deberá asegurar que existan convenios formales que establezcan las condiciones de uso, niveles de acceso, medidas de seguridad y prohibición de uso para fines no autorizados, en concordancia con el principio de interoperabilidad segura.

Estos lineamientos deberán integrarse de manera transversal en los cuatro ámbitos priorizados, con especial énfasis en Seguridad de los Datos y Calidad de los Datos, donde el tratamiento de información de primera infancia requiere los más altos estándares.

La implementación articulada de estos cuatro ámbitos permitirá a JUNJI avanzar desde la etapa Inactiva hacia la etapa Reactiva de gobernanza de datos, conforme a la hoja de ruta definida en el Capítulo X. Los instrumentos sugeridos en cada ámbito se detallan en el Capítulo IX, la estructura organizacional que sostendrá su implementación se define en el Capítulo VIII, y los indicadores que permitirán monitorear el avance se establecen en el Capítulo XI.

Consideraciones transversales: cumplimiento normativo y ciclo de vida de los datos

El cumplimiento normativo y el ciclo de vida de los datos son conceptos transversales a la gestión de datos, no Áreas de Conocimiento del marco DAMA-DMBOK. Su tratamiento se distribuye entre los cuatro ámbitos priorizados. La siguiente tabla traza la correspondencia entre las obligaciones normativas vigentes que aplican a JUNJI y el ámbito priorizado que las absorbe operativamente:

Obligación normativa	Ámbito de DAMA que la absorbe	Instrumento asociado
Ley 21.719 - Registro de Actividades de Tratamiento	Gobierno de Datos	RAT
Ley 21.719 - Modelo de prevención de infracciones y designación (voluntaria) del Delegado de Protección de Datos (arts. 49 y 50; art. quinto transitorio)	Gobierno de Datos	Política de Protección de Datos Personales; evaluación institucional de adopción elevada a la Vicepresidencia Ejecutiva
Ley 21.719 - Derechos ARCO-P	Seguridad de los Datos	Procedimiento ARCO-P
Ley 21.719 - Notificación de vulneraciones a APDP	Seguridad de los Datos	Protocolo de gestión de incidentes; Registro de brechas
Ley 21.719 - Licitud, consentimiento y minimización	Gobierno de Datos + Seguridad de los Datos	Política de Protección de Datos Personales
Ley 21.719 - Conservación y eliminación segura	Documentos y Contenido + Seguridad de los Datos	Tabla de Retención Documental
Ley 21.663 - Reporte de incidentes a ANCI	Seguridad de los Datos	Protocolo de gestión de incidentes
Ley 20.285 - Transparencia y acceso a información pública	Documentos y Contenido	Clasificador Institucional; Política de Gestión Documental
Ley 21.180 - Interoperabilidad[11] y regla de "solo una vez"; Ley 21.719 - Principio de coordinación y cesión entre organismos (arts. 21 y 22)	Gobierno de Datos	Mapa institucional de flujos de datos interinstitucionales; Catálogo de convenios de intercambio; Protocolo de intercambio interinstitucional
Ley 21.658 - Sistema de Transformación Digital (STD-PMG)	Gobierno de Datos	Reporte STD

El ciclo de vida de los datos —creación, uso, conservación, eliminación— también se distribuye entre los cuatro ámbitos: el Gobierno de Datos vela por la trazabilidad y titularidad a lo largo del ciclo; la Seguridad de los Datos protege el activo durante todo el ciclo; la Calidad de los Datos actúa en las etapas de uso y actualización; y Documentos y Contenido regula la conservación, retención y eliminación segura de los soportes documentales.

Este tratamiento transversal se refleja en la etiqueta *"(cumplimiento normativo)"* que acompaña a los indicadores del Capítulo XI directamente vinculados con obligaciones legales.

[11] *Sobre el alcance del término "interoperabilidad". El presente documento emplea el término en su acepción jurídico-administrativa: el deber de los órganos del Estado de intercambiar información entre sí por medios electrónicos y de no requerir a las personas datos que ya obran en poder de la Administración, conforme al principio de interoperabilidad que la Ley N°21.180 incorpora al artículo 16 bis de la Ley N°19.880. En esta acepción, la materia es transversal y se aborda operativamente desde el ámbito Gobierno de Datos, mediante los instrumentos señalados en la tabla precedente. Ello no debe confundirse con el Área de Conocimiento Integración e Interoperabilidad de Datos* (Data Integration & Interoperability*) del marco DAMA-DMBOK, de naturaleza técnica, que comprende el diseño de procesos de extracción y carga, la virtualización de datos, los servicios de interfaz, los buses de integración y la semántica compartida entre instituciones. Dicha Área supone como prerrequisito la Arquitectura de Datos y depende de otros ámbitos no priorizados en esta versión, por lo que se mantiene dentro del horizonte de incorporación progresiva declarado en el Capítulo II y en el Capítulo X.*

VIII. Estructura Organizacional para la Gobernanza de Datos

Para avanzar hacia una gobernanza institucional de los datos, JUNJI adopta un modelo federado que articula lineamientos comunes desde un equipo central, respetando la autonomía funcional y técnica de las distintas unidades. Este modelo se sustenta en el mandato institucional conferido a la Sección de Gobernanza de Datos, conforme se señala en la Introducción.

8.1. Comité de Gobernanza de Datos

Equipo directivo responsable de validar lineamientos, monitorear avances, resolver controversias y canalizar decisiones estratégicas sobre los datos institucionales.

Composición del Comité:

Rol en el Comité	Área / Cargo	Función Principal	Participación
Presidente/a	Por la designación que resuelva la Vicepresidencia Ejecutiva	Patrocina, convoca, aprueba decisiones estratégicas	Permanente
Secretaría Ejecutiva	Jefatura de la Sección de Gobernanza de Datos (Equipo Coordinador)	Coordina agenda, elabora actas, ejecuta acuerdos, da seguimiento	Permanente
Representante TI	Jefe/a Sección Tecnologías de la Información	Articula aspectos técnicos y de seguridad	Permanente
Representante Fiscalía	Fiscalía	Vela por cumplimiento normativo y asesoría jurídica	Permanente
Representante del dominio en pilotaje[12]	Propietario/a de Datos del dominio Gestión de Párvulos	Representa el dominio sustantivo en pilotaje y valida los instrumentos que se le apliquen	Permanente
Coordinador/a de Transformación Digital (CTD)	Contraparte institucional ante la Secretaría de Gobierno Digital	Asegura articulación con el Sistema de Transformación Digital (STD-PMG)	Invitado permanente
Propietarios de Datos (Data Owners)	Jefes/as de áreas dueñas de dominios críticos distintos del dominio en pilotaje	Representan sus dominios, validan lineamientos aplicables	Según agenda
Invitados/as	Encargado/a de Ciberseguridad, auditoría interna u otras áreas	Aportan en temas específicos	Según necesidad

[12] *La silla se establece por dominio y no por persona, de modo que se traslada al titular una vez formalizada su designación, sin requerir modificación del acto administrativo que constituye el Comité. Mientras subsista la asignación transitoria señalada en el apartado de Dominios de Datos y Propietarios, la ocupará la Sección de Gobernanza de Datos en su calidad de Propietario de Datos transitorio del dominio.*

Frecuencia de Reuniones:

Instancia	Frecuencia	Propósito
Comité de Gobernanza de Datos	Mensual (Fase I, primeros 6 meses) / Bimensual (resto de Fase I) / Trimestral (Fase II y Fase III)	Revisión de avances, aprobación de lineamientos, decisiones estratégicas, resolución de controversias entre áreas. Las sesiones se estructuran con agenda enfocada y materiales preparados por la Secretaría Ejecutiva
Mesa de Coordinación TI - Gobernanza	Quincenal (Fase I) / Mensual (Fase II-III)	Alineamiento técnico, revisión de políticas de seguridad, coordinación de implementaciones, seguimiento de incidentes.
Reuniones con Propietarios de Datos	Mensual o según plan piloto	Seguimiento de avances en dominios específicos, validación de instrumentos, resolución de problemas.

Funciones del Comité:

a) Aprobar políticas, lineamientos y estándares de gobernanza de datos.
b) Validar el plan de trabajo anual y priorizar iniciativas.
c) Monitorear indicadores de avance y madurez institucional.
d) Resolver controversias sobre propiedad, acceso o uso de datos entre áreas.
e) Asignar recursos y responsabilidades para la implementación.
f) Reportar avances a la alta dirección institucional.

El Comité requiere de una unidad técnica que operacionalice sus decisiones y coordine la implementación. Este rol lo cumple el Equipo Coordinador de Gobernanza de Datos.

8.2. Equipo Coordinador de Gobernanza de Datos

Unidad técnica que lidera operativamente el desarrollo del modelo, genera propuestas de lineamientos, brinda asesoría a las áreas y coordina acciones entre los distintos actores. Este rol es asumido por la **Sección de Gobernanza de Datos** del Departamento de Planificación.

Funciones del Equipo Coordinador:

a) Elaborar propuestas de políticas, lineamientos e instrumentos de gobernanza.
b) Asesorar a las áreas en la implementación de buenas prácticas de gestión de datos.
c) Coordinar con TI los aspectos técnicos y de seguridad.
d) Preparar reportes de avance e indicadores para el Comité.
e) Gestionar el catálogo de activos de datos y el glosario institucional.
f) Facilitar la capacitación y sensibilización en gobernanza de datos.
g) Actuar como secretaría ejecutiva del Comité de Gobernanza de Datos.

Tanto el Comité como el Equipo Coordinador actúan de manera transversal. Sin embargo, la gestión cotidiana de los datos recae en las áreas de gestión, a través de los Propietarios de Datos de cada dominio.

8.3. Recomendación institucional: evaluación de la designación de un(a) Delegado(a) de Protección de Datos

Con la entrada en vigencia plena de la Ley N°21.719 el 1 de diciembre de 2026, el marco normativo chileno introduce dos instrumentos que, sin ser obligatorios, constituyen la vía institucional principal para gestionar el riesgo del tratamiento de datos personales y acceder al régimen de atenuantes de responsabilidad: el modelo de prevención de infracciones (art. 49) y la figura del Delegado(a) de Protección de Datos (art. 50), cuyo nombramiento es elemento constitutivo de ese modelo.

La presente propuesta recomienda a la Vicepresidencia Ejecutiva evaluar la designación de un(a) Delegado(a) de Protección de Datos en JUNJI, sobre la base de tres consideraciones institucionales:

- **Sensibilidad de los datos que administra JUNJI:** La institución trata datos personales de niños y niñas menores de catorce años, categoría reforzada por la Ley 21.719 (art. 16 quáter), lo que eleva el estándar de diligencia exigible a la institución y agrava las sanciones aplicables en caso de infracción.

- **Gestión del riesgo administrativo personal del jefe superior del servicio:** El artículo 44 de la Ley 21.719 dispone que las infracciones al tratamiento de datos personales cometidas por el órgano público son sancionadas con multa aplicada personalmente al jefe superior del servicio, elevada al 50% de su remuneración mensual cuando el tratamiento involucre datos sensibles. La designación de un(a) Delegado(a), en el marco del modelo de prevención del art. 49, es la vía institucional que la ley reconoce para acreditar el cumplimiento diligente de los deberes de dirección y supervisión, configurando la circunstancia atenuante del artículo 36 N°5.

- **Alineamiento con estándares internacionales de gobernanza de datos:** La figura del Delegado(a) recoge la experiencia consolidada del Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Condiciones de diseño en caso de decidirse la designación. La Ley 21.719 no fija la ubicación orgánica del Delegado(a), pero establece condiciones sustantivas de ejercicio que orientan su diseño institucional:

- **Designación por la máxima autoridad (art. 50 inc. 2):** en el caso de JUNJI, corresponderá a la Vicepresidencia Ejecutiva mediante resolución exenta.

- **Funcionario de la dotación vigente (art. quinto transitorio):** la ley restringe expresamente a los órganos públicos, impidiendo la creación de un cargo externo o la contratación específica.

- **Autonomía funcional (art. 50 inc. 3):** el(la) Delegado(a) no puede recibir instrucciones sobre la forma de ejercer sus funciones. Se recomienda que dependa jerárquicamente de la Vicepresidencia Ejecutiva en calidad de asesor(a), con línea de reporte directa.

- **Ausencia de conflicto de interés (art. 50 inc. 4):** el rol es incompatible con la dependencia jerárquica de, o el ejercicio simultáneo de funciones en, áreas que decidan los fines y medios del tratamiento de datos personales. Esta condición excluye la dependencia respecto de la Sección de Gobernanza de Datos, la Sección de Tecnologías de la Información y el Departamento de Fiscalía y Asesoría Jurídica. Con las dos primeras, por definir instrumentos operativos de tratamiento; con Fiscalía, por asumir la defensa jurídica de la institución, lo que puede entrar en tensión con el deber del Delegado(a) de cooperar con la APDP y notificar vulneraciones.

- **Idoneidad y conocimientos específicos (art. 50, penúltimo inciso):** la designación debe recaer en una persona con formación acreditada en protección de datos personales.

- **Recursos y garantías (art. 50, inciso final):** el(la) Delegado(a) debe contar con los medios materiales suficientes para el desempeño de sus funciones, y con acceso irrestricto a la información necesaria sobre tratamientos, sistemas y eventuales vulneraciones.

Funciones establecidas por la ley (art. 50 in fine). En caso de designarse, corresponderán al(la) Delegado(a) las siguientes funciones, taxativamente enumeradas por la ley:

- Informar y asesorar al responsable de datos, a los terceros encargados o mandatarios y a los dependientes del responsable, respecto de las disposiciones legales y reglamentarias relativas al derecho a la protección de los datos personales y a la regulación de su tratamiento.

- Promover y participar en la política que dicte el responsable de datos respecto de la protección y el tratamiento de los datos personales.

- Supervisar el cumplimiento de la Ley 21.719 y de la política que dicte el responsable, dentro del ámbito de su competencia.

- Preocuparse de la formación permanente de las personas que participan en las operaciones de tratamiento de datos.

- Asistir a los miembros de la organización en la identificación de los riesgos asociados a la actividad de tratamiento y las medidas a adoptar para resguardar los derechos de los titulares de datos personales.

- Desarrollar un plan anual de trabajo y rendir cuenta de sus resultados.

- Absolver las consultas y solicitudes de los titulares de datos.

- Cooperar y actuar como punto de contacto de la Agencia.

Articulación con la estructura organizacional del modelo: El(la) Delegado(a) no reemplaza ni duplica los roles definidos en el modelo federado de gobernanza. Su función es de supervisión y asesoría transversal, complementaria y externa a los roles operativos (Propietario de Datos, Administrador de Datos, Custodio de Datos, Usuario de Datos). Su relación con el Comité de Gobernanza de Datos, la Sección de Tecnologías de la Información, la Sección de Gobernanza de Datos y el Departamento de Fiscalía y Asesoría Jurídica es de colaboración técnica y supervisión especializada, no de dependencia ni de línea jerárquica.

El desarrollo operativo de esta recomendación —incluyendo el análisis de viabilidad, la propuesta de perfil, la ubicación orgánica específica y el acto administrativo correspondiente— se aborda como acción priorizada en el Capítulo IX, en el ámbito de Gobierno de Datos.

8.4. Dominios de Datos y Propietarios

Bajo el modelo federado, cada área de gestión es propietaria de los datos que genera, gestiona y utiliza para cumplir sus funciones. El Propietario de Datos (Data Owner) es el responsable funcional de un dominio de datos, con autoridad para definir reglas de acceso, estándares de calidad y usos autorizados.

Dominios Críticos Identificados:

Dominio	Área Propietaria del Activo (Data Owner)	Datos Principales	Sistemas Relacionados
Gestión de Párvulos	Depto. de Planificación -Sección Gobernanza de Datos (asignación transitoria para efectos del piloto)	Datos referentes al ciclo de vida del párvulo: postulación, matrícula, asistencia y egreso. Este dominio corresponde al foco inicial del proyecto piloto de gobernanza de datos. Dado que la propiedad funcional del dominio no cuenta actualmente con un titular formalmente designado en el organigrama institucional, la Sección de Gobernanza de Datos asume transitoriamente el rol de Data Owner, en ejercicio de las funciones que le han sido conferidas para determinar roles y responsabilidades del modelo de gobernanza. Esto permite aplicar el principio de "partir por casa", validar el modelo institucional y generar aprendizajes antes de escalar a otras áreas. La operación cotidiana del dominio se distribuye en los siguientes roles operativos: la carga y actualización de datos y la coordinación con las Direcciones Regionales es asumida por una unidad operativa dependiente de la propia Sección; la administración funcional del sistema es asumida por un/a funcionario/a con experiencia técnica en la	GesparvuWeb / SIMM

		administración de plataformas institucionales; y el resguardo técnico de la infraestructura (Data Custodian) corresponde a la Sección de Tecnologías de la Información. La designación definitiva del Propietario de Datos del dominio se resolverá junto con la Nómina de Propietarios y Administradores de Datos de la Fase I, y a más tardar al inicio de la Fase II, en coherencia con las definiciones que adopte el proceso de planificación estratégica institucional en curso.	

Nota 1: *El dominio Gestión de Párvulos es el área confirmada para el piloto de gobernanza de datos (Fase II). El alcance se ampliará progresivamente a otros dominios institucionales según los resultados del piloto, los criterios que priorice el Comité de Gobernanza de Datos y la disponibilidad de recursos.*

Nota 2: *Relación con la figura del Propietario del Activo de Información. La Política de Administración de Activos V1.2 vigente en JUNJI ya establece la figura del Propietario del Activo de Información, con responsabilidades sobre inventario, clasificación por confidencialidad-integridad-disponibilidad, definición de restricciones de acceso y gestión del ciclo de vida del activo. El presente modelo unifica esta figura con la del Data Owner: se trata del mismo rol institucional, con responsabilidades ampliadas para incorporar las dimensiones semánticas, de calidad y de uso propias de la gobernanza de datos. Esta unificación evita la coexistencia de dos titularidades paralelas sobre el mismo activo y simplifica la operación en la etapa de madurez actual. La actualización de la Política de Administración de Activos para reflejar formalmente esta unificación se aborda como parte de la articulación TI-Gobernanza en Fase I (ver Capítulo IX).*

Responsabilidades por Rol:

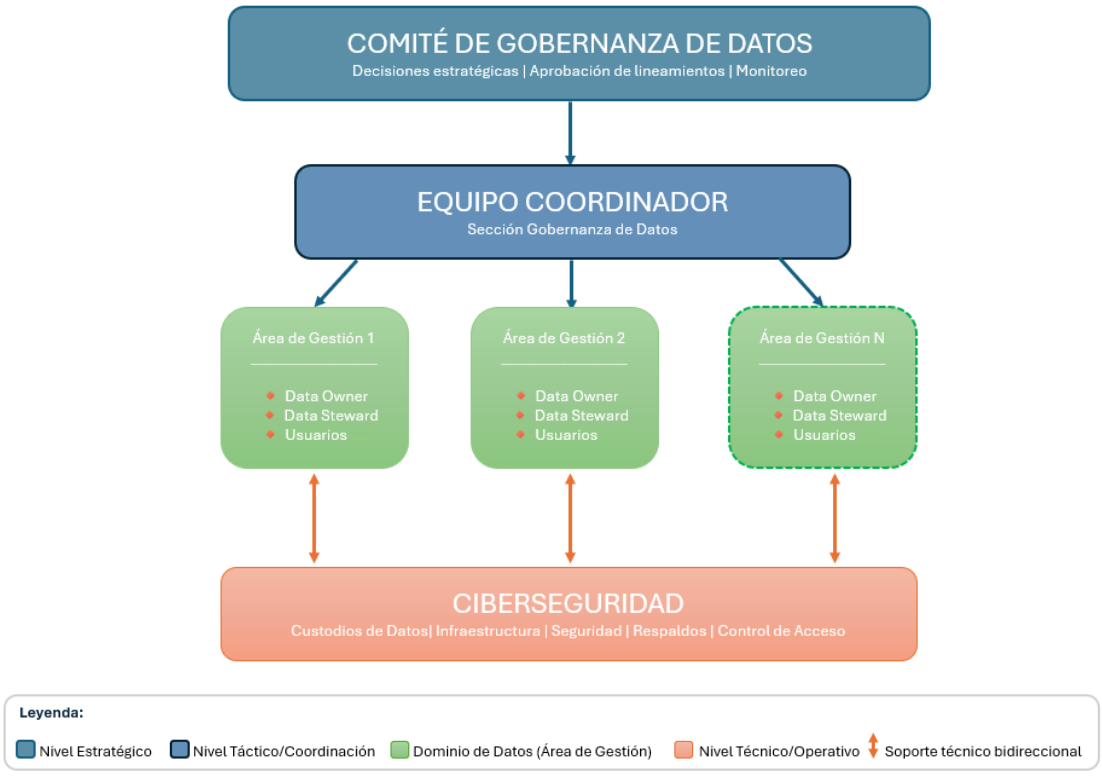
Rol	Responsabilidades
Propietario de Datos (Data Owner)	• Definir el significado y reglas de gestión de los datos de su dominio. • Autorizar accesos y usos de los datos bajo su responsabilidad. • Asegurar la calidad y actualización de los datos. • Validar los instrumentos de gobernanza aplicables a su dominio. • Mantener el inventario y la clasificación por confidencialidad-integridad-disponibilidad de los activos de su dominio (heredado de la Política de Administración de Activos). • Designar al Administrador de Datos de su área. • Participar en el Comité cuando se traten temas de su dominio.
Administrador de Datos (Data Steward)	• Gestionar la calidad de los datos en el día a día. • Documentar metadatos, reglas de validación y definiciones. • Detectar y reportar problemas de calidad o inconsistencias. • Coordinar con TI la implementación de controles. • Capacitar a usuarios de su área en buenas prácticas. • Reportar al Propietario de Datos y al Equipo Coordinador.
Custodio de Datos (Data Custodian)	• Implementar controles técnicos de acceso y seguridad. • Ejecutar respaldos y planes de recuperación. • Administrar la infraestructura donde residen los datos. • Aplicar políticas de seguridad definidas institucionalmente. • Reportar incidentes de seguridad. • Este rol es asumido por la Sección de Tecnologías de la Información, particularmente a través de su Oficina de Continuidad Operativa y Seguridad de la Información, conforme a las funciones de seguridad de la información establecidas en los artículos 72 y 74 de la Resolución Exenta N°408/2026.
Usuario de Datos	• Acceder y utilizar los datos conforme a los permisos otorgados. • Reportar problemas de calidad o acceso al Administrador de Datos. • Cumplir con las políticas y lineamientos institucionales.

	• Participar en capacitaciones de gobernanza de datos. • Proteger la confidencialidad de los datos a los que accede.

La interacción entre estos roles se representa en el siguiente esquema, que ilustra cómo opera el modelo federado en la práctica.

8.5. Modelo Federado: Esquema de Relaciones

El siguiente esquema representa la articulación entre los distintos actores bajo el modelo federado de gobernanza de datos:



Esta estructura busca asegurar una gobernanza efectiva, con participación compartida y roles diferenciados que permitan abordar de forma integral el ciclo de vida de los datos.

8.6. Consideraciones para la Implementación

- **Formalización gradual:** Durante la Fase I se constituirá el Comité y se designarán los primeros Propietarios de Datos en las áreas piloto.

- **Flexibilidad del modelo:** La estructura podrá ajustarse según los aprendizajes del piloto y las capacidades institucionales.

- **Articulación con estructuras existentes:** El Comité de Gobernanza de Datos se articulará con el Comité de Seguridad de la Información existente, evitando duplicidades. La coordinación con la agenda de gobierno digital institucional se asegura mediante la participación del/la Coordinador/a de Transformación Digital (CTD) como invitado/a permanente del Comité, según se detalla en la Sección 8.1. Esta articulación resguarda la coherencia entre las decisiones de gobernanza de datos y los compromisos del Sistema de Transformación Digital (STD-PMG) ante la Secretaría de Gobierno Digital del Ministerio de Hacienda.

  Esta articulación considera, asimismo, la condición de operador de importancia vital de la institución conforme a la Ley N°21.663, cuyos deberes reforzados son conducidos por la Sección de Tecnologías de la Información. El Comité de Gobernanza de Datos recibe, a través de la Mesa de Coordinación TI-Gobernanza, la información relevante para asegurar la coherencia entre dichos deberes y los lineamientos de gobernanza de datos, sin duplicar su gestión.

- **Designación formal:** Los Propietarios y Administradores de Datos serán designados formalmente mediante acto administrativo, estableciendo sus responsabilidades.

- **Capacitación:** Se contempla un plan de formación para los distintos roles, comenzando por el Equipo Coordinador y los Propietarios de Datos.

La efectividad de esta estructura organizacional dependerá de las decisiones estratégicas del Comité, de las coordinaciones técnicas ejecutadas por el Equipo Coordinador y de la responsabilidad operativa distribuida en cada área de gestión. Los instrumentos que sostendrán la operación de este modelo se detallan en el Capítulo IX, y la ruta de implementación se especifica en el Capítulo X.

IX. Instrumentos de Apoyo

La estructura organizacional descrita en el capítulo anterior requiere de instrumentos concretos que permitan operacionalizar los lineamientos de gobernanza de datos, en el marco de las funciones institucionales conferidas a la Sección de Gobernanza de Datos. Estos instrumentos —políticas, procedimientos, catálogos y fichas técnicas— constituyen las herramientas prácticas que guiarán el actuar institucional en cada ámbito priorizado.

A continuación, se presentan los instrumentos clave por ámbito. Algunos de ellos ya existen en la institución (especialmente en el área de seguridad), mientras que otros deberán ser desarrollados como parte de la implementación de esta propuesta.

9.1. Gobierno de Datos

Este documento constituye, una vez aprobado, la Política de Gobernanza de Datos y el Modelo Federado de Gobernanza de JUNJI (desarrollado en el Capítulo VIII). Los siguientes instrumentos complementarios operacionalizan su implementación:

Instrumento	Estado	Fase objetivo
Instrumento de autoevaluación de madurez en gobernanza de datos	No existe	Fase II
Glosario Institucional de Datos	No existe	Fase I (2025-2026)
Nómina de Propietarios y Administradores de Datos designados	No existe	Fase I (2025-2026) — se constituye junto con el Comité
Registro de Actividades de Tratamiento (RAT)	No existe	Fase I (2025-2026) — plazo forzado por entrada en vigencia plena de la Ley N°21.719 (dic. 2026). El artículo 26 de la ley remite a un reglamento que debe dictarse con posterioridad a dicha entrada en vigencia, conforme al artículo segundo transitorio. En consecuencia, el Registro se construirá durante 2026 como instrumento institucional, y su formato y contenidos se ajustarán a lo que disponga el reglamento una vez dictado.
Mapa institucional de flujos de datos interinstitucionales	No existe	Fase I (2025-2026) — versión inicial, priorizando los intercambios con MINEDUC y los requerimientos de información dirigidos a jardines infantiles
Catálogo de convenios de intercambio de datos	No existe	Fase I (2025-2026) — levantamiento en coordinación con el Departamento de Fiscalía y Asesoría Jurídica
Protocolo de intercambio interinstitucional de datos	No existe	Fase II — se desarrolla sobre la base del Mapa de flujos y en articulación con la Política de Protección de Datos Personales
Evaluación institucional para la adopción del modelo de prevención de infracciones y designación del Delegado(a) de Protección de Datos	No existe	Fase I (2025-2026) — informe técnico elaborado por la Sección de Gobernanza de Datos y elevado a la Vicepresidencia Ejecutiva, conforme a la

		recomendación del Capítulo VIII. Incluye análisis de viabilidad, propuesta de perfil, ubicación orgánica.
Catálogo de Datos Institucionales	No existe	Fase II — acotado al dominio piloto (Gestión de Párvulos); expansión institucional en Fase III
Actualización de la Política de Administración de Activos V1.2	Existente — requiere actualización	Fase I (2025-2026) — para formalizar la unificación de la figura del Propietario del Activo de Información con la del Data Owner del presente modelo. Coordinación con la Sección de Tecnologías de Información a través de la Mesa TI-Gobernanza.

9.2. Seguridad de los Datos

Instrumento	Estado	Fase objetivo
Política de Seguridad de la Información	Existente (desarrollada por la Sección de Tecnologías de la Información)	Articulación con el modelo de Gobernanza – Fase I
Procedimiento de respaldo y recuperación	Existente (desarrollada por la Sección de Tecnologías de la Información)	Articulación con el modelo de Gobernanza – Fase I
Procedimiento de Gestión de Incidentes de Seguridad de la Información	Existente (desarrollada por la Sección de Tecnologías de la Información)	Articulación con el modelo de Gobernanza – Fase I
Controles de acceso y trazabilidad	Existente (desarrollada por la Sección de Tecnologías de la Información)	Articulación con el modelo de Gobernanza – Fase I
Protocolo de gestión de incidentes (define la actuación institucional ante incidentes críticos, incluida la notificación a la APDP conforme a la Ley N°21.719 y el reporte a la ANCI en calidad de operador de importancia vital)	No existe (complementario del procedimiento de gestión de incidentes)	Articulación con el modelo de Gobernanza – Fase I
Política de Protección de Datos Personales	No existe	Fase I (2025-2026) — plazo forzado por entrada en vigencia plena de la Ley N°21.719 (dic. 2026). Constituye el fundamento normativo institucional del RAT y del Procedimiento ARCO-P. En caso de que la Vicepresidencia Ejecutiva decida adoptar el modelo de prevención de infracciones del art. 49 de la Ley 21.719, esta política incluirá el capítulo institucional que formaliza el rol, funciones, autonomía y régimen de designación del(la) Delegado(a) de Protección de Datos, conforme al art. 50 y al art. quinto transitorio.
Procedimiento para la atención de derechos ARCO-P	No existe	Fase I (2025-2026) — plazo forzado por entrada en vigencia plena de la Ley 21.719 (dic. 2026)

Nota: *Los instrumentos de Seguridad ya existentes —Política de Seguridad de la Información, Procedimiento de Respaldo y Recuperación, Procedimiento de Gestión de Incidentes y Controles de Acceso y Trazabilidad— fueron desarrollados por la Sección de Tecnologías de la Información. El trabajo de gobernanza de datos consiste en articularlos formalmente con el modelo, no en construirlos desde cero.*

9.3. Calidad de los Datos

Instrumento	Estado	Fase objetivo
Estándares de Calidad de Datos	No existe	Fase II — acotado al dominio piloto; expansión institucional en Fase III
Fichas técnicas de conjuntos de datos	No existe	Fase II — acotado al dominio piloto; expansión institucional en Fase III
Indicadores de calidad	No existe	Fase II — acotado al dominio piloto; expansión institucional en Fase III
Procedimiento de validación y corrección de datos	No existe	Fase II — acotado al dominio piloto; expansión institucional en Fase III
Tableros de monitoreo de calidad	No existe	Fase III

9.4. Documentos y Contenido

Instrumento	Estado	Fase objetivo
Clasificador institucional de documentos	Existente (desarrollada por la Sección de Gestión Estratégica, Depto. de Planificación)	Fase I — articulación con el modelo de gobernanza
Política de gestión documental	Existente (desarrollada por la Sección de Gestión Estratégica, Depto. de Planificación)	Fase II — acotado al dominio piloto; expansión institucional en Fase III
Mapa de activos documentales	No existe	Fase II — acotado al dominio piloto (Gestión de Párvulos); expansión institucional en Fase III
Tabla de Retención Documental	No existe	Fase II — acotado al dominio piloto; expansión institucional en Fase III

Estos instrumentos serán desarrollados de manera progresiva por el Equipo Coordinador de Gobernanza de Datos, en colaboración con TI, la Oficina de Gestión de Procesos y las áreas propietarias de cada dominio, conforme a la ruta de implementación por fases definida en el Capítulo X. Los instrumentos vinculados al cumplimiento de plazos legales (RAT, procedimiento ARCO-P) se priorizarán durante la Fase I; el resto se desarrollará y ampliará progresivamente conforme JUNJI avance en su madurez institucional.

X. Plan de Implementación por Fases

La implementación de esta propuesta será gradual y evolutiva, **en línea con la escala de madurez institucional definida en el Capítulo III** y considerando la capacidad operativa de JUNJI.

Fase	Período	Foco Principal	Etapa de Madurez (Capítulo III)	Meta de Madurez
Fase 0	2024	Diagnóstico y marco metodológico	Inactiva (Nivel 0)	Diagnóstico realizado — completada
Fase I	2025-2026	Diseño y preparación	Transición hacia Reactiva	Establecer fundamentos
Fase II	2027	Piloto y ajustes	Reactiva (Nivel 1)	Alcanzar nivel reactivo
Fase III	2028	Implementación ampliada	Reactiva → Proactiva (Nivel 1-2)	Consolidar nivel reactivo, avanzar a proactivo

Fase 0: Diagnóstico y Marco Metodológico (2024) — Completada

- Elaboración del diagnóstico institucional de madurez en gobernanza de datos.
- Desarrollo del marco metodológico basado en DAMA-DMBOK, documentado en el Informe de Gobernanza de Datos JUNJI (2024).
- Identificación de los cuatro ámbitos priorizados: Gobierno de Datos, Seguridad de los Datos, Calidad de los Datos y Documentos y Contenido.

Este trabajo constituye la base sobre la cual se construye la presente propuesta de políticas y lineamientos.

Fase I: Diseño y Preparación (2025-2026) — Transición hacia la Etapa Reactiva

La Fase I concentra los instrumentos cuyo plazo viene determinado por la entrada en plena vigencia de la Ley N°21.719, el 1 de diciembre de 2026. Antes de esa fecha deben quedar formalizados la Política de Protección de Datos Personales, el Registro de Actividades de Tratamiento y el Procedimiento para la atención de derechos ARCO-P, además de constituirse el Comité de Gobernanza de Datos y la Nómina de Propietarios y Administradores de Datos del dominio piloto. Dado que se trata de un plazo acotado y de fecha cierta, el seguimiento de estos instrumentos se regirá por un cronograma específico aprobado por el Comité de Gobernanza de Datos, con responsable designado por instrumento.

Productos normativos:

- Elaboración del documento de políticas y lineamientos (presente documento).
- Definición de estrategias y lineamientos de seguridad de datos.

- Elaboración y formalización de la Política de Protección de Datos Personales, con plazo forzado por la entrada en vigencia plena de la Ley N°21.719 el 1 de diciembre de 2026. Esta política dará sustento normativo al Registro de Actividades de Tratamiento y al Procedimiento ARCO-P.
- Implementación del Registro de Actividades de Tratamiento (RAT) y del Procedimiento para la atención de derechos ARCO-P, con plazo forzado por la entrada en vigencia plena de la Ley N°21.719 el 1 de diciembre de 2026.

Estructura organizacional:

- Conformación del Comité de Gobernanza de Datos.
- Constitución de la Nómina de Propietarios y Administradores de Datos designados en el dominio piloto.

Coordinación y diagnóstico:

- Reuniones con TI para acordar lineamientos conjuntos de seguridad de la información.
- Revisión de procesos críticos vinculados a datos en GesparvuWeb (Gestión de Párvulos).
- Mapeo preliminar de activos de datos institucionales.
- Elaboración del Mapa institucional de flujos de datos interinstitucionales, priorizando los intercambios con MINEDUC y los requerimientos de información dirigidos a jardines infantiles. Responsable: Equipo Coordinador de Gobernanza de Datos, con la participación de la Sección de Tecnologías de la Información y de las áreas de gestión involucradas.
- Levantamiento del Catálogo de convenios de intercambio de datos vigentes, en coordinación con Fiscalía, como insumo para el cumplimiento del artículo 22 de la Ley N°21.719 antes del 1 de diciembre de 2026.

Fase II: Piloto y Ajustes (2027) — Etapa Reactiva (Nivel 1)

- Desarrollo de un piloto institucional con aplicación acotada de los lineamientos en el sistema GesparvuWeb (Gestión de Párvulos), gestionado por la Sección de Gobernanza de Datos del Departamento de Planificación.
- Desarrollo de los instrumentos de apoyo acotados al dominio piloto: Catálogo de Datos Institucional, Estándares de Calidad de Datos, Fichas técnicas, Mapa de activos documentales y Tabla de Retención Documental (Capítulo IX).
- Generación de resultados tempranos (quick wins) que demuestren el valor de la gobernanza de datos y faciliten la adhesión de otras áreas. Evaluación del piloto, identificando aprendizajes, barreras y oportunidades de mejora.
- Ajustes a políticas, instrumentos y roles según resultados del piloto.

Fase III: Implementación Ampliada y Monitoreo (2028) — Consolidación de la Etapa Reactiva y avance hacia la Etapa Proactiva

- Implementación institucional del modelo ajustado.
- Ampliación institucional de los instrumentos desarrollados durante el piloto (Catálogo de Datos Institucional, Estándares de Calidad, entre otros) y desarrollo de nuevos instrumentos complementarios, como los tableros de monitoreo de calidad.
- Capacitación progresiva en gestión y uso de datos para funcionarios clave.
- Monitoreo periódico del avance, mediante indicadores de madurez.

Este enfoque gradual reconoce que la gobernanza de datos es un proceso de construcción continua. Cada fase genera aprendizajes que alimentan la siguiente, permitiendo ajustar el modelo a la realidad institucional y asegurar su sostenibilidad en el tiempo.

Horizonte posterior a la Fase III. El presente plan compromete metas hasta 2028. La incorporación progresiva de las restantes Áreas de Conocimiento del marco DAMA-DMBOK, declarada en el Capítulo II, constituye el horizonte de mediano y largo plazo del modelo y no lleva plazos asociados en esta versión, por cuanto su viabilidad depende de capacidades que exceden el alcance de las fases aquí definidas. Su secuenciación será propuesta por el Equipo Coordinador y resuelta por el Comité de Gobernanza de Datos en el Plan Plurianual de Gobernanza de Datos, instrumento de gestión interna revisable anualmente.

XI. Indicadores y Métricas de Seguimiento

Para asegurar el seguimiento efectivo de la implementación, se definen indicadores específicos que permitirán evaluar el avance institucional, identificar brechas y orientar las decisiones del Comité de Gobernanza de Datos.

Los indicadores se organizan en cinco grupos: cuatro asociados a los ámbitos priorizados (gobierno, seguridad, calidad y documentos) y uno de carácter transversal que mide la madurez institucional global. Para cada indicador se establecen metas diferenciadas según la fase de implementación, reconociendo que algunos aspectos -como la calidad de los datos- se abordarán con mayor profundidad a partir del piloto (Fase II).

11.1. Indicadores de Gobierno de Datos

Indicador	Fórmula / Descripción	Meta Fase I (2025-2026)	Meta Fase II (2027)	Meta Fase III (2028)
Conformación del Comité de Gobernanza de Datos	Comité constituido formalmente SI / NO	SI	Operativo, sesiones según frecuencia definida	Operativo
Reuniones del Comité realizadas	N° reuniones realizadas / N° reuniones planificadas	≥ 75%	≥ 85%	≥ 90%
Nómina de Propietarios y Administradores de los Datos designados	Nómina formalizada para el dominio piloto (Sí/No)	SI	Vigente y actualizada	Ampliada a nuevos dominios incorporados
Lineamientos institucionales aprobados	N° lineamientos formalizados	≥ 2	≥4	≥ 6
Activos de datos inventariados	N° activos identificados en el catálogo preliminar	Mapeo inicial	Catálogo del dominio piloto completo	Catálogo operativo
Registro de Actividades de Tratamiento implementado	RAT operativo y actualizado (Sí/No) – (cumplimiento normativo – Ley 21.719)	SI (antes del 1 dic. 2026)	Operativo y actualizado	Actualizado
Procedimiento ARCO-P implementado	Procedimiento formalizado y operativo (Sí/No) – (cumplimiento normativo – Ley 21.719)	SI (antes del 1 dic. 2026)	Operativo, con registro de solicitudes atendidas	Actualizado
Mapa de flujos de datos interinstitucionales	Mapa elaborado y validado por el Comité (Sí/No)	Versión inicial	Actualizado y ampliado	Operativo con revisión anual
Catálogo de convenios de intercambio de datos	Catálogo consolidado y publicado conforme al art. 22 Ley 21.719 (Sí/No) — (cumplimiento normativo)	SI (antes del 1 dic. 2026)	Vigente y actualizado mensualmente	Actualizado

11.2. Indicadores de Seguridad de los Datos

Indicador	Fórmula / Descripción	Meta Fase I (2025-2026)	Meta Fase II (2027)	Meta Fase III (2028)
Incidentes de seguridad de datos reportados	N° incidentes por período - (cumplimiento normativo — Leyes 21.663 y 21.719)	Registro activo	Registro consolidado con análisis de causas	Tendencia a la baja
Funcionarios capacitados en seguridad	N° funcionarios capacitados / Total funcionarios objetivo	Equipo central	Equipo central + funcionarios del dominio piloto	≥ 70%

Nota: *Las métricas operativas de seguridad de la información (tiempo de respuesta a incidentes, verificación de respaldos, revisión de accesos) son medidas y reportadas por la Sección de Tecnologías de la Información. La gobernanza de datos las recibe a través de la Mesa de Coordinación TI-Gobernanza, sin duplicar su medición.*

11.3. Indicadores de Calidad de los Datos

Los indicadores de calidad se medirán a partir de la Fase II, dado que su aplicación requiere contar previamente con la estructura organizacional y los instrumentos básicos definidos en la Fase I.

Indicador	Fórmula / Descripción	Meta Fase II (2027)	Meta Fase III (2028)
Dimensiones de calidad definidas	N° dimensiones con criterios y umbrales definidos	≥ 4	≥ 6
Tasa de completitud (área piloto)	Registros completos / Total registros	≥ 85%	≥ 95%
Reglas de validación implementadas	N° reglas activas en sistemas priorizados	≥ 5 reglas	≥ 15 reglas
Fichas técnicas de datos elaboradas	N° fichas técnicas documentadas	≥ 3 (piloto)	≥ 10

11.4. Indicadores de Documentos y Contenido

Indicador	Fórmula / Descripción	Meta Fase I (2025-2026)	Meta Fase II (2027)	Meta Fase III (2028)
Clasificador institucional de documentos	Clasificador aprobado y en uso (Sí/No)	Propuesta	Aprobado y en aplicación en dominio piloto	Implementado
Políticas de gestión documental formalizadas	Política formalizada y vigente (Si/No)	En elaboración	Formalizada	Vigente y actualizada

11.5. Indicadores Transversales de Madurez

Indicador	Fórmula / Descripción	Meta Fase I (2025-2026)	Meta Fase II (2027)	Meta Fase III (2028)
Nivel de madurez global	Evaluación según la curva de madurez definida en el Capítulo III (escala 0-4)	Nivel 0, en transición hacia Nivel 1	Nivel 1 (Reactivo)	Nivel 1-2 (transición a Proactivo)
Áreas piloto con gobernanza implementada	N° áreas con lineamientos aplicados	0 áreas — dominio piloto definido y preparado	1 área (Gestión de Párvulos)	Incorporación progresiva de nuevos dominios (según criterios definidos por el Comité)
Coordinación TI-Gobernanza	N° reuniones de coordinación realizadas / planificadas	≥ 75%	≥ 80%	≥ 90%

11.6. Consideraciones para la Medición

- **Frecuencia de medición:** Durante la Fase I los indicadores serán medidos semestralmente, considerando que la mayoría corresponde a hitos de constitución del modelo. Se exceptúan los indicadores asociados al cumplimiento de la Ley N°21.719 (Política de Protección de Datos Personales, Registro de Actividades de Tratamiento y Procedimiento ARCO-P), cuyo avance será revisado mensualmente hasta su implementación, conforme al cronograma específico que apruebe el Comité de Gobernanza de Datos. A partir de la Fase II, con el piloto en operación, la medición será trimestral, y podrá ajustarse a semestral en Fase III una vez estabilizado el modelo.

- **Responsable del monitoreo:** El Equipo Coordinador de Gobernanza de Datos será responsable de recopilar, consolidar y reportar los indicadores al Comité de Gobernanza de Datos.

- **Fuentes de información:** Los indicadores se alimentan de tres fuentes:
  i. Registros propios del Equipo Coordinador de Gobernanza de Datos, para los indicadores de gobierno y calidad;
  ii. Reportes de la Sección de Tecnologías de la Información, canalizados a través de la Mesa de Coordinación TI-Gobernanza, para los indicadores de seguridad; y
  iii. Reportes de la Sección de Gestión Estratégica, para los indicadores de gestión documental. La responsabilidad de consolidar y reportar al Comité recae en el Equipo Coordinador.

- **Área piloto priorizada:** Los indicadores de calidad se aplicarán inicialmente en el área confirmada: Gestión de Párvulos (GesparvuWeb y SIMM). La incorporación de nuevos dominios será priorizada por el Comité de Gobernanza de Datos según criterios de sensibilidad de los datos, disponibilidad de recursos y madurez del área.

- **Mapa de activos documentales:** El avance de este instrumento —desarrollado durante la Fase II conforme a lo establecido en el Capítulo IX— se reportará como parte del seguimiento cualitativo del piloto, sin meta cuantitativa asociada en esta primera versión del documento.

- **Ajuste de metas:** Las metas podrán ser ajustadas por el Comité de Gobernanza de Datos según los resultados del piloto y la capacidad institucional, manteniendo el principio de mejora progresiva.

- **Trazabilidad de cumplimiento normativo:** los indicadores vinculados con obligaciones legales específicas se identifican con la etiqueta *"(cumplimiento normativo)"* en su descripción, para facilitar el seguimiento agregado del avance en materia de las leyes 20.285, 21.663 y 21.719, sin necesidad de constituir un ámbito propio.

Este conjunto de indicadores representa el punto de partida para una gestión basada en evidencia. A medida que JUNJI avance en su madurez, podrán incorporarse nuevos indicadores o ajustarse las metas según los aprendizajes de cada fase.

XII. Monitoreo y Mejora Continua

La gobernanza de datos no es un proyecto con fecha de término, sino un proceso institucional permanente. Para que el modelo propuesto sea sostenible en el tiempo, es necesario establecer mecanismos formales que permitan monitorear su implementación, evaluar resultados, detectar desviaciones y realizar ajustes oportunos.

Este capítulo define el ciclo de mejora continua que regirá la gobernanza de datos en JUNJI, en el marco de las funciones institucionales de la Sección de Gobernanza de Datos, estableciendo las instancias de revisión, los mecanismos de retroalimentación y las acciones para el desarrollo progresivo de capacidades institucionales.

12.1. Ciclo de Revisión y Actualización

El modelo de gobernanza de datos operará bajo un ciclo de revisión periódica que contempla tres niveles:

Nivel	Frecuencia	Responsable	Alcance
Operativo	Semestral en Fase I, con excepción de los instrumentos con plazo legal, cuyo seguimiento es mensual hasta su implementación (ver Capítulo XI); trimestral desde Fase II	Equipo Coordinador	Revisión de indicadores, identificación de problemas, ajustes a instrumentos si fuese necesario.
Táctico	Semestral	Comité de Gobernanza de Datos	Evaluación de avances por ámbito, validación de ajustes propuestos, priorización de iniciativas.
Estratégico	Anual	Comité de Gobernanza de Datos	Revisión integral del modelo, actualización de lineamientos, definición de prioridades para el período siguiente.

Este ciclo debe asegurar que las decisiones sobre gobernanza de datos se tomen de manera informada y oportuna, anticipándose a posibles obstáculos.

12.2. Gestión de Brechas y Desviaciones

Durante la implementación surgirán brechas entre lo planificado y lo ejecutado. Para gestionarlas de manera sistemática, se establece el siguiente proceso:

1. **Identificación:** Las brechas podrán ser detectadas a través de los indicadores de seguimiento, reportes de los Propietarios de Datos o retroalimentación de usuarios.

2. **Registro:** Toda brecha identificada será documentada por el Equipo Coordinador, indicando su descripción, ámbito afectado, posibles causas y nivel de criticidad.

3. **Análisis:** El Equipo Coordinador evaluará las causas y propondrá acciones correctivas, las que serán presentadas al Comité según su nivel de impacto.

4. **Acción:** Se implementarán las medidas correctivas acordadas, asignando responsables y plazos.

5. **Verificación:** Se dará seguimiento a las acciones hasta verificar que la brecha ha sido cerrada o mitigada.

12.3. Mecanismos de Retroalimentación

Para que el modelo responda a las necesidades reales de la institución, se habilitarán canales de retroalimentación que permitan recoger la experiencia de los distintos actores:

- **Desde los Propietarios de Datos:** Reuniones periódicas con el Equipo Coordinador para reportar dificultades, proponer mejoras y validar instrumentos.

- **Desde los usuarios de datos:** Canal formal (formulario, correo institucional u otro) para reportar problemas de acceso, calidad o disponibilidad de datos.

- **Desde la Sección de Tecnologías de la Información:** Reportes de incidentes, alertas de seguridad y recomendaciones técnicas canalizadas a través de la Mesa de Coordinación TI-Gobernanza.

12.4. Desarrollo de Capacidades

La gobernanza de datos requiere competencias específicas que deben ser desarrolladas de manera progresiva, tanto en el Equipo Coordinador como en el resto de los actores del modelo. Considerando que se trata de una disciplina nueva en la institución, el desarrollo de capacidades contempla dos líneas complementarias: la formación del propio Equipo Coordinador mediante fuentes externas especializadas, y la sensibilización progresiva de los demás actores, apoyada en material de referencia y acompañamiento práctico.

Plan de capacitación diferenciado por rol:

Rol	Contenidos prioritarios	Modalidad	Fase
Equipo Coordinador	Fundamentos DAMA-DMBOK, MGDE, marco normativo (Leyes 21.719, 21.663, 21.180), gestión de calidad de datos, elaboración de instrumentos	Formación externa (autoestudio y aprendizaje aplicado durante la implementación)	Fase I y continua
Comité de Gobernanza	Marco normativo aplicable, rol del Comité, toma de decisiones basada en datos	Sesión de inducción al constituirse el Comité, con material preparado por el Equipo Coordinador.	Fase I
Propietarios y Administradores de Datos designados	Responsabilidades del rol, uso de los instrumentos del dominio piloto	Inducción práctica y acompañamiento del Equipo Coordinador durante el piloto	Fase II (dominio piloto)
Usuarios de Datos	Políticas institucionales, buenas prácticas, canales de reporte	Material de difusión y cápsulas informativas	Fase III

Transferencia de conocimiento: Se documentarán las lecciones aprendidas de cada fase para facilitar la continuidad del modelo ante cambios de personal.

Formación del Equipo Coordinador: Dado que la gobernanza de datos constituye una disciplina de reciente incorporación en la institución, la formación del Equipo Coordinador es condición habilitante para el resto del plan. Se priorizará el acceso a instancias de formación externa, redes de intercambio con otras instituciones públicas que hayan avanzado en gobernanza de datos, y el aprovechamiento de los recursos formativos disponibles a través de la Secretaría de Gobierno Digital en el marco del Sistema de Transformación Digital.

Alcance progresivo: El desarrollo de capacidades se ajustará a la capacidad operativa real del Equipo Coordinador. En las etapas iniciales se privilegiará la sensibilización mediante material de referencia y

acompañamiento práctico, por sobre actividades formativas de mayor envergadura, las que se abordarán conforme avance la madurez institucional y se consoliden las competencias internas.

12.5. Comunicación y Difusión

Para que la gobernanza de datos se instale como práctica institucional, es necesario comunicar sus avances y beneficios de manera regular:

- **Reporte anual de gobernanza de datos:** Producto de la revisión estratégica anual definida en la sección 12.1, consistente en un documento de síntesis con los principales logros, desafíos y proyecciones, dirigido a la alta dirección y disponible para consulta institucional.

- **Difusión interna:** Uso de los canales institucionales disponibles (intranet, boletines internos, plataformas de colaboración institucional y reuniones de coordinación) para informar sobre nuevos lineamientos, instrumentos disponibles y buenas prácticas.

- **Reconocimiento de avances:** Visibilizar los logros de las áreas que implementen exitosamente las prácticas de gobernanza, incentivando la adopción en otras unidades. Este reconocimiento se canalizará a través de las instancias institucionales ya existentes —sesiones del Comité de Gobernanza de Datos, reporte anual y canales de difusión interna—, sin requerir la creación de mecanismos formales adicionales en esta primera versión del modelo.

- **Difusión externa:** Los avances en gobernanza de datos serán puestos a disposición del/la Coordinador/a de Transformación Digital para su incorporación en los reportes institucionales del Sistema de Transformación Digital (STD-PMG) ante la Secretaría de Gobierno Digital, evitando duplicar esfuerzos de reportabilidad.

Estos mecanismos de monitoreo y mejora continua permitirán que la gobernanza de datos en JUNJI no dependa únicamente del impulso inicial, sino que se sostenga como una práctica institucional adaptable, capaz de responder a nuevos desafíos normativos, tecnológicos y de gestión pública. La clave está en aprender de la implementación y ajustar el modelo de manera permanente.

XIII. Consideraciones Finales

Este documento constituye un primer paso estructurado hacia una gobernanza de datos institucional en JUNJI, elaborado en ejercicio de las funciones de la Sección de Gobernanza de Datos. Responde a los desafíos identificados en el diagnóstico de 2024, se alinea con los objetivos de modernización institucional y con marcos de referencia internacionales, y da cumplimiento a las obligaciones normativas vigentes en transparencia, protección de datos personales y ciberseguridad. Su enfoque es progresivo: prioriza cuatro ámbitos —Gobierno, Seguridad y Calidad de los Datos, y Documentos y Contenido—, define una estructura organizacional bajo modelo federado y establece un plan de implementación por fases. Su éxito dependerá del compromiso transversal de los equipos y de la capacidad institucional para sostener el proceso en el tiempo.

En el corto plazo, la prioridad más urgente es la entrada en plena vigencia de la Ley N°21.719 el 1 de diciembre de 2026. Dado que JUNJI trata datos de niños y niñas —categoría sujeta a protección reforzada—, el cumplimiento de esta normativa —en particular la Política de Protección de Datos Personales, el Registro de Actividades de Tratamiento y el procedimiento de atención de derechos ARCO-P— constituye el compromiso de mayor criticidad de la Fase I. En paralelo, el documento se concibe como instrumento evolutivo: sus lineamientos deberán adaptarse a los desarrollos normativos en curso, en particular el proyecto de ley que crea el Sistema Nacional de Gestión de Datos, cuyo avance legislativo será monitoreado por el Comité de Gobernanza de Datos.

Próximos pasos. Una vez aprobado, este documento deberá formalizarse mediante el acto administrativo que corresponda, dando inicio a la ejecución de la Fase I: constitución del Comité de Gobernanza de Datos, designación de los roles operativos definidos en el Capítulo VIII (Propietarios de Datos, Administradores de Datos, Custodios) y desarrollo de los instrumentos priorizados según el Capítulo IX, incluyendo la evaluación institucional de adopción del modelo de prevención de infracciones y la eventual designación del(la) Delegado(a) de Protección de Datos.

Vigencia y actualización de referencias normativas. Las referencias contenidas en este documento a normas legales, reglamentarias e instrumentos institucionales se entienden efectuadas a las disposiciones vigentes a la fecha de su elaboración. En caso de modificación, derogación o reemplazo —incluidas la estructura orgánica institucional y los instrumentos de planificación estratégica—, las referencias se entenderán efectuadas a las disposiciones que los sustituyan, sin afectar la vigencia del presente documento. El Comité de Gobernanza de Datos será responsable de proponer oportunamente las actualizaciones que correspondan.

Vocación de permanencia. El modelo de gobernanza que este instrumento establece se concibe como una capacidad institucional permanente y no como una iniciativa asociada a un período de gestión determinado. Su continuidad se resguarda mediante la formalización por acto administrativo, la definición de la integración del Comité por cargo y no por persona, la incorporación de sus compromisos al Sistema de Transformación Digital y la cláusula de actualización de referencias normativas contenida en este documento. El fortalecimiento del nivel y de la ubicación orgánica de la función de gobernanza de datos

se declara como línea de trabajo de mediano plazo, sujeta a las definiciones que adopte la autoridad institucional en el marco de sus atribuciones.

XIV. Anexo 1: Matriz de Conexión entre Políticas TI y ámbitos de Gobernanza de Datos

La presente matriz establece la articulación entre las políticas de seguridad de la información vigentes en JUNJI y los ámbitos de gobernanza de datos definidos en el marco DAMA-DMBOK.

Esta conexión permite:

- Aprovechar los instrumentos normativos existentes como base para la gobernanza de datos.
- Evitar duplicidades y asegurar coherencia entre las políticas de TI y los lineamientos de datos.
- Priorizar la revisión y actualización de políticas según su relevancia para la gobernanza de datos.

Criterios de Prioridad

Rol en el modelo	Significado
Estructura	Define el marco normativo del ámbito. Sin esta política, el ámbito no puede operarse.
Operativo	Aplica controles concretos que sostienen el ámbito. Su implementación cotidiana es lo que hace efectivo el modelo.
De apoyo	Aporta al ámbito de forma complementaria o transversal. Su ausencia no bloquea el modelo.

Matriz de Conexión

N°	Documentos de Políticas TI	Ámbito DAMA Relacionado	Conexión con Gobernanza de Datos JUNJI	Rol en el modelo
1	JUNJI_A.5.1.1_Política de Seguridad_DGR	- Seguridad de los Datos - Gobierno de Datos	Proporciona principios y estructura para todo el sistema de seguridad; establece roles clave (usuarios, responsables, comité).	Estructura

2	Política de Control de Acceso Lógico V1.3	- Seguridad de los Datos	Limita y audita el acceso a sistemas con datos institucionales. Adicionalmente, establece un modelo institucional de gobernanza de accesos con roles diferenciados: TI ejecuta, Jefaturas solicitan altas y bajas, Propietario del Activo autoriza accesos privilegiados junto con el Encargado de Seguridad de la Información (sección 4.11), y la Unidad de Seguimiento GDP reporta trimestralmente las desvinculaciones (sección 3.4)	Estructura
3	Política de Administración de Activos V1.2	- Gobierno de Datos - Seguridad de los Datos	Es clave para el mapa de activos de datos, roles de propiedad y trazabilidad. Adicionalmente, la sección 3.4 obliga al Propietario a clasificar los activos según su grado de confidencialidad, integridad y disponibilidad (CID), constituyendo el pilar de clasificación por sensibilidad que sustenta los controles diferenciados de Seguridad de los Datos.	Estructura
4	Procedimiento Cambio de Funciones o Desvinculación V1.2	- Seguridad de los Datos - Gobierno de Datos	Controla accesos y transiciones seguras en cambios de rol o salida del personal.	Operativo
5	Política de Continuidad de SSI V1.2	- Seguridad de los Datos - Gobierno de Datos	Respalda la disponibilidad y recuperación frente a incidentes o contingencias.	Operativo
6	Política de Dispositivos Móviles V1.2	- Seguridad de los Datos	Regula el uso, resguardo, configuración y trazabilidad de datos móviles, en línea con normas ISO 27001.	Operativo
7	Política de Seguridad Física y del Ambiente V1.2	- Seguridad de los Datos	Protege físicamente los sistemas que contienen o procesan datos institucionales.	Operativo
8	Política de Seguridad de Redes V1.2	- Seguridad de los Datos	Establece los controles de red que protegen la información en tránsito (ISO 27001 A.13 "Seguridad de las Comunicaciones"): controles de red, mecanismos de seguridad de los servicios de red y segregación en segmentos con firewalls, VPN y gateways. Sustenta la protección perimetral que exige la Ley N°21.663 de Ciberseguridad.	Operativo
9	Política de Trabajo Remoto V1	- Seguridad de los Datos	Regula el acceso remoto y las condiciones de trabajo desde fuera de la red institucional, previniendo filtraciones o exposiciones. Es transversal a todos los funcionarios que operan en modalidad flexible, y la sección 4.8 obliga expresamente a mantener confidencialidad sobre datos personales y/o sensibles "de los funcionarios o funcionarias, como de los niños y niñas que asisten a nuestros jardines infantiles" — invocando directamente las obligaciones reforzadas de la Ley N°21.719.	Operativo
10	Procedimiento de Respaldo y Recuperación V1.3	- Seguridad de los Datos	Regula copias de seguridad y restauración, clave para asegurar disponibilidad y trazabilidad.	Operativo
11	Procedimiento Reutilización o Eliminación de Equipos V1.3	- Seguridad de los Datos	Garantiza eliminación segura de información sensible en activos dados de baja.	Operativo
12	Procedimiento Gestión de Incidentes de Seguridad de la Información V1.4 (JUNJI_A.16.1)	- Seguridad de los Datos	Define el flujo de detección, análisis, clasificación, resolución y cierre de incidentes de seguridad. Utiliza la matriz de clasificación del CSIRT gubernamental. Requiere actualización menor para armonizarse con la Política General V8 (2025) y con Leyes 21.663 y 21.719.	Operativo
13	Política de Seguridad de Desarrollo V1.2	- Seguridad de los Datos	Establece los lineamientos de desarrollo seguro (Secure SDLC) para sistemas que procesan, almacenan	Operativo

			y transmiten información institucional, cubriendo los controles ISO 27001 A.14 sobre adquisición, desarrollo y mantenimiento de sistemas. La sección 4.4 exige considerar explícitamente "la sensibilidad de los datos que el sistema procesará, almacenará y transmitirá" al establecer entornos de desarrollo seguros.	
14	Política de uso correcto del correo electrónico e internet (1096)	- Seguridad de los Datos	Regula el uso institucional del correo e internet como vectores de exposición de información. Establece prohibiciones sobre reenvío de datos sensibles, uso personal y navegación de riesgo. Complementa Control de Acceso Lógico en el flanco de canales de comunicación cotidianos.	Operativo
15	Procedimiento para la Gestión de Perfiles de Navegación y Acceso a Internet (1096)	- Seguridad de los Datos	Operacionaliza el perfilamiento de acceso a internet por rol/función, gestionando el nivel de exposición del usuario según las necesidades de su cargo. Instrumento derivado de la política 1096 anterior.	Operativo
16	Política de Seguridad de Operaciones V1.2	- Seguridad de los Datos	Cubre los controles ISO 27001 A.12 sobre separación de ambientes de desarrollo/prueba/producción, código malicioso, registro y monitoreo de eventos, sincronización de relojes y gestión de vulnerabilidades técnicas.	Operativo
17	Política de Revisiones SSI V1.2	- Gobierno de Datos - Seguridad de los Datos	Define auditorías internas, ciclos de revisión y validación de políticas y procedimientos.	De apoyo
18	Política de Concientización V1.2	- Seguridad de los Datos - Gobierno de Datos	Establece el programa institucional de concientización, educación y formación en Seguridad de la Información (nombre completo del documento). Los contenidos programáticos definidos en la sección 4.1 son íntegramente de seguridad: SGSI, CID, manejo de incidentes, escritorios limpios, control de acceso físico. Aporta secundariamente al ámbito Gobierno de Datos por su función de gestión del cambio cultural, condición habilitante para operacionalizar cualquier lineamiento de gobernanza.	De apoyo
19	Política para la Relación con Proveedores V1	- Gobierno de Datos - Seguridad de los Datos	Establece medidas para asegurar que terceros cumplan con los estándares de resguardo de datos. La Ley 21.719 obliga expresamente a que los encargados/mandantes (JUNJI) se hagan responsables del tratamiento realizado por proveedores.	De apoyo

Análisis de la Matriz

Distribución por ámbito DAMA:

- **Seguridad de los Datos:** 19 políticas conectadas. Es el ámbito con mayor cobertura actual, lo que facilita la implementación de lineamientos de seguridad sobre una base normativa sólida.

- **Gobierno de Datos:** 7 políticas conectadas. Principalmente a través de roles, comités y gestión de activos. Requiere el desarrollo de instrumentos específicos —modelo federado, catálogo de datos, glosario institucional, RAT— para operacionalizar el ámbito.

- **Calidad de los Datos:** 0 políticas conectadas. La revisión de contenido confirmó que ninguna política TI vigente aporta controles sobre atributos de calidad del dato (completitud, exactitud, consistencia, oportunidad, unicidad). Esto refuerza la necesidad de desarrollar instrumentos propios en Fase II.

- **Documentos y Contenido:** 0 políticas TI directamente conectadas. No obstante, la Sección de Gestión Estratégica del Departamento de Planificación se encuentra desarrollando el Clasificador Institucional de Documentos y la Política de Gestión Documental, instrumentos que se articularán con el modelo de gobernanza conforme a lo establecido en el Capítulo IX.

Nota: *La concentración de políticas en el ámbito de Seguridad de los Datos refleja la madurez institucional acumulada en este subdominio y* ***no representa carga de trabajo para la Fase I****. La gran mayoría de estas políticas están vigentes y no requieren intervención por parte de la Sección de Gobernanza de Datos; se articulan con el modelo por vía de reconocimiento, no de reelaboración. Los instrumentos que efectivamente requieren desarrollo o actualización en Fase I se detallan en el Capítulo IX y en el Capítulo X, e incluyen principalmente la Política de Protección de Datos Personales, el Registro de Actividades de Tratamiento, el Procedimiento ARCO-P y el Protocolo de Gestión de Incidentes.*

Esta matriz refleja el estado de las políticas de seguridad de la información vigentes al momento de elaboración del presente documento, identificadas por su versión. Deberá ser actualizada por el Equipo Coordinador de Gobernanza de Datos cuando la Sección de Tecnologías de la Información emita nuevas versiones o incorpore nuevos instrumentos.