UNIVERSIDAD DE TARAPACÁ
ARICA – CHILE

PROMULGA ACUERDO N°35 DEL CONSEJO UNIVERSITARIO DE LA UNIVERSIDAD DE TARAPACÁ, QUE APRUEBA EL MODELO GOBERNANZAS DE DATOS DE LA UNIVERSIDAD DE TARAPACÁ.

DECRETO EXENTO Nº 00.645/2026.

Arica, 16 de junio de 2026.

Con esta fecha, la Rectoría de la Universidad de Tarapacá, ha expedido el siguiente decreto:

VISTOS:

Lo dispuesto en el DFL. N°150, de 11 de diciembre de 1981, del Ex Ministerio de Educación Pública, que Crea la Universidad de Tarapacá; D.F.L. N° 16 de 27 de septiembre de 2023 del Ministerio de Educación; DFL Nº1/19.653 del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; Ley N°19.880, que establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado; Resolución Nº 36, de 2024 de la Contraloría General de la República y sus modificaciones; Resolución Exenta Universitaria CONTRAL. Nº001/2002, de 14 de enero de 2002, Resolución Exenta Universitaria CONTRAL N°001/2025, de marzo de 2025; los antecedentes adjuntos y las facultades que me confiere el citado D.F.L. N° 16, en relación con el Decreto Exento Universitario Nº00. 943/2025, de julio 29 de 2025 y Decreto TRA Nº 335/9/2025, tomado de razón el 02 de junio de 2025.

CONSIDERANDO:

Que, la Universidad de Tarapacá es una entidad autónoma, funcionalmente descentralizada, dotada de personalidad jurídica y patrimonio propio, que se relaciona con el Presidente de la República a través del Ministerio de Educación, y que mediante el DFL N°16, publicado en el Diario Oficial con fecha 11 de julio de 2024, se aprobó su nuevo Estatuto en conformidad con el Título II de la Ley N°21.094 sobre Universidades Estatales, el cual entrará en vigencia transcurridos doce meses desde su publicación, estableciendo un régimen de continuidad institucional que dispone la mantención de las unidades académicas y administrativas, de las autoridades y cargos vigentes, así como de la normativa interna, en todo aquello que no resulte incompatible con el nuevo marco estatutario, mientras se implementan las adecuaciones correspondientes.

Que, el artículo 11 del DFL 16 señala que el gobierno de la universidad será ejercido a través de los siguientes órganos superiores: Consejo Superior, Rector y Consejo Universitario.

Que, el Consejo Universitario es el órgano colegiado representativo de la comunidad universitaria, encargado de ejercer funciones resolutivas en las materias relativas al quehacer académico e institucional de la Universidad de Tarapacá, y dentro de sus funciones consagradas en el artículo 28 del DFL 16, en su letra l) se encuentra: *"Aprobar o pronunciarse sobre toda otra materia académica e institucional que se señale expresamente en este Estatuto".*

Que, en sesión ordinaria N°14, el Consejo Universitario aprobó por unanimidad de los consejeros presentes, aprobar el Modelo Gobernanzas de Datos de la Universidad de Tarapacá.

Que, atendido lo manifestado en sesión ordinaria N°14 de 05 de junio de 2026 del Consejo Universitario de la Universidad de Tarapacá.

DECRETO:

1.- Promúlguese el acuerdo N°35 adoptado en Sesión Ordinaria N°14 del Consejo Universitario, celebrada el 05 de junio de 2026, que señala:

"ACUERDO N° 35

Los Consejeros y Consejeras Universitarios presentes; Presidente Dr. Emilio Rodríguez Ponce; Sra. Mónica Navarrete Álvarez; Sra. Carmen Araneda Guirrimán; Sr. Emilio Ulloa Valenzuela; Sr. Marcos Halty Carmona; Sr. Álvaro Cortínez Pontoni; Sr. Edgar Estupiñán Pulido; Sra. Pilar Mazuela Águila; Sr. Carlos Mondaca Rojas; Sr. Fabián Pinazo Reyes; Sra. Soledad Córdovez Sánchez; Sr. Giovanny Bazaes Pinto y Srta. Samirah Ardiles Cortés; **ACUERDAN APROBAR, POR UNANIMIDAD, EL MODELO GOBERNANZA DE DATOS DE LA UNIVERSIDAD DE TARAPACÁ".**

Lo anterior, conforme a lo expuesto por don Mauricio Arriagada Benítez, Director de Gestión Digital y Transparencia de la Universidad de Tarapacá.

UNIVERSIDAD DE TARAPACÁ | DGDT Dirección de Gestión Digital y Transparencia

Política General de Gobernanza de Datos Universidad de Tarapacá

Elaborado por: Dirección de Gestión Digital y Transparencia Arica, 27 de enero de 2026

Índice general

1 **Introducción** 2

1.1 Declaración Institucional ... 3

1.2 Principios rectores ... 4

1.3 Objetivo ... 5

1.4 Alcance de la Política General de Gobernanza de Datos ... 5

2 **Modelo Institucional de Gobernanza de Datos y Asignación de Roles** 6

2.1 Modelo de Componentes de la Gobernanza de Datos ... 8

3 **Desarrollo de la Política** 10

3.1 Estructura de Gobernanza ... 10

3.2 Inventario y Tipología de Datos Institucionales ... 11

3.3 Gestión del Ciclo de Vida y Clasificación de los Datos Institucionales 12

3.4 Calidad de Datos ... 13

3.5 Metadatos, catálogo y linaje ... 14

3.6 Interoperabilidad, APIs y datos abiertos ... 15

3.7 Riesgos, seguridad y privacidad por diseño ... 16

3.8 Datos para investigación (I+D) ... 16

3.9 Terceros y contratos ... 17

3.10 Medición, madurez y mejora continua ... 17

4 **Mecanismos de Difusión y Capacitación** 19

5 **Cumplimiento y Revisión** 21

6 **Incumplimiento y Sanciones** 22

7 **Glosario de Términos** 23

8 **Términos Abreviados** 27

Índice de figuras

3.1 Ciclo de vida.....13

Índice de tablas

Versión de Cambios

Versión	Fecha	Descripción del Cambio	Autor
1.1	21/01/2026	Creación de la política (basada en propuesta PRAGMA 2023)	Mauricio Arriagada

1. Introducción

La Política General de Gobernanza de Datos de la Universidad de Tarapacá se constituye como un instrumento de gobernanza que posiciona a la institución en un nivel de excelencia respecto al manejo de activos de información en el sistema de educación superior chileno. En este respecto, el documento no solo reconoce los datos como un activo estratégico para el cumplimiento de la misión académica y de investigación, sino que establece un marco de gobernanza federado y coordinado que se alinea con los más altos estándares internacionales como DAMA-DMBOK e ISO/IEC 38505-1. Esta aproximación sistémica demuestra una madurez institucional significativa, integrando la seguridad de la información, la privacidad por diseño y la ética en el uso de tecnologías emergentes como la inteligencia artificial.

Desde la perspectiva del aseguramiento de la calidad y los estándares de la Comisión Nacional de Acreditación (CNA) de nivel de excelencia, esta política representa un avance sustantivo al transitar desde una gestión reactiva hacia una cultura de datos basada en la evidencia y la autorregulación. La definición clara de niveles estratégico, táctico y operativo, junto con la creación del Comité Institucional de Datos (CID) y roles específicos como el Chief Data Officer (CDO) y los Propietarios de los datos, asegura una trazabilidad y rendición de cuentas que es propia de instituciones con niveles de excelencia en su gestión institucional. En este nivel estratégico se sugiere solamente reseñar más explícitamente la articulación entre esta política con el Sistema de Dirección Estratégica, el Sistema Integrado de Gestión de la Información Institucional y el Sistema Integrado de Gestión del Aseguramiento de la Calidad. Esto pues la integración sistémica de estos marcos asegura que la gobernanza de datos actúe como el soporte transversal que dota de integridad, confiabilidad y oportunidad a la información institucional, facilitando demostrar que el flujo de datos alimenta de manera consistente los procesos de autoevaluación y la toma de decisiones estratégicas (nivel 3).

Su implementación será progresiva y medible, con métricas y niveles de madurez, y contemplará acciones de capacitación, mejora continua y revisión periódica de lineamientos, de modo de incorporar aprendizaje institucional y cambios regulatorios o tecnológicos relevantes.

En este contexto, se vuelve necesario definir lineamientos claros en materia de Gobernanza de datos de acuerdo al marco normativo vigente, a saber:

- Ley chilena sobre protección de datos personales (vigente y reformas), y su reglamentación.
- Ley N° 20.285, de Acceso a la Información Pública.
- Ley N° 21.180, de Transformación Digital del Estado, y lineamientos de Gobierno Digital.
- Ley Marco de Ciberseguridad y normativa técnica asociada.
- Normas, instrucciones y dictámenes de la Contraloría General de la República (CGR) y del Consejo para la Transparencia (CPLT).
- Estándares y buenas prácticas: DAMA-DMBOK2; ISO/IEC 38505-1 (gobernanza de datos); ISO/IEC 27001 y 27002 (SGSI); ISO/IEC 27701 (PIMS); principios FAIR para datos de investigación.

1.1. Declaración Institucional

La presente Política General de Gobernanza de Datos de la Universidad de Tarapacá constituye un instrumento normativo institucional de carácter transversal, destinado a establecer el marco estratégico, organizacional y operativo para la gestión y gobernanza de los datos como activos institucionales.

Esta política ha sido elaborada por la Dirección de Gestión Digital y Transparencia (DGDT), en su rol de órgano técnico especializado, en conjunto con la Dirección de Calidad Institucional y será aprobada mediante el acto administrativo correspondiente dictado por la autoridad superior competente, conforme a la normativa interna vigente.

La Política General de Gobernanza de Datos es de cumplimiento obligatorio para todas las unidades académicas y administrativas de la Universidad de Tarapacá, sus autoridades, funcionarios/as, académicos/as, estudiantes y terceros que traten datos institucionales, sin perjuicio de las responsabilidades específicas que establezcan otras normativas internas y la legislación aplicable.

1.2. Principios rectores

Los siguientes principios establecen el marco ético, legal y operativo que guía el tratamiento de los datos en toda la Universidad de Tarapacá. Deben integrarse desde el diseño de procesos, sistemas, contratos y proyectos, incluida la analítica avanzada y el uso de inteligencia artificial, y sirven como criterio para resolver tensiones entre objetivos institucionales, cumplimiento normativo y resguardo de derechos. Toda norma, procedimiento o excepción deberá interpretarse a la luz de estos principios.

- **Valor y propósito**: los datos son un activo institucional; su tratamiento debe responder a objetivos legítimos universitarios.
- **Legalidad y licitud**: todo tratamiento se sustenta en base jurídica y principios de protección de datos.
- **Calidad e integridad**: precisión, completitud, consistencia y trazabilidad durante todo el ciclo de vida.
- **Privacidad y seguridad por diseño**: salvaguardas técnicas y organizativas incorporadas desde el origen.
- **Transparencia y rendición de cuentas**: documentación, trazabilidad de decisiones y métricas.
- **Minimización y proporcionalidad**: solo los datos necesarios, durante el tiempo necesario.
- **Interoperabilidad y apertura responsable**: promoción de datos abiertos conforme a la ley, con anonimización y evaluación de riesgos.
- **Ética y no discriminación: uso responsable, incluyendo IA y analítica avanzada**, evitando sesgos y afectaciones indebidas.

1.3. Objetivo

Establecer el marco institucional de gobernanza de datos de la Universidad de Tarapacá, alineado con la normativa chilena y con estándares internacionales (DAMA-DMBOK, ISO/IEC 38505-1, ISO/IEC 27001/27701), para maximizar el valor de los datos, asegurar su uso ético y responsable, y fortalecer la toma de decisiones basada en evidencia.

1.4. Alcance de la Política General de Gobernanza de Datos

Aplica a todos los datos generados, recibidos o administrados por la UTA, en sus procesos académicos, de investigación, administrativos y de extensión, independientemente del soporte o sistema. Incluye datos personales y no personales, de estudiantes, funcionarios/as, académicos/as, egresados/as, postulantes, proveedores, visitantes y terceros.

2. Modelo Institucional de Gobernanza de Datos y Asignación de Roles

El Modelo Institucional de Gobernanza de Datos define la distribución de decisiones, responsabilidades y mecanismos de control sobre los datos de la Universidad de Tarapacá, estableciendo una estructura organizada en tres niveles complementarios: estratégico, táctico y operativo. Este enfoque asegura la trazabilidad de las decisiones, la rendición de cuentas y la coordinación transversal entre unidades académicas, administrativas y tecnológicas.

El nivel estratégico está representado por el Comité Institucional de Datos (CID), responsable de la definición de lineamientos, la priorización de dominios de datos críticos, la gestión de riesgos estratégicos y la revisión de indicadores de desempeño y madurez del gobierno de datos. El CID es presidido por la autoridad superior que Rectoría determine y actúa como instancia máxima de dirección y resolución en la materia.

El nivel táctico se articula a través de los consejos o instancias de dominio de datos, conformados por los Propietarios de datos y Administradores de datos correspondientes, los cuales tienen por función operacionalizar los lineamientos definidos a nivel estratégico, resolver definiciones de negocio, estándares, calidad y uso de los datos, y canalizar necesidades o conflictos hacia el CID cuando corresponda.

El nivel operativo recae en los roles responsables de la gestión cotidiana de los datos y de la infraestructura tecnológica que los soporta, asegurando su disponibilidad, calidad, seguridad y uso conforme a la normativa institucional.

Este modelo se alinea y articula con los principios y buenas prácticas del Sistema de Gestión de Seguridad de la Información definidos en la norma ISO/IEC 27001 y del Sistema de Gestión de la Privacidad conforme a ISO/IEC 27701, constituyendo un marco compatible y evolutivo para su implementación progresiva, sin perjuicio de los niveles de madurez o certificación que la Institución defina alcanzar, resguardando en todo momento la

independencia funcional del Delegado/a de Protección de Datos (DPO) en su rol de supervisión del cumplimiento normativo en materia de protección de datos personales.

El propósito del modelo es clarificar de manera explícita quién toma decisiones sobre los datos, bajo qué criterios y con qué responsabilidades, incluyendo aspectos relativos a estándares, acceso y uso, calidad, apertura y compartición, seguridad y privacidad. Asimismo, define los mecanismos de escalamiento y resolución de conflictos entre unidades, y los instrumentos para la medición de resultados mediante indicadores clave de desempeño (KPIs) y niveles de madurez.

La asignación formal de los roles de gobernanza de datos se realizará mediante decreto o resolución institucional, incorporando principios de mínimo privilegio, segregación de funciones, y mecanismos de supletoria y continuidad operativa. El modelo es de aplicación transversal a todos los dominios de datos y sistemas institucionales, incluyendo aquellos provistos en modalidad de nube y gestionados por terceros, y será actualizado conforme evolucione la estructura organizacional de la Universidad o el marco normativo aplicable.

Roles definidos del modelo:

- **Comité Institucional de Datos (CID)**: Órgano directivo responsable de aprobar lineamientos de gobernanza de datos, priorizar dominios críticos, gestionar riesgos estratégicos y revisar indicadores de desempeño y madurez.

- **Director/a de datos / Dirección de Datos (en la DGDT)**: Responsable de implementar la presente política, coordinar el modelo de gobernanza, gestionar el portafolio institucional de datos, los catálogos, y los modelos de calidad y madurez.

- Delegado/a de Protección de Datos (DPO): Rol independiente encargado de supervisar el cumplimiento de la normativa de protección de datos personales, asesorar a la institución y gestionar la atención de los derechos de los titulares.

- **Propietario/a del dato**: Autoridad responsable de un dominio de datos específico (por ejemplo, estudiantes, recursos humanos o finanzas), encargada de definir reglas de negocio, prioridades y criterios de uso.

- **Administrador/a de datos**: Responsable de velar por la calidad, los metadatos y el linaje de los datos en su dominio, actuando como enlace entre las unidades usuarias y los sistemas de información.

- **Custodio/a**: Unidad tecnológica, generalmente la Dirección de Tecnologías de la Información u otra que corresponda, responsable de asegurar la disponibilidad, seguridad, respaldo y continuidad operativa de los datos y sistemas.

- **Usuarios/as autorizados/as**: Personas que acceden y tratan datos institucionales conforme a perfiles definidos, principios de mínimo privilegio y a lo establecido en esta política y sus procedimientos asociados.

2.1. Modelo de Componentes de la Gobernanza de Datos

El Gobierno de Datos de la Universidad de Tarapacá se estructura en un conjunto de componentes interrelacionados que aseguran una gestión integral, coherente y sostenible de los datos institucionales. Estos componentes orientan la implementación operativa de la presente política y permiten su articulación con otros sistemas de gestión institucional.

Los componentes del modelo de la Gobernanza de Datos son los siguientes:

a) **Principios y marco ético-legal**, que orientan el tratamiento lícito, proporcional, transparente y responsable de los datos.

b) **Estructura de gobierno y roles**, que define responsabilidades, niveles de decisión y mecanismos de coordinación institucional.

c) **Ciclo de vida y clasificación de los datos**, que regula su creación, uso, conservación y eliminación segura.

d) **Calidad de los datos**, que establece dimensiones, métricas y mecanismos de mejora continua.

e) **Metadatos, catálogo y linaje**, que permiten la trazabilidad, reutilización y comprensión de los activos de datos.

f) **Interoperabilidad, APIs y datos abiertos**, que promueven el intercambio seguro y estandarizado de información.

g) **Riesgos, seguridad y privacidad por diseño**, integrados al Sistema de Gestión de Seguridad de la Información y a la protección de datos personales.

h) **Datos para investigación, innovación y analítica avanzada**, conforme a principios FAIR, ética y normativa aplicable.

i) **Gestión de terceros y contratos**, que regula el acceso y tratamiento de datos por parte de proveedores y colaboradores externos.

j) **Medición, madurez y mejora continua**, que permite evaluar el desempeño del gobierno de datos y orientar decisiones estratégicas.

Cada componente deberá contar con lineamientos operativos, responsables definidos y métricas asociadas, conforme a lo establecido en la presente política y sus instrumentos complementarios.

3. Desarrollo de la Política

3.1. Estructura de Gobernanza

Esta sección define la arquitectura operativa de la gobernanza de datos de la Universidad de Tarapacá, estableciendo las instancias que la componen, su composición, quórum y periodicidad, así como los mecanismos de delegación, coordinación y escalamiento de decisiones. Asimismo, identifica los principales artefactos que se generan en el marco de la gobernanza de datos, tales como actas, estándares, catálogos, resoluciones y hojas de ruta.

La estructura considera su articulación con la arquitectura organizacional, la seguridad de la información y la continuidad operativa, definiendo criterios de priorización que orientan la ejecución de iniciativas y el uso eficiente de los recursos institucionales. El modelo es de carácter federado, con coordinación central a cargo de la Dirección de Gestión Digital y Transparencia, en su rol de CDO institucional, con el propósito de evitar duplicidades, asegurar la interoperabilidad y mantener la trazabilidad de las decisiones y el cumplimiento normativo mediante el tablero de seguimiento del Comité Institucional de Datos.

La gobernanza de datos se organiza en dominios institucionales, entre los cuales se consideran, al menos, los siguientes: Estudiantes, Académico, Investigación, Personas (Recursos Humanos), Finanzas, Infraestructura y Vinculación con el Medio, sin perjuicio de otros que puedan definirse conforme a la evolución institucional.

Para cada dominio se conformarán Consejos de Dominio, como instancias de carácter táctico integradas por los propietarios de los datos y los administradores de los datos, responsables de abordar materias relativas a calidad de datos, definiciones de negocio, resolución de duplicidades y adopción de estándares.

Adicionalmente, se establece un Foro de Arquitectura y Datos, coordinado por la DGDT, encargado de revisar y armonizar modelos de datos, criterios de interoperabilidad (incluidas APIs), estándares técnicos y aspectos de seguridad de la información.

3.2. Inventario y Tipología de Datos Institucionales

Para efectos de la aplicación de la presente política, la Universidad de Tarapacá reconoce, sin carácter exhaustivo, las siguientes categorías de datos institucionales:

- **Datos académicos y estudiantiles**, incluyendo información de admisión, matrícula, trayectoria académica, evaluación, titulación y egreso.
- **Datos de personas y recursos humanos**, relativos a funcionarios/as, académicos/as y prestadores de servicios.
- **Datos financieros y presupuestarios**, asociados a la gestión económica, contable y patrimonial de la Universidad.
- **Datos de investigación, innovación y creación**, incluyendo datos primarios, secundarios, resultados, metadatos y repositorios científicos.
- **Datos de gestión administrativa y documental**, incluidos expedientes, actos administrativos y registros institucionales.
- **Datos de infraestructura, equipamiento y tecnologías de la información**, incluyendo activos tecnológicos y sistemas de información.
- **Datos de vinculación con el medio e internacionalización**, relativos a convenios, proyectos y actividades institucionales.
- **Datos de biblioteca, recursos digitales y patrimonio documental**, conforme a la normativa aplicable.

Cada categoría deberá ser asociada a uno o más dominios de datos, con un/a propietario de dato responsable, y su tratamiento deberá ajustarse a la clasificación, base legal y finalidades institucionales definidas.

3.3. Gestión del Ciclo de Vida y Clasificación de los Datos Institucionales

Esta sección establece los lineamientos mediante los cuales la Universidad de Tarapacá gestiona cada activo de datos a lo largo de todo su ciclo de vida, desde su creación o captura hasta su

eliminación segura, asegurando coherencia operativa entre las distintas unidades y el cumplimiento del marco normativo y regulatorio vigente.

El ciclo de vida de los datos define puntos de control obligatorios asociados, al menos, a la captura lícita, la calidad, el acceso, el uso y la compartición, el archivo, la conservación y la eliminación segura de la información. Dichos controles permiten resguardar la integridad, disponibilidad, confidencialidad y trazabilidad de los datos durante todo su tratamiento.

Complementariamente, la clasificación de los datos asigna categorías de sensibilidad y criticidad que determinan las salvaguardas técnicas y organizativas aplicables, los plazos de retención y los requisitos de anonimización o seudonimización, cuando corresponda. Estas reglas son de aplicación transversal a todos los sistemas institucionales, tanto en infraestructura propia como en servicios en la nube, incluyendo repositorios institucionales, y se articulan con el Procedimiento de Conservación y Destrucción de Información y con la gestión documental institucional.

Toda excepción a las reglas de ciclo de vida o clasificación deberá contar con una base legal debidamente fundada, la aprobación del Comité Institucional de Datos y su correspondiente registro documental.

Ciclo de vida de los datos:

- **Ciclo de vida**:



Figura 3.1. Ciclo de vida.

- **Clasificación (mínima)**:
  - Público/Abierto
  - Interno
  - Confidencial
  - Dato Personal
  - Dato Personal Sensible
  - Restringido Crítico.

- **Reglas**:
  - Etiquetado obligatorio
  - Retención definida
  - Controles de acceso,
  - Registros de tratamiento Anonimización cuando corresponda y eliminación segura conforme al *Procedimiento de Conservación y Destrucción de Información* institucional.

3.4. Calidad de Datos

Esta sección define el marco para asegurar que los datos institucionales cumplan requisitos medibles de calidad, coherentes con el uso previsto y el riesgo asociado. Establece estándares por dominio, reglas de negocio y umbrales (tolerancias) que habilitan controles preventivos, detectivos y correctivos a lo largo del ciclo de vida. La DGDT/CDO fija metodología y tablero; el CID aprueba criterios y prioriza remediación; los Propietarios de datos definen reglas y criticidad; los Administradores de datos perfilan, monitorean y gestionan incidencias; los Custodios (DGDT) implementan controles técnicos y trazabilidad. Se incluyen prácticas como perfilamiento de datos, gestión de incidencias con SLA/OLA, y criterios de aceptación para analítica/IA y datos abiertos, con reporte periódico al CID.

En términos operativos, todo conjunto de datos institucional considerado crítico o destinado a interoperabilidad, analítica avanzada, inteligencia artificial o publicación como dato abierto deberá contar con reglas de calidad formalmente definidas, métricas asociadas y responsables asignados. Ningún dato podrá ser utilizado para fines estratégicos, de reporte institucional o toma de decisiones automatizada si no cumple con los umbrales mínimos de calidad establecidos para su dominio. Las desviaciones relevantes deberán registrarse como incidencias, contar con un plan de remediación aprobado por el Propietario del datos correspondiente y ser monitoreadas hasta su cierre, conforme a los acuerdos de nivel de servicio definidos y a los criterios de priorización establecidos por el Comité Institucional de Datos.

3.5. Metadatos, catálogo y linaje

Esta sección establece el marco para describir y gobernar los activos de datos mediante metadatos estandarizados, un catálogo institucional y mapas de linaje. Su propósito es facilitar el descubrimiento y la reutilización, asegurar interoperabilidad, habilitar el análisis de impacto ante cambios y demostrar cumplimiento normativo. Todo activo (dataset, API, reporte, modelo/algoritmo) deberá contar con metadatos mínimos obligatorios: propietario del dato, administrador del datos, finalidad, base legal cuando corresponda, clasificación y sensibilidad, calidad esperada/KPIs, fuentes, controles y política de conservación. El catálogo actuará como registro maestro con versionamiento y trazabilidad de cambios; el linaje documentará orígenes, transformaciones y destinos a lo largo de pipelines/ETL/ELT. La DGDT/CDO define estándares y taxonomías; los propietarios/administradores de datos mantienen y validan metadatos; DGDT implementa conectores y automatiza su captura, resguardando auditoría y seguridad. A considerar:

- Catálogo institucional de datos y activos analíticos (datasets, reportes, APIs, algoritmos), con glosario de negocio y mapas de linaje.
- Control de versiones, responsables y fecha de actualización.
- Integración con repositorios de investigación y datos abiertos conforme corresponda.

3.6. Interoperabilidad, APIs y datos abiertos

Esta sección define las reglas para compartir e intercambiar datos de forma segura, estandarizada y trazable, tanto al interior de la UTA como con organismos públicos, socios académicos y proveedores. Se establecen criterios técnicos y de gobernanza para el diseño

y operación de APIs (seguridad, versionado, documentación, pruebas, SLA y gestión de cambios), así como lineamientos para la apertura responsable de datos conforme al marco legal chileno (priorización, anonimización y licenciamiento). La interoperabilidad se sustenta en modelos canónicos, glosarios y metadatos comunes, evitando duplicidades, promoviendo el principio "once only" y asegurando consistencia semántica entre sistemas. La DGDT/CDO define estándares y gobierno del ciclo de APIs/datasets; DGDT implementa la plataforma y controles; y los propietarios/administradores de datos validan esquemas, usos y publicaciones, resguardando privacidad y seguridad.

- Estándares para diseño de APIs (seguridad, versionamiento, pruebas, documentación) y acuerdos de intercambio con terceros.
- Datos abiertos: priorización, formatos reutilizables, metadatos, licencias; exclusiones por confidencialidad o presencia de datos personales; anonimización o agregación según riesgos.
- Integración con lineamientos de Gobierno Digital y Transparencia Activa.

3.7. Riesgos, seguridad y privacidad por diseño

Esta sección establece el enfoque integral de gestión de riesgos para el tratamiento de datos en la UTA, articulando seguridad de la información y privacidad desde el diseño y por defecto. Define cómo identificar, evaluar, tratar y monitorear riesgos técnicos, legales, operacionales y reputacionales; cómo incorporar salvaguardas proporcionales en procesos, sistemas y contratos; y cómo operar la prevención, detección y respuesta ante incidentes. Se debe considerar exigencias regulatorias nacionales en ciberseguridad y protección de datos, donde se debe cumplir:

- Medidas técnicas y organizativas (control de acceso, cifrado, respaldo, continuidad, logging, pruebas de seguridad, gestión de identidades).
- Coordinación con la normativa de ciberseguridad nacional.

3.8. Datos para investigación (I+D)

Esta sección establece los lineamientos para el tratamiento y la gestión de datos en actividades de investigación científica, desarrollo tecnológico e innovación en la Universidad de Tarapacá, resguardando un equilibrio adecuado entre apertura, reproducibilidad y generación de valor, con el cumplimiento de principios éticos, legales y de protección de los derechos de los titulares de datos.

Se definen los criterios para la planificación y ejecución de proyectos de investigación mediante Planes de Gestión de Datos (PGD), alineados con los principios FAIR, así como las bases jurídicas aplicables, el uso de consentimiento informado cuando corresponda y las salvaguardas específicas para el tratamiento de datos personales, datos sensibles y datos relativos a poblaciones o contextos vulnerables, incluyendo transferencias nacionales e internacionales.

La política deberá articular la coordinación entre los equipos de investigación, los Comités Ético-Científicos (CEC), la Dirección de Gestión Digital y Transparencia en su rol de CDO institucional, el Delegado/a de Protección de Datos y las unidades tecnológicas

pertinentes mediante un reglamento o protocolo específico de gestión de datos de investigación, por elaborar, asegurando la existencia de un instrumento jurídico que respalde la operación declarada. En este marco, se establecen criterios para la publicación, embargo, preservación y reutilización de los datos de investigación, así como para la aplicación de técnicas de anonimización o seudonimización y el acceso controlado a través de repositorios institucionales o federados, conforme a la normativa chilena vigente y a las buenas prácticas internacionales en ciencia abierta y gobernanza de datos.

3.9. Terceros y contratos

Esta sección regula la relación de la UTA con terceros que tratan o acceden a datos institucionales, encargados y corresponsables del tratamiento, proveedores de nube y software, integradores, socios académicos, laboratorios y otros prestadores, y define exigencias contractuales y de control para proteger la información y los derechos de los titulares. Establece criterios de debida diligencia y evaluación de riesgos previos a la contratación; fija cláusulas mínimas obligatorias (instrucciones de tratamiento, confidencialidad, medidas técnicas y organizativas, gestión de subencargados, ubicación/transferencias internacionales, notificación y gestión de brechas, derecho de auditoría, niveles de servicio y continuidad, plan de salida y devolución/eliminación de datos). Todo intercambio de datos con terceros debe documentarse mediante contrato o anexo de protección de datos (DPA), contar con base legal y, cuando corresponda, una autorización del CID.

3.10. Medición, madurez y mejora continua

Esta sección establece el marco mediante el cual la Universidad de Tarapacá evalúa de forma sistemática el desempeño de su gobernanza de datos y asegura su mejora continua. Para ello, se combinan un modelo institucional de madurez, objetivos y métricas por dominio de datos, revisiones periódicas del Comité Institucional de Datos y procesos de auditoría interna y externa, orientados a verificar la eficacia y sostenibilidad del modelo.

La gestión de la mejora continua se basa en ciclos PDCA (planificar–hacer–verificar–actuar), incorporando mecanismos de detección temprana de brechas, acciones correctivas y preventivas, y ejercicios de comparación y aprendizaje (benchmarking) con marcos de referencia reconocidos, tales como DAMA-DMBOK e ISO/IEC 38505-1.

Los indicadores de desempeño abarcarán, al menos, la calidad y cobertura del catálogo y del linaje de datos; la interoperabilidad y operación de APIs; la protección de la privacidad y la seguridad de la información; la atención de derechos de los titulares; la gestión de incidentes; y el valor y nivel de uso de los datos para fines institucionales. Los resultados serán consolidados en un tablero institucional, con responsables claramente identificados y trazabilidad de las decisiones, sirviendo de base para la priorización de iniciativas y la asignación de recursos del plan anual de gobernanza de datos.

Asimismo, se promoverá la transparencia y la rendición de cuentas mediante reportes ejecutivos periódicos a Rectoría y la publicación de métricas no sensibles, conforme a la normativa vigente.

Elementos del modelo de medición:

- Modelo de madurez de gobernanza de datos con niveles progresivos (1–5).
- OKR y KPI anuales por dominio de datos.
- Revisiones trimestrales por el Comité Institucional de Datos.
- Auditorías internas y externas.
- Planes de mejora continua derivados de los resultados.

4. Mecanismos de Difusión y Capacitación

La Universidad de Tarapacá establecerá y mantendrá mecanismos sistemáticos de difusión y capacitación destinados a asegurar la adecuada comprensión, adopción y cumplimiento de la presente Política General de Gobernanza de Datos en todos los estamentos institucionales. Dichos mecanismos tienen por finalidad desarrollar competencias acordes a los distintos roles y responsabilidades, promoviendo una aplicación coherente y consistente de los principios, lineamientos y procedimientos asociados al gobierno de datos.

La difusión de la política se realizará mediante un plan de comunicación interna permanente, coordinado por la Dirección de Gestión Digital y Transparencia (DGDT), en su rol de CDO institucional, con el apoyo de la Direcciones de Calidad Institucional y de Admisión y Comunicaciones Estratégicas. Este plan contemplará, al menos, la publicación y actualización de contenidos en la intranet institucional, la elaboración y distribución de guías operativas, plantillas, documentos de apoyo y preguntas frecuentes (FAQs), así como comunicaciones dirigidas a públicos específicos cuando corresponda.

La capacitación se estructurará a través de un plan anual de formación, definido por perfiles y funciones, que considerará como públicos destinatarios a las autoridades universitarias; Propietario de datos, Administrador de datos y Custodio de datos; académicos y académicas; funcionarios y funcionarias; investigadores e investigadoras; y, cuando aplique, proveedores y terceros que traten datos institucionales. El plan establecerá objetivos de aprendizaje diferenciados según rol, orientados al conocimiento normativo, la correcta aplicación de los lineamientos en el puesto de trabajo y el cumplimiento de los procesos de gobernanza de datos.

Las modalidades de capacitación podrán incluir instancias de inducción institucional, cursos en modalidad e-learning a través de plataformas oficiales, talleres prácticos presenciales o virtuales, acciones de micro-learning y cápsulas formativas breves, de acuerdo con la naturaleza del contenido y el perfil de los participantes. Se definirá una frecuencia mínima de ejecución para cada modalidad y perfil, así como los mecanismos de respaldo y evidencia, tales como registros de asistencia, aprobaciones en plataformas de aprendizaje institucional y certificaciones cuando corresponda.

El proceso de capacitación incorporará criterios de evaluación orientados a medir el nivel de conocimiento adquirido, la aplicación efectiva de los contenidos en el desempeño laboral y el grado de cumplimiento de los procedimientos asociados a la gobernanza de datos. Asimismo, se definirán métricas de efectividad que permitan evaluar el impacto de estas acciones, incluyendo, entre otras, cobertura de participación, tasa de aprobación, tiempos de respuesta en procesos asociados a derechos de los titulares y reducción de incidentes o incumplimientos evitados.

Complementariamente, la Universidad desarrollará materiales y campañas periódicas de concienciación orientadas a fortalecer una cultura institucional de uso responsable de los datos, abordando temáticas como protección de datos personales, seguridad de la información, datos abiertos, ética de los datos y uso responsable de la analítica avanzada e inteligencia artificial.

5. Cumplimiento y Revisión

La presente Política General de Gobernanza de Datos será objeto de revisión periódica al menos una vez cada doce (12) meses, con el propósito de asegurar su vigencia, coherencia normativa y

alineación con la estrategia institucional, el marco regulatorio y las buenas prácticas internacionales.

La revisión será coordinada por la Dirección de Gestión Digital y Transparencia, en conjunto con el Comité Institucional de Datos y las instancias de aseguramiento de la calidad institucional.

Adicionalmente, la política deberá ser revisada de manera extraordinaria cuando concurran cambios normativos relevantes, incidentes graves de seguridad o privacidad, modificaciones sustantivas en los sistemas de información institucionales, o instrucciones de la autoridad superior.

6. Incumplimiento y Sanciones

El incumplimiento de la presente política dará lugar a las medidas disciplinarias establecidas en el Estatuto Administrativo, así como en las ordenanzas académicas y estudiantiles, en virtud de las infracciones a los deberes establecidos en dichas normativas. Lo anterior es sin perjuicio de la aplicación de los protocolos institucionales vinculados a la Ley Nº 21.369, la Ley Karin u otras normativas equivalentes que resulten pertinentes, cuando corresponda.

Asimismo, las personas contratadas como prestadores de servicios a honorarios deberán considerar como infracción a los deberes establecidos en sus respectivos contratos el incumplimiento de la presente política, lo que dará lugar a las sanciones contempladas en dichos contratos.

7. Glosario de Términos

Activo: Todo elemento lógico o físico, componente de hardware, equipamiento o sistema relacionado con la información, que permita su generación, almacenamiento, soporte, envío o intercambio, sea a otros órganos de la Administración del Estado o con personas naturales o jurídicas.

Activo de Información: Datos o información cuyo tratamiento es esencial para el funcionamiento y desarrollo del órgano de la Administración del Estado que lo utiliza, genera, almacena, envía o intercambia, y que deben ser protegidos en su confidencialidad, integridad, disponibilidad u otros factores de importancia.

API´s: Conjunto de reglas y mecanismos que permite que distintos sistemas o aplicaciones se comuniquen e intercambien datos o funcionalidades de forma segura y estandarizada, sin necesidad de conocer la implementación interna del otro sistema.

Ciberseguridad y Seguridad de la Información: Conjunto de acciones, políticas, medidas preventivas y reactivas destinadas a la prevención, mitigación, manejo, respuesta y estudio de las amenazas y riesgos de incidentes de seguridad, a la reducción de sus efectos y el daño causado; antes, durante y después de su ocurrencia; respecto de los activos y activos de información y la continuidad de servicios, con el fin de proteger, preservar y restablecer la

confidencialidad, integridad y disponibilidad de aquellos y de las plataformas electrónicas de los órganos de la Administración del Estado, aumentando su resiliencia en el tiempo.

Confidencialidad: Atributo de los activos y los activos de información que asegura que estos sean conocidos y accedidos exclusivamente por quienes están autorizados para ello.

Disponibilidad: Atributo de los activos y activos de información, relativo a su accesibilidad y utilización a requerimiento de una entidad o proceso autorizado.

Evaluación de Riesgo: Proceso consistente en la comparación de los niveles de riesgo encontrados contra los criterios de riesgo prestablecidos (si es que han sido establecidos por la institución) considerando el balance entre los beneficios potenciales y resultados adversos, para posteriormente ordenar y priorizar mediante un ranking los riesgos analizados.

Gestión de Riesgo: Proceso estructurado y proactivo por el cual se identifican, evalúan, controlan y tratan los riesgos derivados de una o más amenazas determinadas.

Gobernanza de Datos (Estratégico): Se centra en la propiedad de los datos, políticas, seguridad, cumplimiento normativo y definición de reglas. Define las estructuras organizativas y asegura la calidad y el cumplimiento.

Incidente de Seguridad: Todo evento de seguridad o una serie de ellos, de carácter indeseado o inesperado, que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas informáticos, los activos y activos de información, datos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y que puedan afectar al normal funcionamiento de los mismos.

Integridad: Atributo de los activos y activos de información relativo a la exactitud, autenticidad y completitud de los mismos.

Mapas de linaje de datos: Documentación trazable que describe el origen, transformaciones y destinos de los datos a lo largo de su ciclo de vida, permitiendo análisis de impacto, control de calidad, auditoría y cumplimiento.

OLA (Operational Level Agreement): Acuerdo operativo interno que establece los niveles de servicio y responsabilidades entre unidades internas, necesarios para cumplir los compromisos definidos en un SLA.

Plataforma electrónica (en adelante también "plataforma"): Software o conjunto de software, datos e infraestructura tecnológica que sustenta procesos o procedimientos.

Principios FAIR: Conjunto de principios que establecen que los datos deben ser localizables, accesibles, interoperables y reutilizables, mediante metadatos estandarizados, identificadores persistentes, formatos abiertos y condiciones claras de acceso y uso, resguardando el cumplimiento normativo.

Principio "Once Only": Principio según el cual los datos deben capturarse y mantenerse una sola vez en su fuente oficial, siendo reutilizados mediante interoperabilidad segura y trazable, evitando duplicidades y reprocesos.

Proceso: Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un fin determinado.

Riesgo: Efecto de la incertidumbre sobre los activos de información y los objetivos de una entidad, habitualmente expresado en relación a las consecuencias de un evento o incidente de seguridad y su probabilidad de ocurrencia.

Sanción: Consecuencia jurídica de naturaleza administrativa, civil o penal derivada del incumplimiento de un deber.

Seguridad de la Información: Proceso encargado de asegurar y proteger los recursos de un

sistema de información para que sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, preservando la Integridad, Confidencialidad y Disponibilidad.

Sistema informático: Conjunto de componentes lógicos y físicos que, interactuando entre sí, permiten que su totalidad o una parte de ellos, realicen la función para la cual fueron diseñados.

SLA (Service Level Agreement): Acuerdo formal que define los niveles de servicio comprometidos, incluyendo tiempos de respuesta, disponibilidad, calidad y responsabilidades, entre una unidad proveedora y sus usuarios o clientes internos/externos.

Terceras partes: Persona u organismo ajeno a la relación directa establecida entre dos partes principales. Para estos efectos, se entenderá como terceras partes, entre otros a los proveedores de servicios y de red, los proveedores de productos de software y servicios de información, outsourcing de instalaciones y operaciones, servicios de asesoría de seguridad y auditores externos.

Usuarios(as): Personas naturales o sus apoderados(as), y los(as) representantes de las personas jurídicas o entidades y agrupaciones sin personalidad jurídica que actúan como interesados(as) en un procedimiento administrativo, así como los(as) funcionarios(as) que acceden a las plataformas electrónicas que soportan procedimientos administrativos o procesos relacionados con estos.

8. Términos Abreviados

API: Interfaz de Programación de Aplicaciones (Application Programming Interface).

DPO: Data Protection Officer, en español Delegado de Protección de Datos (DPD)

CPLT: Consejo para la Transparencia

CGR: Contraloría General de la República

UTA: Universidad de Tarapacá

IA: Inteligencia Artificial

CID: Comité Institucional de Datos

CDO: Chief Data Officer, en español Director de Datos

DGDT: Dirección de Gestión Digital y Transparencia

DCI: Dirección de Calidad Institucional

DACE: Dirección de Admisión y Comunicaciones Estratégicas

ETL: Extract, Transform, Load, en español Extraer, Transformar y Cargar.

CEC: Comité Ético y Científico

KPI: Key Performance Indicator, en español Indicador Clave de Desempeño

2.- Oficialícese El Modelo Gobernanzas de Datos de la Universidad de Tarapacá, contenido en documento adjunto, compuesto de treinta y dos (32) páginas, rubricadas por el Secretario General de la Universidad".

3.- Publíquese en el sistema informático conforme lo señalado en el art.7 de la Ley N° 20.285 de 2008, del Ministerio Secretaría General de la Presidencia, sobre Acceso a la información pública.

Anótese, y remítase a la Contraloría de la Universidad, para su control y registro. Comuníquese una vez tramitado totalmente el acto.

UNIVERSIDAD DE TARAPACA SECRETARIO GENERAL DE LA UNIVERSIDAD ARICA CHILE

DINO RAMIREZ HUANCA
Secretario General de la Universidad

UNIVERSIDAD DE TARAPACA RECTOR (S) ARICA

JORGE BERNAL PERALTA
Rector (S)

JBP.DRH.cdg

UNIVERSIDAD DE TARAPACA CONTRALORIA ARICA

07 JUL 2026

UNIVERSIDAD DE TARAPACÁ
ARICA – CHILE

CERTIFICADO DE ACUERDO
CONSEJO UNIVERSITARIO

Que, el ministro de fe que suscribe da fe que en sesión ordinaria N° 14, celebrada el 05 de junio de 2026, el Consejo Universitario de la Universidad de Tarapacá, adoptó el siguiente acuerdo:

"ACUERDO N° 35

Los Consejeros y Consejeras Universitarios presentes; Presidente Dr. Jorge Bernal Peralta; Sra. Mónica Navarrete Álvarez, Sra. Carmen Araneda Guirrimán, Sr. Emilio Ulloa Valenzuela, Sr. Marcos Halty Carmona, Sr. Álvaro Cortínez Pontoni, Sr. Edgar Estupiñán Pulido, Sra. Pilar Mazuela Águila, Sr. Carlos Mondaca Rojas, Sr. Fabián Pinazo Reyes, Sr. Soledad Cordovez Sánchez, Sr. Giovanny Bazaes Pinto y Srta. Samirah Ardiles Cortés; **ACUERDAN APROBAR, POR UNANIMIDAD, EL MODELO GOBERNANZAS DE DATOS DE LA UNIVERSIDAD DE TARAPACÁ.**

Lo anterior, conforme a lo expuesto don Mauricio Arriagada Benítez, Director de Gestión Digital y Transparencia de la Universidad de Tarapacá.

DOY FE

UNIVERSIDAD DE TARAPACÁ SECRETARIO GENERAL DE LA UNIVERSIDAD ARICA - CHILE

DINO RAMÍREZ HUANCA
SECRETARIO GENERAL DE LA UNIVERSIDAD

UNIVERSIDAD DE TARAPACÁ
Universidad del Estado

DGDT
Dirección de Gestión
Digital y Transparencia

Política General de Gobernanza de Datos Universidad de Tarapacá

Elaborado por: Dirección de Gestión Digital y Transparencia

Arica, 27 de enero de 2026

UNIVERSIDAD DE TARAPACÁ
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

Índice general

1 Introducción **2**

1.1 Declaración Institucional 3

1.2 Principios rectores 4

1.3 Objetivo 5

1.4 Alcance de la Política General de Gobernanza de Datos 5

2 Modelo Institucional de Gobernanza de Datos y Asignación de Roles **6**

2.1 Modelo de Componentes de la Gobernanza de Datos 8

3 Desarrollo de la Política **10**

3.1 Estructura de Gobernanza 10

3.2 Inventario y Tipología de Datos Institucionales 11

3.3 Gestión del Ciclo de Vida y Clasificación de los Datos Institucionales 12

3.4 Calidad de Datos 13

3.5 Metadatos, catálogo y linaje 14

3.6 Interoperabilidad, APIs y datos abiertos 15

3.7 Riesgos, seguridad y privacidad por diseño 16

3.8 Datos para investigación (I+D) 16

3.9 Terceros y contratos 17

UNIVERSIDAD DE TARAPACA
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

3.10 Medición, madurez y mejora continua 17

4 Mecanismos de Difusión y Capacitación **19**

5 Cumplimiento y Revisión **21**

6 Incumplimiento y Sanciones **22**

7 Glosario de Términos **23**

8 Términos Abreviados **27**

UNIVERSIDAD DE TARAPACÁ
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

Índice de figuras

3.1 Ciclo de vida. 13

UNIVERSIDAD DE TARAPACA
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

Índice de tablas

UNIVERSIDAD DE TARAPACA
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

Versión de Cambios

Versión	Fecha	Descripción del Cambio	Autor
1.1	21/01/2026	Creación de la política (basada en propuesta PRAGMA 2023)	Mauricio Arriagada

UNIVERSIDAD DE TARAPACÁ
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

1. Introducción

La Política General de Gobernanza de Datos de la Universidad de Tarapacá se constituye como un instrumento de gobernanza que posiciona a la institución en un nivel de excelencia respecto al manejo de activos de información en el sistema de educación superior chileno. En este respecto, el documento no solo reconoce los datos como un activo estratégico para el cumplimiento de la misión académica y de investigación, sino que establece un marco de gobernanza federado y coordinado que se alinea con los más altos estándares internacionales como DAMA-DMBOK e ISO/IEC 38505-1. Esta aproximación sistémica demuestra una madurez institucional significativa, integrando la seguridad de la información, la privacidad por diseño y la ética en el uso de tecnologías emergentes como la inteligencia artificial.

Desde la perspectiva del aseguramiento de la calidad y los estándares de la Comisión Nacional de Acreditación (CNA) de nivel de excelencia, esta política representa un avance sustantivo al transitar desde una gestión reactiva hacia una cultura de datos basada en la evidencia y la autorregulación. La definición clara de niveles estratégico, táctico y operativo, junto con la creación del Comité Institucional de Datos (CID) y roles específicos como el Chief Data Officer (CDO) y los Propietarios de los datos, asegura una trazabilidad y rendición de cuentas que es propia de instituciones con niveles de excelencia en su gestión institucional. En este nivel estratégico se sugiere solamente reseñar más explícitamente la articulación entre esta política con el Sistema de Dirección Estratégica, el Sistema Integrado de Gestión de la Información Institucional y el Sistema Integrado de Gestión del Aseguramiento de la Calidad. Esto pues la integración sistémica de estos marcos asegura que la gobernanza de datos actúe como el soporte transversal que dota de integridad, confiabilidad y oportunidad a la información institucional, facilitando demostrar que el flujo de datos alimenta de manera consistente los procesos de autoevaluación y la toma de decisiones estratégicas (nivel 3).

Su implementación será progresiva y medible, con métricas y niveles de madurez, y contemplará acciones de capacitación, mejora continua y revisión

UNIVERSIDAD DE TARAPACÁ
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

periódica de lineamientos, de modo de incorporar aprendizaje institucional y cambios regulatorios o tecnológicos relevantes.

En este contexto, se vuelve necesario definir lineamientos claros en materia de Gobernanza de datos de acuerdo al marco normativo vigente, a saber:

- Ley chilena sobre protección de datos personales (vigente y reformas), y su reglamentación.
- Ley N° 20.285, de Acceso a la Información Pública.
- Ley N° 21.180, de Transformación Digital del Estado, y lineamientos de Gobierno Digital.
- Ley Marco de Ciberseguridad y normativa técnica asociada.
- Normas, instrucciones y dictámenes de la Contraloría General de la República (CGR) y del Consejo para la Transparencia (CPLT).
- Estándares y buenas prácticas: DAMA-DMBOK2; ISO/IEC 38505-1 (gobernanza de datos); ISO/IEC 27001 y 27002 (SGSI); ISO/IEC 27701 (PIMS); principios FAIR para datos de investigación.

1.1. Declaración Institucional

La presente Política General de Gobernanza de Datos de la Universidad de Tarapacá constituye un instrumento normativo institucional de carácter transversal, destinado a establecer el marco estratégico, organizacional y operativo para la gestión y gobernanza de los datos como activos institucionales.

Esta política ha sido elaborada por la Dirección de Gestión Digital y Transparencia (DGDT), en su rol de órgano técnico especializado, en conjunto con la Dirección de Calidad Institucional y será aprobada mediante el acto administrativo correspondiente dictado por la autoridad superior competente, conforme a la normativa interna vigente.

La Política General de Gobernanza de Datos es de cumplimiento obligatorio para todas las unidades académicas y administrativas de la

UNIVERSIDAD DE TARAPACA SECRETARIO GENERAL DE LA UNIVERSIDAD ARICA - CHILE

Universidad de Tarapacá, sus autoridades, funcionarios/as, académicos/as, estudiantes y terceros que traten datos institucionales, sin perjuicio de las responsabilidades específicas que establezcan otras normativas internas y la legislación aplicable.

1.2. Principios rectores

Los siguientes principios establecen el marco ético, legal y operativo que guía el tratamiento de los datos en toda la Universidad de Tarapacá. Deben integrarse desde el diseño de procesos, sistemas, contratos y proyectos, incluida la analítica avanzada y el uso de inteligencia artificial, y sirven como criterio para resolver tensiones entre objetivos institucionales, cumplimiento normativo y resguardo de derechos. Toda norma, procedimiento o excepción deberá interpretarse a la luz de estos principios.

- **Valor y propósito**: los datos son un activo institucional; su tratamiento debe responder a objetivos legítimos universitarios.
- **Legalidad y licitud**: todo tratamiento se sustenta en base jurídica y principios de protección de datos.
- **Calidad e integridad**: precisión, completitud, consistencia y trazabilidad durante todo el ciclo de vida.
- **Privacidad y seguridad por diseño**: salvaguardas técnicas y organizativas incorporadas desde el origen.
- **Transparencia y rendición de cuentas**: documentación, trazabilidad de decisiones y métricas.
- **Minimización y proporcionalidad**: solo los datos necesarios, durante el tiempo necesario.
- **Interoperabilidad y apertura responsable**: promoción de datos abiertos conforme a la ley, con anonimización y evaluación de riesgos.
- **Ética y no discriminación: uso responsable, incluyendo IA y analítica avanzada**, evitando sesgos y afectaciones indebidas.

UNIVERSIDAD DE TARAPACÁ SECRETARIO GENERAL DE LA UNIVERSIDAD ARICA - CHILE

1.3. Objetivo

Establecer el marco institucional de gobernanza de datos de la Universidad de Tarapacá, alineado con la normativa chilena y con estándares internacionales (DAMA-DMBOK, ISO/IEC 38505-1, ISO/IEC 27001/27701), para maximizar el valor de los datos, asegurar su uso ético y responsable, y fortalecer la toma de decisiones basada en evidencia.

1.4. Alcance de la Política General de Gobernanza de Datos

Aplica a todos los datos generados, recibidos o administrados por la UTA, en sus procesos académicos, de investigación, administrativos y de extensión, independientemente del soporte o sistema. Incluye datos personales y no personales, de estudiantes, funcionarios/as, académicos/as, egresados/as, postulantes, proveedores, visitantes y terceros.

UNIVERSIDAD DE TARAPACA
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

2. Modelo Institucional de Gobernanza de Datos y Asignación de Roles

El Modelo Institucional de Gobernanza de Datos define la distribución de decisiones, responsabilidades y mecanismos de control sobre los datos de la Universidad de Tarapacá, estableciendo una estructura organizada en tres niveles complementarios: estratégico, táctico y operativo. Este enfoque asegura la trazabilidad de las decisiones, la rendición de cuentas y la coordinación transversal entre unidades académicas, administrativas y tecnológicas.

El nivel estratégico está representado por el Comité Institucional de Datos (CID), responsable de la definición de lineamientos, la priorización de dominios de datos críticos, la gestión de riesgos estratégicos y la revisión de indicadores de desempeño y madurez del gobierno de datos. El CID es presidido por la autoridad superior que Rectoría determine y actúa como instancia máxima de dirección y resolución en la materia.

El nivel táctico se articula a través de los consejos o instancias de dominio de datos, conformados por los Propietarios de datos y Administradores de datos correspondientes, los cuales tienen por función operacionalizar los lineamientos definidos a nivel estratégico, resolver definiciones de negocio, estándares, calidad y uso de los datos, y canalizar necesidades o conflictos hacia el CID cuando corresponda.

El nivel operativo recae en los roles responsables de la gestión cotidiana de los datos y de la infraestructura tecnológica que los soporta, asegurando su disponibilidad, calidad, seguridad y uso conforme a la normativa institucional.

UNIVERSIDAD DE TARAPACÁ SECRETARIO GENERAL DE LA UNIVERSIDAD ARICA - CHILE

Este modelo se alinea y articula con los principios y buenas prácticas del Sistema de Gestión de Seguridad de la Información definidos en la norma ISO/IEC 27001 y del Sistema de Gestión de la Privacidad conforme a ISO/IEC 27701, constituyendo un marco compatible y evolutivo para su implementación progresiva, sin perjuicio de los niveles de madurez o certificación que la Institución defina alcanzar, resguardando en todo momento la independencia funcional del Delegado/a de Protección de Datos (DPO) en su rol de supervisión del cumplimiento normativo en materia de protección de datos personales.

El propósito del modelo es clarificar de manera explícita quién toma decisiones sobre los datos, bajo qué criterios y con qué responsabilidades, incluyendo aspectos relativos a estándares, acceso y uso, calidad, apertura y compartición, seguridad y privacidad. Asimismo, define los mecanismos de escalamiento y resolución de conflictos entre unidades, y los instrumentos para la medición de resultados mediante indicadores clave de desempeño (KPIs) y niveles de madurez.

La asignación formal de los roles de gobernanza de datos se realizará mediante decreto o resolución institucional, incorporando principios de mínimo privilegio, segregación de funciones, y mecanismos de supletoria y continuidad operativa. El modelo es de aplicación transversal a todos los dominios de datos y sistemas institucionales, incluyendo aquellos provistos en modalidad de nube y gestionados por terceros, y será actualizado conforme evolucione la estructura organizacional de la Universidad o el marco normativo aplicable.

Roles definidos del modelo:

- **Comité Institucional de Datos (CID)**: Órgano directivo responsable de aprobar lineamientos de gobernanza de datos, priorizar dominios críticos, gestionar riesgos estratégicos y revisar indicadores de desempeño y madurez.
- **Director/a de datos / Dirección de Datos (en la DGDT)**: Responsable de implementar la presente política, coordinar el modelo de gobernanza, gestionar el portafolio institucional de datos, los catálogos, y los modelos de calidad y madurez.
- **Delegado/a de Protección de Datos (DPO)**: Rol independiente

UNIVERSIDAD DE TARAPACÁ
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

encargado de supervisar el cumplimiento de la normativa de protección de datos personales, asesorar a la institución y gestionar la atención de los derechos de los titulares.

- **Propietario/a del dato**: Autoridad responsable de un dominio de datos específico (por ejemplo, estudiantes, recursos humanos o finanzas), encargada de definir reglas de negocio, prioridades y criterios de uso.
- **Administrador/a de datos**: Responsable de velar por la calidad, los metadatos y el linaje de los datos en su dominio, actuando como enlace entre las unidades usuarias y los sistemas de información.
- **Custodio/a**: Unidad tecnológica, generalmente la Dirección de Tecnologías de la Información u otra que corresponda, responsable de asegurar la disponibilidad, seguridad, respaldo y continuidad operativa de los datos y sistemas.
- **Usuarios/as autorizados/as**: Personas que acceden y tratan datos institucionales conforme a perfiles definidos, principios de mínimo privilegio y a lo establecido en esta política y sus procedimientos asociados.

2.1. Modelo de Componentes de la Gobernanza de Datos

El Gobierno de Datos de la Universidad de Tarapacá se estructura en un conjunto de componentes interrelacionados que aseguran una gestión integral, coherente y sostenible de los datos institucionales. Estos componentes orientan la implementación operativa de la presente política y permiten su articulación con otros sistemas de gestión institucional.

Los componentes del modelo de la Gobernanza de Datos son los siguientes:

a) **Principios y marco ético-legal**, que orientan el tratamiento lícito, proporcional, transparente y responsable de los datos.

UNIVERSIDAD DE TARAPACÁ SECRETARIO GENERAL DE LA UNIVERSIDAD ARICA - CHILE

b) **Estructura de gobierno y roles**, que define responsabilidades, niveles de decisión y mecanismos de coordinación institucional.

c) **Ciclo de vida y clasificación de los datos**, que regula su creación, uso, conservación y eliminación segura.

d) **Calidad de los datos**, que establece dimensiones, métricas y mecanismos de mejora continua.

e) **Metadatos, catálogo y linaje**, que permiten la trazabilidad, reutilización y comprensión de los activos de datos.

f) **Interoperabilidad, APIs y datos abiertos**, que promueven el intercambio seguro y estandarizado de información.

g) **Riesgos, seguridad y privacidad por diseño**, integrados al Sistema de Gestión de Seguridad de la Información y a la protección de datos personales.

h) **Datos para investigación, innovación y analítica avanzada**, conforme a principios FAIR, ética y normativa aplicable.

i) **Gestión de terceros y contratos**, que regula el acceso y tratamiento de datos por parte de proveedores y colaboradores externos.

j) **Medición, madurez y mejora continua**, que permite evaluar el desempeño del gobierno de datos y orientar decisiones estratégicas.

Cada componente deberá contar con lineamientos operativos, responsables definidos y métricas asociadas, conforme a lo establecido en la presente política y sus instrumentos complementarios.



3. Desarrollo de la Política

3.1. Estructura de Gobernanza

Esta sección define la arquitectura operativa de la gobernanza de datos de la Universidad de Tarapacá, estableciendo las instancias que la componen, su composición, quórum y periodicidad, así como los mecanismos de delegación, coordinación y escalamiento de decisiones. Asimismo, identifica los principales artefactos que se generan en el marco de la gobernanza de datos, tales como actas, estándares, catálogos, resoluciones y hojas de ruta.

La estructura considera su articulación con la arquitectura organizacional, la seguridad de la información y la continuidad operativa, definiendo criterios de priorización que orientan la ejecución de iniciativas y el uso eficiente de los recursos institucionales. El modelo es de carácter federado, con coordinación central a cargo de la Dirección de Gestión Digital y Transparencia, en su rol de CDO institucional, con el propósito de evitar duplicidades, asegurar la interoperabilidad y mantener la trazabilidad de las decisiones y el cumplimiento normativo mediante el tablero de seguimiento del Comité Institucional de Datos.

La gobernanza de datos se organiza en dominios institucionales, entre los cuales se consideran, al menos, los siguientes: Estudiantes, Académico, Investigación, Personas (Recursos Humanos), Finanzas, Infraestructura y Vinculación con el Medio, sin perjuicio de otros que puedan definirse conforme a la evolución institucional.

Para cada dominio se conformarán Consejos de Dominio, como instancias de carácter táctico integradas por los propietarios de los datos y los administradores de los datos, responsables de abordar materias relativas a calidad de datos, definiciones de negocio, resolución de duplicidades y adopción de estándares.

UNIVERSIDAD DE TARAPACÁ SECRETARIO GENERAL DE LA UNIVERSIDAD ARICA - CHILE

Adicionalmente, se establece un Foro de Arquitectura y Datos, coordinado por la DGDT, encargado de revisar y armonizar modelos de datos, criterios de interoperabilidad (incluidas APIs), estándares técnicos y aspectos de seguridad de la información

3.2. Inventario y Tipología de Datos Institucionales

Para efectos de la aplicación de la presente política, la Universidad de Tarapacá reconoce, sin carácter exhaustivo, las siguientes categorías de datos institucionales:

- **Datos académicos y estudiantiles**, incluyendo información de admisión, matrícula, trayectoria académica, evaluación, titulación y egreso.
- **Datos de personas y recursos humanos**, relativos a funcionarios/as, académicos/as y prestadores de servicios.
- **Datos financieros y presupuestarios**, asociados a la gestión económica, contable y patrimonial de la Universidad.
- **Datos de investigación, innovación y creación**, incluyendo datos primarios, secundarios, resultados, metadatos y repositorios científicos.
- **Datos de gestión administrativa y documental**, incluidos expedientes, actos administrativos y registros institucionales.
- **Datos de infraestructura, equipamiento y tecnologías de la información**, incluyendo activos tecnológicos y sistemas de información.
- **Datos de vinculación con el medio e internacionalización**, relativos a convenios, proyectos y actividades institucionales.
- **Datos de biblioteca, recursos digitales y patrimonio documental**, conforme a la normativa aplicable.

UNIVERSIDAD DE TARAPACÁ SECRETARIO GENERAL DE LA UNIVERSIDAD ARICA - CHILE

Cada categoría deberá ser asociada a uno o más dominios de datos, con un/a propietario de dato responsable, y su tratamiento deberá ajustarse a la clasificación, base legal y finalidades institucionales definidas.

3.3. Gestión del Ciclo de Vida y Clasificación de los Datos Institucionales

Esta sección establece los lineamientos mediante los cuales la Universidad de Tarapacá gestiona cada activo de datos a lo largo de todo su ciclo de vida, desde su creación o captura hasta su eliminación segura, asegurando coherencia operativa entre las distintas unidades y el cumplimiento del marco normativo y regulatorio vigente.

El ciclo de vida de los datos define puntos de control obligatorios asociados, al menos, a la captura lícita, la calidad, el acceso, el uso y la compartición, el archivo, la conservación y la eliminación segura de la información. Dichos controles permiten resguardar la integridad, disponibilidad, confidencialidad y trazabilidad de los datos durante todo su tratamiento.

Complementariamente, la clasificación de los datos asigna categorías de sensibilidad y criticidad que determinan las salvaguardas técnicas y organizativas aplicables, los plazos de retención y los requisitos de anonimización o seudonimización, cuando corresponda. Estas reglas son de aplicación transversal a todos los sistemas institucionales, tanto en infraestructura propia como en servicios en la nube, incluyendo repositorios institucionales, y se articulan con el Procedimiento de Conservación y Destrucción de Información y con la gestión documental institucional.

Toda excepción a las reglas de ciclo de vida o clasificación deberá contar con una base legal debidamente fundada, la aprobación del Comité Institucional de Datos y su correspondiente registro documental.

Ciclo de vida de los datos:

- **Ciclo de vida**:

UNIVERSIDAD DE TARAPACÁ SECRETARIO GENERAL DE LA UNIVERSIDAD ARICA - CHILE



Figura 3.1. Ciclo de vida.

- **Clasificación (mínima)**:
  - Público/Abierto
  - Interno
  - Confidencial
  - Dato Personal
  - Dato Personal Sensible
  - Restringido Crítico.
- **Reglas**:
  - Etiquetado obligatorio
  - Retención definida
  - Controles de acceso,
  - Registros de tratamiento Anonimización cuando corresponda y eliminación segura conforme al *Procedimiento de Conservación y Destrucción de Información* institucional.

3.4. Calidad de Datos

Esta sección define el marco para asegurar que los datos institucionales cumplan requisitos medibles de calidad, coherentes con el uso previsto y el riesgo asociado. Establece estándares por dominio, reglas de negocio y umbrales (tolerancias) que habilitan controles preventivos, detectivos y correctivos a lo largo del ciclo de vida. La DGDT/CDO fija metodología y tablero; el CID aprueba criterios y prioriza remediación; los Propietarios de datos definen reglas y criticidad; los Administradores de datos pe

UNIVERSIDAD DE TARAPACA
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

monitorean y gestionan incidencias; los Custodios (DGDT) implementan controles técnicos y trazabilidad. Se incluyen prácticas como perfilamiento de datos, gestión de incidencias con SLA/OLA, y criterios de aceptación para analítica/IA y datos abiertos, con reporte periódico al CID.

En términos operativos, todo conjunto de datos institucional considerado crítico o destinado a interoperabilidad, analítica avanzada, inteligencia artificial o publicación como dato abierto deberá contar con reglas de calidad formalmente definidas, métricas asociadas y responsables asignados. Ningún dato podrá ser utilizado para fines estratégicos, de reporte institucional o toma de decisiones automatizada si no cumple con los umbrales mínimos de calidad establecidos para su dominio. Las desviaciones relevantes deberán registrarse como incidencias, contar con un plan de remediación aprobado por el Propietario del datos correspondiente y ser monitoreadas hasta su cierre, conforme a los acuerdos de nivel de servicio definidos y a los criterios de priorización establecidos por el Comité Institucional de Datos.

3.5. Metadatos, catálogo y linaje

Esta sección establece el marco para describir y gobernar los activos de datos mediante metadatos estandarizados, un catálogo institucional y mapas de linaje. Su propósito es facilitar el descubrimiento y la reutilización, asegurar interoperabilidad, habilitar el análisis de impacto ante cambios y demostrar cumplimiento normativo. Todo activo (dataset, API, reporte, modelo/algoritmo) deberá contar con metadatos mínimos obligatorios: propietario del dato, administrador del datos, finalidad, base legal cuando corresponda, clasificación y sensibilidad, calidad esperada/KPIs, fuentes, controles y política de conservación. El catálogo actuará como registro maestro con versionamiento y trazabilidad de cambios; el linaje documentará orígenes, transformaciones y destinos a lo largo de pipelines/ETL/ELT. La DGDT/CDO define estándares y taxonomías; los propietarios/administradores de datos mantienen y validan metadatos; DGDT implementa conectores y automatiza su captura, resguardando auditoría y seguridad. A considerar:

UNIVERSIDAD DE TARAPACA
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

- Catálogo institucional de datos y activos analíticos (datasets, reportes, APIs, algoritmos), con glosario de negocio y mapas de linaje.
- Control de versiones, responsables y fecha de actualización.
- Integración con repositorios de investigación y datos abiertos conforme corresponda.

3.6. Interoperabilidad, APIs y datos abiertos

Esta sección define las reglas para compartir e intercambiar datos de forma segura, estandarizada y trazable, tanto al interior de la UTA como con organismos públicos, socios académicos y proveedores. Se establecen criterios técnicos y de gobernanza para el diseño y operación de APIs (seguridad, versionado, documentación, pruebas, SLA y gestión de cambios), así como lineamientos para la apertura responsable de datos conforme al marco legal chileno (priorización, anonimización y licenciamiento). La interoperabilidad se sustenta en modelos canónicos, glosarios y metadatos comunes, evitando duplicidades, promoviendo el principio "once only" y asegurando consistencia semántica entre sistemas. La DGDT/CDO define estándares y gobierno del ciclo de APIs/datasets; DGDT implementa la plataforma y controles; y los propietarios/administradores de datos validan esquemas, usos y publicaciones, resguardando privacidad y seguridad.

- Estándares para diseño de APIs (seguridad, versionamiento, pruebas, documentación) y acuerdos de intercambio con terceros.
- Datos abiertos: priorización, formatos reutilizables, metadatos, licencias; exclusiones por confidencialidad o presencia de datos personales; anonimización o agregación según riesgos.
- Integración con lineamientos de Gobierno Digital y Transparencia Activa.

UNIVERSIDAD DE TARAPACÁ
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

3.7. Riesgos, seguridad y privacidad por diseño

Esta sección establece el enfoque integral de gestión de riesgos para el tratamiento de datos en la UTA, articulando seguridad de la información y privacidad desde el diseño y por defecto. Define cómo identificar, evaluar, tratar y monitorear riesgos técnicos, legales, operacionales y reputacionales; cómo incorporar salvaguardas proporcionales en procesos, sistemas y contratos; y cómo operar la prevención, detección y respuesta ante incidentes. Se debe considerar exigencias regulatorias nacionales en ciberseguridad y protección de datos, donde se debe cumplir:

- Medidas técnicas y organizativas (control de acceso, cifrado, respaldo, continuidad, logging, pruebas de seguridad, gestión de identidades).
- Coordinación con la normativa de ciberseguridad nacional.

3.8. Datos para investigación (I+D)

Esta sección establece los lineamientos para el tratamiento y la gestión de datos en actividades de investigación científica, desarrollo tecnológico e innovación en la Universidad de Tarapacá, resguardando un equilibrio adecuado entre apertura, reproducibilidad y generación de valor, con el cumplimiento de principios éticos, legales y de protección de los derechos de los titulares de datos.

Se definen los criterios para la planificación y ejecución de proyectos de investigación mediante Planes de Gestión de Datos (PGD), alineados con los principios FAIR, así como las bases jurídicas aplicables, el uso de consentimiento informado cuando corresponda y las salvaguardas específicas para el tratamiento de datos personales, datos sensibles y datos relativos a poblaciones o contextos vulnerables, incluyendo transferencias nacionales e internacionales.

La política deberá articular la coordinación entre los equipos de investigación, los Comités Ético-Científicos (CEC), la Dirección de Gestión Digital y

UNIVERSIDAD DE TARAPACA SECRETARIO GENERAL DE LA UNIVERSIDAD ARICA - CHILE

Transparencia en su rol de CDO institucional, el Delegado/a de Protección de Datos y las unidades tecnológicas pertinentes mediante un reglamento o protocolo específico de gestión de datos de investigación, por elaborar, asegurando la existencia de un instrumento jurídico que respalde la operación declarada. En este marco, se establecen criterios para la publicación, embargo, preservación y reutilización de los datos de investigación, así como para la aplicación de técnicas de anonimización o seudonimización y el acceso controlado a través de repositorios institucionales o federados, conforme a la normativa chilena vigente y a las buenas prácticas internacionales en ciencia abierta y gobernanza de datos.

3.9. Terceros y contratos

Esta sección regula la relación de la UTA con terceros que tratan o acceden a datos institucionales, encargados y corresponsables del tratamiento, proveedores de nube y software, integradores, socios académicos, laboratorios y otros prestadores, y define exigencias contractuales y de control para proteger la información y los derechos de los titulares. Establece criterios de debida diligencia y evaluación de riesgos previos a la contratación; fija cláusulas mínimas obligatorias (instrucciones de tratamiento, confidencialidad, medidas técnicas y organizativas, gestión de subencargados, ubicación/transferencias internacionales, notificación y gestión de brechas, derecho de auditoría, niveles de servicio y continuidad, plan de salida y devolución/eliminación de datos). Todo intercambio de datos con terceros debe documentarse mediante contrato o anexo de protección de datos (DPA), contar con base legal y, cuando corresponda, una autorización del CID.

3.10. Medición, madurez y mejora continua

Esta sección establece el marco mediante el cual la Universidad de Tarapacá evalúa de forma sistemática el desempeño de su gobernanza de datos y

UNIVERSIDAD DE TARAPACÁ
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

asegura su mejora continua. Para ello, se combinan un modelo institucional de madurez, objetivos y métricas por dominio de datos, revisiones periódicas del Comité Institucional de Datos y procesos de auditoría interna y externa, orientados a verificar la eficacia y sostenibilidad del modelo.

La gestión de la mejora continua se basa en ciclos PDCA (planificar–hacer–verificar–actuar), incorporando mecanismos de detección temprana de brechas, acciones correctivas y preventivas, y ejercicios de comparación y aprendizaje (benchmarking) con marcos de referencia reconocidos, tales como DAMA-DMBOK e ISO/IEC 38505-1.

Los indicadores de desempeño abarcarán, al menos, la calidad y cobertura del catálogo y del linaje de datos; la interoperabilidad y operación de APIs; la protección de la privacidad y la seguridad de la información; la atención de derechos de los titulares; la gestión de incidentes; y el valor y nivel de uso de los datos para fines institucionales. Los resultados serán consolidados en un tablero institucional, con responsables claramente identificados y trazabilidad de las decisiones, sirviendo de base para la priorización de iniciativas y la asignación de recursos del plan anual de gobernanza de datos.

Asimismo, se promoverá la transparencia y la rendición de cuentas mediante reportes ejecutivos periódicos a Rectoría y la publicación de métricas no sensibles, conforme a la normativa vigente.

Elementos del modelo de medición:

- Modelo de madurez de gobernanza de datos con niveles progresivos (1–5).
- OKR y KPI anuales por dominio de datos.
- Revisiones trimestrales por el Comité Institucional de Datos.
- Auditorías internas y externas.
- Planes de mejora continua derivados de los resultados.

UNIVERSIDAD DE TARAPACA SECRETARIO GENERAL DE LA UNIVERSIDAD ARICA - CHILE

4. Mecanismos de Difusión y Capacitación

La Universidad de Tarapacá establecerá y mantendrá mecanismos sistemáticos de difusión y capacitación destinados a asegurar la adecuada comprensión, adopción y cumplimiento de la presente Política General de Gobernanza de Datos en todos los estamentos institucionales. Dichos mecanismos tienen por finalidad desarrollar competencias acordes a los distintos roles y responsabilidades, promoviendo una aplicación coherente y consistente de los principios, lineamientos y procedimientos asociados al gobierno de datos.

La difusión de la política se realizará mediante un plan de comunicación interna permanente, coordinado por la Dirección de Gestión Digital y Transparencia (DGDT), en su rol de CDO institucional, con el apoyo de la Direcciones de Calidad Institucional y de Admisión y Comunicaciones Estratégicas. Este plan contemplará, al menos, la publicación y actualización de contenidos en la intranet institucional, la elaboración y distribución de guías operativas, plantillas, documentos de apoyo y preguntas frecuentes (FAQs), así como comunicaciones dirigidas a públicos específicos cuando corresponda.

La capacitación se estructurará a través de un plan anual de formación, definido por perfiles y funciones, que considerará como públicos destinatarios a las autoridades universitarias; Propietario de datos, Administrador de datos y Custodio de datos; académicos y académicas; funcionarios y funcionarias; investigadores e investigadoras; y, cuando aplique, proveedores y terceros que traten datos institucionales. El plan establecerá objetivos de aprendizaje diferenciados según rol, orientados al conocimiento normativo, la correcta aplicación de los lineamientos en el puesto de trabajo y el cumplimiento de los procesos de gobernanza de datos.

UNIVERSIDAD DE TARAPACÁ
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

Las modalidades de capacitación podrán incluir instancias de inducción institucional, cursos en modalidad e-learning a través de plataformas oficiales, talleres prácticos presenciales o virtuales, acciones de micro-learning y cápsulas formativas breves, de acuerdo con la naturaleza del contenido y el perfil de los participantes. Se definirá una frecuencia mínima de ejecución para cada modalidad y perfil, así como los mecanismos de respaldo y evidencia, tales como registros de asistencia, aprobaciones en plataformas de aprendizaje institucional y certificaciones cuando corresponda.

El proceso de capacitación incorporará criterios de evaluación orientados a medir el nivel de conocimiento adquirido, la aplicación efectiva de los contenidos en el desempeño laboral y el grado de cumplimiento de los procedimientos asociados a la gobernanza de datos. Asimismo, se definirán métricas de efectividad que permitan evaluar el impacto de estas acciones, incluyendo, entre otras, cobertura de participación, tasa de aprobación, tiempos de respuesta en procesos asociados a derechos de los titulares y reducción de incidentes o incumplimientos evitados.

Complementariamente, la Universidad desarrollará materiales y campañas periódicas de concienciación orientadas a fortalecer una cultura institucional de uso responsable de los datos, abordando temáticas como protección de datos personales, seguridad de la información, datos abiertos, ética de los datos y uso responsable de la analítica avanzada e inteligencia artificial.

UNIVERSIDAD DE TARAPACÁ
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

5. Cumplimiento y Revisión

La presente Política General de Gobernanza de Datos será objeto de revisión periódica al menos una vez cada doce (12) meses, con el propósito de asegurar su vigencia, coherencia normativa y alineación con la estrategia institucional, el marco regulatorio y las buenas prácticas internacionales.

La revisión será coordinada por la Dirección de Gestión Digital y Transparencia, en conjunto con el Comité Institucional de Datos y las instancias de aseguramiento de la calidad institucional.

Adicionalmente, la política deberá ser revisada de manera extraordinaria cuando concurran cambios normativos relevantes, incidentes graves de seguridad o privacidad, modificaciones sustantivas en los sistemas de información institucionales, o instrucciones de la autoridad superior.

UNIVERSIDAD DE TARAPACÁ
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

6. Incumplimiento y Sanciones

El incumplimiento de la presente política dará lugar a las medidas disciplinarias establecidas en el Estatuto Administrativo, así como en las ordenanzas académicas y estudiantiles, en virtud de las infracciones a los deberes establecidos en dichas normativas. Lo anterior es sin perjuicio de la aplicación de los protocolos institucionales vinculados a la Ley N.° 21.369, la Ley Karin u otras normativas equivalentes que resulten pertinentes, cuando corresponda.

Asimismo, las personas contratadas como prestadores de servicios a honorarios deberán considerar como infracción a los deberes establecidos en sus respectivos contratos el incumplimiento de la presente política, lo que dará lugar a las sanciones contempladas en dichos contratos.

UNIVERSIDAD DE TARAPACÁ
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

7. Glosario de Términos

Activo: Todo elemento lógico o físico, componente de hardware, equipamiento o sistema relacionado con la información, que permita su generación, almacenamiento, soporte, envío o intercambio, sea a otros órganos de la Administración del Estado o con personas naturales o jurídicas.

Activo de Información: Datos o información cuyo tratamiento es esencial para el funcionamiento y desarrollo del órgano de la Administración del Estado que lo utiliza, genera, almacena, envía o intercambia, y que deben ser protegidos en su confidencialidad, integridad, disponibilidad u otros factores de importancia.

API´s: Conjunto de reglas y mecanismos que permite que distintos sistemas o aplicaciones se comuniquen e intercambien datos o funcionalidades de forma segura y estandarizada, sin necesidad de conocer la implementación interna del otro sistema.

Ciberseguridad y Seguridad de la Información: Conjunto de acciones, políticas, medidas preventivas y reactivas destinadas a la prevención, mitigación, manejo, respuesta y estudio de las amenazas y riesgos de incidentes de seguridad, a la reducción de sus efectos y el daño causado; antes, durante y después de su ocurrencia; respecto de los activos y activos de información y la continuidad de servicios, con el fin de proteger, preservar y restablecer la confidencialidad, integridad y disponibilidad de aquellos y de las plataformas electrónicas de los órganos de la Administración del Estado, aumentando su resiliencia en el tiempo.

Confidencialidad: Atributo de los activos y los activos de información que asegura que estos sean conocidos y accedidos exclusivamente por quienes están autorizados para ello.

Disponibilidad: Atributo de los activos y activos de información, relativo a su accesibilidad y utilización a requerimiento de una entidad o proceso autorizado.

UNIVERSIDAD DE TARAPACA
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

Evaluación de Riesgo: Proceso consistente en la comparación de los niveles de riesgo encontrados contra los criterios de riesgo prestablecidos (si es que han sido establecidos por la institución) considerando el balance entre los beneficios potenciales y resultados adversos, para posteriormente ordenar y priorizar mediante un ranking los riesgos analizados.

Gestión de Riesgo: Proceso estructurado y proactivo por el cual se identifican, evalúan, controlan y tratan los riesgos derivados de una o más amenazas determinadas.

Gobernanza de Datos (Estratégico): Se centra en la propiedad de los datos, políticas, seguridad, cumplimiento normativo y definición de reglas. Define las estructuras organizativas y asegura la calidad y el cumplimiento.

Incidente de Seguridad: Todo evento de seguridad o una serie de ellos, de carácter indeseado o inesperado, que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas informáticos, los activos y activos de información, datos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y que puedan afectar al normal funcionamiento de los mismos.

Integridad: Atributo de los activos y activos de información relativo a la exactitud, autenticidad y completitud de los mismos.

Mapas de linaje de datos: Documentación trazable que describe el origen, transformaciones y destinos de los datos a lo largo de su ciclo de vida, permitiendo análisis de impacto, control de calidad, auditoría y cumplimiento.

OLA (Operational Level Agreement): Acuerdo operativo interno que establece los niveles de servicio y responsabilidades entre unidades internas, necesarios para cumplir los compromisos definidos en un SLA.

Plataforma electrónica (en adelante también "plataforma"): Software o conjunto de software, datos e infraestructura tecnológica que sustenta procesos o procedimientos.

Principios FAIR: Conjunto de principios que establecen que los datos deben ser localizables, accesibles, interoperables y reutilizables, mediante metadatos estandarizados, identificadores persistentes, formatos abiertos

UNIVERSIDAD DE TARAPACA
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

y condiciones claras de acceso y uso, resguardando el cumplimiento normativo.

Principio "Once Only": Principio según el cual los datos deben capturarse y mantenerse una sola vez en su fuente oficial, siendo reutilizados mediante interoperabilidad segura y trazable, evitando duplicidades y reprocesos.

Proceso: Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un fin determinado.

Riesgo: Efecto de la incertidumbre sobre los activos de información y los objetivos de una entidad, habitualmente expresado en relación a las consecuencias de un evento o incidente de seguridad y su probabilidad de ocurrencia.

Sanción: Consecuencia jurídica de naturaleza administrativa, civil o penal derivada del incumplimiento de un deber.

Seguridad de la Información: Proceso encargado de asegurar y proteger los recursos de un sistema de información para que sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, preservando la Integridad, Confidencialidad y Disponibilidad.

Sistema informático: Conjunto de componentes lógicos y físicos que, interactuando entre sí, permiten que su totalidad o una parte de ellos, realicen la función para la cual fueron diseñados.

SLA (Service Level Agreement): Acuerdo formal que define los niveles de servicio comprometidos, incluyendo tiempos de respuesta, disponibilidad, calidad y responsabilidades, entre una unidad proveedora y sus usuarios o clientes internos/externos.

Terceras partes: Persona u organismo ajeno a la relación directa establecida entre dos partes principales. Para estos efectos, se entenderá como terceras partes, entre otros a los proveedores de servicios y de red, los proveedores de productos de software y servicios de información, outsourcing de instalaciones y operaciones, servicios de asesoría de seguridad y auditores externos.

UNIVERSIDAD DE TARAPACA
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

Usuarios(as): Personas naturales o sus apoderados(as), y los(as) representantes de las personas jurídicas o entidades y agrupaciones sin personalidad jurídica que actúan como interesados(as) en un procedimiento administrativo, así como los(as) funcionarios(as) que acceden a las plataformas electrónicas que soportan procedimientos administrativos o procesos relacionados con estos.

UNIVERSIDAD DE TARAPACÁ
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE

8. Términos Abreviados

API: Interfaz de Programación de Aplicaciones (Application Programming Interface).

DPO: Data Protection Officer, en español Delegado de Protección de Datos (DPD)

CPLT: Consejo para la Transparencia

CGR: Contraloría General de la República

UTA: Universidad de Tarapacá

IA: Inteligencia Artificial

CID: Comité Institucional de Datos

CDO: Chief Data Officer, en español Director de Datos

DGDT: Dirección de Gestión Digital y Transparencia

DCI: Dirección de Calidad Institucional

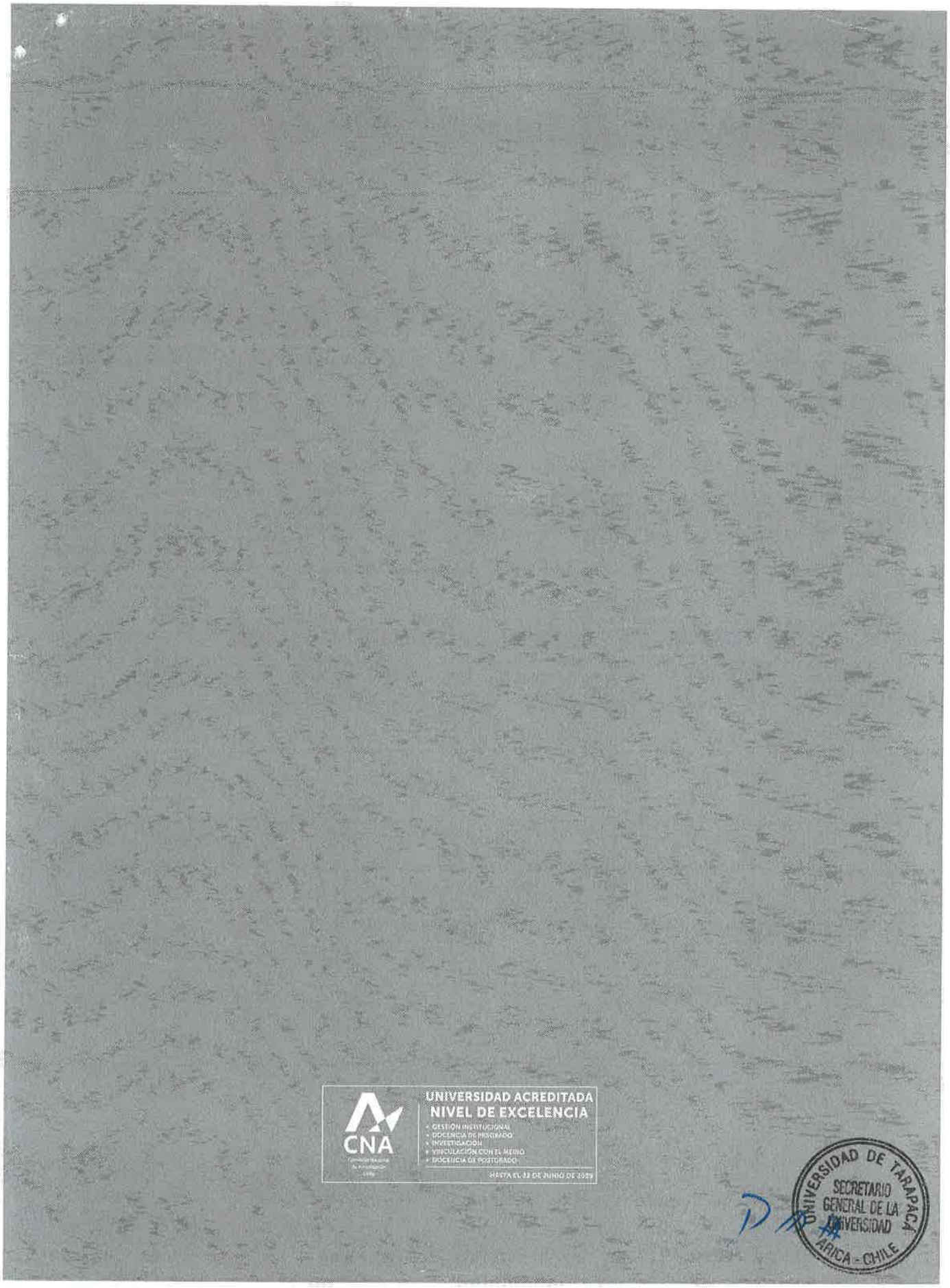
DACE: Dirección de Admisión y Comunicaciones Estratégicas

ETL: Extract, Transform, Load, en español Extraer, Transformar y Cargar.

CEC: Comité Ético y Científico

KPI: Key Performance Indicator, en español Indicador Clave de Desempeño

UNIVERSIDAD DE TARAPACA
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE


CNA
UNIVERSIDAD ACREDITADA
NIVEL DE EXCELENCIA
• GESTIÓN INSTITUCIONAL
• DOCENCIA DE PREGRADO
• INVESTIGACIÓN
• VINCULACIÓN CON EL MEDIO
• DOCENCIA DE POSTGRADO
HASTA EL 22 DE JUNIO DE 2029
UNIVERSIDAD DE TARAPACÁ
SECRETARIO GENERAL DE LA UNIVERSIDAD
ARICA - CHILE