



Universidad de Concepción

DECRETO U. DE C. N°2026-079

VISTO:

1. Lo acordado por el Consejo Académico de la Universidad de Concepción, en sesión de fecha 16 de abril de 2026, y por el conocimiento tomado por el Directorio en sesión de 7 de mayo de 2026; en orden a aprobar la Política de Protección de Datos Personales y la Política de Gobierno de Datos, elaboradas por la Dirección de Desarrollo Estratégico de la Universidad de Concepción.
2. Lo establecido en el Decreto U. de C. N°2022-048, de 21 de abril de 2022, y en los Estatutos de la Corporación.

DECRETO:

Apruébase la siguiente Política de Protección de Datos Personales y la Política de Gobierno de Datos, las cuales se adjuntan al presente Decreto formando parte integrante del mismo, una vez rubricados conforme por el Secretario General.

Transcribese electrónicamente: a las Vicerrectoras y al Vicerrector de Asuntos Económicos y Administrativos; a la Directora y el Director General de los Campus; a las Decanas y a los Decanos de Facultades; al Director o Directora: del Instituto GEA; del Centro de Biotecnología; del Centro EULA; del Centro de Vida Saludable; de la Dirección de Relaciones Internacionales; de la Dirección de Desarrollo Estratégico; de la Dirección de Comunicaciones; de la Dirección de Equidad de Género y Diversidad; a la Jefa de la Unidad Universidad de Concepción, Santiago; al Director o Directora: de la Dirección de Docencia; de la Dirección de Postgrado; de la Dirección de Extensión; de la Dirección de Bibliotecas; de la Dirección de Servicios Estudiantiles; de la Dirección de Investigación y Creación Artística; de la Dirección de Desarrollo e Innovación; al Director o Directora: de la Dirección de Relaciones Institucionales; de la Dirección de Vinculación Social; de la Dirección de Finanzas; de la Dirección de Personal; de la Dirección de Tecnologías de la Información; de la Dirección de Servicios y al Contralor. Regístrese y archívese en Secretaría General, publíquese en www.documentos.udec.cl.

Concepción, 08 de mayo de 2026.



CARLOS SAAVEDRA RUBILAR
RECTOR

Decretado por don CARLOS SAAVEDRA RUBILAR, Rector de la UNIVERSIDAD DE CONCEPCIÓN.



MARCELO TRONCOSO ROMERO
SECRETARIO GENERAL

CRP/MMH/AGG/nam.



Política de Protección de Datos Personales

A. Introducción

La Universidad de Concepción gestiona datos personales de miles de personas — estudiantes, académicos, funcionarios, investigadores y proveedores, entre otros — en los distintos procesos de todas las áreas del quehacer institucional. Esta realidad, sumada a la entrada en vigor de la Ley N° 21.719 que moderniza la protección de datos en Chile y crea la Agencia de Protección de Datos Personales, hace indispensable contar con un marco normativo interno claro. La privacidad es además un derecho fundamental reconocido en la Constitución y en tratados internacionales ratificados por Chile, lo que obliga a la institución a actuar con coherencia ética y no solo legal.

La política debe estar en operación antes de la entrada en vigor de la Ley 21.719 en diciembre de 2026, para garantizar que los titulares puedan ejercer sus derechos, prevenir incidentes de seguridad y dotar a la Universidad de la capacidad de responder ante la autoridad fiscalizadora. En un entorno de digitalización creciente, tener esta política vigente es la base para que la institución opere con integridad, proteja la confianza de su comunidad y consolide su responsabilidad social.

La Universidad de Concepción, en su calidad de Corporación de Derecho Privado con misión pública, asume el compromiso de garantizar la privacidad, integridad, confidencialidad y seguridad de los datos personales de todas las personas con quienes se relaciona, ya sea en su rol de estudiantes, académicos, funcionarios, investigadores, colaboradores, proveedores, usuarios de sus servicios o cualquier otro titular de datos asegurando su tratamiento conforme a los principios y derechos establecidos en la legislación vigente.

Este compromiso se fundamenta en lo dispuesto por la Ley N° 19.628 sobre Protección de la Vida Privada y su reforma mediante la Ley N° 21.719 que Regula la protección y tratamiento de los datos personales y crea la agencia de protección de datos personales, así como en el respeto a los derechos fundamentales garantizados en la Constitución y en los tratados internacionales ratificados por Chile.

La política se aplica con enfoque de derechos, en concordancia con los valores institucionales de probidad, ética, responsabilidad social, inclusión y transparencia.

Para los efectos de esta Política son datos personales los que la ley 19.628 modificada por la ley 21.719 Regula la protección y tratamiento de los datos personales y crea la agencia de protección de datos personales define como tales en el art. 2 f).

B. Objetivo y alcance

Esta política tiene por objetivo establecer el marco normativo y los lineamientos generales que deben seguir todos quienes intervienen en el tratamiento de datos personales al interior de la Universidad de Concepción, para asegurar:

- El respeto de los derechos de los titulares de los datos.



- El cumplimiento de las normas legales vigentes en materia de protección de datos personales.
- La implementación de principios y prácticas institucionales de seguridad de la información y control del tratamiento de datos personales.
- La prevención de incidentes que puedan afectar la privacidad, confidencialidad o integridad de los datos personales tratados por la Universidad.

C. Base legal y normativa aplicable

Esta política se ajusta a las disposiciones de la Ley N° 19.628 sobre Protección de la Vida Privada y su reforma mediante la Ley N° 21.719 Regula la protección y tratamiento de los datos personales y crea la agencia de protección de datos personales, a la Ley 21.091, sobre Educación Superior; a los Estatutos de la Corporación, al Reglamento Orgánico de Universidad de Concepción, y al Modelo de Prevención del Delito de la Corporación Universidad de Concepción.

Lo anterior, en el marco de lo dispuesto en el art. 19 n° 4 de la Constitución Política de la República y en el art. 12 de la Declaración Universal de Derechos Humanos y el art. 17 del Pacto Internacional de Derechos Civiles y Políticos.

D. Principios generales del tratamiento de datos

El tratamiento de datos se regirá por los siguientes principios:

- **Licitud y Lealtad:** Todo tratamiento debe realizarse de manera lícita, con una base jurídica válida, como el consentimiento, el cumplimiento de obligaciones legales, o el interés legítimo institucional.
- **Finalidad:** Los datos sólo serán tratados para fines específicos, legítimos y previamente informados. En aplicación de este principio, no se pueden tratar los datos personales con fines distintos a los informados al momento de la recolección, salvo que el tratamiento sea para fines compatibles con los autorizados originalmente; que exista una relación contractual o precontractual entre el titular y el responsable que justifique el tratamiento de los datos con una finalidad distinta, siempre que se enmarque dentro de los fines del contrato o sea coherente con las tratativas o negociaciones previas a la celebración del mismo; que el titular otorgue nuevamente su consentimiento, y cuando lo disponga la ley.
- **Proporcionalidad:** Se recopilarán únicamente los datos estrictamente necesarios, adecuados y pertinentes para cumplir los fines institucionales. Los datos serán almacenados sólo durante el tiempo necesario para cumplir los fines institucionales que motivaron su recopilación, de conformidad a la ley y al reglamento.
- **Seguridad:** Se garantizarán medidas técnicas, organizativas y legales para evitar accesos no autorizados, pérdida o alteración de los datos. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza de los datos
- **Principio de calidad:** Los datos personales deben ser exactos, completos, actuales y pertinentes en relación con su proveniencia y los fines del tratamiento.

- **Principio de transparencia e información:** El responsable debe entregar al titular toda la información que sea necesaria para el ejercicio de los derechos que le reconocen la ley y esta política, debiendo adoptar las medidas adecuadas y oportunas para esa finalidad.
- La transparencia implica la trazabilidad de la manipulación de los datos
- **Responsabilidad:** La Universidad es responsable de asegurar y demostrar que el tratamiento de datos cumple con la normativa aplicable.
- **Principio de confidencialidad:** El responsable de datos personales y quienes tengan acceso a ellos deberán asegurar la confidencialidad de los mismos estableciendo medidas adecuadas para preservarla, aun después de concluida la relación con el titular

E. Derechos de los titulares de datos

Toda persona, actuando por sí o a través de su representante legal o mandatario, según corresponda, tiene derecho de acceso, rectificación, supresión, oposición, portabilidad y bloqueo de sus datos personales. Tales derechos son personales, intransferibles e irrenunciables y no pueden limitarse por ningún acto o convención.

- **Acceso:** solicitar conocer, y obtener, los datos personales que están siendo tratados por la Universidad.
- **Rectificación:** Solicitar la corrección de datos inexactos, desactualizados o incompletos.
- **Eliminación** (supresión): Solicitar la supresión de sus datos cuando ya no sean necesarios o cuando se haya retirado el consentimiento, todo de conformidad a la ley.
- **Oposición:** Oponerse al tratamiento de sus datos en casos legalmente procedentes.
- **Portabilidad:** solicitar y recibir una copia de los datos personales que le conciernen en un formato estructurado, cuando sea técnicamente posible y procedente de conformidad a la ley.

Los canales habilitados para ejercer estos derechos son:

- Plataforma de Transparencia UdeC: <https://transparencia.udec.cl>
- Oficina de Partes o Secretaría General.
- Encargado/a de Protección de Datos Personales

F. Roles y responsabilidades institucionales

La Universidad, a través del rector o rectora, designará un/a **Encargado de Datos personales**, cuyas funciones incluirán:

- Supervisar el cumplimiento de esta política y de la normativa vigente
- Adoptar las medidas necesarias para la formación permanente de las personas que participan en tratamiento de datos.



- Promover la cultura de protección de datos en la Institución.
- Atender las solicitudes de los titulares de datos personales.
- Asesorar a las unidades en materia de protección de datos.
- Coordinar la respuesta a incidentes de seguridad o vulneración de datos personales y mantener a las autoridades universitarias permanentemente informadas de estos incidentes.
- Representar a la Universidad ante la Agencia de Protección de Datos Personales o autoridad competente.

Dependerá administrativamente de la Contraloría de la Universidad de Concepción, y gozará de autonomía para el ejercicio de sus funciones.

- **Existirá un Consejo** integrado por un representante de la Secretaría General, de la Vicerrectoría de Asuntos Económicos y Administrativos (DTI), de la Contraloría y de la Dirección de Desarrollo Estratégico, y por el Encargado de Datos Personales el cual tendrá como principal función asesorar a la autoridad superior en lo relativo a la normativa necesaria para la correcta aplicación de esta política, así como supervigilar su correcta ejecución.
- **Dirección de Tecnologías de Información:** Responsable de implementar, mantener y supervisar las medidas técnicas y organizativas necesarias para preservar la seguridad e integridad de los datos personales.
- **Responsables de tratamiento:** Autoridades o funcionarios que determinen los fines y medios del tratamiento de datos personales, asumiendo el deber de garantizar el cumplimiento de las obligaciones legales y de la presente política.
- **Usuarios autorizados:** Personas que, en virtud de sus funciones, tengan acceso a datos personales, quienes deberán ajustarse estrictamente a los principios, finalidades y medidas de seguridad establecidas. Estos usuarios autorizados deberán estar expresamente definidos.
- **Todas las personas vinculadas a la institución:** Tienen el deber de cumplir las disposiciones, principios y obligaciones establecidos en esta política y colaborar con las medidas de resguardo de datos que la misma contempla.

G. Tratamiento de datos personales

El tratamiento de datos personales se efectuará

- a) Con el consentimiento libre, expreso e informado del titular, cuando sea requerido.
- b) En el marco del cumplimiento de una obligación legal, contractual o reglamentaria.
- c) En el ejercicio de funciones propias de una institución de educación superior.
- d) En atención al interés público, interés legítimo o autorizaciones legales específicas.

Fases del Tratamiento:



1. **Recolección:** Obtención, revisión y organización de datos personales, informando la finalidad del tratamiento y previa obtención, en su caso, del consentimiento previo, libre e informado.
2. **Uso:** Empleo de los datos personales para los fines declarados o compatibles, conforme a la ley y a esta política.
3. **Conservación:** Almacenamiento, resguardo seguro y actualización en su caso, de los datos por el tiempo necesario para el cumplimiento de sus fines, de conformidad a la ley.
4. **Eliminación:** Supresión o anonimización de los datos cuando hayan dejado de ser necesarios para el fin que motivó su recolección, salvo las excepciones legales.

Categorías de datos tratados:

Datos personales de identificación y contacto, datos sensibles siempre de conformidad a la ley.

Consentimiento informado:

Será previo, libre, específico, inequívoco y verificable, pudiendo revocarse en cualquier momento sin efecto retroactivo, siempre que no exista otra base legal habilitante.

Los datos personales serán tratados con fines relacionados con las funciones y atribuciones propias de la Universidad, sin que la enumeración sea exhaustiva:

- Gestión académica y administrativa de estudiantes, desde el ingreso hasta la titulación.
- Gestión de personal académico y no académico.
- Gestión de servicios estudiantiles (bibliotecas, salud, alimentación, deportes, bienestar, entre otros).
- Investigación científica y desarrollo tecnológico, asegurando anonimización o consentimiento cuando sea exigible.
- Vinculación con el medio, extensión y actividades de difusión institucional.
- Cumplimiento de obligaciones legales, normativas o contractuales.
- Gestión financiera, tributaria y contable.
- Seguridad institucional y control de acceso.
- Implementación de sistemas y plataformas tecnológicas institucionales.
- Mejoramiento de los procesos institucionales

H. Transferencia y comunicación de datos

La Universidad podrá comunicar datos personales a terceros únicamente cuando:

- Exista una obligación legal o el tercero asuma contractualmente las obligaciones necesarias para garantizar un tratamiento conforme a los principios de esta política y la normativa aplicable, con las medidas de seguridad adecuadas



- En el caso de transferencias internacionales, se requerirá que el país de destino ofrezca un nivel adecuado de protección o que el tercero ofrezca garantías apropiadas conforme a la ley.
- Medie el consentimiento informado del titular.

Registro y trazabilidad: Toda transferencia o comunicación se registrará en el registro institucional, indicando destinatario, fecha, finalidad y base legal y consentimiento informado.

I. Medidas de seguridad y gestión de incidentes

La Universidad adoptará medidas de seguridad físicas, lógicas, administrativas y técnicas, conforme a los estándares internacionales de gestión de la seguridad de la información (ISO/IEC 27001 y similares), que permitan:

- Prevenir accesos no autorizados, pérdida, alteración o destrucción de datos personales.
- Establecer controles de acceso lógico a sistemas de información.
- Aplicar protocolos de resguardo y respaldo.
- Realizar auditorías y análisis de riesgo periódicos.
- Establecer procedimientos de respuesta ante incidentes de seguridad.

J. Registro de actividades de tratamiento

La Universidad de Concepción llevará un registro actualizado de todas las actividades que impliquen tratamiento de datos personales. Será administrado por el Encargado/a de Protección de Datos y estará disponible para la autoridad competente. El inventario incluirá, como mínimo:

- Identificación del responsable del tratamiento.
- Identificación de lugar en que se encuentran almacenados.
- Finalidad del tratamiento.
- Categorías de datos y de titulares.
- Destinatarios
- Base legal que lo habilita.
- Plazos de conservación.
- Medidas de seguridad aplicadas.

K. Capacitación, difusión y sensibilización

La Institución garantizará la capacitación continua y sistemática de las autoridades, funcionarios, académicos, estudiantes y demás personas que intervengan en el tratamiento de datos personales, con el fin de asegurar su conocimiento y cumplimiento de la normativa

legal vigente y de esta política. Dicha función corresponderá ser desarrollada por el Encargado de Protección de Datos Personales.

SECRETARIO GENERAL

Para estos efectos, se implementarán planes y programas de formación, difusión y sensibilización, incluyendo talleres, guías, protocolos y recursos informativos, así como campañas periódicas de concientización sobre la relevancia de la protección de datos personales.

L. Evaluación, revisión y actualización de la política

La presente política será objeto de revisión y evaluación periódica, al menos cada dos (2) años o antes, en caso de producirse modificaciones normativas, tecnológicas o de procesos que así lo requieran.

La responsabilidad de la evaluación y propuesta de actualización recaerá en el Encargado/a de Protección de Datos, en coordinación con las unidades institucionales involucradas, siguiendo procedimientos de mejora continua y considerando la retroalimentación de la comunidad universitaria.

M. Vigencia y publicación

La presente política entrará en vigor a contar de la fecha en que se decrete, debiendo ser publicada en el sitio web institucional, en los canales oficiales de comunicación interna y en cualquier otro medio que la Institución determine idóneo para su difusión.

Toda modificación o actualización será igualmente publicada, indicando su fecha de aprobación y un resumen de los cambios introducidos.

N. Anexo

Glosario

- **Datos personales:** Información que identifica o permite identificar a una persona, ya sea de forma directa (como nombre o RUT) o indirecta mediante la combinación de datos (como correo, número de estudiante o dirección).
- **Datos sensibles:** Datos personales que se refieren a aspectos íntimos de una persona, como salud, origen racial o creencias, y cuyo uso indebido puede generar discriminación o afectar sus derechos. Su tratamiento debe realizarse siempre de conformidad a la ley, especialmente cuando se refieran a aspectos íntimos del titular.
- **Titular de los datos:** Persona natural a quien pertenecen los datos personales.
- **Tratamiento de datos:** Cualquier operación realizada sobre datos personales, como su recolección, almacenamiento, uso, modificación, comunicación o eliminación.
- **Responsable del tratamiento:** Autoridades o funcionarios que determinan los fines y medios del tratamiento de datos, asumiendo el deber de garantizar el cumplimiento de las obligaciones legales.
- **Usuario autorizado:** Persona que tiene acceso a datos personales debido a sus funciones y responsabilidades dentro de la institución.
- **Finalidad:** Propósito específico para el cual se recolectan y utilizan los datos personales.
- **Consentimiento:** Autorización otorgada por el titular para el uso de sus datos personales, la cual debe ser libre, informada y específica.
- **Anonimización:** Proceso mediante el cual los datos dejan de estar asociados a una persona identificable.
- **Transferencia de datos:** Comunicación de datos personales a un tercero externo a la institución.
- **Incidente de seguridad:** Situación en la que los datos personales se ven comprometidos, ya sea por acceso no autorizado, pérdida, alteración o divulgación.
- **Encargado de Protección de Datos Personales:** Persona designada por el Rector que, con autonomía y dependencia administrativa de la Contraloría, supervisa el cumplimiento de la política, asesora a las unidades y representa a la Universidad ante la autoridad competente.



Dirección de
Desarrollo Estratégico
Universidad de Concepción



Estrategia
y Calidad

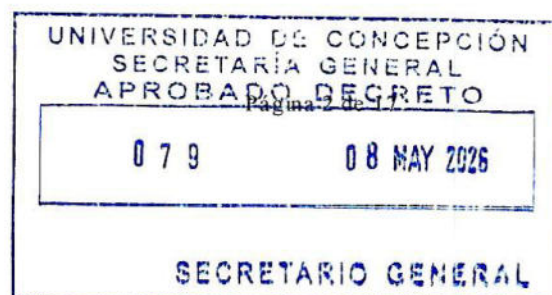
Propuestas de Política de Gobierno de Datos

Abril 2026



Contenido

Declaración Institucional.....	3
Objetivos y propósitos	4
Principios rectores	4
Alcance Institucional	5
Niveles y Roles	6
Clasificación de datos y niveles de confidencialidad y sensibilidad.....	8
Gestión del ciclo de Vida de los Datos	9
Seguridad de los datos y la protección de datos personales	9
Formación, Cultura Institucional y Uso Éticos de los Datos	10
Evaluación, Revisión y Actualización de la Política	10
Glosario	11
Anexo	12





Contexto

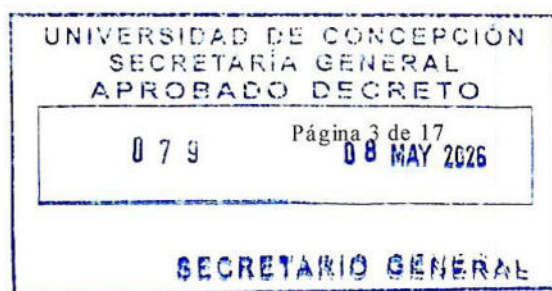
En el actual escenario de transformación digital, las instituciones de educación superior enfrentan crecientes desafíos en la gestión de la información, derivados del aumento en el volumen, diversidad y uso de los datos. En este marco, la Universidad de Concepción genera y administra una amplia cantidad de información proveniente de sus funciones académicas, administrativas, de investigación y vinculación con el medio, lo que refuerza la necesidad de gestionarla de manera coherente con su complejidad institucional y sus objetivos estratégicos.

La gestión de estos datos ha evolucionado de manera organizada en las distintas unidades, generando capacidades relevantes a nivel local. Sin embargo, el fortalecimiento de la toma de decisiones basada en evidencia, junto con las crecientes exigencias normativas en materia de protección de datos y transparencia, hacen necesario avanzar hacia un modelo institucional más articulado. En este contexto, se requiere la implementación de una Política de Gobierno de Datos que establezca un marco común de principios, roles y procesos, permitiendo gestionar los datos como un activo estratégico, mejorando la eficiencia institucional, fortalecer la confianza en la información y potenciar el desarrollo de capacidades analíticas que aporten valor a la comunidad universitaria y a la sociedad.

Declaración Institucional

La Universidad de Concepción valora sus datos como un activo estratégico que apoyan el cumplimiento de sus mandatos misionales. Se compromete a gestionar sus datos institucionales bajo principios de responsabilidad, seguridad, transparencia, interoperabilidad, usabilidad y respeto a la normativa vigente.

Esta política formaliza dicho compromiso, estableciendo las directrices que orientan la gestión de los datos como un recurso esencial para la toma de decisiones basada en evidencia, la trazabilidad y la confianza institucional.





Objetivos y propósitos

El propósito de esta política es establecer un marco institucional que reconozca y gestione los datos como un activo estratégico esencial para la Universidad de Concepción, asegurando una administración responsable, transparente y alineada con la normativa vigente y las buenas prácticas. Se busca garantizar que los datos sean confiables, accesibles, seguros, íntegros, interoperables y tratados de forma ética, con especial énfasis en la protección de los derechos de las personas y su privacidad.

Este marco promueve la innovación y la mejora continua institucional, la analítica avanzada, la vinculación con el entorno en materia de datos, y el apoyo a la toma de decisiones en todas las áreas de la institución —formación, investigación, gestión y aseguramiento de la calidad—, en coherencia con el Plan Estratégico Institucional.

El objetivo de esta política es definir los principios, la estructura, los roles y los procesos necesarios para implementar un modelo integral y sostenible de gobierno de datos, que asegure la calidad, seguridad y uso responsable de la información. Este modelo debe facilitar una gestión eficiente y estandarizada, promover el cumplimiento normativo, fortalecer la confianza institucional, la rendición de cuentas y generar valor para toda la comunidad universitaria

Principios rectores

La política de gobierno de datos se fundamenta en los siguientes principios, que orientan la gestión de los datos como un activo estratégico, ético y conforme a la normativa vigente para la Universidad de Concepción:

- **Dato como Activo Estratégico:** Los datos son un activo estratégico clave para la innovación, la toma de decisiones y la generación de conocimiento en la Universidad.
- **Integridad y Confiabilidad:** Se garantizará la completitud, consistencia y vigencia de los datos a lo largo de su ciclo de vida.

UNIVERSIDAD DE CONCEPCIÓN
SECRETARÍA GENERAL
APROBADO DECRETO

079

Página 4 de 17

08 MAY 2026

SECRETARIO GENERAL



- **Protección y Privacidad:** La protección de la información, especialmente la personal, será prioritaria, asegurando el respeto de los derechos de los titulares y evitando usos indebidos.
- **Acceso y Uso Controlado:** Se facilitará el acceso a los datos para fines legítimos, bajo autorizaciones definidas y criterios de privacidad.
- **Interoperabilidad y Estandarización:** Se promoverá el uso de estándares que permitan el intercambio fluido de datos entre sistemas y unidades, facilitando su reutilización y el análisis integrado.
- **Uso Ético y Responsable:** El uso de los datos se basará siempre en criterios de ética, equidad y respeto, evitando toda forma de sesgo o discriminación.
- **Usabilidad:** Se garantiza que los datos sean comprensibles, accesibles y útiles para los distintos usuarios institucionales, facilitando su interpretación y aplicación en los procesos de toma de decisiones.
- **Valor Público y Analítica:** El uso de los datos se orientará a generar valor para la comunidad universitaria y la sociedad, promoviendo capacidades analíticas que fortalezcan los mandatos misionales.

Alcance Institucional

La Política de Gobierno de Datos de la Universidad de Concepción se aplica a toda la información institucional asociada a los distintos ámbitos de acción de la Universidad, desde su generación hasta su disposición final, sin distinción de formato, soporte o naturaleza. Incluye a todas las unidades académicas, administrativas, técnicas y de apoyo que participen en cualquiera de las etapas del ciclo de vida de los datos. Es de cumplimiento obligatorio para todas las personas vinculadas a la Universidad, así como para terceros autorizados que gestionen, utilicen o accedan a información institucional, asegurando su tratamiento conforme a las políticas y normativas vigentes.

UNIVERSIDAD DE CONCEPCIÓN
SECRETARÍA GENERAL
APROBADO DECRETO

Página 5 de 17
079 08 MAY 2026

SECRETARIO GENERAL



Asimismo, esta política se articula con otras políticas institucionales relacionadas y se adapta a la evolución tecnológica y normativa, promoviendo una cultura de responsabilidad compartida, transparente y con la gestión de los datos.

Niveles y Roles

Para asegurar una gestión de datos efectiva y coordinada, la Universidad de Concepción adopta un modelo de gobernanza distribuida en tres niveles principales, que promueve la corresponsabilidad y el trabajo colaborativo en toda la institución.

Niveles	Rol
Nivel estratégico	Comité Institucional de Gobierno de Datos es la instancia máxima, encargado de definir la visión, aprobar las directrices clave y asegurar la alineación del gobierno y la gestión de datos con los objetivos estratégicos de la Universidad.
Nivel de gestión	El Equipo de Gobierno de Datos Institucional implementa las directrices estratégicas, desarrolla estándares, herramientas y procedimientos y coordinará su ejecución con las distintas unidades institucionales, para la correcta implementación de la Política de Gobierno de Datos. El Consejo Asesor de Gobierno de Datos, asesora al Equipo de Gobierno de Datos Institucional para una correcta implementación de la política de gobierno de datos, en ámbitos asociados a cultura del dato, capacidades organizacionales, gestión del cambio, análisis institucional, seguridad de la información, la articulación con la Política de Protección de Datos Personales, entre otros.

UNIVERSIDAD DE CONCEPCIÓN
SECRETARÍA GENERAL
APROBADO DECRETO

079

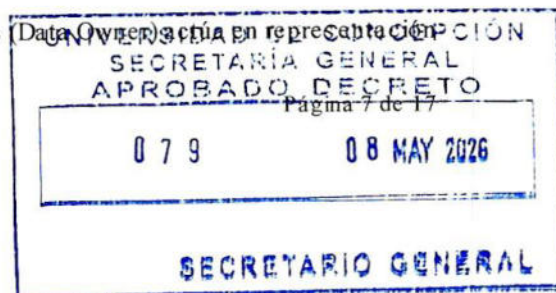
08 MAY 2026

SECRETARIO GENERAL



Nivel Funcional	Los Propietario Funcional de Datos ¹ (Data Owners), asume la autoridad y rendición de cuenta sobre los datos de un área del negocio (dominio). Es responsables de la información en su área, definen el uso, calidad y reglas de gestión de los datos en un área de negocio, conforme a las políticas institucionales y normativas legales vigentes.
Nivel Operativo	Los delegados de Datos (Data Stewards) velan por la calidad, la documentación y las buenas prácticas en el uso de los datos dentro de su ámbito. Los Administradores técnicos de Datos (Data Custodians) se encargan del almacenamiento, seguridad, infraestructura y mantenimiento de los datos.
Nivel Usuario	Usuarios de sistemas institucionales son las personas autorizadas dado su rol a usar, ya sea para ingresar o acceder a información de un sistema institucional, información que debe ser resguardada. Usuarios de datos (analistas, académicos, administrativos, estudiantes u otros perfiles autorizados) son personas que pueden acceder a los datos de los sistemas no teniendo acceso a los mismos directamente, los que deben cautelar la confidencialidad y el buen uso y seguridad de la información que manejan.

¹ Para efectos de datos personales, el Propietario Funcional de Datos (Data Owner) es el responsable del Tratamiento definido por la Ley N° 21.719





Este modelo articula la toma de decisiones estratégicas con una ejecución descentralizada y adaptable, fomentando la colaboración entre niveles y fortaleciendo una cultura institucional de corresponsabilidad, transparencia y gestión sostenible de los datos.

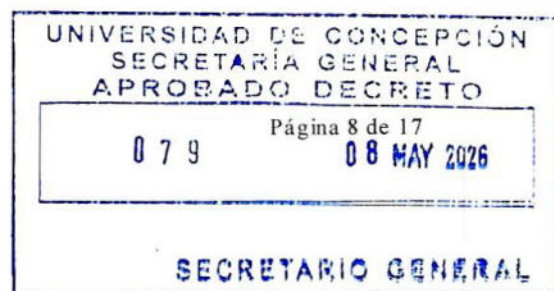
Clasificación de datos y niveles de confidencialidad y sensibilidad

La Universidad de Concepción establece un modelo de clasificación de los datos institucionales que promueva no solo la protección, el uso ético y la responsabilidad compartida en su gestión, sino también la transparencia y el valor público de la Universidad. Esta clasificación debe ser documentada en un Catálogo de Datos Institucional a cargo del Equipo de Gobierno de Datos Institucional.

Los datos se clasificarán atendiendo a su sensibilidad, valor estratégico y el impacto potencial ante un uso indebido bajo las siguientes categorías:

- Datos públicos
Información disponible al público o la comunidad universitaria, cuyo acceso o difusión no representa riesgos para la Universidad o terceros.
- Datos de uso controlado
Información de carácter interno u operativo, cuyo acceso está restringido a personal autorizado o terceros con autorización expresa.
- Datos críticos o sensibles
Datos cuyo acceso indebido pueda comprometer la seguridad, la integridad, los intereses estratégicos de la Universidad o los derechos de las personas, incluyendo aquellos protegidos por la Ley N° 21.719 que regula la protección y el tratamiento de los datos personales.

La clasificación será gestionada y revisada periódicamente por los propietarios funcionales de los datos, bajo la supervisión del Equipo de Gobierno de Datos Institucional.





Gestión del ciclo de Vida de los Datos

La Universidad de Concepción promueve la gestión del ciclo de vida de los datos como un componente estratégico de su quehacer institucional y de su modelo de gobernanza de datos. Este ciclo comprende la planificación, desde la generación o adquisición de datos, su almacenamiento y resguardo, el uso responsable y análisis de la información, así como su disposición final mediante conservación o eliminación segura, siempre en conformidad con la normativa vigente y las políticas institucionales.

Para asegurar su correcta aplicación, se deberá definir responsabilidades claras y procedimientos específicos en cada etapa del ciclo de vida, de modo que se garantice la calidad, la seguridad y el aprovechamiento estratégico de la información. Asimismo, la revisión constante y la adaptación del ciclo a las mejores prácticas forman parte del compromiso institucional con la mejora continua en la gestión de los datos.

Seguridad de los datos y la protección de datos personales

La Universidad de Concepción promueve un enfoque integral de seguridad de los datos y la protección de datos personales, entendiéndolo como un eje estratégico de su gestión institucional. La información será resguardada mediante medidas de seguridad proporcionales a su criticidad y sensibilidad, garantizando tanto la protección de los derechos de las personas como la reputación institucional.

La Universidad fomentará una cultura de seguridad transversal, basada en la prevención, la gestión de riesgos y la responsabilidad compartida, involucrando a toda la comunidad universitaria. Asimismo, se asegurará que todas las personas conozcan y cumplan las normativas vigentes en materia de protección de datos, junto con los protocolos internos y los estándares técnicos que regulan su manejo seguro. Esta política se sustenta en el marco legal nacional aplicable y en las buenas prácticas internacionales, manteniendo su vigencia frente a eventuales cambios regulatorios.

UNIVERSIDAD DE CONCEPCIÓN
SECRETARÍA GENERAL
APROBADO DECRETO

Página 9 de 17

079

08 MAY 2026

SECRETARIO GENERAL



Formación, Cultura Institucional y Uso Éticos de los Datos

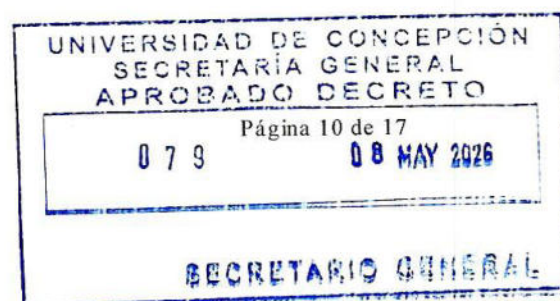
La Universidad de Concepción considera la formación y la promoción del uso ético de los datos como pilares esenciales de su desarrollo institucional y de su política de gobierno de datos, en concordancia con los lineamientos del Plan Estratégico Institucional (PEI). A través de programas de formación continua, difusión de buenas prácticas y el fomento de la cultura de responsabilidad, la Universidad promoverá competencias en ámbitos como la usabilidad, analítica de datos, innovación y gestión del cambio, contribuyendo a fortalecer la cultura organizacional y la adaptabilidad institucional.

La comunidad universitaria será parte activa de este compromiso, participando en programas de formación que se integrarán de manera sistemática al proceso de transformación institucional, asegurando el aprendizaje permanente y la sensibilización respecto al valor estratégico de los datos.

Evaluación, Revisión y Actualización de la Política

La Política de Gobierno de Datos de la Universidad de Concepción será evaluada y actualizada periódicamente, como parte del compromiso institucional con la mejora continua y la gestión responsable de los datos. Las revisiones se efectuarán al menos cada tres años, o antes si así lo determina el Comité de Gobierno de Datos, asegurando la coherencia con la normativa vigente, los estándares internacionales, los avances tecnológicos y las prioridades estratégicas de la Universidad.

La responsabilidad de este proceso recaerá en el Comité de Gobierno de Datos y será implementado por el Equipo de Gobierno de Datos Institucional.





Glosario

Gobernanza de Datos: Conjunto de normas, roles, procesos y responsabilidades que aseguran que los datos se gestionen de manera controlada, confiable y estratégica en la institución.

Fiabilidad: Capacidad de un sistema o proceso para funcionar de manera consistente bajo condiciones específicas, incluyendo tolerancia a fallos y capacidades de recuperación.

Interoperabilidad: Capacidad de distintos sistemas y aplicaciones para intercambiar datos entre sí de manera efectiva, evitando duplicidad o pérdida de información.

Integridad: Condición que garantiza que los datos se mantengan completos, exactos y sin alteraciones no autorizadas a lo largo de su ciclo de vida.

Privacidad: Derecho de las personas a controlar cómo se recopila, utiliza y comparte su información personal.

Trazabilidad: Posibilidad de seguir el historial de un dato, identificando su origen, cambios realizados y responsables de esos cambios.

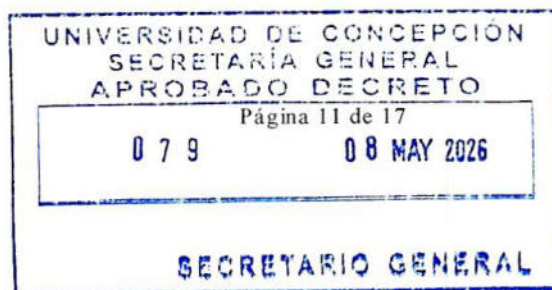
Usabilidad: Grado en que los datos son comprensibles, accesibles y útiles para quienes los utilizan en sus funciones o procesos.

Propietario Funcional de Datos (Data Owner): responsable Funcional de los datos en un área específica. Define reglas de uso, calidad y gestión de los datos bajo su dominio.

Delegado de datos (Data Steward): Encargado de velar por la calidad, documentación y buenas prácticas en el uso cotidiano de los datos dentro de su unidad.

Administrador técnico de datos (Data Custodian): Persona o unidad encargada de la infraestructura tecnológica, almacenamiento y seguridad de los datos. Garantiza que estén disponibles y protegidos.

Delegado de protección de Datos: Rol definido en la Ley N.º 21.719 de Chile, responsable de supervisar el cumplimiento de la normativa de protección de datos personales en la Universidad.





Anexo

Para asegurar una comprensión clara del modelo de gobernanza de datos de la Universidad de Concepción, se presentan a continuación los roles y responsabilidades asociados a cada uno de los niveles definidos en esta política.

Esta definición permite establecer un marco común de funciones y ámbitos de acción, garantizando que la gestión de los datos institucionales sea coherente, transparente y sostenible. Cabe señalar que la identificación detallada de personas o unidades responsables será determinada de manera progresiva durante la implementación de esta política, con el acompañamiento de la empresa consultora y en concordancia con la estructura organizacional vigente.

Por otra parte, es relevante mencionar que esta organización sugerida incluye sólo la creación de una unidad. El resto de la gobernanza está sustentada en instancias de coordinación institucional nuevas y en el reconocimiento oficial de tareas que hoy se realizan de manera implícita y desorganizada dentro de la organización en los cargos de esta propuesta.

Nivel	Rol/integrante	Descripción	Responsabilidad específica
Estratégico Comité Institucional de Gobierno de Datos	Propuesta: • Rector • Vicerrectores • Un representante por grupo de Facultades y Escuelas • Apoyado técnicamente por el	Instancia máxima de conducción del gobierno de datos Institucional. Garantiza legitimidad institucional y la integración de las distintas áreas en la toma de decisiones estratégicas.	• Aprobar la visión y los lineamientos de la gobernanza de datos • Asegurar la lineación con la misma misión y el plan estratégico institucional. • Aprobar políticas y directrices institucionales. • Respalda la implementación y asignar prioridades a nivel

Institucional
UNIVERSIDAD DE CONCEPCIÓN
SECRETARÍA GENERAL
APROBADO DECRETO

Página 12 de 17

079

08 MAY 2026

SECRETARIO GENERAL



	jefe del Equipo de Gobierno de Datos		
Gestión Equipo de Gobierno de Datos	Propuesta: • Conformación de Equipo con integrantes 2 o 3 personas dependientes de la Unidad de Analisis Institucional (de la Dirección de Desarrollo Estratégico	Nivel encargado de traducir las decisiones estratégicas en directrices operativas, coordinando estándares y procesos.	• Desarrollar procedimientos y lineamientos de gestión de datos. • Coordinar acciones con facultades y direcciones. • Monitorear calidad y cumplimiento normativo. • Servir de enlace entre el comité estratégico y el nivel funcional, operativo y usuario. • Coordinar el trabajo de los niveles funcionales y operativo para la correcta implementación de esta política.
Consejo Asesor de Gobierno de Datos	Propuesta: • Estará compuesta por representantes de las direcciones de: • Personal • Comunicación • Desarrollo Estratégico	Asesorar al Equipo de Gobierno de Datos Institucional para una correcta implementación de la política de gobierno de datos.	Asesorar y proponer iniciativas para el correcto despliegue de la política de Gobierno de Datos en ámbitos de: • Gestión del cambio organizacional. • Instalación de Capacidades • Seguridad y protección de los

UNIVERSIDAD DE CONCEPCIÓN
SECRETARÍA GENERAL
APROBADO DECRETO

Página 13 de 17

079

08 MAY 2026

SECRETARIO GENERAL



	• Tecnologías de Información • Delegado de Protección de Datos Personales.		• Disponibilidad y Uso de los datos.
Funcional	• Propietario Funcional de Datos (Data Owners) Se debe definir si esta función se cumplirá a nivel de Vicerrectorías (Aconsejable para mantener homogeneidad en los criterios en casos como Formación), las direcciones dueñas de sistemas u otra propuesta.	Representan la autoridad funcional sobre los datos de su ámbito de responsabilidad. Son responsables de definir su propósito, estándares de calidad y condiciones de acceso.	• Definir los metadatos obligatorios y atributos de los datos bajo su responsabilidad. • Establecer matrices de acceso y permisos por rol. • Determinar criterios de calidad y validación de los datos. • Definir reglas de conservación, intercambio y publicación de los datos (internos, externos e internacionales). • Rendir cuentas por las decisiones y prácticas de gestión de datos en su dominio.
Operativo	• Delegado de datos (Data Stewards) Se debe definir quién es el encargado que	Nivel encargado de ejecutar la gestión técnica y funcional de los datos en el día a	• Administrar la infraestructura tecnológica y las plataformas asociadas al ciclo de vida de los datos.



	ayuda al Propietario funcional, normalmente son personas que ya trabajan y hacen esto en Vicerrectorías y Direcciones. Será apoyado por el Equipo de Gobierno de Datos. • Administrador técnico de datos (Data Custodian) Se debe definir quienes serán, estos perfiles son más técnicos y son contrapartes que corresponderían a DTL.	día, asegurando su correcta administración y documentación.	• Implementar controles técnicos que aseguren la calidad, disponibilidad, integridad y seguridad de la información. • Documentar procesos, transformaciones y flujos de datos según los estándares institucionales. • Promover buenas prácticas en el uso, registro y resguardo de los datos dentro de cada unidad.
Usuario	• Usuarios de sistemas institucionales • Usuarios de datos (analistas, académicos, administrativos, estudiantes u otros	Corresponde a todas las personas que consultan, registran, procesan o utilizan datos institucionales en el ejercicio de sus funciones o actividades. Son	• Utilizar los datos institucionales conforme a las políticas de seguridad, confidencialidad y uso responsable. • Registrar y mantener la información en los sistemas

UNIVERSIDAD DE CONCEPCIÓN
SECRETARÍA GENERAL
APROBADO DECRETO

Página 15 de 17

079

08 MAY 2026

SECRETARIO GENERAL



perfiles
autorizados)

responsables de
aplicar las políticas y
buenas prácticas
definidas por los
niveles superiores del
modelo

procedimientos y estándares
definidos.

- Reportar errores, inconsistencias o incidentes relacionados con los datos.
- Proteger sus credenciales de acceso y respetar los niveles de autorización asignados.
- Participar en las instancias de capacitación o sensibilización que promueva la Universidad sobre gestión y protección de datos.

UNIVERSIDAD DE CONCEPCIÓN
SECRETARÍA GENERAL
APROBADO DECRETO

Página 16 de 17

079

08 MAY 2026

SECRETARIO GENERAL



Estrategia y Calidad



Dirección de
Desarrollo Estratégico
Universidad de Concepción