



Política de Protección de Datos Personales



A. Introducción

Política de Protección de Datos Personales

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

Política de Protección de Datos Personales



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

Política de Protección de Datos Personales



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

Política de Protección de Datos Personales



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

Política de Protección 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

Política de Protección de Datos Personales



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

Política de Protección de Datos Personales



La Universidad podrá comunicar datos personales a terceros únicamente cuando:

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

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.

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.



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.

Política de Protección de Datos Personales