

**APRUEBA PROTOCOLOS DE DATOS
PERSONALES Y ACUERDO DE
CONFIDENCIALIDAD PARA ACCESO A
INFORMACIÓN DE SISTEMAS.**

SANTIAGO, 01/12/2025 - 6891.-

VISTOS: El Decreto con Fuerza de Ley 29 de 2023, del Ministerio de Educación, que fija el Estatuto Orgánico de la Universidad de Santiago de Chile, adecuado al Título II de la Ley 21.094, sobre Universidades Estatales; el Decreto con Fuerza de Ley 1-19653, de 2000, que fija el texto refundido, coordinado y sistematizado de la Ley 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; el Decreto con Fuerza de Ley 29, de 2004, del Ministerio de Hacienda, sobre Estatuto Administrativo; la Ley 19.880, que establece Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; la Ley 21.094 sobre Universidades Estatales; la Ley 19.628 sobre Protección de la Vida Privada; la Resolución 1414 de 2025, que establece nueva estructura orgánica de la Universidad de Santiago de Chile, del Rector; el Decreto TRA 323/44/2024; el Decreto Universitario N° 1381 de 2007, que modifica Decreto Universitario N° 755 de 1988, sobre el régimen de subrogación en el cargo de Rector; las Resoluciones 36 de 2024 y 8 de 2025, ambas de Contraloría General de la República.

CONSIDERANDO:

a) Que, la Ley N° 19.628, sobre Protección de la Vida Privada, establece en su artículo 4° que el tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.

b) Que, en el mismo sentido, la Ley N° 21.719, que regula la protección y el tratamiento de los datos personales y crea la agencia de protección de datos personales, la cual entra en vigencia el 01 de diciembre de 2026, estipula en su artículo 1° que todo tratamiento de datos personales que realice una persona natural o jurídica, incluidos los órganos públicos, debe respetar los derechos y libertades de las personas y quedará sujeto a las disposiciones de esta ley.

d) Que, en concordancia con lo ya preceptuado, el Consejo para la Transparencia, durante diciembre de 2020, emitió recomendaciones sobre protección de datos personales por parte de los órganos de la Administración del Estado.

e) Que, por medio de la Resolución Exenta N° 1414 de 2025, que establece nueva estructura orgánica de la Universidad de Santiago de

Chile, indica la Dirección Estratégica Informática, señalando entre sus funciones el velar por el cumplimiento de la legislación vigente en materia de ética en el diseño, implementación y operación de los sistemas informáticos, así como de la protección de los datos y la privacidad de las personas; gestionar los sistemas informáticos y la interoperabilidad de los mismos, gestionar la infraestructura computacional y de comunicación, definiendo estándares tecnológicos y asegurando la ciberseguridad de los sistemas.

f) Que, con el fin de proteger la información personal de la comunidad universitaria, la Dirección Estratégica Informática ha establecido una serie de protocolos. Estos detallan las acciones y procesos que la universidad aplicará para asegurar la vigilancia, transparencia y exactitud de los datos. De esta forma, no solo se garantizará el cumplimiento de la normativa vigente, sino que también se mejorará la eficiencia de los procesos institucionales. Adicionalmente, se comunicará a los dueños de la información el propósito de su uso y los procesos específicos en los que se emplearán sus datos.

g) Que, debido a la amplitud del contenido de los protocolos, mencionados en el considerando anterior, aquellos fueron subdivididos en Protocolo de Datos Personales, Sección: Tratamiento de Datos Personales; Protocolo de Datos Personales, Sección: Consentimiento Informado; y Acuerdo de Confidencialidad Para Acceso a Información de Sistemas.

h) Que, en tal orden de ideas, por medio de Memorándum N°31448 de 2025, la Dirección Estratégica Informática de esta Casa de Estudios, solicitó a esta Dirección Jurídica elaborar el acto administrativo aprobatorio de dichos protocolos.

RESUELVO:

1. APRUÉBENSE el Protocolo de Datos Personales, Sección: Tratamiento de Datos Personales; Protocolo de Datos Personales, Sección: Consentimiento Informado; y Acuerdo de Confidencialidad Para Acceso a Información de Sistemas, cuyos textos son los siguientes:

	Protocolo de datos personales Sección: Tratamiento de datos personales	Versión: 1.0 04/08/2025
Elaborado por: - Felipe Andrés Fuentes Bravo Revisado por: - Gustavo Valdés Pérez	Aprobado por: -	

1-. Introducción

El presente documento tiene como objetivo establecer las bases para el tratamiento de datos personales en nuestra organización, garantizando la protección de la privacidad y seguridad de los datos de nuestros estudiantes, académicos y funcionarios. En este sentido, velamos estrictamente por el cumplimiento del marco normativo aplicable a estas materias.

2-. Marco Legal

Marco normativo vigente:

- Ley N° 19.628/1999 sobre Protección de la Vida Privada (Chile): Esta ley regula el tratamiento de datos personales en Chile y establece los principios y derechos que deben ser respetados.
- Ley N° 21.719/2024 sobre la Protección de Datos Personales: La cual regula cómo se debe hacer el tratamiento de este tipo de datos y la mejora de la protección de los derechos de los titulares de ésta información, y cuáles son los procedimientos y medios para que los titulares hagan valer sus derechos.
- Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado, de diciembre de 2020.
- Reglamento General de Protección de Datos (GDPR) (Unión Europea): Este reglamento establece los principios y obligaciones para el tratamiento de datos personales en la Unión Europea.
- Resolución 1414/2025 de la Universidad de Santiago de Chile: Establece la Dirección Estratégica Informática dentro de la estructura orgánica de la Universidad, dando dentro de las funciones a realizar el "... *velar por el cumplimiento de la legislación vigente en materia de ética en el diseño, implementación y operación de los sistemas informáticos, así como de la protección de los datos y la privacidad de las personas; gestionar los sistemas informáticos y la interoperabilidad de los mismos; gestionar la infraestructura computacional y de comunicación, definiendo estándares tecnológicos y asegurando la ciberseguridad de los sistemas ...*"

3-. Principios de Protección de Datos

La Universidad, dentro de la Dirección Estratégica Informática se compromete a los siguientes principios de protección de datos personales:

- **Licitud:** El tratamiento de datos personales se realizará de manera lícita y transparente.
- **Lealtad:** El tratamiento de datos personales se realizará de manera leal y sin intención de engañar o perjudicar a los titulares.
- **Transparencia:** Los titulares tendrán acceso a información clara y precisa sobre el tratamiento de sus datos personales.
- **Minimización de datos:** Solo se recopilarán y tratarán los datos personales necesarios para el propósito específico.
- **Exactitud:** Los datos personales serán exactos y actualizados, acorde a los protocolos y reglamentos que se establezcan en la organización.
- **Confidencialidad:** Se adoptarán por parte de la Universidad las medidas tendientes a proteger los datos frente el tratamiento no autorizado o ilícito.

	Protocolo de datos personales Sección: Tratamiento de datos personales	Versión: 1.0 04/08/2025
Elaborado por: - Felipe Andrés Fuentes Bravo Revisado por: - Gustavo Valdés Pérez	Aprobado por: -	

- **Seguridad:** Los datos deben poseer medidas de protección y control para asegurar la confidencialidad, integridad y disponibilidad con el propósito de evitar divulgaciones, accesos y modificaciones no autorizadas, daños o eliminación.
- **Responsabilidad:** La Comunidad Universitaria en su conjunto es la responsable de la protección de los datos. Asimismo, quienes por su rol realicen tratamiento de datos personales, serán responsables de conformidad a las obligaciones que les impone la ley.
- **Calidad de los datos:** Los datos contenidos en las bases de datos deben ser exactos, actualizados y responder con veracidad a la situación real de su titular.
- **Finalidad:** Los datos personales se utilizarán sólo para las materias propias de la competencia de nuestra institución, considerando la función legal específica que se está ejecutando y que justifica el procesamiento de los datos personales.
- **Deber de protección especial de los datos personales sensibles (artículo 10 de la Ley N°19.628):** Existe una prohibición general de tratamiento de datos personales sensibles, salvo cuando una disposición legal lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.
- **Deber de información (artículos 4 y 20 de la Ley N°19.628):** Como universidad estatal nos obligamos a informar al titular acerca de la identidad del órgano responsable de la base de datos, la finalidad perseguida con el tratamiento de la información y de su posible comunicación a terceros.

4. Derechos de los Titulares

Los titulares de datos personales tienen los siguientes derechos:

- **Derecho a acceder a sus propios datos:** Los titulares tienen derecho a exigir información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.
- **Derecho a conocer:** Los titulares tienen derecho a conocer si sus datos personales están siendo tratados por la Universidad y, en ese caso, a conocer la información sobre el tratamiento y protección que ésta está recibiendo.
- **Derecho a rectificar:** Los titulares tienen derecho a exigir que los datos que sean erróneos, inexactos, equivocados o incompletos, se modifiquen, siempre que se acredite debidamente cualquiera de dichas circunstancias y se indique con claridad la corrección solicitada.
- **Derecho a cancelar o eliminar:** Los titulares tienen derecho a solicitar que se eliminen aquellos datos cuyo almacenamiento carece de fundamento legal; los que haya proporcionado voluntariamente; o aquellos se utilicen para comunicaciones de carácter comercial y el titular no desee seguir figurando en el registro de datos.
- **Derecho al bloqueo de los datos:** Los titulares tienen derecho a exigir la suspensión temporal de cualquier operación de tratamiento de los datos almacenados, cuando el titular ha proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones meramente informativas y no desee continuar figurando en el registro respectivo de modo temporal o definitivo. También procede cuando la exactitud de los datos personales no pueda ser establecida o cuya vigencia sea dudosa y respecto a los cuales no corresponda la cancelación.
- **Sobre el ejercicio de estos derechos: El ejercicio de estos derechos no es absoluto,** por lo que antes de determinar su procedencia, la institución verificará la

	Protocolo de datos personales Sección: Tratamiento de datos personales	Versión: 1.0 04/08/2025
Elaborado por: - Felipe Andrés Fuentes Bravo Revisado por: - Gustavo Valdés Pérez	Aprobado por: -	

concurrencia de alguna de las causales de denegación que establece la Ley N°19.628, como, por ejemplo, cuando el ejercicio de los derechos impida o entorpezca el cumplimiento de funciones del organismo; cuando afecte la reserva o secreto establecido en disposiciones legales o reglamentarias; o cuando el ejercicio de los derechos se efectúe respecto de datos personales que están siendo almacenados por mandato legal.

5-. Responsabilidades y Obligaciones

La Universidad asume las siguientes responsabilidades y obligaciones:

- **Informar al titular de los datos el propósito del almacenamiento de sus datos personales**, es decir, la finalidad perseguida con el tratamiento de la información, la posible comunicación a terceros, y la denominación del órgano o servicio responsable del tratamiento (artículos 4 y 20 de la Ley N°19.628).
- **Efectuar el tratamiento de los datos personales cumpliendo con el principio de finalidad** (artículo 9 de la Ley N°19.628).
- **Responsable del tratamiento de datos**: La Universidad designará un responsable del tratamiento de datos que se encargará de garantizar el cumplimiento de las leyes y regulaciones aplicables.
- **Obligaciones de los encargados del tratamiento de datos**: Los encargados del tratamiento de datos tendrán la obligación de cumplir con las instrucciones del responsable del tratamiento de datos y de garantizar la seguridad y confidencialidad de los datos personales. La Universidad es responsable de cuidar que los datos personales se traten con la **debida diligencia** (artículo 11 de la Ley N°19.628).
- **Cumplir con la obligación de secreto o confidencialidad** (artículo 7 de la Ley N°19.628).
- **Notificación de incidentes de seguridad**: La Universidad notificará a los titulares y a las autoridades competentes en caso de incidentes de seguridad que afecten la protección de sus datos personales.

6-. Unidades relacionadas

Dentro del tratamiento de la información, la Dirección Estratégica Informática deberá relacionarse con unidades que manejan información privada de las personas que poseen relación con la Universidad, dentro de las cuales se encuentran:

- **Vicerrectoría Académica**: Unidad que posee dentro de sus actividades la gestión general de los servicios educativos, principalmente hacia estudiantes de pregrado. Gestionando de ésta forma toda la información del estudiante de la Universidad y los datos no contractuales de los docentes. A pesar que el foco es el estudiantado de pregrado, dentro del Departamento de Registro Académico y Curricular, se mantiene, trabaja y almacena información relativa a los programas de postgrado. Otra información relacionada a los estudiantes de postgrado es generada por la Vicerrectoría de Posgrado, mientras que aquella relacionada a los cursos de formación continua e internacionalización es provista por la Vicerrectoría de Vinculación con el Medio.
- **Vicerrectoría de Apoyo al Estudiante**: Unidad que dentro de las funciones es mantener contacto con el estamento estudiantil, en temas particulares como en las distintas agrupaciones que éste maneje. Además, debe velar por el bienestar de la comunidad estudiantil. Dentro de ésta Vicerrectoría se encuentran unidades que

	Protocolo de datos personales Sección: Tratamiento de datos personales	Versión: 1.0 04/08/2025
Elaborado por: - Felipe Andrés Fuentes Bravo Revisado por: - Gustavo Valdés Pérez	Aprobado por: -	

utilizan y generan información relativa de los estudiantes, tales como el Departamento de Beneficios Estudiantiles, Departamento de Gestión del Deporte, Departamento de las Culturas y las Artes, Departamento de Promoción de Vida Saludable.

- **Vicerrectoría de Finanzas y Logística:** Unidad encargada de las personas, bienes inmuebles y muebles, principalmente encargada de temas financieros, recibiendo información desde otras vicerrectorías, como lo es la Vicerrectoría de Apoyo al estudiante que indica rebajas arancelarias del estudiantado, para los cobros correspondientes; desde la Vicerrectoría Académica, informando los matriculados y docentes de la Universidad en temas académicos. Además es quien ve todo el tema contractual de los miembros de la institución y compras que ésta realice.
- **Vicerrectoría de Calidad de Vida, Género, Equidad y Diversidad:** Es quién da coherencia y articulación a las políticas que promuevan la transversalización de la perspectiva de género, inclusión, diversidad y bienestar. Lo que lleva a la institución a cumplir normativas vigentes en este ámbito, trabajando en conjunto con instituciones de educación superior, organizaciones de la sociedad civil, organismos gubernamentales y otros.
- **Dirección Jurídica:** Unidad que a través de su orgánica interna especializada brindará apoyo jurídico en la materia.

7-. Procesos

La Universidad se compromete a proteger la privacidad de la información declarada como personal acorde a lo estipulado en las leyes y protocolos vigentes, dando seguridad, disponibilidad, trazabilidad y transparencia de la información de los miembros de la comunidad universitaria.

Para validar el cumplimiento de las diversas normas, asociadas a la Ley N° 21.719/2024 sobre la Protección de Datos Personales, se establecen distintos procesos.

7.1-. Obtención de información personal

Para la obtención de datos personales se debe realizar siempre la entrega de un consentimiento informado, el cual establece como base los siguientes puntos:

- **Identificación de responsables:** Quién es la persona responsable de la administración de los datos que se obtendrán.
- **Indicar qué datos serán obtenidos en el proceso:** Listado y explicación de cada uno de los datos que se están obteniendo en el proceso correspondiente.
- **Finalidad del tratamiento:** Indicar para qué será utilizada la información obtenida, indicar los distintos procesos y reportes tanto internos como externos.
- **Periodo de conservación de información:** Informar cuánto tiempo se resguardarán los datos.
- **Forma de actualización de información:** Se debe establecer cómo el usuario podrá actualizar información en caso de equivocación e informar cambios en caso que, dentro del periodo de conservación, sea necesario informar.
- **Forma de informar reversibilidad:** Se debe establecer la forma de que el usuario puede dar pie atrás del consentimiento indicado.

Para esto se ha realizado un [documento base](#) en donde el cual se dejará disponible para ser utilizado posteriormente.

	Protocolo de datos personales Sección: Tratamiento de datos personales	Versión: 1.0 04/08/2025
Elaborado por: - <u>Felipe Andrés Fuentes Bravo</u> Revisado por: - Gustavo Valdés Pérez	Aprobado por: -	

7.2-. Actualización de información personal

Cada unidad de receptora y encargada de información que sea considerada personal, además de la de sus procesos internos, debe implementar un proceso de cambio de información por parte de los usuarios, y cómo esos cambios son informados a la Dirección Estratégica Informática, dada la centralización de información en la qué ésta es encargada. Por parte de la Dirección Estratégica Informática, se establece que los cambios se deben hacer de la siguiente manera para los sistemas internos:

1. Se debe actualizar la información relacionada con la cuenta institucional, asociada al correo electrónico, de ser necesaria.
2. Se debe actualizar la información relacionada a los sistemas de matrícula y contratos, de ser necesaria.
3. Se debe actualizar la información relacionada a los servicios web, de ser necesaria.

7.3-. Eliminación de datos personales

El usuario siempre puede solicitar el proceso de eliminación de su información personal, por lo cual, cada unidad que maneje este tipo de información, debe establecer un protocolo que permita al usuario solicitar la eliminación de la información y el cómo eso se informará a la Dirección Estratégica Informática, dado qué:

- Se debe establecer qué información se puede o no eliminar, por los procesos internos de cada unidad y de la Universidad en sí.
- Por temas estadísticos generales que informa la Universidad, la información deberá ser anonimizada, proceso en el cual se puede solicitar apoyo a la Dirección Estratégica Informática.

7.4-. Consulta de datos personales

El usuario podrá consultar a la Dirección Estratégica Informática, mediante solicitud formal, siendo entregada la información centralizada que se posee, indicando desde qué unidades se posee la información.

La información entregada solo corresponde a la información personal del solicitante, no se puede hacer solicitud de terceros, a menos que exista requerimiento formal de información mediante orden judicial o solicitud del Ministerio Público, lo cual deberá estar visado y remitido desde la Dirección Jurídica de la Universidad de Santiago de Chile.

	Protocolo de datos personales Sección: Consentimiento informado	Versión: 1.0 04/08/2025
Elaborado por: - <u>Felipe Andrés Fuentes Bravo</u> Revisado por: - Gustavo Valdés Pérez	Aprobado por: -	

1-. Introducción

El presente documento posee la finalidad de mostrar el documento de Consentimiento Informado que utiliza la Dirección Estratégica Informática para los datos que solicita.

2-. Datos solicitados

Dentro de los datos solicitados, se solicitan siempre información asociada a las normas legales correspondientes a los distintos procesos que están vinculados al desarrollo de las actividades de la Universidad, dentro de lo cual, se puede solicitar información transversal e información específica, acorde a los procesos donde la persona se encuentra vinculada a la institución.

2.1-. Detalle de los datos solicitados a nivel general

La Dirección Estratégica Informática, solicita los siguientes datos para la identificación de las personas:

- **RUN o Número de pasaporte:** Identificador único de la persona, tomando el RUN como identificador general en sí, o pasaporte en caso de personas extranjeras.
- **Tipo de identificación:** Indicador para ver si el identificador es un RUN o pasaporte.
- **Nombres:** Nombres y apellidos de la persona asociada.
- **Nacionalidad:** Nacionalidad de la persona asociada.
- **Sexo:** Sexo registral de la persona asociada.
- **Género:** Identidad de género de la persona asociada.
- **Dirección:** Lugar de residencia de la persona.
- **Correo electrónico personal:** Correo electrónico de la persona asociada.
- **Teléfono de contacto:** Número de teléfono directo donde se puede localizar a la persona indicada.
- **Número de teléfono personal:** Número telefónico de contacto de la persona asociada.
- **Estudios previos:** Información de los estudios de la persona en temas universitarios o técnicos.

2.2-. Otro tipo de información utilizada

Dependiendo de los procesos que se estén llevando a cabo, los datos indicados acá pueden variar, de todas formas, los proveedores de ésta información proviene de:

- **Vicerrectoría Académica:** Encargada de los datos académicos de los estudiantes de la Universidad.
- **Vicerrectoría de Apoyo al Estudiante:** Encargada de los datos de beneficios y servicios estudiantiles.
- **Vicerrectoría de Finanzas y Logística:** Encargada de los datos contractuales de los miembros de la comunidad universitaria y de los pagos y uso de recursos de los estudiantes.
- **Vicerrectoría de Calidad de Vida, Género, Equidad y Diversidad:** Encargada de temas de datos de género y diversidad.

	Protocolo de datos personales Sección: Consentimiento informado	Versión: 1.0 04/08/2025
Elaborado por: - Felipe Andrés Fuentes Bravo Revisado por: - Gustavo Valdés Pérez	Aprobado por: -	

3-. Finalidad de uso

Los datos obtenidos serán utilizados para:

- Comunicación intersistemas, para mantener y cumplir con la exactitud y datos actualizados, permitiendo de ésta manera que cualquier cambio que interfiera en más de un sistema, ésta pueda ser visualizada por todos los sistemas correspondientes.
- Estadísticas institucionales, con el fin de permitir obtener información agrupada de las personas, con el fin de sacar estadísticas que permitan a los sistemas de gestión institucional tomar decisiones estratégicas para la continuidad de la operación universitaria.
- Entrega de información ministerial, en conjunto con la Dirección de Desarrollo Institucional y Aseguramiento de la Calidad, entregar la información al Ministerio de Educación y otras entidades gubernamentales, solicitada a la Universidad para velar el funcionamiento y gestión correspondiente a lo solicitado a las Universidades estatales del país. Esta información puede ser de forma agrupada como desagrupada sin anonimización, dependiendo del proceso solicitado, dentro de los cuales, se encuentran:
 - Procesos de información de matrícula de los estudiantes de la Universidad.
 - Procesos de información de avance académico de los estudiantes de la Universidad.
 - Procesos de información de titulados de los estudiantes de la Universidad.
 - Procesos asociados a la acreditación de programas de estudios y la acreditación institucional.
- Entrega de información a la Dirección Jurídica de la Universidad, para casos donde se solicite para sus procesos legales.
- Entrega de información a Secretaría General de la Universidad, con el fin de que pueda realizar sus procesos asociados a la normativa y resoluciones internas de la Universidad.

4-. Período de conservación de la información

La información será almacenada con detalle de las personas por un tiempo de 15 años desde la última aceptación del acuerdo de confidencialidad entre la persona y la Universidad, esto permitirá el uso estadístico correspondiente para la gestión universitaria y tomando en cuenta qué dentro de los procesos de acreditación se solicita información de los últimos 5 años, y teniendo en cuenta que la duración máxima de un plan de estudios es de 7 años, se queda con un tiempo acorde para poder entregar esa información.

Después de los 15 años, los datos no serán eliminados, sino que serán anonimizados para los procesos estadísticos, pero no para procesos de información detallada a entregar al Ministerio de Educación, temas jurídicos y participación universitaria; como por ejemplo, para gestionar validación de certificados de titulación de estudiantes de programas de estudios de la Universidad, que les permita acceso a ofertas laborales o de estudios, solicitadas por los mismos estudiantes.

5-. Forma de actualización de la Información

La información será manejada por las distintas vicerrectorías asociadas, teniendo en cuenta lo mencionado en el punto 2.2 del presente documento, donde se indica el origen de la información acorde a la temática.

	Protocolo de datos personales Sección: Consentimiento informado	Versión: 1.0 04/08/2025
Elaborado por: - <u>Felipe Andrés Fuentes Bravo</u> Revisado por: - Gustavo Valdés Pérez	Aprobado por: -	

Cada vicerrectoría establecerá sus procesos de actualización de información acorde a la gestión que ellas posean.

6-. Reversibilidad

El proceso de reversibilidad del consentimiento informado, para dar cumplimiento a la ley, es la generación de un sistema en dónde la Universidad provee a cada miembro de la comunidad saber el estado de su información y la forma de dar pie atrás a lo que se ha indicado previamente, sin perjuicio de lo anterior, se establece qué todo miembro de la comunidad debe entregar información básica para gestionar:

- Su trayectoria académica según corresponda a lo indicado por el Ministerio de Educación y otras entidades correspondientes a este ámbito, informado por la Vicerrectoría Académica y Vicerrectoría de Apoyo al Estudiante.
- Datos básicos para la gestión contractual de las personas y seguimiento del cumplimiento de las normativas legales asociadas a las Instituciones públicas y Universidades del Estado de Chile, informadas por la Vicerrectoría de Finanzas y Logística.

7-. Comunicación de datos a terceros

La Universidad podrá comunicar, ceder, transferir, transmitir o realizar cualquier otra de las actuaciones dispuestas en la letra o) del artículo 2º de la Ley N°19.628, siempre que se trate de materias de su competencia y con sujeción a las normas establecidas en dicha ley.

En tales casos, no necesitará el consentimiento del titular. Sin perjuicio de lo anterior, la Universidad podrá entregar los datos personales que maneje, según lo prescrito en la Ley N°19.628, en los siguientes casos:

- Comunicación de datos personales que sea necesaria para la prestación de servicios con terceros, y siempre que ese tercero cumpla con las garantías necesarias sobre protección de datos.
- Se trate de datos estadísticos, agregados y/o anónimos.
- Se realice en cumplimiento de un mandato legal o un requerimiento judicial o en los casos en que sea necesario para garantizar el interés público.
- En el contexto de la comisión de un delito y estos sean requeridos mediante orden judicial por el tribunal competente en la materia o ante requerimiento del Ministerio Público.

8-. Incumplimiento y responsabilidades asociadas

El incumplimiento de alguna de las disposiciones que regulan la Política de Datos Personales de la Universidad dará lugar a la responsabilidad y eventuales sanciones de conformidad a los deberes y obligaciones que el (la) infractor(a) le corresponda, según su calidad dentro de la institución (estudiante, académico, funcionario).

Tratándose del incumplimiento por parte de una entidad externa o empresa que se vincule con las bases de datos de la Universidad, se estará a las sanciones contenidas en el respectivo contrato.

	Protocolo de datos personales Sección: Consentimiento informado	Versión: 1.0 04/08/2025
Elaborado por: - <u>Felipe Andrés Fuentes Bravo</u> Revisado por: - Gustavo Valdés Pérez	Aprobado por: -	

Lo anterior, sin perjuicio de la responsabilidad civil y/o penal que en cada caso corresponda, y de lo establecido en el artículo 23 de la Ley N°19.628, sobre Protección de la Vida Privada.

	Acuerdo de Confidencialidad para acceso a información de sistemas	Versión: 1.1 11/06/2025
Elaborado por: - Felipe Andrés Fuentes Bravo - Rodrigo Canales Ramirez	Aprobado por:	

1-. Introducción

En Santiago, a <Día> del <Mes> del <Año> entre <NOMBRE ENCARGADO DE RECEPCIONAR LA INFORMACIÓN>, <RUT>, en su rol de <CARGO> y don <NOMBRE DEL VICERRECTOR>, <RUN del Vicerrector>, <CARGO>, en adelante referidas conjuntamente como las "Partes" y, en forma individual cada una de ellas como "Parte", han convenido el presente acuerdo de confidencialidad, en adelante el "Acuerdo", el que consta en las cláusulas que más adelante se indican.

2-. Antecedentes

Las partes están colaborando en proyectos de centralización de información de la Universidad de Santiago de Chile, dentro de lo cual la <UNIDAD ASOCIADA, DEBE SER LA DIRECCIÓN ESTRÁTÉGICA INFORMÁTICA O LA UNIDAD DE GESTIÓN DE LA INFORMACIÓN E INNOVACIÓN> necesita poder acceder a los datos generados por el <UNIDAD, SISTEMA O PROCESO DE DÓNDE SE CONSUMIRÁ LA INFORMACIÓN>, con el fin de informar a sistemas de gestión interna de la Universidad sobre temas relacionados a <TEMAS RELACIONADOS>. Dentro del trabajo se proyecta a lo siguiente:

- <ACTIVIDAD QUE SE REALIZARÁ>: <DETALLE DE LO QUE SE REALIZARÁ>

3-. Definiciones

- **Información Confidencial:** Cubre toda información verbal o escrita, ya sea en formato digital, gráfico o físico, que incluye conocimientos técnicos, datos financieros, diseños, software, patentes, análisis, procesos, entre otros, que pueda ser propiedad de cualquiera de las partes o de sus filiales. También incluye información comercial o administrativa que, si se divulga, podría ser útil para competidores.
- **Parte Divulgadora:** La parte que revela o entrega la información confidencial.
- **Parte Receptora:** La parte que recibe la información confidencial.

4-. Uso de la información confidencial

- **No divulgación:** La Parte Receptora no puede compartir la Información Confidencial, salvo con sus representantes involucrados en el proyecto, quienes deben ser informados sobre su naturaleza confidencial.
- **Formato y seguridad:** La información se accederá a nivel de bases de datos, por parte de la Unidad de Gestión de la Información e Innovación, a lo cual solo los miembros de la Unidad tendrán acceso, restringido a solo poder observar.
- **Requerimientos legales:** Si la Parte Receptora debe divulgar información por orden legal, debe notificar a la Parte Divulgadora y solo compartir lo requerido.
- **Uso limitado:** La Parte Receptora no puede usar la Información Confidencial para fines distintos a los procesos, sin autorización previa la cual debe ser por escrito.
- **Precauciones de seguridad:** Ambas partes deben tomar medidas de seguridad estrictas y no realizar ingeniería inversa sobre el software o hardware recibido.
- **Remedios no monetarios:** En caso de incumplimiento, la Parte Divulgadora puede buscar medidas no monetarias, como el cumplimiento forzado del acuerdo.

	Acuerdo de Confidencialidad para acceso a información de sistemas	Versión: 1.1 11/06/2025
Elaborado por: - Felipe Andrés Fuentes Bravo - Rodrigo Canales Ramírez	Aprobado por:	

- **Uso en futuros contratos:** Si se celebran nuevos acuerdos, la información intercambiada sólo puede usarse dentro del marco de esos contratos y bajo las mismas obligaciones de confidencialidad estipuladas en este acuerdo.

5-. Excepciones a la confidencialidad

No se considerará Información Confidencial, bajo este acuerdo, aquella donde la Parte Receptora pueda demostrar que:

1. Es o se convierte en información de dominio público sin violar el acuerdo.
2. Era conocida por la Parte Receptora antes de recibirla, y pueda acreditarse.
3. Fue proporcionada por un tercero no vinculado que tiene derecho a divulgar sin restricciones.
4. Fue desarrollada de forma independiente por la Parte Receptora o sus representantes.

Además, la Parte Receptora podrá revelar Información Confidencial en los siguientes casos:

- **Obligaciones legales:** Si la Parte Receptora debe divulgar la información por ley o regulaciones, debe consultar previamente a la Parte Divulgadora cuando sea posible. En caso de que no sea factible, deberá entregar una copia de la revelación realizada tan pronto como sea posible y sólo revelará lo estrictamente necesario.
- **Procedimientos legales:** La Parte Receptora puede divulgar la información en procedimientos legales derivados del acuerdo, siempre que se respeten los procedimientos de confidencialidad que solicite la Parte Divulgadora y apruebe el tribunal.

6-. Cesión del acuerdo, modificación, efecto vinculante y notificaciones

El presente Acuerdo y los derechos y obligaciones que de él emanen no podrán ser cedidos por las Partes sin el consentimiento escrito de la contraparte, quien lo otorgará a su entera discreción. Este Acuerdo podrá ser modificado sólo por mutuo acuerdo escrito de ambas Partes.

Las partes son y seguirán siendo contratantes independientes. La firma de este acuerdo no crea un vínculo contractual entre las unidades. El acuerdo no establece una relación de representación, sociedad, o fideicomiso entre ellas.

Las notificaciones del acuerdo deben realizarse por escrito y se considerarán recibidas cuando se envíen por correo electrónico, siguiendo el formato indicado para cada parte.

6.1-. Parte receptora

Nombre: <NOMBRE DE LA UNIDAD, PUEDE SER LA DIRECCIÓN ESTRATÉGICA INFORMÁTICA O UNA UNIDAD INTERNA DE ÉSTA>

Representante: <Nombre de la persona> - <Cargo>

e-mail: <correos institucionales asociados>

fono: <forma de contacto directo de la persona>

6.2-. Parte Divulgadora

- Nombre:
- Representante:

	Acuerdo de Confidencialidad para acceso a información de sistemas	Versión: 1.1 11/06/2025
Elaborado por: - Felipe Andrés Fuentes Bravo - Rodrigo Canales Ramirez	Aprobado por:	

- e-mail:
- Teléfono:

7-. Vigencia y Término del acuerdo de confidencialidad

- Este acuerdo no tendrá un término determinado, mientras los apoyos entre unidades sean necesarios,
- Este documento representa el acuerdo total entre las partes. No existen otros acuerdos o condiciones fuera de lo aquí establecido.

**<NOMBRE DEL ENCARGADO QUE
RECEPCIONARÁ O MANIPULARÁ
LA INFORMACIÓN>**
<CARGO>
<UNIDAD MENOR, SI CORRESPONDE>
<UNIDAD MAYOR>

**<Vicerrector o Jefatura de
Departamento de Beneficios
Estudiantiles>**

2. DISPÓNGASE que los protocolos mencionados en el Resuelvo 1 serán revisados por la Dirección Estratégica Informática de forma anual. Esto, fundamentado en la necesidad de realizar adecuaciones pertinentes, en concordancia con eventuales cambios normativos respecto a la materia.

3. PUBLÍQUESE la presente resolución, una vez totalmente tramitada, en el sitio electrónico de la Universidad, específicamente en el banner “Actos y Resoluciones con efecto sobre terceros”, con el objeto de dar cumplimiento a lo previsto en el artículo 7º de la Ley 20.285 sobre Acceso a la Información Pública y en el artículo 51º de su reglamento.



TESE Y COMUNÍQUESE,



Cristian Muñoz

Cristian Alejandro Muñoz Canales
Rector (S)
Universidad de Santiago de Chile
01/12/2025 16:40:05

**DR. CRISTIÁN MUÑOZ CANALES
RECTOR (S)**

Distribución:

1. Rectoría;
1. Prorrectoría
1. Dirección Estratégica Informática
1. Contraloría Universitaria
1. Secretaría General
1. Dirección Jurídica,
1. Unidad de Probidad y Transparencia
1. Unidad de Partes, Informaciones y Archivo