UCSC SECRETARÍA GENERAL

DECRETO DE RECTORÍA N°121/2026

PROMULGA ACUERDO DEL H. CONSEJO SUPERIOR QUE APRUEBA LA POLÍTICA DE GOBERNANZA Y GESTIÓN DE DATOS DE LA UNIVERSIDAD CATÓLICA DE LA SANTÍSIMA CONCEPCIÓN.

VISTO:

1. La presentación en el punto N°6 de la tabla al H. Consejo Superior, en Sesión Ordinaria N°08 de 03 de septiembre de 2026, por el equipo de trabajo a cargo de esta política;

2. Lo informado por la Prorrectora y la Secretaria General de la Universidad;

3. Las atribuciones que me confieren los Estatutos Generales de la Universidad.

DECRETO:

Promulga el acuerdo N°02 del H. Consejo Superior adoptado en sesión ordinaria N°08 de fecha 03 de septiembre de 2026, que es del siguiente tenor:

Acuerdo N°02: El Honorable Consejo Superior aprueba por unanimidad, la Política de Gobernanza y Gestión de Datos de la Universidad Católica de la Santísima Concepción.

POLÍTICA INSTITUCIONAL DE GOBERNANZA Y GESTIÓN DE DATOS

I. Antecedentes y Fundamentos

La Universidad Católica de la Santísima Concepción, dada la creciente complejización de sus funciones y en un contexto de transformación digital, requiere un uso cada vez más intensivo, articulado y responsable de sus datos. Los procesos relacionados a la gestión institucional, docencia, investigación, innovación y vinculación con el medio generan información que debe ser administrada con criterios comunes, responsabilidades definidas y estándares institucionales.

En este contexto, se vuelve necesario avanzar hacia un modelo de gobernanza de datos que permita ordenar, administrar y gestionar de forma estratégica y operativa los datos institucionales durante todo su ciclo de vida, considerando su captura, almacenamiento, integración, uso, protección, intercambio, publicación, archivo y eliminación.

La presente política se funda en los siguientes antecedentes:

a) La necesidad de avanzar hacia un marco institucional común que oriente la administración, definición, calidad, trazabilidad, protección, seguridad y uso de los datos institucionales durante todo su ciclo de vida.

b) La necesidad de establecer lineamientos comunes y articulados para el desarrollo de los pilares estratégicos de la Gobernanza de Datos: Arquitectura y Calidad de datos, Protección de Datos Personales y Ciberseguridad.

c) La necesidad de establecer una arquitectura de datos institucional de acuerdo al nivel de desarrollo alcanzado que permita fortalecer la integración de sistemas, definir fuentes oficiales, garantizar la calidad de los datos y evitar duplicidades, inconsistencias y/o usos no autorizados, incorporando los modelos institucionales de organización e integración de datos (ODS)[1] que la Universidad determine.

d) La entrada en vigencia de nuevas normativas que exigen fortalecer las capacidades institucionales en materia de protección y tratamiento de datos personales, y ciberseguridad. La Universidad reconoce las disposiciones legales contenidas en 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 y crea la Agencia de Protección de Datos Personales y la Ley N°21.663 sobre Marco de ciberseguridad.

e) El deber de fortalecer la seguridad de la información y la ciberseguridad institucional, considerando la creciente digitalización de los procesos académicos y administrativos, promoviendo la prevención, gestión y mitigación de incidentes que puedan afectar la continuidad operacional, la confidencialidad, la integridad o la disponibilidad de la información.

II. Principios Rectores

En consideración a lo anterior, se determinan los siguientes principios rectores que orientan la Gobernanza y Gestión de Datos en la Universidad:

a) **Integración y Uso de Fuentes Oficiales:** La Universidad fortalecerá la integración de sus sistemas de información, la definición de fuentes oficiales y la utilización de modelos institucionales autorizados, con el propósito de reducir duplicidades e inconsistencias en la información para una adecuada gestión institucional.

b) **Calidad y Trazabilidad de Datos:** Los datos deberán ser precisos, completos, oportunos, consistentes y trazables, garantizando su confiabilidad para la toma de decisiones basada en evidencia, así como para procesos de auditoría y rendición de cuentas, a partir de fuentes oficiales y validadas. Asimismo, deberán permitir identificar su origen, responsables, transformaciones y usos relevantes.

c) **Seguridad, Privacidad y Continuidad Operacional:** Los datos serán considerados y gestionados como activos estratégicos institucionales, resguardando su confidencialidad, integridad y disponibilidad, mediante la implementación de medidas de seguridad, protección de datos personales,

[1] ODS (Operational Data Store) conecta el modelo de negocio con la arquitectura de datos al actuar como un repositorio centralizado en tiempo real que limpia e integra datos transaccionales.

prevención y gestión de incidentes orientados a asegurar la continuidad operacional, conforme a la normativa vigente.

d) **Responsabilidad y Corresponsabilidad:** Todos los miembros de la Universidad, según correspondan, que tengan acceso al uso o tratamiento de datos serán responsables del cumplimiento de los principios de esta política, así como de las normas internas y externas. Asimismo, todas las reparticiones que participan del ciclo de vida del dato deberán contribuir a que la información sea correcta, validada, segura y utilizada de forma correcta y pertinente.

e) **Transparencia y Ética en el Uso:** El uso y análisis de datos, incluyendo su aplicación en herramientas tecnológicas o de inteligencia artificial, deberá realizarse con criterios éticos, de pertinencia, transparencia y en resguardo de los derechos de las personas, evitando sesgos y asegurando su adecuada aplicación a la gestión institucional.

f) **Confidencialidad:** Los miembros de la comunidad universitaria, así como quienes, en el ejercicio de sus funciones, tengan acceso a datos o información institucional, deben guardar estricto secreto y confidencialidad respecto de aquellos a los que accedan, procurando evitar su divulgación, utilización, alteración, filtración, o accesos no autorizados.

g) **Mejora Continua y Adaptación Institucional:** Esta política será evaluada periódicamente, incorporando ajustes derivados de cambios normativos, avances tecnológicos, aprendizajes institucionales resultante de su monitoreo y nuevas necesidades de la Universidad y su entorno; de acuerdo al Sistema Interno de Asegura miento de la Calidad.

III. Política

La Universidad Católica de la Santísima Concepción reconoce los datos como un activo estratégico institucional, cuya adecuada gestión contribuye al cumplimiento de su misión y al desarrollo de su gestión institucional y funciones fundamentales de docencia, investigación e innovación y vinculación con el medio. En este marco, promoverá una gobernanza de datos orientada a asegurar que estos sean gestionados, protegidos y utilizados de manera ética, segura, confiable, trazable y oportuna durante todo su ciclo de vida, en coherencia con los principios y valores institucionales.

Para ello, la Universidad fortalecerá progresivamente sus capacidades en gobernanza, arquitectura y calidad de datos, protección de datos personales y ciberseguridad, mediante la definición de roles, responsabilidades, estándares, procedimientos, fuentes oficiales, mecanismos de control, gestión de riesgos y acciones de formación, bajo lineamientos comunes y articulados, resguardando que las unidades académicas y administrativas sean responsables de la definición, actualización, validación, calidad y uso de los datos correspondientes a sus respectivos ámbitos de competencia.

IV. Objetivo General y Específicos

Objetivo General:

Establecer un marco institucional de Gobernanza de Datos que permita a la Universidad administrar, proteger y utilizar sus datos de manera ética, segura, confiable, trazable, interoperable y conforme a la normativa vigente, fortaleciendo su uso estratégico para la gestión institucional, la planificación, la mejora continua y la toma de decisiones.

Objetivos específicos:

a) Fortalecer la gobernanza, arquitectura y calidad de los datos institucionales, mediante la definición de roles, responsabilidades, lineamientos comunes, fuentes oficiales, catálogos, diccionarios, criterios de interoperabilidad y mecanismos de trazabilidad, resguardando que las unidades académicas y administrativas mantengan la responsabilidad sobre los datos propios de su ámbito de competencia.

b) Resguardar la privacidad y protección de los datos personales tratados por la Universidad, promoviendo su tratamiento conforme a la normativa vigente y a criterios de licitud y equidad, finalidad y minimización, transparencia sobre derechos de las personas, seguridad, confidencialidad y responsabilidad institucional.

c) Fortalecer la seguridad de la información y la ciberseguridad institucional, protegiendo los datos y activos de información frente a accesos no autorizados, pérdida, alteración, divulgación indebida, incidentes o amenazas digitales, e impulsando mecanismos de prevención, monitoreo, evaluación y mejora continua.

V. Público de Interés

Esta política será aplicable a todas las unidades académicas y administrativas de la Universidad, así como a sus autoridades, directivos, académicos, administrativos, estudiantes (en todos sus niveles formativos y modalidades), prestadores de servicios, proveedores tecnológicos y terceros que, en virtud de una relación contractual, accedan, traten o administren datos de la Universidad Católica de la Santísima Concepción.

VI. Consideraciones

Un Comité de Gobernanza de Datos actuará como el máxima órgano asesor, consultivo y de estandarización sobre la información institucional, en coordinación con el Delegado/a de Protección de Datos (DPD) o responsable institucional de Protección de Datos Personales si existiere, velará por la implementación y seguimiento de esta política.

La Universidad se compromete a crear o fortalecer la estructura organizacional pertinente, así como proveer los recursos necesarios que permitan la implementación de la presente política.

La política será evaluada cada tres años, o en su defecto, cuando los cambios sean necesarios de acuerdo al Sistema Interno del Aseguramiento de la Calidad (SIAC) o cambios normativos externos.

ANEXO

VII. Glosario

a) **Activo de información:** Conjunto de datos, documentos, sistemas, bases de datos, reportes, plataformas o repositorios que poseen valor para la Universidad y requieren ser gestionados y protegidos adecuadamente.

b) **Arquitectura de datos:** Estructura que define la forma en que los datos se capturan, almacenan, integran, organizan, relacionan, protegen, consultan y utilizan en la Universidad, considerando sistemas, repositorios, flujos de información y fuentes oficiales.

c) **Calidad de datos:** Grado en que los datos cumplen criterios de exactitud, completitud, oportunidad, consistencia, validez, unicidad y trazabilidad, permitiendo su uso confiable para la gestión institucional y la toma de decisiones.

d) **Corresponsabilidad sobre el dato:** Deber compartido de todas las unidades y personas que participan en el ciclo de vida del dato de contribuir a que la información sea correcta, validada, segura, trazable y utilizada de manera adecuada, conforme a los lineamientos institucionales.

e) **Ciclo de vida del dato:** Conjunto de etapas por las que transita un dato, desde su creación o captura, registro, validación, almacenamiento, uso, intercambio, hasta su almacenamiento o eliminación segura, según corresponda.

f) **Ciberseguridad:** Preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.

g) **Dato:** Representación de hechos, atributos, mediciones o registros que pueden ser usados, procesados, analizados e interpretados para generar información. Aquella información relativa a una persona natural identificada e identificable, es un dato personal el cual debe ser tratado conforme a la normativa vigente.

h) **Fuente oficial de datos:** Sistema, repositorio o unidad responsable reconocida institucionalmente como origen válido, autorizado y confiable para un dato determinado, o conjunto de datos.

i) **Gobernanza de datos:** Conjunto de principios, roles, procesos, estándares, normas y mecanismos que permiten gestionar los datos de manera ética, responsable, segura, confiable y trazable; en alineación con los objetivos institucionales.

j) **Interoperabilidad:** Capacidad de los sistemas, plataformas, procesos o bases de datos para intercambiar, integrar y utilizar información de manera coordinada, no duplicada y consistente, favoreciendo la articulación entre unidades y sistemas institucionales.

k) **Incidente de Ciberseguridad:** Todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos

l) **Modelos Institucionales:** Formas definidas por la Universidad para ordenar y conectar información proveniente de distintas unidades y sistemas, permitiendo que los datos sean comprendidos de manera común y utilizados de forma confiable en reportes, análisis, planificación y toma de decisiones.

m) **Resiliencia:** Capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque este en estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.

n) **Responsabilidad funcional del dato:** Unidad académica o administrativa responsable de los datos propios de su ámbito de competencia, encargada de definir su significado, reglas de actualización, validación, calidad, acceso y uso.

o) **Trazabilidad:** Capacidad de identificar y seguir el recorrido de un dato a lo largo de su ciclo de vida, incluyendo su origen, responsables, transformaciones, validaciones, usos, accesos y destino final.

Comuníquese, publíquese y archívese.
Concepción, 08 de septiembre de 2026.
CMC/PRT/pgv/mer.

UNIVERSIDAD CATÓLICA DE LA SANTÍSIMA CONCEPCIÓN · Secretaria General

PIEDAD ROSSI TORREALBA
Secretaria General

UNIVERSIDAD CATÓLICA DE LA SANTÍSIMA CONCEPCIÓN · RECTOR

DR. CRISTHIAN MELLADO CID
Rector