POLÍTICAS Y PROTOCOLOS

POLÍTICA DE **PROTECCIÓN, GOBERNANZA** Y **MANEJO** DE **DATOS**

UNIVERSIDAD ACADEMIA DE HUMANISMO CRISTIANO

Presentación

La Universidad Academia de Humanismo Cristiano, comprometida con el desarrollo ético, responsable y sostenible de sus funciones institucionales —docencia, investigación y vinculación con el medio— establece la presente Política de Protección, Gobernanza y Manejo de Datos, la cual forma parte integral del sistema de gestión institucional de la Universidad.

El propósito de esta política es establecer un marco institucional para la toma de decisiones, la gestión y el uso adecuado de los datos, reconociendo a la información como un activo estratégico para el cumplimiento de los objetivos misionales y para la toma de decisiones informada. Asimismo, busca asegurar que los datos institucionales sean gestionados de manera coherente, confiable, oportuna y conforme a la normativa vigente.

En un contexto marcado por la creciente digitalización de los procesos universitarios y el uso intensivo de información, la Universidad reconoce la necesidad de contar con lineamientos claros que definan responsabilidades, principios y criterios para el manejo de los datos a lo largo de su ciclo de vida, desde su generación hasta su conservación o eliminación. Este marco permite prevenir riesgos asociados al uso inadecuado de la información, tales como inconsistencias, pérdida de trazabilidad o utilización no autorizada.

La presente política se sustenta en buenas prácticas y estándares internacionales, incorporando principios de gestión de la información y del riesgo que favorecen la transparencia, la rendición de cuentas y la mejora continua. En particular, se articula con los enfoques establecidos en las normas ISO/IEC 27001 e ISO 27701, en lo referido a la gestión de la información y la privacidad, así como con la norma ISO 31000 y el modelo COSO ERM, orientados a una gestión integral del riesgo y al fortalecimiento del control interno, los cuales serán abordados en mayor detalle en la Política de Ciberseguridad.

De igual forma, esta política se encuentra alineada con el marco normativo chileno vigente, especialmente con las disposiciones relativas a la protección de datos personales, la responsabilidad institucional y las buenas prácticas en el manejo de la información, entre las que se consideran:

- **Ley N° 21.719**, sobre protección de datos personales.
- **Ley N° 21.459**, que regula los delitos informáticos, en cuanto a responsabilidades asociadas al uso de información digital.
- **Ley N° 20.393**, sobre responsabilidad penal de las personas jurídicas, en lo relativo al uso y resguardo de información institucional.

La finalidad de este marco normativo es consolidar una cultura institucional de gobernanza y manejo responsable de los datos, promoviendo el uso ético, consistente y transparente de la información. De este modo, se busca que cada integrante de la comunidad universitaria asuma un rol activo en la adecuada gestión de los datos, contribuyendo al fortalecimiento de una institución confiable, eficiente y alineada con sus principios y obligaciones legales.

I. Propósitos y principios de la política

El manejo responsable de los datos constituye un elemento fundamental para la adecuada gestión de la información institucional, contribuyendo a la continuidad de los procesos universitarios, a la calidad de la toma de decisiones y al fortalecimiento de la confianza de la comunidad universitaria. En este sentido, el propósito central de esta política es establecer directrices claras para la gestión, uso y resguardo de los datos institucionales, asegurando su disponibilidad, integridad, confidencialidad y trazabilidad a lo largo de todo su ciclo de vida.

La política abarca la información asociada al quehacer universitario, incluyendo los datos del personal administrativo, académicos, estudiantes y postulantes, promoviendo un uso ético, responsable y conforme a la normativa vigente, así como prácticas consistentes en el tratamiento de la información en los distintos sistemas y procesos institucionales.

En un contexto de creciente digitalización y uso intensivo de datos, esta política busca ordenar y estandarizar las prácticas de manejo de datos, reduciendo riesgos asociados a la inconsistencia, uso indebido, pérdida de información o falta de control sobre los datos institucionales. Para ello, se asegura el cumplimiento del marco normativo aplicable y la alineación con estándares y buenas prácticas internacionales, particularmente aquellos relacionados con la gestión de la información, la privacidad y la gestión del riesgo, tales como ISO/IEC 27001, ISO/IEC 27701, ISO 31000 y el modelo COSO ERM que se aborda el lineamiento general de las responsabilidades en la presente política y la aplicación en la Política de Ciberseguridad.

Los objetivos de la Política de Protección, Gobernanza y Manejo de Datos comprenden los siguientes puntos:

1.1. Alcance

Esta política aplica a:

- **La Comunidad Universitaria y terceros:** Incluye a estudiantes, académicos, personal administrativo, asesores, proveedores externos y cualquier tercero que posea acceso a los sistemas de la Universidad.
- **Los Activos Tecnológicos y la información:** Abarca todos los sistemas informáticos, servicios digitales, plataformas educativas que se mencionen en la Política de Ciberseguridad.

1.2. Principios Rectores

Los siguientes principios fundamentales rigen la aplicación de esta política:

- **Confidencialidad:** Garantizar que la información sea accesible únicamente a aquellos individuos, entidades o procesos que se encuentren debidamente autorizados para ello.
- **Integridad:** Asegurar la exactitud, completitud y trazabilidad de las bases de datos y la información, protegiéndola contra modificaciones no autorizadas.
- **Disponibilidad:** Mantener la alta operatividad y el acceso oportuno a los servicios y sistemas. El manejo de los plazos y tiempos de accesibilidad de los datos debe estar definido explícitamente por la política de Ciberseguridad.
- **Legalidad**: Observar el estricto cumplimiento de la legislación chilena vigente en materia de protección de datos personales y delitos informáticos.
- **Responsabilidad Compartida:** Establecer que cada integrante de la comunidad universitaria es corresponsable de la seguridad digital institucional, exigiendo un rol activo en su mantenimiento.

1.3. Roles y Responsabilidades

La implementación y cumplimiento de la presente Política de Protección, Gobernanza y Manejo de Datos se sustenta en una asignación clara de roles y responsabilidades, distribuidas en distintos niveles organizacionales. Esta estructura permite asegurar una adecuada toma de decisiones, una gestión coherente de los datos institucionales y el cumplimiento del marco normativo vigente.

1. Nivel Estratégico y Gobernanza — Alta Dirección

La Alta Dirección es responsable de establecer el marco institucional para la gobernanza y el manejo de los datos. Para efectos de esta política, la Alta Dirección está conformada por el Rector, quien lidera la gestión y administración del proceso, junto con el Directorio, órgano responsable de la supervisión, aprobación y alineamiento estratégico de las decisiones institucionales.

El Rector podrá apoyarse en los representantes y equipos que estime pertinentes para la implementación operativa de este marco, mientras que el Directorio coordina y valida los requerimientos y lineamientos que correspondan, considerando los informes y recomendaciones del Delegado de Protección de Datos, en cumplimiento de la normativa vigente.
Responsabilidades:

- Aprobar la Política de Protección, Gobernanza y Manejo de Datos y sus modificaciones.
- Velar por su cumplimiento a nivel institucional.
- Autorizar definiciones estratégicas o lineamientos generales que impacten de manera relevante la gestión de los datos institucionales, en particular aquellos de carácter personal o sensible.
- Resolver o canalizar requerimientos transversales relacionados con el uso, acceso o tratamiento de los datos institucionales.
- Coordinarse con el Delegado/a de Protección de Datos Personales en materias de cumplimiento normativo.

2. Nivel de Soporte — Dirección de Informática

La Dirección de Informática es responsable de apoyar la gestión de los datos desde la perspectiva de los sistemas de información institucionales.
Responsabilidades:

- Asegurar la disponibilidad y operación de los sistemas que soportan el tratamiento de los datos institucionales.
- Implementar los lineamientos definidos por la Alta dirección en los sistemas de información.
- Apoyar la continuidad operativa de los procesos institucionales asociados al uso de datos y los controles generales para la ejecución correcta de los procesos.

3. Nivel Funcional — Unidades Académicas y Administrativas

Las unidades académicas y administrativas son responsables del uso y manejo de los datos en el ejercicio de sus funciones.

Responsabilidades:

- Gestionar los datos bajo su responsabilidad conforme a los fines institucionales y a la normativa vigente.

- Velar por la calidad, actualización y uso adecuado de la información que administran mediante los controles institucionales definidos por la Política de Ciberseguridad y los controles individuales que respondan adecuadamente a lo definido por esta política.
- Solicitar accesos, modificaciones o tratamientos especiales de datos a través de los mecanismos institucionales definidos.
- Colaborar con las instancias de gobernanza de datos y con el Delegado/a de Protección de Datos cuando corresponda.

4. Delegado/a Institucional de Protección de Datos Personales (Ley N° 21.719)

La Universidad designa a un/a Delegado/a Institucional de Protección de Datos Personales, quien ejercerá sus funciones adscrito/a orgánicamente a la Dirección de Control de Gestión, la cual proveerá el soporte administrativo necesario para el desempeño de su rol.

El/la Delegado/a actuará como referente técnico en materias de protección de datos personales y privacidad, en conformidad con la Ley N° 21.719 y la normativa vigente, q asegurando la coherencia y alineación de sus actuaciones con los lineamientos y controles establecidos en la Política de Ciberseguridad institucional.

En el ejercicio de sus funciones, se garantiza expresamente su autonomía funcional, independencia técnica y operativa, ausencia de conflicto de intereses y la prohibición de recibir instrucciones respecto del desempeño de sus atribuciones. La Universidad asegura que el/la Delegado/a contará con independencia real y efectiva para el cumplimiento de sus funciones.

Asimismo, el/la Delegado/a de Protección de Datos no podrá ser sancionado/a, removido/a ni objeto de represalias por el ejercicio legítimo de sus funciones, debiendo contar con las garantías institucionales necesarias para actuar con objetividad, imparcialidad y resguardo de los derechos de los titulares de datos personales.
Responsabilidades:

- Supervisar el cumplimiento de la Ley N° 21.719 y de las disposiciones internas aplicables al tratamiento de datos personales.
- Mantener y supervisar el Registro Institucional de Actividades de Tratamiento de Datos.
- Asesorar a las unidades institucionales en materias de protección de datos personales.

- Actuar como contraparte técnica ante la autoridad competente y los titulares de datos personales, siendo responsable de atender oportunamente sus consultas, requerimientos y fiscalizaciones, así como de gestionar y dar respuesta a las notificaciones de brechas de seguridad, conforme a la normativa vigente.
- Emitir recomendaciones para fortalecer las prácticas institucionales de manejo responsable de datos.
- Coordinación con los controles institucionales abordados por el Encargado de Ciberseguridad.

5. Comunidad Universitaria y Terceros Autorizados

La comunidad universitaria y los terceros autorizados que accedan o traten datos institucionales son responsables de cumplir con los lineamientos establecidos en la presente política.

Responsabilidades:

- Utilizar los datos institucionales exclusivamente para los fines autorizados.
- Respetar la normativa vigente y las disposiciones internas relativas al manejo de datos.
- Cumplir los compromisos contractuales y de confidencialidad asociados al tratamiento de información institucional.

2. Lineamientos Generales

Este apartado tiene como objetivo explicar de manera clara y sencilla los conceptos fundamentales que orientan la gestión de los datos en la institución. Busca establecer un lenguaje común y una comprensión compartida sobre cómo se organizan, utilizan y protegen los datos, diferenciando los roles estratégicos, operativos y de resguardo de la información. Para ello, se presentan los conceptos de Gobierno de Datos, Manejo de Datos y Ciberseguridad, los cuales se complementan entre sí para asegurar un uso responsable, ordenado y seguro de la información institucional. Siendo el último punto abordado por la Política de Ciberseguridad.

2.1. Gobierno de Datos

El Gobierno de Datos corresponde al marco rector que define cómo la institución organiza, regula y supervisa el uso de sus datos durante todo su ciclo de vida. Incluye lineamientos, roles, estándares y responsabilidades que garantizan que la información sea confiable, íntegra, trazable, disponible y utilizada correctamente conforme a la Ley 21.719.

2.2. Manejo de Datos

El Manejo de Datos corresponde a la implementación operativa del Gobierno de Datos. Son las actividades prácticas que realizan las unidades para capturar, ingresar, validar, depurar, integrar y disponer datos, siguiendo los lineamientos institucionales.

2.3. Ciberseguridad

La Ciberseguridad comprende los controles, procesos y tecnologías destinadas a proteger sistemas, redes y datos institucionales frente a accesos no autorizados, vulneraciones, ataques y pérdidas. Las cuales se abordarán en la Política de Ciberseguridad

3. Relación entre Gobierno de Datos, Manejo de Datos y Ciberseguridad

El Gobierno de Datos es definido por la Alta Dirección; el Manejo de Datos es ejecutado por cada unidad académica/administrativa y la comunidad Universitaria y Terceros Autorizados; y la Ciberseguridad es responsabilidad de la Dirección de Informática, reflejado por Institucional de Protección de Datos Personales, en conjunto con el delegado institucional de Protección de Datos Personales.

Complementariamente, la Universidad clasifica la información que administra según su nivel de sensibilidad y criticidad, con el objetivo de definir los controles necesarios para su adecuada protección. Esta clasificación permite determinar el tipo y nivel de controles requeridos, los cuales se abordan en los lineamientos generales establecidos en la Política de Ciberseguridad, así como en los controles específicos implementados por cada unidad, de acuerdo con la clasificación de los datos que utilizan.

4. Clasificación de la información según sensibilidad y criticidad

4.1. Información Pública

Definición: Información destinada a ser difundida a la comunidad interna y externa, cuya divulgación no implica riesgos institucionales ni operativos.

Ejemplos:

- Contenidos del sitio web institucional y redes sociales
- Documentos normativos de acceso público

- Comunicados oficiales
- Información promocional o estadística no sensible

Nivel de controles requerido: Requiere un nivel básico de controles, orientados a asegurar la integridad, disponibilidad y correcta difusión de la información.

4.2. Información Interna

Definición: Información de uso exclusivo dentro de la institución, cuya divulgación externa podría generar inconvenientes operativos o administrativos.
Ejemplos:

- Procedimientos, instructivos y manuales
- Minutas y comunicaciones internas
- Información académica o administrativa de circulación interna

Nivel de controles requerido: Requiere un nivel intermedio de resguardo, asociado al acceso restringido y al manejo adecuado dentro de la comunidad universitaria.

4.3. Información Confidencial

Definición: Información cuyo acceso está limitado a usuarios autorizados y cuya divulgación no autorizada podría generar impactos legales, reputacionales o financieros para la Universidad o para las personas involucradas.
Ejemplos:

- Datos personales de estudiantes, funcionarios y académicos
- Información financiera o estratégica
- Bases de datos académicas con identificadores personales
- Documentos contractuales o administrativos sensibles

Nivel de controles requerido: Requiere un nivel elevado de resguardo, acorde a su sensibilidad y criticidad, las cuales deben ser abordadas mediante protocolos específicos y una adecuada coordinación de los controles con el Delegado Institucional de Protección de Datos Personales.

4.4 Información Altamente Sensible

Definición: Información crítica cuya exposición, pérdida o alteración podría generar daños severos a la institución o afectar significativamente los derechos de las personas.

Ejemplos:

- Datos personales sensibles (salud, género, vida sexual, convicciones morales, políticas o religiosas, situación socioeconómica, antecedentes disciplinarios, entre otros que cumplan con el criterio)
- Información de seguridad, configuraciones de sistemas y credenciales administrativas
- Planes de continuidad operativa, ciberseguridad o gestión de incidentes críticos
- Información asociada a procesos disciplinarios o reservados

Nivel de controles requerido: Requiere el más alto nivel de resguardo, acorde a su sensibilidad y criticidad, las cuales deben ser abordadas mediante protocolos específicos, coordinación de los controles con el Delegado Institucional de Protección de Datos Personales y seguimiento por parte del Encargado de Ciberseguridad con los accesos.

En función de esta clasificación, la Universidad determina los controles que deben aplicarse para asegurar la protección de la información, los cuales se establecen y detallan de acuerdo con el tipo de dato y su nivel de sensibilidad. Este también debe estar en concordancia con lo definido en los controles o lineamientos generales definidos en la Política de Ciberseguridad.

5. Ciclo de vida del dato.

Las etapas de los datos son relevantes para que los datos cumplan con los principios definidos anteriormente en todo el ciclo de la vida de los datos.

1. **Creación y captura** Los datos deben ser generados o capturados desde fuentes autorizadas, utilizando sistemas institucionales validados y procedimientos formales que aseguren su integridad, exactitud y oportunidad desde el origen.
2. **Almacenamiento** Los datos deberán almacenarse en repositorios institucionales definidos, considerando su clasificación y nivel de criticidad, asegurando controles de acceso, respaldo y conservación conforme a las políticas vigentes.
3. **Uso y procesamiento** El uso de los datos debe responder a fines institucionales legítimos, en el marco de las funciones y atribuciones de cada unidad, resguardando la confidencialidad, integridad y disponibilidad de la información.

4. **Compartición y transferencia** La transferencia interna o externa de datos deberá estar autorizada, registrada y alineada con la normativa vigente, considerando acuerdos de confidencialidad y medidas de protección acordes al tipo de dato.
5. **Archivo y conservación** Los datos deberán conservarse durante los plazos definidos por la normativa interna y externa, considerando criterios académicos, administrativos que defina la Universidad.
6. **Eliminación o disposición final** La eliminación de datos deberá realizarse de manera segura, trazable y documentada, evitando su recuperación no autorizada y cumpliendo los plazos de retención establecidos.

Este ciclo es abordado con más detalle en la Política de Ciberseguridad.

6. Calidad de los datos

Los datos institucionales, incluyendo los datos personales y sensibles, deben ser gestionados con altos estándares de calidad, seguridad y confidencialidad, de manera de resguardar los derechos de los titulares, cumplir con la normativa vigente y respaldar adecuadamente los procesos académicos, administrativos y de gestión institucional.

1. Estándares de calidad de los datos

La Universidad establece los siguientes estándares mínimos de calidad, aplicables a todos los datos institucionales y, de manera reforzada, a los datos personales:

1) **Exactitud:** Los datos deben representar fielmente la información que describen, evitando errores que puedan afectar decisiones institucionales o los derechos de los titulares de datos personales.
2) **Completitud:** Los datos deben encontrarse íntegros y contener toda la información requerida para el cumplimiento de los fines para los cuales fueron recolectados, evitando registros incompletos o redundantes.
3) **Oportunidad:** Los datos deben mantenerse actualizados y disponibles dentro de los plazos requeridos, especialmente cuando su desactualización pueda afectar la gestión académica, administrativa o el ejercicio de derechos de los titulares.
4) **Consistencia:** Los datos deben mantener coherencia entre los distintos sistemas institucionales, evitando duplicidades o inconsistencias que puedan generar riesgos de uso indebido o errores en el tratamiento de datos personales.

2. Protección de datos personales

El tratamiento de datos personales se realizará conforme a los principios de licitud, finalidad, proporcionalidad, confidencialidad y seguridad, resguardando los derechos de los titulares y limitando su uso a los fines institucionales autorizados.

En particular, la Universidad velará por qué:

- La recolección y el uso de datos personales sean pertinentes, necesarios y proporcionales a los fines definidos, informando adecuadamente a los titulares cuando corresponda y obteniendo su consentimiento en los casos exigidos por la normativa vigente.
- El acceso a los datos personales se encuentre restringido de acuerdo con roles y perfiles previamente autorizados, aplicando el principio de mínimo privilegio.
- Se implementen medidas de seguridad técnicas y organizacionales acordes al nivel de sensibilidad del dato, en coordinación con el área de ciberseguridad y en concordancia con la Política de Ciberseguridad institucional.
- Los datos personales se encuentren protegidos frente a accesos no autorizados, pérdida, alteración o divulgación indebida, considerando controles preventivos, detectivos y correctivos.
- Se respeten y faciliten los derechos de los titulares de datos personales, tales como acceso, rectificación, actualización, cancelación y eliminación, mediante procedimientos y protocolos formales definidos por la Universidad.
- El uso secundario de datos personales para fines de análisis, reportes o investigación se realice, cuando corresponda, mediante técnicas de anonimización o seudonimización, resguardando la identidad de los titulares y minimizando los riesgos de identificación.

La Universidad definirá y mantendrá protocolos específicos para la gestión del consentimiento, el ejercicio de los derechos de los titulares, la anonimización de datos y la gestión de incidentes de seguridad, los cuales deberán ser aplicados de manera coordinada entre las áreas responsables de la protección de datos personales, el manejo y gobierno de datos y el área de ciberseguridad.

3. Mecanismos de control y validación

Para asegurar la calidad de los datos y la adecuada protección de los datos personales, la Universidad implementa mecanismos de control y validación a lo largo de todo el ciclo de vida del dato, considerando su nivel de criticidad, sensibilidad e impacto, tales como:

- **Controles en el origen del dato**: Validaciones automáticas en los sistemas institucionales que aseguren el correcto ingreso, formato, obligatoriedad y legitimidad del tratamiento de los datos, reforzadas en el caso de datos que, por su naturaleza o sensibilidad, requieren mayores controles técnicos.
- **Revisiones periódicas de calidad y cumplimiento**: Evaluaciones sistemáticas de la información crítica y de los tratamientos de datos personales, realizadas por los responsables y custodios de los datos, en coordinación con el Delegado Institucional de Protección de Datos Personales y conforme a los lineamientos establecidos en la Política de Ciberseguridad.
- **Indicadores de calidad y protección de datos**: Definición y seguimiento de indicadores asociados a calidad, seguridad y cumplimiento normativo en el tratamiento de los datos personales, diferenciando aquellos datos que requieren controles reforzados.
- **Gestión de incidencias y brechas**: Procedimientos formales para el reporte, análisis y mitigación de incidentes relacionados con la calidad de los datos o la protección de datos personales, articulados con los procesos de gestión de incidentes definidos en la Política de Ciberseguridad.
- **Trazabilidad y auditoría**: Registro de accesos, modificaciones y tratamientos de datos personales, permitiendo auditorías internas y externas y asegurando la rendición de cuentas, con niveles de trazabilidad acordes a la criticidad del dato.
- **Responsabilidades y mejora continua**: Asignación clara de responsabilidades sobre la calidad y protección de los datos a los dueños y custodios, promoviendo una cultura institucional de mejora continua y de coordinación permanente con el área de ciberseguridad.

Todos estos controles serán evaluados y aplicados de acuerdo con la criticidad del riesgo, del proceso y del tipo de dato, en concordancia con lo definido en la Política de Ciberseguridad de la Universidad.

Cumplimiento Normativo

Esta política se adscribe a:

- Ley N°19.628/Ley Nº 21.719 (protección de datos personales y la vida privada).
- Ley N° 21.459 (delitos informáticos).
- Ley N° 20.393 (sobre responsabilidad penal de las personas jurídicas, en lo relativo al uso y resguardo de información institucional).
- Normativas internacionales (ISO/IEC 27001, ISO/IEC 27032).

- Política de Ciberseguridad.
- Política de Gestión del Riesgo.

Revisión y Actualización

La presente política será revisada al menos una vez al año por la Vicerrectoría de Administración y Finanzas en conjunto con la Secretaria General. Este proceso contará con el apoyo de los integrantes relevantes en el manejo de datos. La política se actualizará de manera obligatoria cuando se produzcan cambios normativos, tecnológicos o estratégicos que así lo requieran.

Vigencia

La presente política entrará en vigor a partir de su aprobación por las autoridades competentes de la Universidad Academia de Humanismo Cristiano.

Cualquier situación no contemplada o vacío normativo que surja de la aplicación e interpretación de la presente Política de Protección, Gobernanza y Manejo de Datos será resuelto por la Rectoría de la Universidad o por la unidad en quien esta delegue dicha facultad, velando por la coherencia con los principios éticos e institucionales.

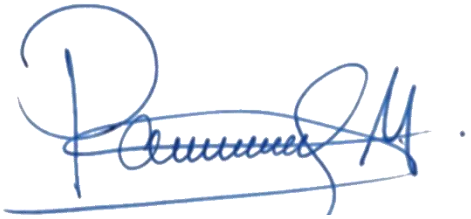
Anexos

La Política se complementa con los siguientes documentos, divididos en Anexos Normativos, siendo cumplimiento obligatorio y forman parte integrante del sistema de control institucional:

Anexos Normativos

- Anexo 1: Protocolo de Manejo de Datos Marketing.
- Anexo 2: Protocolo de Manejo de Datos Registro Curricular.
- Anexo 3: Protocolo de Manejo de Datos Admisión y Matriculas.
- Anexo 4: Protocolo de Manejo de Datos Dirección de Desarrollo Académico.
- Anexo 5: Protocolo de Manejo de Datos Recursos Humanos.

- Anexo 6: Protocolo de Manejo de Datos Secretaria General.
- Anexo 7: Protocolo de Manejo de Datos Dirección de Géneros y Diversidad.
- Anexo 7: Protocolo de Manejo de Datos Dirección de Géneros y Diversidad.



Paulina Miranda Santana, Secretaria General y ministra de fe de la Universidad Academia de Humanismo Cristiano, certifica que, con fecha 28 de enero de 2026, en sesión extraordinaria del Consejo Superior Universitario se aprueba la Política de Protección, Gobernanza y Manejo de Datos, ratificada por Decreto de Rectoría N° 034/2026 de fecha 29 de enero de 2026.