FIJA TEXTO POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES Y DA CUENTA NOMBRAMIENTO DELEGADA DE PROTECCIÓN DE DATOS PERSONALES (DPO)

RECTORÍA

D.U.N°45-2026

Santiago, 23 de septiembre de 2026

TENIENDO PRESENTE:

Que con motivo de la dictación de la ley 21.719, sobre la Protección de Datos Personales, que modificó la ley 19.628, la Universidad ha determinado dictar la Política institucional sobre la materia y designar al Delegado de Protección de Datos Personales (DPO).

VISTOS:

Lo acordado por la Junta Directiva en sesión del 20 de agosto de 2026, y las atribuciones que me otorga la reglamentación vigente, en particular la facultad de dictar los decretos que sean necesarios para la Institución, que se encuentra contemplada en el literal i) del artículo 4° del Reglamento General de la Universidad.

D E C R E T O

PRIMERO: Fijase el siguiente texto de la Política:

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

INDICE

TÍTULO I: DISPOSICIONES GENERALES……..2
TÍTULO II: PRINCIPIOS RECTORES……3
TÍTULO III: GOBERNANZA INSTITUCIONAL……...4
TÍTULO IV: LINEAMIENTOS GENERALES DE TRATAMIENTO……..……..6
TÍTULO V: CUMPLIMIENTO, DESARROLLO NORMATIVO Y VIGENCIA……..……..8

TÍTULO I: DISPOSICIONES GENERALES

Artículo 1°. Propósito

La Universidad Andrés Bello (en adelante e indistintamente, “UNAB” o la “Universidad”) adopta la presente Política General de Protección de Datos Personales (la “Política”) como expresión de su compromiso con el respeto de los derechos fundamentales de las personas, en cumplimiento del derecho consagrado en el artículo 19 N° 4 de la Constitución Política de la República y de las obligaciones establecidas en la Ley N° 19.628, modificada por la Ley N° 21.719.

Esta Política establece el marco normativo, los principios y los lineamientos generales que rigen el tratamiento de datos personales que la Universidad realiza respecto de estudiantes, postulantes, egresados, docentes, apoderados, tutores financieros, trabajadores, proveedores y todo otro titular con quien se relacione, con el fin de asegurar un tratamiento lícito, leal, transparente y responsable de sus datos.

La Política tiene el carácter de norma marco. Su desarrollo operativo se efectuará mediante políticas específicas, procedimientos, protocolos, anexos por categoría de titulares y cláusulas contractuales, instrumentos que deberán ser coherentes con los principios y obligaciones aquí establecidos.

Artículo 2°. Alcance

La presente Política tiene alcance institucional y obliga a todas las personas naturales o jurídicas que traten datos personales por cuenta o en representación de UNAB, incluyendo directivos, académicos, funcionarios, colaboradores, proveedores y prestadores de servicios. Cada persona es responsable de asegurar su cumplimiento efectivo en el ejercicio de sus funciones.

Artículo 3°. Definiciones

Para los efectos de esta Política, los términos que se indican a continuación tendrán el significado que les asigna la Ley y, en particular, el siguiente:

1. **Agencia de Protección de Datos Personales:** órgano público autónomo creado por la Ley N° 21.719, encargado de velar por la protección de los datos personales, fiscalizar el cumplimiento de la normativa, dictar instrucciones y aplicar sanciones.

2. **Anonimización:** todo tratamiento efectuado de manera que la información obtenida no pueda asociarse a una persona determinada o determinable. Los datos anonimizados dejan de regirse por la normativa de protección de datos personales.

3. **Base de datos:** conjunto organizado de datos personales, cualquiera sea la finalidad, forma o modalidad de su creación, almacenamiento, organización y acceso, que permita relacionar los datos entre sí y realizar su tratamiento.

4. **Brecha de seguridad (violación de la seguridad de los datos personales):** toda vulneración de la seguridad que ocasione la destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales, ya sea de forma accidental o ilícita.

5. **Consentimiento:** toda manifestación de voluntad libre, específica, inequívoca e informada, otorgada mediante una declaración o una clara acción afirmativa, por la cual el titular, su representante legal o mandatario autoriza el tratamiento de los datos personales que le conciernen.

6. **Dato caduco:** aquel que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, a falta de norma expresa, por el cambio de los hechos o circunstancias que consigna.

7. **Datos personales:** cualquier información vinculada o referida a una persona natural identificada o identificable. Es identificable toda persona cuya identidad pueda

determinarse, directa o indirectamente, mediante los medios que razonablemente puedan utilizarse al momento del tratamiento.

8. **Datos personales sensibles:** aquellos que se refieren a las características físicas o morales de las personas o a los hechos o circunstancias de su vida privada o intimidad, tales como los que revelen el origen étnico o racial, la afiliación política, sindical o gremial, la situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos y la información relativa a la vida sexual, la orientación sexual y la identidad de género.

9. **Encargado del tratamiento:** persona natural o jurídica que trata datos personales por cuenta del responsable del tratamiento, conforme a sus instrucciones y al contrato o instrumento jurídico respectivo.

10. **Ley:** la Ley N° 19.628, sobre protección de la vida privada, considerando las modificaciones introducidas por la Ley N° 21.719.

11. **Delegado de Protección de Datos Personales (DPO):** rol especializado e independiente que asesora, articula y supervisa el cumplimiento institucional en materia de protección de datos personales en UNAB.

12. **Responsable del tratamiento:** persona natural o jurídica que decide acerca de los fines y medios del tratamiento de datos personales. UNAB actúa como responsable respecto de las bases de datos que administra en el marco de sus funciones académicas, administrativas, de investigación, vinculación con el medio, financieras y de apoyo estudiantil. Sin perjuicio de lo anterior, la Universidad podrá actuar en calidad de encargada o de corresponsable del tratamiento en los términos del artículo 11° de esta Política.

13. **Seudonimización:** tratamiento efectuado de manera que los datos ya no puedan atribuirse a un titular sin utilizar información adicional, la que se mantiene separada y bajo medidas que aseguren su acceso solo por personas autorizadas.

14. **Titular de los datos personales:** persona natural, identificada o identificable, a quien se refieren los datos personales objeto de tratamiento.

15. **Transferencia internacional de datos:** comunicación de datos personales a un receptor situado fuera del territorio nacional.

16. **Tratamiento de datos personales:** cualquier operación o conjunto de operaciones, automatizadas o no, efectuadas sobre datos personales, tales como su recolección, almacenamiento, comunicación, cesión, transferencia o eliminación, entre otras señaladas en la Ley.

TÍTULO II: PRINCIPIOS RECTORES

Artículo 4°. Principios

Todo tratamiento de datos personales que efectúe la Universidad se sujetará a los principios establecidos en la Ley, los que constituyen el eje estructurante de esta Política y el criterio de interpretación y aplicación de sus disposiciones y de los instrumentos que la desarrollen:

1. **Licitud y lealtad.** El tratamiento de datos personales deberá ajustarse a la ley, a la buena fe y a la transparencia, garantizando el respeto de los derechos de los titulares. La Universidad deberá poder acreditar la base de licitud que justifica cada tratamiento. El tratamiento se fundará en alguna de las bases de licitud que contempla la Ley. La Universidad documentará y evaluará la base de licitud aplicable con anterioridad a cada tratamiento. Los datos personales sensibles solo se tratarán en los casos expresamente autorizados por la ley o con el consentimiento expreso del titular, adoptándose medidas de seguridad reforzadas. Queda prohibida la obtención de datos personales de fuentes ilegítimas o que no garanticen suficientemente su procedencia lícita.

2. **Finalidad.** Los datos personales sólo se tratarán para fines determinados, explícitos y lícitos, definidos antes de su recolección e informados a los titulares. No podrán tratarse

con fines distintos o incompatibles con los declarados, salvo tratamiento ulterior compatible con la finalidad original o autorización legal expresa.

3. **Proporcionalidad.** El tratamiento se limitará a los datos adecuados, pertinentes y estrictamente necesarios en relación con sus fines. Los datos se conservarán sólo durante el tiempo indispensable para cumplir la finalidad que justificó su obtención, subsistir una obligación legal o contractual, o permitir la formulación, ejercicio o defensa de derechos, y transcurrido dicho período serán eliminados, anonimizados o bloqueados conforme a la Política de Conservación y Eliminación de Datos Personales.

4. **Calidad.** Los datos personales deberán ser exactos, completos, actuales y pertinentes en relación con su origen y sus finalidades. La Universidad rectificará o completará los datos inexactos o incompletos, eliminará o anonimizará los datos caducos o carentes de fundamento legal para su tratamiento y bloqueará aquellos cuya exactitud o vigencia no pueda establecerse y cuya supresión no corresponda.

5. **Responsabilidad.** La Universidad responde por el cumplimiento de los principios y obligaciones establecidos en la Ley y en esta Política, y deberá estar en condiciones de acreditarlo. Asegurará la adecuada asignación de roles, competencias y recursos en materia de protección de datos. La responsabilidad de UNAB como responsable del tratamiento subsiste aun cuando encargue a terceros labores asociadas a la gestión de los datos.

6. **Seguridad.** El tratamiento se realizará bajo estándares adecuados de seguridad, con medidas técnicas y organizativas proporcionales a la naturaleza de los datos, al riesgo de cada operación y al posible impacto sobre los derechos de los titulares, orientadas a garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos durante todo su ciclo de vida. Las medidas de seguridad específicas se regularán en la normativa institucional de seguridad de la información y tecnologías.

7. **Transparencia e información.** La Universidad mantendrá a disposición de los titulares, de manera permanente, comprensible, inequívoca y gratuita, la información sobre sus políticas y prácticas de tratamiento exigida por la Ley, a través de los respectivos avisos de privacidad y de sus canales institucionales. Toda comunicación relativa al tratamiento de datos personales se expresará en un lenguaje claro, preciso y accesible, y la Universidad facilitará el ejercicio de los derechos de los titulares dentro de los plazos legales.

8. **Confidencialidad.** Todo el personal de la Universidad y los terceros que intervengan en cualquier fase del tratamiento deberán guardar secreto y confidencialidad respecto de los datos personales a los que accedan en razón de sus funciones, deber que subsistirá aun después de terminada la relación laboral, contractual o comercial. Su incumplimiento constituirá una infracción grave.

TÍTULO III: GOBERNANZA INSTITUCIONAL

Artículo 5°. Modelo de gobernanza

La Universidad implementará un modelo interno de gobernanza de datos personales basado en la responsabilidad proactiva, la protección de datos desde el diseño y por defecto, y la mejora continua, articulado con la estructura de gobierno de datos establecida en la Política de Gobierno de Datos de la Universidad. Dicho modelo se estructura sobre las siguientes instancias:

1. La Junta Directiva aprueba esta Política y sus modificaciones.

2. La Rectoría es responsable de que la Universidad cumpla con la Ley y con la demás normativa aplicable en materia de protección de datos personales, debiendo asegurar las condiciones institucionales y los recursos necesarios para ello.

3. El Comité de Gobierno de Datos es la instancia colegiada de gobernanza en esta materia, conforme al artículo siguiente.

4. El Delegado de Protección de Datos Personales (DPO) es responsable de la implementación y supervisión operativa de esta Política, conforme al artículo 7°.

Artículo 6°. Comité de Gobierno de Datos

El Comité de Gobierno de Datos (CGD) es el mismo órgano directivo de nivel táctico-estratégico establecido en la Política de Gobierno de Datos de la Universidad, encargado de aprobar estándares, procedimientos y procesos, definir prioridades sobre los dominios de información y resolver los conflictos de uso de datos entre áreas. Está presidido por el Director General de Planificación Institucional / CDO; integrado por cada Data Owner (Directores/Líderes de Área), el Responsable de Seguridad de la Información (CISO/Dirección de TI), el Director de Datos y el DPO que asiste con rol de asesor en cumplimiento, en su calidad de supervisor autónomo con facultad de instrucción, sin derecho a voto en las materias que posteriormente debe supervisar. En su caso, su opinión disidente se deberá consignar en acta.

En materia de protección de datos personales, corresponderá especialmente al Comité: supervisar la aplicación de esta Política y de las medidas de seguridad asociadas; asesorar a la Universidad siguiendo las recomendaciones del DPO en las decisiones relativas a la protección de datos personales; revisar los informes de auditoría, verificaciones y evaluaciones de impacto; analizar los incidentes o brechas de seguridad que afecten datos personales; velar por la coordinación e implementación de medidas de cumplimiento al interior de la institución; proponer mejoras y actualizaciones normativas; promover la cultura institucional de privacidad; y las demás que se le asignan en esta política. Los asuntos que requieran supervisión estratégica, financiamiento o alineación con los objetivos institucionales serán elevados a la Junta Directiva, conforme a la estructura definida en la Política de Gobierno de Datos.

Artículo 7°. Delegado de Protección de Datos Personales

La Junta Directiva de UNAB designará un Delegado de Protección de Datos Personales, figura independiente y con autonomía funcional respecto de la administración, encargada de supervisar la correcta aplicación de las disposiciones legales, reglamentarias e internas relativas al tratamiento de datos personales de acuerdo a la Ley. El Delegado podrá impartir instrucciones de cumplimiento en materia de protección de datos personales a las demás áreas de la Universidad. El área destinataria deberá acatarlas o fundar por escrito su discrepancia; en este último caso, el Delegado registrará la instrucción, la discrepancia y su fundamento, y podrá elevar el asunto al Comité de Gobierno de Datos y, cuando la naturaleza o la gravedad del riesgo lo justifique, a la Junta Directiva.

El DPO se situará en un nivel de acceso directo e incondicional a la Junta Directiva de la Universidad, contará con los recursos humanos, técnicos y materiales necesarios para el ejercicio de sus funciones, podrá formular instrucciones en materia de protección de datos a las demás áreas de la Universidad y no podrá asumir funciones que le generen conflicto de interés con su labor de supervisión.

Corresponderá al DPO, como principal encargado por Ley del tratamiento de datos personales en la universidad, la planificación, implementación, control y supervisión operativa de esta Política, debiendo mantener un sistema de control interno que permita detectar, registrar, reportar y corregir oportunamente los incumplimientos e incidentes de datos personales. En el ejercicio de dicha función le corresponderá especialmente: informar y comandar a la Universidad, sus directivos y trabajadores acerca de sus obligaciones en materia de protección de datos; supervisar el cumplimiento de la Ley, de esta Política y de los instrumentos que la desarrollen; liderar el diseño, implementación y actualización del Modelo de Prevención de Infracciones (MPI); asesorar en la elaboración de las evaluaciones de impacto en protección de datos y supervisar su ejecución; actuar como punto de contacto y nexo oficial con la Agencia de Protección de Datos Personales, gestionando las notificaciones que corresponda efectuar; supervisar el canal de atención de las consultas, reclamaciones y solicitudes de ejercicio de derechos de los titulares; impulsar acciones de formación y sensibilización; informar los riesgos o incumplimientos relevantes al Comité de Gobierno de Datos y, cuando corresponda, a la Rectoría y la Junta Directiva; y elaborar un plan anual de trabajo y reportar su ejecución a esta última.

El DPO actuará con plena independencia y objetividad, no recibirá instrucciones de las áreas cuyos tratamientos supervisa y no podrá ser sancionado ni destituido por el cumplimiento de sus obligaciones legales o reglamentarias. Las consultas y solicitudes de orientación en materia de

protección de datos personales deberán dirigirse al Delegado a través del correo institucional protecciondatos@unab.cl.

Artículo 8°. Deberes generales del personal

Los directivos, académicos, funcionarios, colaboradores y prestadores de servicios de la Universidad solo podrán acceder a datos personales y tratarlos en el marco de sus funciones y de los permisos que les hayan sido expresamente otorgados, y únicamente para finalidades institucionales. Deberán utilizar exclusivamente los sistemas, repositorios y canales autorizados por la Universidad, guardar estricta reserva sobre los datos a los que accedan, incluso después de terminada su relación con la Universidad, y reportar de inmediato al Delegado de Protección de Datos Personales o, en su defecto, al Responsable de Seguridad de la Información, cualquier incidente, anomalía o uso indebido que afecte o pueda afectar datos personales.

Las obligaciones específicas de los usuarios de los sistemas y plataformas institucionales se regularán en la normativa de seguridad de la información y tecnologías y en la Política de Gobierno de Datos.

TÍTULO IV: LINEAMIENTOS GENERALES DE TRATAMIENTO

Artículo 9°. Derechos de los titulares

La Universidad garantizará a los titulares el ejercicio de los derechos que les reconoce la Ley: de acceso, a solicitar confirmación del tratamiento de sus datos y acceder a ellos y a las condiciones de su tratamiento; de rectificación, a que se modifiquen o completen los datos inexactos, desactualizados o incompletos; de supresión, a que se eliminen los datos en los casos previstos por la Ley; de oposición, a que no se realice un tratamiento determinado, incluida la oposición a ser objeto de decisiones basadas únicamente en tratamientos automatizados, incluida la elaboración de perfiles; de portabilidad, a recibir copia de los datos que haya facilitado, en formato estructurado y de uso común, y a comunicarlos a otro responsable; y de bloqueo, a obtener la suspensión temporal del tratamiento mientras se resuelve una solicitud de rectificación, supresión u oposición.

Las solicitudes se responderán por escrito dentro de los plazos establecidos en la Ley. Toda denegación total o parcial deberá ser fundada, informando al titular su derecho a reclamar ante la Agencia de Protección de Datos Personales. La Universidad mantendrá canales accesibles y gratuitos para el ejercicio de estos derechos en su sitio web, portales estudiantiles e intranet, sin perjuicio del correo institucional habilitado al efecto. Todo trabajador que reciba una solicitud de un titular deberá derivarla de inmediato al Delegado de Protección de Datos Personales. El procedimiento de tramitación se regulará en un protocolo específico.

Artículo 10°. Encargados del tratamiento

La contratación de terceros que traten datos personales por cuenta de la Universidad deberá formalizarse mediante un contrato u otro instrumento jurídicamente vinculante que establezca, al menos, el objeto y duración del encargo, la finalidad del tratamiento, el tipo de datos y categorías de titulares, los derechos y obligaciones de las partes y el destino de los datos al término de la relación.

La Universidad verificará que el encargado ofrezca garantías suficientes de confidencialidad, seguridad y cumplimiento normativo, y supervisará el cumplimiento de estas obligaciones durante toda la vigencia del contrato. El encargado no podrá delegar el tratamiento en un tercero sin autorización previa, expresa y por escrito de la Universidad.

Artículo 11°. Tratamiento por encargo de terceros y corresponsabilidad

La Universidad al tratar datos personales por cuenta de un tercero y conforme a sus instrucciones, actuará en calidad de encargada del tratamiento, deberá sujetarse a las instrucciones del responsable y a los términos del contrato o instrumento jurídico respectivo, y no podrá utilizar los datos para fines propios ni distintos de los instruidos.

Además, cuando la Universidad determine conjuntamente con una o más entidades los fines y medios de un tratamiento, actuará en calidad de corresponsable del tratamiento, deberá acordar

mediante un instrumento escrito, la distribución de sus responsabilidades respectivas en el cumplimiento de las obligaciones establecidas en la Ley, sin perjuicio de la responsabilidad que a cada uno corresponda frente a los titulares.

Artículo 12°. Comunicación de datos a terceros

La Universidad solo podrá comunicar datos personales a terceros –tales como autoridades competentes, encargados del tratamiento, entidades en convenio o instituciones académicas o financieras– cuando la comunicación cumpla copulativamente los siguientes requisitos: existencia de una base de licitud válida; finalidad específica, explícita y legítima; estricta proporcionalidad entre los datos comunicados y esa finalidad; medidas de seguridad adecuadas, utilizando exclusivamente canales institucionales seguros; y formalización mediante el instrumento jurídico que corresponda.

Ante cualquier duda sobre la procedencia de una comunicación, deberá consultarse previamente al Delegado de Protección de Datos Personales.

Artículo 13°. Transferencias internacionales de datos

Las transferencias internacionales de datos personales sólo podrán efectuarse hacia países u organismos que aseguren niveles adecuados de protección conforme a la Ley o, en su defecto, adoptando las garantías apropiadas que ésta contempla, tales como cláusulas contractuales u otros mecanismos reconocidos. Toda transferencia internacional deberá verificarse previamente en cuanto a su licitud, finalidad y proporcionalidad, con la colaboración del área jurídica y la supervisión del Delegado de Protección de Datos Personales.

Artículo 14°. Datos personales de niños, niñas y adolescentes

El tratamiento de datos personales de niños, niñas y adolescentes sólo podrá realizarse atendiendo a su interés superior y con respeto a su autonomía progresiva, y se limitará a los datos estrictamente indispensables para la finalidad que justifica su recolección.

El tratamiento de datos personales de niños y niñas menores de catorce años requerirá el consentimiento previo, expreso e informado de su padre, madre, representante legal o de quien tenga a su cargo su cuidado personal, otorgado por medios que permitan acreditar fehacientemente su otorgamiento. Los datos personales de los adolescentes de catorce años o más se tratarán conforme a las reglas aplicables a los adultos, salvo sus datos personales sensibles que, tratándose de adolescentes menores de dieciséis años, se sujetarán a las reglas anteriores.

La información sobre las finalidades, condiciones y alcance del tratamiento deberá expresarse en un lenguaje especialmente claro, sencillo y accesible. La Universidad aplicará a estos datos medidas de seguridad reforzadas y los eliminará de manera segura una vez cumplida la finalidad que justificó su recolección, salvo obligación legal de conservación.

Artículo 15°. Gestión de riesgos, incidentes y brechas que afecten el tratamiento de datos personales

La Universidad, por intermedio del Delegado de Protección de Datos Personales, velará por la realización de evaluaciones periódicas de los riesgos asociados a los tratamientos de datos personales. Deberá efectuarse previamente una Evaluación de Impacto en la Protección de Datos Personales cuando un tratamiento pueda implicar un alto riesgo para los derechos de los titulares y, en todo caso, en los siguientes supuestos: (a) Evaluación sistemática y exhaustiva de aspectos personales de los titulares de datos, basadas en tratamiento o decisiones automatizadas, como la elaboración de perfiles, y que produzcan en ellos efectos jurídicos significativos; (b) Tratamiento masivo de datos o a gran escala; (c) Tratamiento que implique observación o monitoreo sistemático de una zona de acceso público; (d) Tratamiento de datos sensibles y especialmente protegidos, en las hipótesis de excepción del consentimiento; (e) Los demás casos que establezca la Ley o que determine la Agencia de Protección de Datos Personales.

Detectado un incidente o brecha que afecte o pueda afectar datos personales, éste deberá reportarse de inmediato conforme al artículo 8° de esta Política. Cuando la brecha pueda implicar un riesgo para los derechos y libertades de los titulares, la Universidad la notificará a la Agencia de Protección de Datos Personales y, cuando corresponda conforme a la Ley, a los propios

titulares, sin dilación indebida, informando su naturaleza, posibles consecuencias y las medidas adoptadas. Los incidentes serán documentados en el registro correspondiente. Los procedimientos de gestión, evaluación y notificación se regularán en un protocolo específico.

TÍTULO V: CUMPLIMIENTO, DESARROLLO NORMATIVO Y VIGENCIA

Artículo 16°. Cumplimiento

En cumplimiento de la presente Política, el Delegado de Protección de Datos Personales propondrá al Comité de Gobierno de Datos las políticas, procedimientos, protocolos y directrices necesarios para asegurar la aplicación efectiva de sus principios y de la legislación vigente, y supervisará de manera independiente su correcta implementación una vez aprobados conforme al artículo 19° de esta Política.

La Universidad velará por su correcta implementación, promoviendo la mejora continua y la adopción de buenas prácticas en materia de protección de datos personales, seguridad de la información y gobernanza.

Artículo 17°. Compromiso institucional

La Universidad Andrés Bello declara su compromiso firme y permanente con la protección de los datos personales de todas las personas que se relacionan con ella. En ejercicio de los principios de responsabilidad proactiva, transparencia y rendición de cuentas, UNAB se compromete a: adoptar medidas razonables para el cumplimiento de la legislación vigente y de la normativa interna que la desarrolle; incorporar la protección de datos personales desde la etapa de diseño de todo proceso, sistema, producto o servicio que implique su tratamiento, y por defecto, tratando únicamente los datos estrictamente necesarios para cada finalidad específica; promover en todos sus niveles una cultura de respeto a los derechos fundamentales y de responsabilidad en el uso de la información personal; asegurar la formación y sensibilización permanente de su personal, cuya participación en las instancias de capacitación será obligatoria; mantener y actualizar las medidas de seguridad apropiadas al riesgo de cada tratamiento; ejercer un liderazgo activo, asignando los recursos humanos, técnicos y financieros necesarios; y revisar y mejorar continuamente sus políticas, protocolos y procedimientos.

Artículo 18°. Infracciones y consecuencias del incumplimiento

El incumplimiento de esta Política, de los instrumentos que la desarrollen o de la legislación vigente constituirá una infracción sancionable conforme al ordenamiento jurídico aplicable, al Reglamento Interno de Orden, Higiene y Seguridad de la Universidad y a las estipulaciones contractuales que correspondan, atendiendo a la naturaleza de la conducta, su intencionalidad, la reiteración, el volumen y sensibilidad de los datos afectados y la magnitud del perjuicio causado o potencial. La tipificación de las infracciones, el procedimiento de investigación y sanción y las garantías del debido proceso se desarrollarán en un instrumento normativo específico, aprobado por la Junta Directiva. Lo anterior es sin perjuicio de las responsabilidades civiles, administrativas o penales que procedan conforme a derecho.

Artículo 19°. Desarrollo normativo

El desarrollo normativo de esta Política corresponderá al Comité de Gobierno de Datos, el que actuará conforme a la propuesta técnica del DPO, de acuerdo con lo previsto en el artículo 16° de esta Política. Para estos efectos, el Comité podrá aprobar las políticas específicas, procedimientos, protocolos, instructivos, registros, formatos, cláusulas contractuales y demás instrumentos internos necesarios para desarrollar, complementar y hacer operativas las obligaciones establecidas en esta Política y en la legislación vigente sobre protección de datos personales.

Dichos instrumentos podrán referirse, entre otras materias, al registro de actividades de tratamiento, al ejercicio de derechos de los titulares, a la gestión de incidentes y brechas de seguridad, a las evaluaciones de impacto, a la conservación y eliminación de datos, a las transferencias internacionales y a las reglas aplicables a tratamientos, procesos o categorías específicas de titulares.

Una vez aprobados por el Comité, estos instrumentos serán obligatorios para todas las autoridades, unidades, directivos, académicos, funcionarios, colaboradores, proveedores y terceros que traten datos personales por cuenta o en representación de la Universidad, sin perjuicio de aquellos casos en que, por su naturaleza o jerarquía institucional, deban ser sometidos a aprobación de la Rectoría o de la Junta Directiva.

Los instrumentos dictados en desarrollo de esta Política formarán parte de su marco normativo complementario, deberán interpretarse de manera coherente con sus principios y obligaciones y no podrán contradecirla. En caso de conflicto, prevalecerá la presente Política.

Artículo 20°. Evaluación y revisión

El Delegado de Protección de Datos Personales elaborará un informe anual de cumplimiento, con los avances, incidentes, hallazgos y medidas adoptadas, el que será presentado a la administración superior de la Universidad y a la Junta Directiva junto con las recomendaciones de mejora que correspondan. La Política se revisará al menos una vez al año y, adicionalmente, cada vez que se produzcan cambios normativos, tecnológicos o institucionales relevantes, o incidentes significativos de seguridad o incumplimiento.

Artículo 21°. Vigencia y actualización

La presente Política entrará en vigor a partir de su aprobación por la Junta Directiva de la Universidad Andrés Bello y tendrá validez indefinida. Sus modificaciones serán aprobadas por la Junta Directiva, a propuesta del Delegado de Protección de Datos Personales y del Comité de Gobierno de Datos, y serán comunicadas oportunamente a la comunidad universitaria. La fecha de aprobación y el número de versión de esta Política y de cada una de sus modificaciones se consignarán en la tabla de control del documento y se publicarán junto con ella, conforme al artículo 14 ter letra a) de la Ley.

Artículo 22°. Disposición transitoria. Plan institucional de implementación progresiva

1. Exigibilidad legal. Las obligaciones que esta Política reproduce, desarrolla o implementa a partir de la entrada en vigencia de las modificaciones que la Ley 21.719 introduce a la Ley 19.628 serán exigibles desde la fecha en que lo sean conforme a ella. El plan institucional a que se refiere el numeral siguiente no podrá diferirlas ni condicionarlas.

2. Plan institucional. Las obligaciones que esta Política establece por sobre el estándar legal se implementarán conforme a un plan institucional de implementación progresiva, único para esta Política y para la Política de Gobierno de Datos, que la Junta Directiva aprobará a más tardar en noviembre de 2026. El plan priorizará los tratamientos, bases de datos, procesos y categorías de titulares de mayor criticidad o exposición regulatoria, y fijará la fecha de exigibilidad de cada obligación, ninguna de las cuales podrá ser posterior a la entrada en vigencia de las modificaciones que la Ley 21.719 introduce a la Ley 19.628.

3. Regla supletoria. Mientras no se apruebe el plan, el Delegado de Protección de Datos Personales determinará el orden de implementación conforme al criterio de priorización del numeral anterior e informará su ejecución al Comité de Gobierno de Datos. La falta de aprobación del plan no obsta a la exigibilidad de las restantes disposiciones de esta Política.

4. Caducidad. El numeral 1 caduca de pleno derecho el día de la entrada en vigencia de las modificaciones que la Ley 21.719 introduce a la Ley 19.628, y los numerales 2 y 3 con la aprobación del plan y el vencimiento de la última fecha de exigibilidad que éste fije. Producida la caducidad, este artículo se entiende suprimido, sin necesidad de modificación formal de la Política.

SEGUNDO: Declárase que la Junta Directiva nombró como Delegada de Protección de Datos Personales (DPO), a la abogada **Sra. XIMENA SEPÚLVEDA BARRERA**, a partir del 20 de agosto de 2026, sin plazo determinado, y de conformidad con lo establecido en esta Política, en la Política de Gobierno de Datos y en los artículos 49 y 50 de la ley 19.628. Asimismo, ratificó todo lo obrado por la Sra. Sepúlveda Barrera, en el ejercicio de esta función, desde el 1° de mayo de 2026, fecha desde la cual ha venido desempeñándola.

Anótese y Comuníquese,

JULIO CASTRO SEPÚLVEDA
RECTOR

PEDRO COVARRUBIAS BESA
SECRETARIO GENERAL