UNIVERSIDAD DE LAS AMÉRICAS

DECRETO RECTORIA NÚMERO 22072026-03

Aprueba y Promulga la "Política de Gobierno de Datos"

VISTOS:

1. La dictación de la "Política de Protección de Datos Personales", aprobada por la Junta Directiva en la sesión del 22 de julio de 2026 y promulgada por Decreto de Rectoría N°22072026-02;

2. La propuesta complementaria formulada por la Vicerrectoría de Finanzas, por intermedio de su Dirección de Gobierno de la Información, en coordinación con la Dirección General de Cumplimiento y Secretaría General, proponiendo la dictación de una Política de Gobierno de Datos, cuyo objeto es establecer el marco institucional para gobernar el uso eficaz, íntegro, seguro y trazable de los datos y la información, en su creación, captura, clasificación, acceso, uso, intercambio, conservación y disposición fina, asegurando la toma de decisiones confiable, el fortalecimiento de la eficiencia operativa, el resguardo los derechos de las personas y la protección de la Institución;

3. El acuerdo de la Junta Directiva de fecha 22 de julio de 2026, que aprueba la "Política de Gobierno de Datos";

4. Lo dispuesto en el artículo 18 letra b), i) y p) del Reglamento Orgánico de la Universidad;

DECRETO:

Promúlguese el acuerdo de la Junta Directiva que aprueba la "Política Gobierno de Datos", cuyo texto se anexa al presente instrumento.

Comuníquese, publíquese y archívese.

Santiago de Chile, 22 de julio de 2026.

MARÍA DEL PILAR ROMAGUERA GRACIA
RECTORA

MARÍA PAULINA HERNÁNDEZ PEDRAZA
SECRETARIA GENERAL

UNIVERSIDAD DE LAS AMÉRICAS

UDLA
DOCUMENTO OFICIAL
SECRETARÍA GENERAL

POLÍTICA DE GOBIERNO DE DATOS
UNIVERSIDAD DE LAS AMÉRICAS

Introducción.

Universidad de Las Américas, reconoce que los datos y la información generada o recolectada con ocasión del relacionamiento con los distintos partícipes de la comunidad universitaria, son un recurso estratégico necesario tanto para el cumplimiento de sus fines institucionales como para el desarrollo de las actividades académicas, administrativas, financieras de la institución. Es por ello, que UDLA se compromete a mantener y profundizar la gestión responsable de los datos, promoviendo su realización conforme a criterios de calidad, trazabilidad, seguridad, proporcionalidad y responsabilidad, con roles claramente definidos y controles verificables, constituyendo así un pilar fundamental para la toma de decisiones, la eficiencia operativa, el cumplimiento normativo y la protección adecuada de los derechos de las personas y de los intereses institucionales.

En ese contexto la presente Política viene a establecer los principios rectores, que orientan la gestión de los datos y la información en la Universidad, asegurando su uso conforme a la normativa vigente y a las mejores prácticas institucionales.

La protección de los datos personales se regirá por la Política General de Protección de Datos Personales y sus instrumentos complementarios, sin perjuicio de que los principios generales contenidos en la presente Política les serán igualmente aplicables en lo que corresponda.

1. Objeto.

La presente Política establece el marco institucional de la Universidad de Las Américas (en adelante, "UDLA" o la "Institución") para gobernar el uso eficaz, íntegro, seguro y trazable de los datos y la información, en su creación, captura, clasificación, acceso, uso, intercambio, conservación y disposición fina, asegurando la toma de decisiones confiable, el fortalecimiento de la eficiencia operativa, el resguardo los derechos de las personas y la protección de la Institución.

2. Alcance.

La presente Política es aplicable a todas las autoridades, colaboradores, académicos y administrativos, proveedores y terceros que creen, registren, procesen, administren, custodien, usen o compartan datos e información institucional, cualquier sea la unidad académica o administrativa en la cual presten servicios o a través de la cual se relacionen con la Institución, sea que se trate de datos estructurados o no estructurados, que consten en soporte físico o digital.

Asimismo, es aplicable a los sistemas institucionales, repositorios colaborativos, archivos, expedientes, bases de datos, plataformas de análisis, ambientes de prueba cuando contengan datos reales o sensibles y también a los tratamientos realizados por terceros por cuenta de la Institución.

La protección de datos personales se rige por la Política General de Protección de Datos Personales de la Institución, sin perjuicio de la aplicación de la presente Política en todo lo que sea compatible. La gestión documental se regirá además por sus instrumentos específicos.

3. Definiciones.

Para efectos de esta Política, se entenderá por:

Dato: Representación elemental de un hecho, atributo, evento, transacción o condición, susceptible de registro, procesamiento, intercambio o análisis.

Información: Resultado de procesar, organizar, relacionar, interpretar o contextualizar datos, de modo que adquieran significado y utilidad institucional.

Documento: Instrumento que contiene datos y/o información, en cualquier soporte o formato.

Registro: Documento que da cuenta de la realización de una actividad y/o de la toma de una decisión.

Dato personal: Información numérica, alfabética, gráfica, fotográfica, acústica, biométrica o de cualquier otro tipo vinculada o referida a una persona natural identificada o identificable.

Dato personal sensible: Dato personal que se refiere a las características físicas o morales de las personas, los hechos o circunstancias de su vida privada o intimidad, que revele 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, a la orientación sexual y a la identidad de género de una persona natural, cuya utilización indebida pueda dar lugar a discriminación o conlleve un riesgo grave para sus derechos fundamentales.

Información sensible institucional: información no pública cuya divulgación, alteración, pérdida o uso no autorizado puede afectar de manera significativa a la Institución, su operación, su estrategia, su seguridad, su cumplimiento normativo, su posición competitiva o su reputación. Su tratamiento se regirá por los instrumentos institucionales de clasificación y seguridad de la información.

Dominio de información: agrupación de datos, información y activos relacionados bajo una lógica común de negocio, responsabilidad y control.

Dato crítico: Dato cuya afectación compromete significativamente la operación, el cumplimiento, la toma de decisiones, la continuidad de servicios o la reputación institucional.

Metadato: dato que describe el contexto, estructura, origen, clasificación, uso, trazabilidad, conservación o administración de otros datos, información o documentos.

El glosario ampliado y las definiciones orgánicas y funcionales especializadas se desarrollarán en los instrumentos normativos o técnicos correspondientes.

4. Principios rectores.

La gobernanza de datos e información en la Institución se rige por los siguientes principios:

4.1 Calidad por diseño. Los datos y la información deben gestionarse con criterios de exactitud, completitud, consistencia, oportunidad y trazabilidad proporcionales a su criticidad y uso.

4.2 Responsabilidad y rendición de cuentas. Todo dominio, dato crítico o activo de información relevante debe contar con responsabilidades claramente asignadas y verificables.

4.3 Seguridad y acceso por necesidad. El acceso, uso y compartición de datos e información se realizará conforme a perfiles autorizados, finalidad legítima y controles de seguridad aplicables.

4.4 Cumplimiento normativo. La gestión de datos, información y documentos debe cumplir con la normativa externa e interna vigente.

4.5 Trazabilidad. Debe ser posible identificar, según corresponda, el origen, las definiciones, las transformaciones, los responsables, los accesos relevantes y la disposición final de los datos y la información.

4.6 Minimización y proporcionalidad. Solo deben recopilarse, usarse, compartirse y conservarse los datos y la información necesarios para fines institucionales legítimos.

4.7 Interoperabilidad y consistencia. Las definiciones, estructuras y reglas institucionales deben favorecer la integración, evitar duplicidades injustificadas y promover fuentes autorizadas.

4.8 Conservación y disposición controlada. Los activos documentales e informacionales deben conservarse y eliminarse conforme a criterios aprobados, plazos definidos y evidencia trazable.

5. Estructura de gobernanza, roles y responsabilidades.

La Institución implementará un modelo de gobernanza de datos e información con roles, responsabilidades, procedimientos y controles claramente definidos para asegurar la correcta gestión de los datos, la información y sus activos asociados.

6. Compromisos específicos.

La Institución adopta los siguientes compromisos específicos:

6.1 Asignación de responsables. Todo dominio priorizado y todo dato crítico deberá contar con uno o más responsables designados por la institución.

6.2 Definiciones y metadatos. Los datos críticos y activos de información priorizados deberán contar con definición aprobada, fuente identificada, clasificación, responsable, reglas mínimas de calidad y uso permitido.

6.3 Clasificación y acceso. Todo dato o información dentro del ámbito de aplicación de esta Política deberá ser clasificado y su acceso deberá otorgarse por necesidad, función y autorización.

6.4 Fuente autorizada y control de duplicidades. Los dominios priorizados deberán identificar fuentes autorizadas y gestionar duplicidades o inconsistencias de manera controlada.

6.5 Ciclo de vida del dato. Los datos, la información y los documentos deberán gestionarse considerando, según corresponda, su creación o captura, clasificación, almacenamiento, acceso, uso, intercambio, conservación, archivo, transferencia y disposición final.

6.6 Protección de datos personales. Cuando existan datos personales o datos personales sensibles, se aplicarán también las disposiciones previstas en la Política de Protección de Datos Personales y en la normativa reglamentaria y de ejecución y control complementaria.

6.7 Terceros. Todo tercero que procese o custodie datos, información o documentos institucionales o personales, sensibles o no, deberá sujetarse a obligaciones contractuales, de seguridad, confidencialidad y cumplimiento definidas por la Institución.

6.8 Evidencia y trazabilidad. Toda decisión relevante de clasificación, cambio sustancial, excepción, eliminación o acceso privilegiado deberá quedar documentada conforme a los instrumentos aplicables.

6.9 Transferencias o almacenamiento fuera del territorio nacional. Cuando datos, información o activos institucionales sean almacenados, procesados o transferidos fuera del territorio nacional (incluyendo el uso de servicios de almacenamiento o procesamiento en la nube provistos por proveedores internacionales), deberá evaluarse el riesgo asociado y cumplirse con las condiciones normativas aplicables. Cuando se trate de datos personales, se aplicarán las reglas de transferencia internacional previstas en la Política de Protección de Datos Personales.

7. Revisión y actualización.

Cada dos años, la institución evaluará la pertinencia y eficacia de las disposiciones de la presente política, a menos que por una modificación en la legislación aplicable, por un cambio en la estrategia, estructura o tecnologías institucionales o bien por existir hallazgos o incidentes de seguridad, se haga necesaria la inmediata revisión y actualización de la presente Política.