

POLÍTICA DE CALIDAD DE DATOS

I. OBJETIVO

En este documento se establecen medidas y estándares indispensables en el tratamiento de los datos utilizados y generados por la Universidad Adolfo Ibáñez, en el marco de sus competencias, para asegurar su calidad.

La calidad se entiende como el grado en el que los datos cumplen con los principios que se declaran en esta política.

Una elevada calidad en los datos es esencial para la gestión de la institución, pues permite tomar decisiones, sobre la base de información fidedigna, y planificar sobre elementos precisos, veraces y actualizados, así como también cumplir satisfactoriamente con los requerimientos externos de información cuando ésta es requerida por otros organismos, en el marco de sus respectivas competencias.

La Universidad Adolfo Ibáñez está comprometida con lograr el más alto estándar de calidad en los datos que maneja y es responsabilidad de todos sus miembros, particularmente aquellos con responsabilidades precisas, verificar que sus datos cumplan tales estándares.

II. ALCANCE

Los datos corresponderán a aquellos registros de estudiantes, colaboradores, académicos e indicadores institucionales que son útiles para gestionar la institución aportando, entre otros aspectos, a la toma de decisiones, a la definición de cursos de acción, a la verificación de los planes de la Universidad y sus distintas unidades y a dar cumplimiento a las regulaciones definidas por la propia institución u organismos externos. Al mismo tiempo, son la base para informar solicitudes de organizaciones que desarrollan rankings y acreditaciones.

Esta política se aplica al tratamiento de todos los datos de la Universidad Adolfo Ibáñez, por lo que todas las personas que recolectan, procesan, almacenan, comunican, transmiten o utilizan de cualesquiera formas datos, deberán conocer y dar cumplimiento íntegro a la presente política.

III. PRINCIPIOS

Esta política provee un marco para mantener un alto estándar de calidad de los datos, a través del aseguramiento de los siguientes principios:

Privacidad: los datos deben resguardarse de modo tal de asegurar la confidencialidad y privacidad, sobre todo en caso que correspondan a información personal o sensible.

Finalidad: en caso de datos personales, estos deben ser recolectados con fines específicos, explícitos y lícitos. Lo anterior supone que sólo se recolectarán datos cuyo fin lo justifique, y que no se pueden tratar los datos personales con fines distintos a los informados al momento de su recolección, salvo consentimiento del titular, que los datos provengan de fuentes accesibles al público o así lo disponga la ley.

Fiabilidad: los datos deben reflejar procesos de obtención y recopilación estables y coherentes a través del tiempo. Si algún dato cambia, los usuarios deben estar seguros que ello corresponde a un cambio real, no a una visión diferente del mismo o a un cambio en la forma de recopilarlo o a un cambio en la fuente de origen. Los errores deben ser informados y corregidos a la brevedad, para mantener el alto nivel de certeza en la información.

Relevancia: los datos recogidos deben ser relevantes para los propósitos para los cuales van a ser usados. Esto implicará, revisiones regulares para reflejar el cambio que puedan tener esos propósitos.

Precisión: los datos deben ser precisos para cumplir su propósito y deben reflejar genuinamente las características que hicieron valiosa su recolección o generación. Los procesos y sistemas para crear, recolectar, preparar y transmitir datos, deben asegurar que esa meta se alcance.

Unicidad: los datos deben ser únicos, es decir, se deben tomar una sola vez, aunque pueden tener múltiples usos conforme a la autorización otorgada por el titular del dato o la ley, en caso de corresponder, conforme lo establecido en la ley 19.628.

Propósito: la recolección, generación, acumulación y eliminación de datos deben servir objetivos institucionales claros y a propósito de ello, tener procesos bien diseñados para el cumplimiento de esas tareas.

Responsabilidad: las tareas de recolección, generación, acumulación y eliminación de datos deben tener responsables claros. Estas responsabilidades no pueden ser delegadas. También deben definirse claramente los usuarios elegibles de estos datos. Tanto responsables como usuarios tienen el deber de resguardar

identidades personales, cumplir con protocolos de seguridad de los datos y asegurar la integridad de los datos.

Oportunidad: los datos deben ser capturados tan rápido como sea posible después que ocurre una actividad y debe estar disponible para su uso en un tiempo razonable.

Validez: los datos deben ser registrados en conformidad con los requisitos para los que fueron creados o solicitados. No corresponde simular datos para compensar la ausencia de información real.

Compleitud: los requerimientos de datos deben ser especificados claramente en función de las necesidades de información de la institución. Datos mal registrados, no válidos o incompletos proporcionan una indicación de la calidad de los datos, por lo que se recomienda algún tipo de monitoreo permanente.

Imparcialidad: los datos deben ser creados, recogidos y resguardados con imparcialidad, sin permitir la influencia de grupos o personas con intereses propios.

Rigurosidad: los datos deben ser preparados, recogidos y resguardados usando procesos documentados y repetitivos que puedan ser revisados. Si se produce algún cambio, este debe quedar reflejado en un documento y registrado en el mismo repositorio. Si los procesos incluyen supuestos o estimaciones, éstos deberían ser revisados regularmente.

IV. LINEAMIENTOS EN EL TRATAMIENTO DE LOS DATOS

Todos los datos que se recolecten, almacenen, procesen, generen o transformen como parte de las acciones desarrolladas en la gestión institucional están destinados a ser tratados de manera exclusiva por la Universidad Adolfo Ibáñez. Las personas que trabajen o colaboren con ella deben cumplir los siguientes lineamientos al efectuar el tratamiento de datos administrados por la Universidad:

- a) Todos los datos deben ser tratados y protegidos, en su creación, recopilación, utilización, uso, conservación y eliminación, según corresponda.
- b) Para todos los datos se debe velar por asegurar la autenticidad e integridad. Durante toda la vida del dato, se debe verificar que éstos sean completos y precisos.
- c) Cuando se identifique un dato incorrecto o inconsistente, se debe notificar al área responsable que corresponda para su revisión y corrección.
- d) Siempre se debe mantener la confidencialidad de los datos, a menos que éstos sean de acceso público.
- e) Los datos protegidos por ley, deben ser tratados como ésta lo indica, especialmente aquellos relacionados con información personal, conforme

lo dispone la Ley de Protección de la Vida Privada y la Política General de Protección de Datos de la Universidad.

- f) Deben existir evaluaciones periódicas que identifiquen riesgos internos y externos para preservar razonablemente la seguridad, confidencialidad e integridad de los datos.

IV. ROLES Y RESPONSABILIDADES

1. Comité Ejecutivo de Gobierno Datos

Estará conformado por los integrantes del Comité de Rectoría, o las personas de su dependencia que ellas designen, y tendrá las siguientes funciones:

- a) Definir y aprobar modificaciones a la presente política y monitorear el cumplimiento de la misma.
- b) Proponer y definir su funcionamiento periódico.
- c) Aprobar metas en los distintos ámbitos donde sea necesario monitorear la calidad de los datos.
- d) Evaluar y garantizar el seguimiento de los planes de acción y las actividades formuladas por las distintas unidades responsables de la implementación, respetando su autonomía, en el marco de la presente Política.
- e) Hacer la difusión de la presente política entre la comunidad, unidades académicas y administrativas.
- f) La definición y ajustes de estándares de la calidad de los datos cuando corresponda, recaerá en el Comité Ejecutivo de Gobierno de Datos o en quien ellos designen.

2. Vicerrectorías, Unidades Académicas y Administrativas

Las Vicerrectorías, unidades académicas y unidades administrativas, serán responsables de velar por la correcta aplicación de la presente política en cada una de sus áreas, incluyendo la implementación de acciones que corrijan errores detectados en los diversos procesos asociados.

3. Dirección de Análisis Institucional y Gobierno de Datos

En esta materia cumplirá las siguientes funciones:

- a) Hará operativos e implementará los lineamientos definidos por el Comité Ejecutivo de Datos, lo que incluye la supervisión general de la aplicación de la política en las distintas unidades. Para estos

- propósitos podrá hacer supervisiones aleatorias e informará periódicamente a dicho Comité los resultados de esta labor.
- b) Recomendará cambios en la política a propósito de la experiencia acumulada en la supervisión o la evolución comparada de esta política en Chile o el extranjero.
 - c) Dará respuesta a las dudas que surjan en la interpretación y aplicación de la presente política, sin perjuicio de las facultades que competen al Rector.

Integración de Políticas

En cuanto a la creación, manejo y resguardo de los datos, esta política se integrará al conjunto de políticas UAI existentes, relacionadas con seguridad y manejo de datos personales. En particular, con la Política General de Protección de Datos Personales y Políticas de Seguridad de la Información.

Esta política será revisada o actualizada al menos cada 3 años.