

Política de Datos para la Transformación Digital

Versión 1.0 – 2019

Este documento ha sido elaborado por Agesic (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

Usted es libre de copiar, distribuir, comunicar y difundir públicamente este documento, así como hacer obras derivadas, siempre y cuando tengan en cuenta citar la obra de forma específica y no utilizar esta obra para fines comerciales. Toda obra derivada de esta deberá ser generada con estas mismas condiciones.

Prefacio

La Agenda Uruguay Digital 2016-2020 establece que una de las iniciativas prioritarias para avanzar en la transformación digital del país es el “Gobierno integrado e inteligente”, que busca “Profundizar el desarrollo de infraestructuras, plataformas, arquitecturas y sistemas para avanzar hacia un Estado que actúe como una unidad e intensificar el aprovechamiento de los datos para la toma de decisiones, la orientación de políticas públicas y el mejoramiento permanente, mediante servicios proactivos que se anticipen a las necesidades” (Objetivo VII).

Uruguay ha alcanzado un nivel sumamente importante en interoperabilidad técnica y sus aplicaciones en el gobierno y la ciudadanía, cuyo punto culminante ha sido la incorporación de los trámites en línea. Sin perjuicio de continuar avanzando en esas áreas, el nuevo desafío son los datos¹, la información² y el conocimiento³. Las nuevas capacidades a desarrollar deberán considerar los datos como un activo de gobierno, transformándose en un instrumento para la toma de decisiones, la orientación de políticas públicas y la mejora permanente mediante servicios que se anticipen a las necesidades de la ciudadanía.

La formulación de políticas basadas en evidencia y los servicios públicos digitales proactivos y centrados en el usuario son las características de una administración pública basada en datos, moderna y transparente.

Cuestiones tales como la calidad de los datos, la soberanía, los derechos, la integridad, la accesibilidad, la disponibilidad, el uso compartido y la protección de datos deben abordarse para lograr un salto cuantitativo y cualitativo en el desarrollo del Gobierno Digital.

Surge la necesidad de crear una política de datos que establezca principios que sienten las bases de una estrategia nacional, que promueva y desarrolle proyectos específicos para la gestión de datos del sector público.

1 **Dato:** Es un conjunto de valores en formato digital sobre algo concreto que puede ser recolectado, medido y analizado.

2 **Información:** Es un conjunto de datos procesados y analizados en un determinado contexto.

3 **Conocimiento:** Es un conjunto de información adquirido mediante el aprendizaje, la experiencia o la introspección.

Principios

Se definen un conjunto de principios generales y otros que acompañan el ciclo de vida de los datos y buscan identificar sus principales características.



Ilustración 1 - Ciclo de vida de los datos

POLÍTICA DE DATOS PARA LA TRANSFORMACIÓN DIGITAL

GENERAL	GENERAR Y GESTIONAR	PROTEGER Y PRESERVAR	COMPARTIR Y UTILIZAR
DATOS COMO ACTIVOS	GENERACIÓN	PROTECCIÓN DE DATOS	ACCESO A LOS DATOS
RESPONSABILIDAD DE DATOS	EFICIENCIA	SEGURIDAD	COMPARTIR Y UTILIZAR
	CALIDAD	PRESERVACIÓN	DATOS ABIERTOS

Principios generales

Principio 1: Datos como activos

Los datos del sector público son un activo del Estado y deben ser exactos, consistentes, oportunos, accesibles, completos, auditables y trazables.

Principio 2: Responsabilidad de datos

Los datos del sector público tendrán una entidad pública responsable de su gestión y custodia durante todo el ciclo de vida, el cual es asignado según sus cometidos.

Las entidades públicas que usen datos deberán respetar el contenido, no alterar la integridad ni la consistencia e informar de cualquier anomalía detectada.

Principios asociados al ciclo de vida de los datos

Principio 3: Generación

Cada entidad pública genera (recolecta, produce, elabora) datos según sus cometidos. Los datos deberán ser generados atendiendo las definiciones de este documento, permitiendo su utilización por parte de otras entidades públicas.

Principio 4: Eficiencia

Cada entidad pública deberá recolectar y gestionar eficientemente los datos que estén bajo su responsabilidad, no debiendo recolectar datos que estén fuera de ella de acuerdo a lo establecido en el “Principio 2: Responsabilidad de datos”.

Se deberá evitar la generación de datos producidos por otra entidad pública.

Principio 5: Calidad

La calidad de los datos es fundamental para el uso que se realice en una administración basada en datos. Los datos deberán ser exactos, oportunos y conformes con la realidad.

Las entidades públicas deberán implementar procedimientos de gestión de calidad de datos para asegurar su veracidad, integridad y consistencia.

Principio 6: Acceso a los datos

Los datos del sector público deberán estar disponibles para las personas, salvo las restricciones que apliquen o se establezcan al respecto.

Si las entidades públicas poseen datos referidos a las personas físicas o jurídicas, deberán proveer mecanismos que les permitan acceder a esos datos, así como a los intercambios que se realicen sobre ellos.

Principio 7: Compartir y utilizar

Los datos deberán ser compartidos entre entidades públicas de forma tal que sean fáciles de (re)utilizar, entregar e intercambiar, cumpliendo con los estándares de datos, integración e intercambio que se establezcan para este fin.

Las entidades públicas no deberán poner condiciones financieras para el intercambio de datos entre ellas.

Los datos personales no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su recolección.

Se deberán explicitar las fuentes de los datos que se utilizan.

Principio 8: Datos abiertos

Los datos del sector público deberán ser abiertos por defecto.

Los principios vigentes de datos abiertos del Uruguay se consideran parte integrante de este documento.

Principio 9: Protección de datos

Las entidades públicas deberán proteger los datos personales persiguiendo los siguientes principios:

- Legalidad.
- Veracidad.
- Finalidad.
- Previo consentimiento informado.
- Seguridad de los datos.
- Reserva.
- Responsabilidad.

Los principios vigentes relacionados con la protección de datos personales en Uruguay se consideran parte integrante de este documento.

Principio 10: Seguridad

Las entidades públicas deberán implementar procedimientos de gestión de datos para proporcionar un nivel adecuado de confidencialidad, integridad, disponibilidad y autenticidad. Los lineamientos y la normativa vigentes en relación a ciberseguridad del Uruguay que apliquen a la seguridad de los datos se consideran parte integrante de este documento.

Principio 11: Preservación

Los datos se deberán preservar y conservar adecuadamente para mantener su integridad y asegurar la continuidad de acceso (disponibilidad) durante el tiempo que sea necesario, de acuerdo con la normativa vigente.

Cada entidad pública deberá preservar y conservar aquellos datos que estén bajo su responsabilidad de acuerdo a lo establecido en el “Principio 2: Responsabilidad de datos”.