

POLÍTICA DE PRIVACIDAD Y TRATAMIENTO DE DATOS PERSONALES PROYECTO SOCIAL TECH

1. Introducción y marco normativo

La Universidad Distrital Francisco José de Caldas, en su calidad de **Responsable del Tratamiento de Datos Personales** del proyecto **SOCIAL TECH**, garantiza el adecuado manejo, protección y tratamiento de la información suministrada por los usuarios, beneficiarios, aliados, proveedores y demás personas vinculadas con el proyecto.

Esta política se establece en cumplimiento de la **Ley Estatutaria 1581 de 2012**, el **Decreto 1377 de 2013**, el **Decreto 1074 de 2015**, la jurisprudencia de la Corte Constitucional respecto del derecho fundamental al **hábeas data**, la protección de la intimidad y la información personal, así como los estándares internacionales de protección de datos inspirados en el enfoque de responsabilidad demostrada (*accountability*).

2. Responsable del Tratamiento

Universidad Distrital Francisco José de Caldas

Proyecto SOCIAL TECH

Correo de contacto del proyecto: ci1572pqr25ofex@udistrital.edu.co

Domicilio: Bogotá D.C., Colombia.

3. Finalidades del Tratamiento

La Universidad Distrital Francisco José de Caldas utilizará la información suministrada única y exclusivamente para los fines indicados, por lo tanto, salvaguardará las bases de datos que contenga la información recolectada, y no permitirá el acceso a personal no autorizado, salvo las excepciones constitucionales y legales vigentes y aplicables sobre la materia. E

n ese sentido tomará todas las precauciones y medidas necesarias para garantizar la reserva de la información, de conformidad con el principio de confidencialidad que trata la Ley 1581 de 2012, y demás información vigente sobre la materia. El titular asiste los derechos que le otorga la normatividad vigente sobre la protección de datos y el derecho a la información.

El tratamiento que realizará la Universidad será el de recolectar, almacenar, procesar, usar y transmitir o transferir (según corresponda) los datos personales, atendiendo de forma estricta los deberes de seguridad y confidencialidad ordenados por la Ley 1581 de 2012 y el Decreto 1377 de 2013.

Los datos personales recolectados serán utilizados exclusivamente para las finalidades necesarias y proporcionales al desarrollo del proyecto SOCIAL TECH. Entre ellas:

1. **Gestión académica, administrativa y operativa del proyecto**, incluyendo inscripción, registro, segmentación, seguimiento y certificación de beneficiarios.
2. **Verificación de identidad, validación de requisitos y control de asistencia**, tanto presenciales como virtuales.
3. **Generación de reportes estadísticos, análisis de impacto, comportamiento de inscripciones y trazabilidad de participación.**
4. **Comunicación oficial con los beneficiarios**, mediante correo electrónico, llamadas, mensajería instantánea o cualquier canal dispuesto por el proyecto.
5. **Atención de consultas, solicitudes, reclamos o ejercicios de derechos de los titulares.**
6. **Entrega de informes al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)** como entidad aliada o financiadora del proyecto.
7. **Cumplimiento de obligaciones legales, contractuales o requerimientos de autoridades competentes.**

En ningún caso se realizará tratamiento para finalidades diferentes a las aquí descritas sin autorización previa del titular.

4. Datos recolectados

4.1. Datos Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

4.1.1. Tratamiento de Datos Sensibles: Se prohíbe el Tratamiento de datos sensibles, excepto cuando: a) El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización. b) El Tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización. c) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. d) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

4.1.2. Autorización Especial de Datos Personales Sensibles El equipo SocialTech, informará a través de los diversos medios de obtención de la autorización a todos sus titulares, que en virtud de la ley 1581 del 2012 y normas reglamentarias, en donde estos no están obligados a otorgar la autorización para el tratamiento de datos sensibles.

En caso de tratamiento de datos relativos a la salud, se implementarán las medidas necesarias para proteger la confidencialidad de la información. Los datos sensibles biométricos tratados tienen como finalidad la identificación de las personas, la seguridad, el cumplimiento de obligaciones legales y la adecuada prestación de los servicios.

4.2. Dato Público: Es el dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados. Ejemplo: Nombres y apellidos, número de cedula de ciudadanía, datos relativos al estado civil de las personas, su profesión u oficio, su calidad de comerciante o servidor público y aquellos que pueden obtenerse sin reserva alguna.

4.3. Dato Privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información. Ejemplo: Fotografías, videos, datos relacionados con su estilo de vida, entre otros.

4.4. Dato Semiprivado Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas. Ejemplo: Datos financieros y crediticios, dirección, teléfono, correo electrónico, entre otros.

SOCIAL TECH recolecta, entre otros:

- Datos de identificación: nombres, apellidos, tipo y número de documento.
- Datos de contacto: correo electrónico, teléfono, municipio de residencia.
- Datos demográficos: sexo biológico, género, fecha de nacimiento, etnia, discapacidad (si aplica).
- Datos académicos y de participación: cursos seleccionados, progreso, asistencia, certificaciones.
- Datos sensibles: aquellos definidos en el artículo 5 de la Ley 1581, los cuales serán tratados con especial protección.

Los datos sensibles solo se tratarán cuando:

1. El titular otorgue autorización explícita.
2. Sea necesario para el cumplimiento de un deber legal.
3. Sea indispensable para proteger intereses vitales del titular.

5. Transmisión y transferencia de datos

Los datos personales podrán ser transmitidos o compartidos con:

A. El Ministerio TIC, exclusivamente para fines de seguimiento, verificación, auditoría y cumplimiento del proyecto SOCIAL TECH.

B. Proveedores tecnológicos estrictamente necesarios, exclusivamente para:

- almacenamiento seguro,
- envío de comunicaciones,
- soporte operativo,
- procesamiento técnico de información.

En todos los casos:

- se garantizan las medidas de seguridad adecuadas,
- se firman acuerdos de confidencialidad o encargos de tratamiento,

- no se autoriza la reutilización de datos para finalidades distintas a SOCIAL TECH.

6. Principios aplicados al tratamiento

Esta política se rige por los principios de la Ley 1581 y estándares internacionales:

a) Principio de Legalidad en Materia de Tratamiento de Datos: La recolección, uso y el tratamiento es una actividad reglada que debe sujetarse a lo establecido en la Ley 1581 del 17 de octubre de 2012, decretos reglamentarios y demás disposiciones que la desarrollen.

b) Principio de Finalidad: La recolección, uso y el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

c) Principio de Libertad y consentimiento: La recolección, uso y el tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

d) Principio de Veracidad o Calidad: La información sujeta a La recolección, uso y tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de Datos parciales, incompletos, fraccionados o que induzcan a error.

e) Principio de Transparencia: En la recolección, uso y tratamiento debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

f) Principio de Acceso y Circulación Restringida: La recolección, uso y el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los titulares o terceros autorizados.

g) Principio de Seguridad: La información sujeta a recolección, uso y tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

h) Principio de Confidencialidad: Todos los funcionarios y contratistas que intervengan en el Tratamiento de Datos Personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de esta. El Ministerio de Ambiente y

Desarrollo Sostenible, se compromete a tratar los datos personales de los titulares, tal como lo define el literal g) del artículo 3 de la Ley 1581 de 2012 de forma absolutamente confidencial haciendo uso de estos, exclusivamente, para las finalidades indicadas en el apartado anterior, siempre que el titular no se haya opuesto a dicho tratamiento. El Ministerio, informa que tiene implantadas las medidas de seguridad de índole técnica y organizativas necesarias que garanticen la seguridad de sus datos personales y eviten su alteración, pérdida, tratamiento y/o acceso no autorizado.

i) Principio de temporalidad: Los datos personales se conservarán únicamente por el tiempo razonable y necesario para cumplir las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Los datos serán conservados cuando ello sea necesario para el cumplimiento de una obligación legal o contractual. Una vez cumplida la finalidad del tratamiento y los términos establecidos anteriormente, se procederá a la supresión de los datos.

j) Interpretación integral de los derechos constitucionales: Los derechos se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los derechos constitucionales aplicables.

k) Principio de Necesidad: Los datos personales tratados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos.

7. Derechos de los titulares

Los titulares podrán ejercer los siguientes derechos:

1. Conocer, actualizar y rectificar sus datos personales.
2. Solicitar prueba de la autorización otorgada.
3. Ser informados sobre el uso que se ha dado a sus datos.
4. Presentar quejas ante la Superintendencia de Industria y Comercio.
5. Revocar la autorización o solicitar la supresión del dato cuando no exista deber legal o contractual que lo impida.
6. Acceder gratuitamente a sus datos personales.

De igual manera, en el Tratamiento de los datos personales se requiere la autorización previa e informada del Titular, la cual debe ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

Se entenderá que la autorización cumple con los requisitos cuando se manifieste (i) por escrito, (ii) de forma oral, (iii) o por firmas de formatos (iv), las cuales son conductas inequívocas del titular que permiten concluir de forma razonable que otorgó la autorización, como por ejemplo, cuando se solicita autorización para la grabación de reuniones virtuales o presenciales la cual debe quedar grabada y se tendrá durante el tiempo que perdura la grabación, de igual forma en los eventos institucionales en los que se deje constancia grabada o escrita de la autorización del titular, cuando se remitan a la Entidad hojas de vida para participar en procesos de selección.

Cuando la recolección de datos personales se realice a través de medios digitales institucionales como el diligenciamiento de formularios en línea, portales web u otros

canales similares, se entenderá que el titular de los datos indica su conducta inequívoca cuando (I) acepte mediante casilla de verificación (II) realice el diligenciamiento del formulario.

8. Procedimiento para ejercer derechos

El titular podrá presentar solicitudes de consulta, corrección o supresión mediante:

Correo oficial del proyecto: ci1572pqr25ofex@udistrital.edu.co

Asunto: "Solicitud de ejercicio de derechos – Hábeas Data – SOCIAL TECH".

Plazos de respuesta:

- **Consultas:** 10 días hábiles prorrogables por 5 más.
- **Reclamos:** 15 días hábiles prorrogables por 8 más.

9. Medidas de seguridad

La Universidad adoptará medidas técnicas, administrativas y organizacionales que garanticen:

- Prevención de accesos no autorizados.
- Protocolos de custodia, integridad y disponibilidad de la información.
- Gestión de riesgos acorde a estándares institucionales.
- Tratamiento diferenciado para datos sensibles.
- Principio de "mínimo privilegio" y "necesidad de conocer".

10. Vigencia

Esta política rige a partir de su publicación y permanecerá vigente mientras se mantenga la información objeto de tratamiento.