MANUAL

MANUAL DE DATOS ADL Y ECOSISTEMAS

GESTIÓN LEGAL

Revisado por: Nombre: Vanessa García Cargo: Partner Legal Sr	**Aprobado por:** Nombre: María Fernanda Sánchez Cargo: General Counsel
Fecha de aprobación:	06/03/2025

Toda copia impresa o guardada magnéticamente en medios diferentes a la intranet de este documento se constituyen en copias no controladas

TABLA DE CONTENIDO

1. OBJETIVO **3**

2. ALCANCE **3**

3. GLOSARIO **3**

4. GENERALIDADES **4**

5. MANUAL **4**

5.1. PRINCIPIOS **4**

5.2. POLÍTICAS Y PROCEDIMIENTOS **5**

5.3. GOBIERNO EN LA PROTECCIÓN DE DATOS PERSONALES **5**

6. OBLIGACIONES **6**

6.1. ÁREAS ADMINISTRADORAS DE BASES DE DATOS RESPECTO DEL TRATAMIENTO DE DATOS PERSONALES. **6**

6.2. EQUIPO LEGAL RESPECTO DEL TRATAMIENTO DE DATOS PERSONALES **7**

6.3. GERENCIA DE CUMPLIMIENTO RESPECTO DEL TRATAMIENTO DE DATOS PERSONALES **8**

6.4. SEGURIDAD TI RESPECTO DEL TRATAMIENTO DE DATOS PERSONALES **9**

6.5. OBLIGACIONES DE LA GERENCIA DE ANALÍTICA RESPECTO DEL TRATAMIENTO DE DATOS PERSONALES **9**

7. SEGURIDAD Y CONFIDENCIALIDAD **9**

7.1. SEGURIDAD **9**

7.2. CONFIDENCIALIDAD **10**

8. PROTECCIÓN DE DATOS DESDE EL DISEÑO **10**

8.1. PRINCIPIOS DE PRIVACIDAD DESDE EL DISEÑO **10**

8.2. APLICABILIDAD DE LA RECOLECCIÓN DE DATOS **11**

9. TIPO DE INFORMACIÓN **12**

10. APLICABILIDAD **12**

11. CONTROL DE CAMBIOS **12**

En ADL DIGITAL LAB S.A.S (en adelante "ADL") y sus filiales y subsidiarias (también denominados internamente como los "Ecosistemas") nos importa la protección de los Datos Personales, por lo que, en cumplimiento de nuestras obligaciones legales, se elabora el presente Manual para el Tratamiento de Datos Personales (el "Manual"), el cual contiene la descripción de los principios, procedimientos y demás aspectos fundamentales que regirán el tratamiento que le daremos a los Datos Personales y que deben ser atendidos por todos y cada uno de los colaboradores y administradores de ADL y sus filiales y subsidiarias .

1. OBJETIVO

Establecer los lineamientos y procedimientos para la adecuada gestión y tratamiento de los Datos Personales de los Colaboradores, Visitantes, Usuarios, Proveedores, Clientes, Aliados, Inversionistas y Terceros en general, que han autorizado a ADL y/o sus filiales y subsidiarias para el Tratamiento de sus Datos Personales.

2. ALCANCE

Los lineamientos y procedimientos señalados en este Manual están dirigidos a orientar el Tratamiento de los Datos Personales que realice ADL y/o los Ecosistemas y todo su personal que entre en contacto, administre y en general realice tratamiento de bases de Datos Personales cuyo Responsable o Encargado sea ADL y/o los Ecosistemas.

3. GLOSARIO

- **Autorización.** Consentimiento previo, expreso e informado del Titular de los Datos Personales, para llevar a cabo el Tratamiento de dichos Datos Personales. En Colombia el Tratamiento de Datos Personales debe partir de una autorización tomada previamente o al momento de captura de los datos, salvo por excepciones que indica de manera expresa la ley. **La autorización debe ser resguardada para posterior consulta.**
- **Cookies o Datos de Navegación:** Pequeños fragmentos de información que se almacenan en una computadora o dispositivo por su navegador web; pueden o no contener datos personales.
- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables
- **Datos Financieros:** Información personal comercial, crediticia y financiera, contenida en centrales de información públicas o privadas. Ley 1266 de 2008.
- **Encargado:** Persona que por sí misma o en asocio con otros, realice el Tratamiento de Datos Personales por cuenta del Responsable.
- **Responsable:** Persona que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los Datos Personales, para este caso ADL y/o sus Ecosistemas.
- **Titular:** Persona natural, dueño de los Datos Personales;

- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre Datos Personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

4. GENERALIDADES

Descripción del contenido según el tipo documental y su finalidad.

Tampoco deben nombrar personas, sino cargos, deben ser específicas y pueden ir agrupadas por temas y subtemas, siguiendo una numeración lógica y secuencial. La redacción es en tercera persona, utilizando un lenguaje comprensible y conciso para que no haya dudas en su aplicación y seguimiento.

5. MANUAL

Los Datos Personales pueden categorizarse en **públicos, semiprivados y privados,** dependiendo del mayor o menor espectro de privacidad.
Hay categorías especiales de datos que implican una mayor responsabilidad para su recolección, uso y almacenamiento:

1. **Datos sensibles** (e.j. datos biométricos como la foto, huella, videos, etc.)
2. **Datos de niños, niñas y adolescentes.**

Formas jurídicas que habilitan compartir datos:

Contrato de Transferencia: Se suscribe cuando al receptor se le da la calidad de Responsable y por tanto puede decidir de forma autónoma sobre los datos entregados.

Contrato de Transmisión: Se suscribe cuando al receptor se le da la calidad de Encargado y por tanto solo puede hacer con los datos lo que se le ha permitido de forma expresa en dicho instrumento.

5.1. PRINCIPIOS

- **Legalidad:** El Tratamiento de los Datos Personales es una actividad reglada que debe sujetarse a lo establecido en la ley
- **Finalidad:** El Tratamiento de los Datos Personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al Titular
- **Libertad:** El Tratamiento de los Datos Personales 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.
- **Veracidad o calidad:** La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

- **Transparencia:** En el Tratamiento se 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 conciernen.
- **Acceso y circulación restringida:** 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 sólo a los Titulares o terceros autorizados conforme a la ley.
- **Seguridad:** La información sujeta a Tratamiento por el Responsable o el Encargado del Tratamiento, 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.
- **Confidencialidad:** Todas las personas 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 la misma.

5.2. POLÍTICAS Y PROCEDIMIENTOS

ADL y cada uno de los Ecosistemas cuentan con una **Política de Tratamiento de Datos Personales,** procedimientos y diferentes artefactos que definen las responsabilidades, controles y registros que permiten dar cumplimiento a los requerimientos legales que deben ser atendidos por las compañías y que se encuentran publicadas en los respectivos Sites de procesos y páginas de los ecosistemas.

5.3. GOBIERNO EN LA PROTECCIÓN DE DATOS PERSONALES

En ADL y los Ecosistemas hemos encontrado los siguientes actores vinculados con el Tratamiento de los Datos Personales:

- Áreas administradoras de bases de datos:

  1. Crean/modifican/ eliminan las bases de datos.
  2. Recogen y custodian las autorizaciones.
  3. Comparten las bases de datos con terceros.

- Dirección Legal

  1. Es el área responsable de la atención de peticiones, consultas y reclamos
  2. Determina los lineamientos legales para el Tratamiento de Datos Personales.

3. Elabora y actualiza las políticas, procesos/ procedimientos, los artefactos y el Manual
4. Reportes RNBD y respuestas requerimientos SIC

- Seguridad TI

1. Determina los criterios de seguridad TI aplicables a las bases de datos.

- Gerencia de Cumplimiento

1. Determina los lineamientos de seguridad de la información para el Tratamiento de Datos Personales.
2. Acompaña al área encargada para el seguimiento y gestiona los riesgos en el cumplimiento normativo y en la operación.
3. Apoya la documentación y adherencia de los procesos.

- Gerencia de Analítica

1. Encargada del gobierno de datos dentro de la plataforma de datos - Augusta.
2. Determina los criterios técnicos para la administración (almacenamiento, procesamiento, seguridad, entrega, entre otros) de datos siguiendo los lineamientos corporativos.

6. OBLIGACIONES

6.1. ÁREAS ADMINISTRADORAS DE BASES DE DATOS RESPECTO DEL TRATAMIENTO DE DATOS PERSONALES.

En ADL y los Ecosistemas hemos encontrado los siguientes actores vinculados con el Tratamiento de los Datos Personales:

Un área administradora de base de datos es la estructura dentro de la compañía que crea, usa, comparte, modifica, elimina y en general dispone de una base de datos.

Sus obligaciones son:

- Reportar la creación, modificación y eliminación de las bases de Datos Personales de acuerdo con el procedimiento GLE02-PR-02 Reporte Bases Datos Personales.

  Nota: A través del Reporte Bases Datos Personales se estructurará la hoja de vida de la base de datos donde se contempla el ciclo de vida del dato frente a su captura, almacenamiento, tratamiento y eliminación.

- Reportar las bases de datos creadas al Área de Ciberseguridad y Seguridad de la Información, en tanto que constituyen activos de información.

- Definir una persona o cargo para atender los requerimientos que la Dirección Legal traslade de los titulares y ejecutar las actividades correspondientes (eliminación, no contacto, rectificación, entre otras) conforme la solicitud del titular en la Base de datos personales que

corresponda. Para ello deberá notificar el correo electrónico de acuerdo con el formulario del procedimiento GLE02-PR-02 Reporte Bases Datos Personales.

- Registrar en la base de datos la leyenda "Reclamo en trámite ", cuando la Dirección Legal remita un reclamo al correo electrónico notificado por el área administradora y eliminarlo una vez se ejecute el procedimiento objeto de reclamo.
- Insertar en la base de datos la leyenda "Información en discusión judicial" cuando así lo solicite la Dirección Legal al correo registrado.
- Validar que se cuente con la autorización por cada titular reportado en la base de Datos Personales.
- Solicitar la autorización conforme los textos legales definidos por la Dirección Legal.
- Apoyar con la gestión de incidentes de seguridad de la información de Datos Personales y cualquier requerimiento relacionado con la gestión de las bases de Datos Personales.
- Antes de realizar la transmisión o transferencia de los datos, realizar las consultas a la Dirección Legal y solicitar el aval al área de Seguridad TI, Seguridad de la información y de Analítica.

6.2. EQUIPO LEGAL RESPECTO DEL TRATAMIENTO DE DATOS PERSONALES

Las obligaciones del equipo legal frente al tratamiento de datos personales:

1. Mantener actualizado el normograma respecto a las obligaciones de Datos Personales para ADL y sus Ecosistemas. Este artefacto debe ser revisado una vez cada semestre.
2. Definir y mantener actualizadas las proformas de contratos de transmisión y transferencia de Datos Personales.
3. Definir y actualizar los textos legales que habilitan la captura de los Datos Personales.
4. Definir y actualizar las finalidades alineadas con las necesidades del negocio y los lineamientos corporativos.
5. Elaborar los conceptos y prestar el asesoramiento sobre los asuntos relacionados con el manejo de Datos Personales.
6. Documentar y actualizar las políticas, manual, procedimientos y artefactos para cumplir los requerimientos legales en protección de Datos Personales.
7. Gestionar las consultas y reclamos de los Titulares.
8. Registrar las bases de datos ante la SIC.
9. Suministro de información de Datos Personales para el reporte a la SIC y las entidades de control que lo requieran.

10. Con la ayuda de la Gerencia de Cumplimiento y de acuerdo con la metodología indicada por dicha área, identificar y evaluar riesgos, causas y controles sobre el cumplimiento en Datos Personales.
11. Con la ayuda de la Gerencia de Cumplimiento y de acuerdo con la metodología indicada por dicha área, realizar el tratamiento de los riesgos dentro del Tratamiento de Datos Personales
12. Con la ayuda de la Gerencia de Cumplimiento y de acuerdo con el procedimiento establecido por dicha dirección, participar en la gestión de incidentes.
13. Con la ayuda de la Gerencia de Cumplimiento y de acuerdo con la metodología indicada por dicha área, reportar ante los entes competentes la gestión de incidentes sobre Datos Personales.
14. Revisión y apoyo en proyectos estratégicos a demanda de ADL y los Ecosistemas.
15. Realizar capacitaciones periódicas sobre los requerimientos legales en protección de Datos Personales.

6.3. GERENCIA DE CUMPLIMIENTO RESPECTO DEL TRATAMIENTO DE DATOS PERSONALES

Las obligaciones de la Gerencia de Cumplimiento son:

- Área de Riesgos
    - Monitorear cumplimiento normativo
    - Gestionar eventos de riesgo operacional
    - Testeo de controles
    - Apoyar con la identificación de riesgos causas y controles
- Área de Procesos
    - Apoyar con la documentación de políticas, manuales, procesos y artefactos
    - Apoyar con la definición de ANS e indicadores
    - Realizar análisis de métodos y tiempos
    - Realizar adherencia de los procesos
    - Consolidar la medición de la excelencia operacional de los procesos
- Área de Ciberseguridad y Seguridad de la Información
    - Definir lineamientos para garantizar la integridad, confidencialidad, disponibilidad y privacidad de la información
    - Identificar y clasificar los activos de información
    - Monitorear el nivel de madurez de CbSySI
    - Análisis de riesgos de ciberseguridad y seguridad de la información
    - Gestión de incidentes:
        - Contención y erradicación del incidente

- Actividades post incidente y cierre
- Planes de acción para cierre de incidentes

6.4. SEGURIDAD TI RESPECTO DEL TRATAMIENTO DE DATOS PERSONALES

Las obligaciones del área de seguridad TI son:

- Definir los controles de seguridad para la adecuada administración de la información en cumplimiento de los lineamientos establecidos.
- Participar en la gestión de incidentes:
  - Contención y erradicación del incidente
  - Actividades post incidente y cierre
  - Planes de acción para cierre de incidentes
- Análisis de riesgos de seguridad TI
- Avalar el canal y el receptor en el evento de una transmisión o transferencia de los datos.

6.5. OBLIGACIONES DE LA GERENCIA DE ANALÍTICA RESPECTO DEL TRATAMIENTO DE DATOS PERSONALES

Las obligaciones de la Gerencia de Analítica son:

- Aplicar los lineamientos corporativos de estrategia de datos para proyectos de analítica.
- Dar cumplimiento a los lineamientos determinados por la Gerencia de Cumplimiento para el Tratamiento de Datos Personales de ADL y de los Ecosistemas que reposan en Augusta.
- Cumplir con los protocolos establecidos por el área de Seguridad TI para los procesos de almacenamiento, procesamiento y transmisión de datos con entes internos y externos, sobre los Datos Personales de ADL y de los Ecosistemas que reposan en Augusta.
- Disponibilizar, a solicitud del área administradora de la base de datos, los datos pertinentes a terceros, previo concepto favorable legal (contrato de transmisión o transferencia), de seguridad de la información y de seguridad TI.

  Importante. Cualquier Dato Personal de clientes o usuarios de ADL y de los Ecosistemas deben reposar única y exclusivamente en la plataforma de datos Augusta, conforme los lineamientos corporativos que se han fijado para este fin.

7. SEGURIDAD Y CONFIDENCIALIDAD

7.1. SEGURIDAD

La gerencia que cree una base de datos deberá informarlo de manera inmediata a la Dirección Legal de acuerdo con el procedimiento GLE02-PR-02 Reporte Bases Datos Personales.
Las bases de datos son activos de información y por tanto deberán ser reportadas igualmente a la Gerencia de Cumplimiento.

7.2. CONFIDENCIALIDAD

Los Datos Personales tratados por ADL y los Ecosistemas son catalogados como información confidencial.
Podrá compartirse con terceros siempre que:

1. Se suscriban acuerdos que incluyan disposiciones sobre confidencialidad (cláusulas o acuerdos de no divulgación).
2. Se suscriban los acuerdos que habiliten compartir los datos.

Los colaboradores tienen las obligaciones de confidencialidad establecidas en sus contratos de trabajo. La violación de dichas estipulaciones será sancionada conforme los procedimientos que considere necesarios la compañía.

8. PROTECCIÓN DE DATOS DESDE EL DISEÑO

8.1. PRINCIPIOS DE PRIVACIDAD DESDE EL DISEÑO

8.1.1. PRINCIPIO: PROACTIVO NO REACTIVO: PREVENTIVO, NO CORRECTIVO

- Debemos anticiparnos a los eventos que pueden afectar la privacidad del producto o servicio, antes que sucedan
- Debemos concebir y diseñar el producto o servicio identificando a priori, los posibles riesgos que pueden llegar a tener los titulares de los datos personales.

8.1.2. PRINCIPIO: LA PRIVACIDAD COMO CONFIGURACIÓN PREDETERMINADA

- Se debe proporcionar al usuario el mayor nivel de privacidad sobre los datos personales suministrados ya sea en un sistema, en una aplicación, producto o servicio.
- La configuración por defecto deberá quedar establecida desde el diseño hasta aquel nivel que permita el mayor respeto posible de la protección de datos del titular.

8.1.3. PRINCIPIO: PRIVACIDAD INCORPORADA EN LA FASE DE DISEÑO

- La privacidad debe estar desde el momento en el que se planea el producto o servicio
- No puede ser una capa adicional, o una nueva funcionalidad que se le incorpora, sino que debe integrarse en todo su conjunto con los requisitos no funcionales desde el momento en que es concebido.

8.1.4. PRINCIPIO: FUNCIONALIDAD TOTAL

- Se debe abordar el pensamiento de todos ganan, debido a que normalmente las organizaciones tienen la percepción que cuando se incorporan funcionalidades para proteger la privacidad se sacrifican otro tipo de funcionalidades.
- Se deben acercar y revisar los puntos de vista, en detalle, que permita un equilibrio entre dichas funcionalidades, así como explorar nuevas soluciones que permitan que los sistemas puedan coexistir con intereses diferentes.

8.1.5. PRINCIPIO: ASEGURAMIENTO DE LA PRIVACIDAD EN TODO EL CICLO DE VIDA

- La privacidad debe pensarse desde el diseño, antes de que entre en funcionamiento el sistema.
- Cada ciclo de datos personales, se debe garantizar la seguridad de la información, lo cual impone, la confidencialidad, la integridad y la disponibilidad de la información.

8.1.6. PRINCIPIO: VISIBILIDAD Y TRANSPARENCIA

- Aborda la transparencia en el tratamiento de los datos personales, que en efecto este se realice según los fines que estamos informando que se van a usar.
- Se debe demostrar diligencia y responsabilidad proactiva ante la Superintendencia de Industria y Comercio ante una eventual inspección, auditoría o investigación.

8.1.7. PRINCIPIO: RESPETO POR LA PRIVACIDAD DE LOS USUARIOS

- Se debe garantizar en todo momento el respeto de los derechos de los titulares de los datos personales; en ese sentido, se debe mantener un enfoque centrado en el usuario, sin perder los intereses que tiene la organización en sus actividades.
- Todas las medidas que lleguen a adoptar en un futuro, en cuanto a procesos, aplicaciones, productos o servicios, deben tener el usuario en su perspectiva, de manera anticipada.

8.2. APLICABILIDAD DE LA RECOLECCIÓN DE DATOS

Cuando pretendas recoger Datos Personales, involucra desde el inicio a la Dirección Legal.

En conjunto con el equipo legal deberán revisar:

1. El tipo de datos a capturar, para determinar si son privados, semiprivados o públicos, o si pertenecen a una categoría especial como lo son los datos sensibles o los de niños, niñas y adolescentes. Esto establecerá la forma en la que se deberá solicitar la Autorización del Titular.
2. La experiencia de usuario, con el fin de validar para qué se toma el dato y cuándo se toma el dato.
3. El uso que se va a dar de los datos y si será o no compartido con terceros (internos o externos), con el fin de validar si este está cubierto por las finalidades de la respectiva Política de Tratamiento de Datos.

TOOL TIPS:

- Por ningún motivo cambiar los textos legales que ha proporcionado la Dirección Legal, sin que medie consulta previa y autorización expresa de dicha dirección.
- No pre-diligenciar los checkbox.

- Revisar bien el texto. No se autoriza la política, se autoriza el Tratamiento de Datos Personales conforme a la Política de Tratamiento de Datos Personales.
- La mera notificación no constituye una Autorización.
- Continuar navegando no es autorizar el uso de Datos Personales.

9. TIPO DE INFORMACIÓN

Público	Interno	Restringido
	X	

10. APLICABILIDAD

Compañías	Transversal
	X

11. CONTROL DE CAMBIOS

Versión	Fecha Aprobación	Descripción
01	04/07/2023	Versión inicial
02	06/03/2025	Se actualizan responsabilidades de los administradores de las bases de datos frente al reporte de base de datos y el ciclo de vida del dato