ASD SERVICIOS LEGALES SAS
NIT 901.795.000-1
MONTERÍA - BOGOTÁ
WhatsApp: +57 322 660 5404
asdservicioslegales.co

ASD

SERVICIOS LEGALES

POLÍTICA INTERNA PARA EL TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

Instrumento interno de obligatorio cumplimiento

Código PDP-001 | Versión 1.0

Montería, Córdoba
21 de julio de 2026

DOCUMENTO CONTROLADO - USO INSTITUCIONAL

TABLA DE CONTENIDO

TABLA DE CONTENIDO 2
1. IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO 4
2. OBJETO 4
3. FINALIDAD INSTITUCIONAL 4
4. MARCO JURÍDICO 4
5. ÁMBITO DE APLICACIÓN 5
6. DEFINICIONES 5
7. PRINCIPIOS RECTORES 5
8. CATEGORÍAS DE INFORMACIÓN TRATADA 5
9. FINALIDADES GENERALES DEL TRATAMIENTO 6
10. DATOS DE CLIENTES Y POTENCIALES CLIENTES 6
11. DATOS DE TRABAJADORES, ASPIRANTES Y CONTRATISTAS 6
12. DATOS DE PROVEEDORES 6
13. DATOS DE VISITANTES 6
14. DATOS SENSIBLES 6
15. DATOS DE NIÑOS, NIÑAS Y ADOLESCENTES 7
16. AUTORIZACIÓN DEL TITULAR 7
17. EVENTOS EN QUE NO SE REQUIERE AUTORIZACIÓN 7
18. DERECHOS DE LOS TITULARES 7
19. LEGITIMACIÓN 7
20. CANAL PARA CONSULTAS Y RECLAMOS 8
21. PROCEDIMIENTO PARA CONSULTAS 8
22. PROCEDIMIENTO PARA RECLAMOS 8
23. REQUISITO DE PROCEDIBILIDAD ANTE LA SIC 8
24. VIDEOVIGILANCIA 8
25. FOTOGRAFÍAS, VIDEOS Y GRABACIONES DEL PERSONAL 9
26. WHATSAPP Y MENSAJERÍA INSTANTÁNEA 9
27. CORREO ELECTRÓNICO 9
28. REDES SOCIALES, PUBLICIDAD Y TESTIMONIOS 9

29. SECRETO PROFESIONAL 9
30. ACCESO A EXPEDIENTES Y BASES DE DATOS 10
31. MEDIDAS DE SEGURIDAD 10
32. INCIDENTES DE SEGURIDAD 10
33. TRANSMISIÓN Y TRANSFERENCIA 10
34. CONSERVACIÓN Y SUPRESIÓN 10
35. RETIRO DE TRABAJADORES Y CONTRATISTAS 11
36. DEBERES DE TRABAJADORES Y COLABORADORES 11
37. PROHIBICIÓN GENERAL DE DIVULGACIÓN 11
38. CONSECUENCIAS DEL INCUMPLIMIENTO 11
39. CAPACITACIÓN 11
40. RESPONSABLE INTERNO DE PROTECCIÓN DE DATOS 11
41. REGISTRO NACIONAL DE BASES DE DATOS 12
42. AUDITORÍA Y REVISIÓN 12
43. APROBACIÓN INTERNA 12
44. VIGENCIA 12
A. APROBACIÓN 13

1. IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

Razón social: ASD SERVICIOS LEGALES S.A.S.

NIT: 901.795.000-1

Domicilio: Montería, Córdoba

Dirección: Calle 62B No. 8-10, Montería, Córdoba

Correo de protección de datos: asdlegal@icloud.com

Página web: www.asdservicioslegales.co

ASD Servicios Legales, en adelante "ASD", actuará como responsable del tratamiento cuando decida las finalidades, medios, recolección, almacenamiento, circulación, utilización y supresión de datos. Podrá actuar como encargada cuando trate información por cuenta de un tercero, sin perjuicio de las obligaciones legales y contractuales aplicables.

2. OBJETO

Establecer los principios, reglas, obligaciones, procedimientos y controles internos aplicables al tratamiento de datos personales de clientes, potenciales clientes, trabajadores, aspirantes, practicantes, judicantes, contratistas, proveedores, visitantes, testigos, peritos, contrapartes, apoderados, familiares y personas captadas por videovigilancia.

Comprende toda operación de recolección, almacenamiento, uso, consulta, circulación, transmisión, transferencia, actualización, corrección, conservación, archivo, eliminación o supresión, en soportes físicos o digitales.

3. FINALIDAD INSTITUCIONAL

ASD reconoce que la información jurídica puede comprometer la intimidad, el buen nombre, la imagen, el patrimonio, la salud, la situación familiar o laboral y otros derechos de sus titulares.

El tratamiento se realizará dentro de finalidades autorizadas o permitidas, bajo confidencialidad y secreto profesional, con acceso limitado, medidas proporcionales al riesgo, garantía de derechos y evidencia del cumplimiento. Esta política es obligatoria para toda persona que preste servicios o desarrolle actividades en ASD.

4. MARCO JURÍDICO

Constitución Política de Colombia, especialmente artículos 15, 20, 21, 29 y 74.

Ley Estatutaria 1581 de 2012; Decreto 1074 de 2015; Ley 1266 de 2008 cuando resulte aplicable; Ley 1273 de 2009; Ley 1123 de 2007; Código Sustantivo del Trabajo; instrucciones de la Superintendencia de Industria y Comercio; y jurisprudencia constitucional sobre hábeas data, intimidad, imagen y privacidad.

5. ÁMBITO DE APLICACIÓN

Aplica a todas las bases de datos y archivos físicos o digitales administrados por ASD; a sus sedes, oficinas, equipos, correos, líneas, mensajería, nubes y cámaras; y a trabajadores, abogados, dependientes, contratistas, proveedores, practicantes, judicantes y asesores.

También comprende datos almacenados en servicios o dispositivos fuera de Colombia cuando resulte aplicable la legislación colombiana.

6. DEFINICIONES

Autorización: consentimiento previo, expreso e informado del titular.

Aviso de privacidad: comunicación sobre la política, finalidades y forma de consulta.

Base de datos: conjunto organizado de datos personales objeto de tratamiento.

Dato personal: información vinculada o asociable a una persona natural determinada o determinable.

Dato público, privado, semiprivado y sensible: categorías definidas por la normativa según su naturaleza, circulación y nivel de protección.

Responsable: quien decide sobre la base y sus finalidades. Encargado: quien trata datos por cuenta del responsable. Titular: persona natural a quien pertenecen los datos.

Tratamiento: cualquier operación sobre datos. Transferencia: envío a otro responsable. Transmisión: comunicación a un encargado.

Incidente de seguridad: evento que compromete o puede comprometer la confidencialidad, disponibilidad, integridad o seguridad. Videovigilancia: captación o manejo de imágenes o sonidos mediante dispositivos tecnológicos.

7. PRINCIPIOS RECTORES

Legalidad; finalidad legítima, específica e informada; libertad y autorización; veracidad o calidad; transparencia; acceso y circulación restringida; seguridad; confidencialidad; necesidad y minimización; temporalidad; y responsabilidad demostrada.

La vinculación con ASD no concede acceso general a expedientes. Solo se recolectarán datos pertinentes y se conservarán durante el tiempo necesario o legalmente exigido.

8. CATEGORÍAS DE INFORMACIÓN TRATADA

Datos de identificación y contacto; profesionales, académicos y laborales; financieros, económicos y patrimoniales; judiciales y jurídicos; sensibles; tecnológicos; y audiovisuales.

Incluyen, entre otros, documentos de identidad, firma, fotografía, contacto, hoja de vida, información bancaria, expedientes, poderes, pruebas, salud, biometría, datos de menores, direcciones IP, registros de acceso, audios, videos e imágenes de seguridad.

9. FINALIDADES GENERALES DEL TRATAMIENTO

Prestar servicios jurídicos y administrativos; evaluar solicitudes; elaborar documentos; ejercer representación; gestionar expedientes y comunicaciones; verificar identidad; facturar y cobrar; cumplir obligaciones; prevenir fraude y conflictos; gestionar riesgos; atender titulares y autoridades; realizar auditorías; proteger instalaciones e información; gestionar relaciones laborales y comerciales; y defender derechos e intereses legítimos.

10. DATOS DE CLIENTES Y POTENCIALES CLIENTES

Podrán usarse para analizar viabilidad, verificar conflictos, preparar propuestas, ejecutar encargos, adelantar actuaciones, solicitar pruebas, comunicar información necesaria, gestionar pagos, conservar expedientes y cumplir deberes legales.

La autorización para prestar servicios no comprende publicidad. El uso del nombre, imagen, voz, testimonio o historia del cliente exige autorización específica e independiente.

11. DATOS DE TRABAJADORES, ASPIRANTES Y CONTRATISTAS

Podrán tratarse para selección, verificación, formalización, seguridad social, nómina, vacaciones, desempeño, asignación de accesos, seguridad y salud, procedimientos disciplinarios, investigaciones, certificaciones y conservación de la historia laboral o contractual.

No podrán utilizarse para discriminación, persecución o controles desproporcionados.

12. DATOS DE PROVEEDORES

Podrán tratarse para cotizaciones, selección, contratación, verificación, pagos, obligaciones fiscales, control de acceso, garantías, reclamaciones, seguridad y auditorías.

Los proveedores con acceso a datos por cuenta de ASD deberán asumir obligaciones como encargados del tratamiento.

13. DATOS DE VISITANTES

Se recolectarán solo los datos necesarios para controlar ingresos y salidas, proteger personas e instalaciones, identificar accesos a zonas restringidas, investigar incidentes y atender emergencias.

14. DATOS SENSIBLES

Tendrán protección reforzada. Cuando se requiera autorización, se informará su carácter facultativo, la naturaleza sensible, finalidad, accesos y consecuencias de no suministrarlos.

Solo se tratarán con autorización explícita o bajo las excepciones legales, incluida la defensa de derechos en procesos judiciales, intereses vitales, datos manifiestamente públicos o fines históricos, estadísticos o científicos con medidas de anonimización.

15. DATOS DE NIÑOS, NIÑAS Y ADOLESCENTES

Su tratamiento responderá al interés superior, respetará derechos fundamentales, será necesario y limitará accesos. Se obtendrá autorización del representante cuando corresponda y se considerará la opinión del menor según su madurez.

Se prohíbe publicar información identificable de menores sin soporte jurídico suficiente.

16. AUTORIZACIÓN DEL TITULAR

Será previa, expresa e informada, obtenida por escrito, medios electrónicos, grabación, mecanismos técnicos o conductas inequívocas. El silencio no constituye autorización.

ASD informará los datos, finalidades, derechos, canales de contacto y carácter facultativo de datos sensibles o de menores, y conservará prueba verificable.

17. EVENTOS EN QUE NO SE REQUIERE AUTORIZACIÓN

Información requerida por autoridad competente u orden judicial; datos públicos; urgencia médica o sanitaria; fines históricos, estadísticos o científicos autorizados; registro civil; ejercicio o defensa de derechos con fundamento suficiente; y demás casos legales.

La excepción no elimina los deberes de finalidad, seguridad, confidencialidad, acceso restringido y calidad.

18. DERECHOS DE LOS TITULARES

Conocer, actualizar y rectificar; solicitar prueba de autorización; ser informados del uso; presentar consultas y reclamos; solicitar supresión o revocatoria cuando proceda; acceder gratuitamente; conocer la circulación; presentar quejas ante la SIC; y exigir seguridad y confidencialidad.

La supresión o revocatoria no procede frente a deberes legales, contractuales, judiciales, probatorios, administrativos o disciplinarios de conservación.

19. LEGITIMACIÓN

Podrán ejercer derechos el titular, sus causahabientes, representante o apoderado acreditado, quien actúe por estipulación a favor de otro y el representante de menores o incapaces. ASD verificará identidad y legitimación.

20. CANAL PARA CONSULTAS Y RECLAMOS

Dependencia: ÁREA JURÍDICA.

Correo: Asdlegal@icloud.com

Dirección: Cale 62B #8-10, Barrio la Castellana.

Teléfono: 3226605404

Horario de atención: De 8:00am a 12:00pm y de 2:00pm a 6:00pm de Lunes a Viernes.

21. PROCEDIMIENTO PARA CONSULTAS

ASD verificará identidad y legitimación, localizará la información y responderá de forma clara, completa y comprensible dentro de diez (10) días hábiles. Si requiere ampliación, informará razones y fecha; la prórroga no excederá cinco (5) días hábiles.

22. PROCEDIMIENTO PARA RECLAMOS

Si el reclamo está incompleto, se requerirá subsanación dentro de cinco (5) días hábiles. Transcurridos dos (2) meses sin respuesta, se entenderá desistido. Si ASD no es competente, trasladará e informará cuando sea posible.

Recibido completo, se marcará “reclamo en trámite”. Se resolverá en quince (15) días hábiles; la ampliación motivada no excederá ocho (8) días hábiles adicionales.

23. REQUISITO DE PROCEDIBILIDAD ANTE LA SIC

El titular o causahabiente agotará previamente la consulta o reclamo ante ASD antes de acudir a la Superintendencia de Industria y Comercio, cuando la normativa así lo exija.

24. VIDEOVIGILANCIA

Las imágenes identificables son datos personales. Las cámaras se usarán para proteger personas, instalaciones, equipos, expedientes, controlar accesos, verificar incidentes y preservar evidencia.

Se prohíbe espiar, escuchar consultas, humillar, divulgar, realizar controles discriminatorios o vigilar espacios con expectativa reforzada de privacidad. No habrá cámaras en baños, vestidores, duchas, lactarios ni áreas de comunicaciones jurídicas confidenciales, salvo justificación excepcional.

No se grabará audio salvo autorización de Gerencia, concepto previo, necesidad demostrada y controles reforzados. Se instalarán avisos visibles.

Acceso limitado al representante legal, gerencia, responsable de datos, seguridad autorizada y autoridades. Toda consulta o copia se registrará.

25. FOTOGRAFÍAS, VIDEOS Y GRABACIONES DEL PERSONAL

Solo podrán realizarse cuando sean necesarias para funciones, exista finalidad legítima y autorización institucional, sean proporcionales, se almacenen en medios autorizados y se eliminen de dispositivos personales al terminar la finalidad.

Se prohíbe fotografiar expedientes o identidades para uso personal; captar pantallas, correos, chats o claves; grabar reuniones sin informar; grabar conversaciones ajenas; copiar videos de seguridad; crear memes; publicar o enviar material interno; y conservar copias innecesarias.

26. WHATSAPP Y MENSAJERÍA INSTANTÁNEA

Se verificará el destinatario y se enviará solo la información necesaria. No se remitirán expedientes o datos sensibles a grupos generales; se preferirán líneas institucionales; se protegerán dispositivos y se evitarán nubes personales y conservación indefinida.

La pérdida, hurto o acceso no autorizado se reportará inmediatamente. La información recibida mantiene su confidencialidad.

27. CORREO ELECTRÓNICO

Se verificarán destinatarios, se usará copia oculta en envíos masivos, doble autenticación y archivos protegidos cuando corresponda. Se evitarán correos personales y reenvíos no autorizados, y se reportarán mensajes sospechosos.

28. REDES SOCIALES, PUBLICIDAD Y TESTIMONIOS

No se publicarán datos identificables de clientes, demandas, memoriales, audiencias, conversaciones, capturas, información médica, financiera o de menores sin soporte válido.

El uso publicitario de imagen, voz, nombre, historia o testimonio requiere autorización específica.

29. SECRETO PROFESIONAL

Comprende consultas, estrategias, opiniones, pruebas, negociaciones, documentos, antecedentes, información familiar, financiera o médica, claves, conversaciones y honorarios, incluso antes de formalizar el contrato.

Obliga a abogados, trabajadores, auxiliares, practicantes, dependientes, proveedores y toda persona con acceso.

30. ACCESO A EXPEDIENTES Y BASES DE DATOS

Se aplicará mínimo privilegio. Se prohíbe consultar por curiosidad; acceder a casos no asignados; usar cuentas ajenas; compartir claves; descargar bases completas; usar USB personales; enviar a cuentas personales; conservar archivos al retirarse; extraer listados; o captar clientes para beneficio propio.

31. MEDIDAS DE SEGURIDAD

Técnicas: contraseñas individuales, doble factor, bloqueo, antivirus, actualizaciones, copias, permisos, cifrado, control de dispositivos, registros, borrado seguro y recuperación.

Físicas: archivos bajo llave, áreas restringidas, control de visitantes, protección de servidores y grabadores, destrucción segura, pantallas protegidas y escritorio limpio.

Administrativas: inventarios, matriz de riesgos, capacitación, confidencialidad, ingreso y retiro, evaluación de proveedores, auditorías, incidentes y revisión de permisos.

32. INCIDENTES DE SEGURIDAD

Se reportarán de inmediato pérdidas, envíos erróneos, accesos no autorizados, claves reveladas, expedientes extraviados, publicaciones accidentales, ataques, phishing, descargas, divulgación de videos o software no autorizado.

Canal: Asdlegal@icloud.com

ASD contendrá, evaluará, preservará evidencia, recuperará, cambiará credenciales, valorará riesgos y reportes, corregirá y documentará. Ningún colaborador ocultará incidentes.

33. TRANSMISIÓN Y TRANSFERENCIA

ASD podrá comunicar datos a autoridades, despachos, notarías, centros de conciliación, peritos, auxiliares, proveedores tecnológicos, mensajería, contadores, bancos, aseguradoras y profesionales necesarios.

Los encargados asumirán obligaciones de finalidad, confidencialidad, seguridad, atención de derechos, reporte, devolución o supresión, prohibición de uso propio, subcontratación y auditoría. Las transferencias internacionales cumplirán la ley.

34. CONSERVACIÓN Y SUPRESIÓN

Se conservarán datos mientras sean necesarios para el servicio, obligaciones, responsabilidad profesional, defensa de derechos, normas fiscales, laborales y archivísticas, investigaciones y evidencia.

Cumplida la finalidad y vencidos los plazos, serán eliminados, destruidos, devueltos, anonimizados o bloqueados mediante métodos que impidan razonablemente su reconstrucción.

35. RETIRO DE TRABAJADORES Y CONTRATISTAS

Se revocarán usuarios, cambiarán claves, recuperarán equipos y documentos, ordenará eliminar copias, recordará la reserva, documentará el cierre y revisarán accesos recientes si existe riesgo. La confidencialidad subsiste al retiro.

36. DEBERES DE TRABAJADORES Y COLABORADORES

Conocer y cumplir la política; usar datos solo para funciones; guardar confidencialidad; proteger credenciales; reportar incidentes; ordenar expedientes; evitar conversaciones públicas; verificar destinatarios; usar canales autorizados; capacitarse; devolver información; informar riesgos; abstenerse de accesos no asignados; y colaborar con auditorías.

37. PROHIBICIÓN GENERAL DE DIVULGACIÓN

Queda prohibido tomar, copiar, grabar, almacenar, descargar, reproducir, transmitir, reenviar, publicar, revelar, entregar o utilizar fotografías, videos, audios, documentos, expedientes, comunicaciones, pantallas, bases de datos, claves o videovigilancia sin autorización institucional y necesidad legítima.

La información no se usará para fines personales, familiares, comerciales propios, publicitarios no autorizados, humorísticos, discriminatorios, políticos, de presión, venganza o ajenos a la finalidad institucional.

38. CONSECUENCIAS DEL INCUMPLIMIENTO

Podrá generar medidas correctivas, restricción de accesos, requerimientos, procesos disciplinarios, terminación contractual con fundamento legal, reclamaciones, denuncias, quejas, reportes y acciones judiciales.

Toda actuación respetará debido proceso, defensa y proporcionalidad.

39. CAPACITACIÓN

ASD realizará formación periódica sobre protección de datos, secreto profesional, expedientes, seguridad informática, mensajería, correo, videovigilancia, fotografías, incidentes, atención de titulares, ingeniería social y datos sensibles. Se documentarán asistencia y evaluación.

40. RESPONSABLE INTERNO DE PROTECCIÓN DE DATOS

Cargo: Gerente

Nombre: Jaime Ramos Vergara

Promoverá cumplimiento, atenderá solicitudes, coordinará capacitación, inventarios e incidentes, evaluará riesgos, revisará contratos y seguridad, informará a Gerencia, conservará evidencias, propondrá actualizaciones y coordinará relaciones con la SIC.

41. REGISTRO NACIONAL DE BASES DE DATOS

ASD verificará periódicamente si está obligada a inscribir sus bases en el RNBD. La inexistencia de obligación registral no exime del cumplimiento de la Ley 1581 de 2012 ni de esta política.

42. AUDITORÍA Y REVISIÓN

Se revisará al menos anualmente y cuando cambie la normativa, tecnología, cámaras, bases, actividades, ocurra un incidente grave o la SIC emita instrucciones. Las modificaciones serán aprobadas por Gerencia y comunicadas.

43. APROBACIÓN INTERNA

Se adoptará mediante acta, resolución, circular o decisión formal. Todo el personal deberá recibirla, conocerla y suscribir constancia de lectura y compromiso.

44. VIGENCIA

Entra en vigencia el 21 de julio del año 2026. Las bases permanecerán vigentes durante el tiempo necesario para las finalidades y obligaciones aplicables.

A. APROBACIÓN

JAIME ANDRÉS RAMOS VERGARA

Representante legal / gerente

ASD Servicios Legales

C.C. 1.020.768.769

Fecha: 21 julio de 2026.