

# EMPRESA URRÁ S.A. E.S.P.

NIT 800.175.746-9

## POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

*Para el cumplimiento de la Ley Estatutaria 1581 de 2012 y normas concordantes*

<b>Versión:</b> 04
<b>Vigente desde:</b> Marzo de 2026
<b>Reemplaza la</b> Versión 03 de Marzo 2024
<b>Aprobado por:</b> Alta Dirección de URRÁ S.A. E.S.P.

### CONTENIDO

1. Datos del Responsable del Tratamiento
2. Objetivo y Alcance
3. Marco Legal Aplicable
4. Definiciones
5. Principios Rectores
6. Categorías Especiales de Datos

Tratamiento de Datos Sensibles  
Derechos de los niños, niñas y adolescentes.

7. Derechos de los Titulares
8. Autorización para el Tratamiento de Datos Personales
9. Aviso de Privacidad
10. Finalidades del Tratamiento

Titulares Empleados, Colaboradores Y/O Candidatos  
Titulares Terceros (Contratistas Y Proveedores)  
Titulares Clientes  
Titulares Comunidades  
Otros Titulares

11. Temporalidad del Tratamiento
12. Encargados del Tratamiento
13. Transmisión y Transferencia de Datos
14. Reporte de Incidentes de Seguridad
15. Atención de Consultas y Reclamos
16. Procedimiento y Plazos para atender derechos de los titulares
17. Registro Nacional de Bases de Datos
18. Responsabilidad Demostrada
19. Deberes del Responsable y Encargados del Tratamiento
20. Capacitación del Talento Humano
21. Seguridad de la Información
22. Entrega de Datos a Autoridades
23. Vigencia y Actualización de la Política
24. Resumen de Cambios respecto de la versión anterior

## 1. DATOS DEL RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES

<b>Razón Social:</b> EMPRESA URRÁ S.A. E.S.P.
<b>NIT:</b> 800.175.746-9
<b>Correo Protección de Datos:</b> protecciondedatos@urra.com.co
<b>Teléfono:</b> 604 784 8991 Ext. 533 y 542
<b>Domicilio:</b> Cra 2 # 48-08 Esq., Montería, Córdoba, Colombia
<b>Sitio Web:</b> www.urra.com.co

URRÁ, como Responsable del Tratamiento de datos personales, incluye en esta calidad de responsable a su equipo humano y a todas las áreas que intervienen en el tratamiento. El Oficial de Protección de Datos Personales (OPD) lidera el cumplimiento normativo con el respaldo de la Alta Dirección.

## 2. OBJETIVO Y ALCANCE

Informar a los Titulares de datos personales y a la ciudadanía en general sobre los lineamientos de URRÁ para el tratamiento de datos personales, garantizando el cumplimiento de la normatividad vigente y las buenas prácticas en materia de Protección de Datos Personales.

Esta Política aplica a todas las bases de datos físicas y automatizadas (electrónicas o digitales) usadas por URRÁ en calidad de Responsable o de Encargado. Todos los colaboradores, contratistas, proveedores y terceros involucrados en el tratamiento de datos personales deben conocer, aplicar y cumplir esta Política, so pena de las sanciones disciplinarias, civiles o penales que correspondan.

URRÁ adopta un Programa Integral de Gestión de Datos Personales que incluye entre otros puntos: (i) esta Política; (ii) Avisos de Privacidad diferenciados; (iii) formatos de autorización; (iv) manual de procedimientos de consultas y reclamos; (v) inventario de bases de datos; y (vi) medidas de seguridad de la información.

## 3. MARCO LEGAL APLICABLE

- Constitución Política de Colombia, artículos 15 y 20.
- Sentencias Corte Constitucional C-1011 de 2008 y C-748 de 2011.
- Ley Estatutaria 1581 de 2012.
- Decreto Único Reglamentario 1074 de 2015, Capítulos 25 y 26 (que compila los Decretos 1377 de 2013 y 886 de 2014).
- Decreto 255 de 2022 (Normas Corporativas Vinculantes, adiciona Sección 7 al Capítulo 25 del Decreto 1074 de 2015).
- Circular Externa 001 del 8 de noviembre de 2016, SIC.

- Decreto 090 del 18 de enero de 2018.
- Guía para el Oficial de Protección de Datos Personales (SuperIndustria, 2023).
- Ley 1266 de 2008 (Habeas Data financiero, cuando aplique).
- Demás normas que modifiquen, adicionen o complementen la Ley 1581 de 2012.

## 4. DEFINICIONES - Glosario Data Privacy Risk®

Los conceptos descritos a continuación permiten comprender esta Política. Han sido tomados de la Ley 1581 de 2012, el Decreto 1074 de 2015 Capítulo 25, la Guía OPD de la SuperIndustria (2023) y consolidados en el Glosario Data Privacy Risk:

TÉRMINO	DEFINICIÓN
<b>Ambito de Aplicación</b>	<p>Los principios y disposiciones contenidas en la ley 1581 de 2012 serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.</p> <p>La ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.</p>
<b>Área a cargo de la Protección de Datos Personales</b>	<p>URRÁ asignará una persona o área que velará por el cumplimiento de la Ley 1581 de 2012. Cuando lo estime necesario se apoyará en consultores externos especializados para fortalecer con buenas prácticas este cumplimiento.</p>
<b>Autorización</b>	<p>Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de sus datos personales.</p>
<b>Aviso de Privacidad</b>	<p>Comunicación verbal o escrita del Responsable al Titular, informando sobre las políticas de tratamiento, forma de acceso y finalidades del mismo.</p>
<b>Base de Datos</b>	<p>Conjunto organizado de datos personales objeto de tratamiento, en medios físicos o automatizados.</p>
<b>Biometría</b>	<p>Datos derivados del reconocimiento inequívoco de personas basado en características físicas o conductuales únicas (voz, rostro, iris, huella digital). Son datos sensibles.</p>
<b>Calidad del Dato</b>	<p>El dato debe ser veraz, completo, exacto, actualizado, comprobable y comprensible. Se prohíbe tratar datos parciales, fraccionados o que induzcan a error, por lo cual debe implementar los procesos necesarios para verificarlos, completarlos y corregirlos cuando sea requerido.</p>
<b>Confidencialidad</b>	<p>Es una propiedad que otorga el carácter de reservado a una información. Es decir que esta información no podrá ser divulgada o revelada a personas no autorizadas para conocerla.</p>

<b>Dato Personal</b>	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
<b>Dato Público</b>	Dato que no es semiprivado, privado ni sensible. Ej: Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Puede estar en registros públicos, documentos públicos o gacetas oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
<b>Data Privacy Risk®</b>	Metodología de la empresa colombiana Data & Business Risk SAS, para el cumplimiento de la Ley de Protección de Datos Personales y en general de la normalidad colombiana e internacional en privacidad.
<b>Dato Semiprivado</b>	Dato cuyo conocimiento interesa al titular y a cierto sector o a la sociedad. Ej: datos financieros, crediticios o de actividades comerciales.
<b>Dato Sensible</b>	Afecta la intimidad del Titular o puede generar su discriminación: origen racial o étnico, orientación política, creencias religiosas, pertenencia a sindicatos, datos de salud, vida sexual y datos biométricos.
<b>Derechos de niños, niñas y adolescentes</b>	Sólo podrán tratarse aquellos datos de menores que sean de naturaleza pública. El tratamiento de datos no públicos requiere autorización. En el Tratamiento de Datos Personales se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.
<b>Encargado del Tratamiento</b>	Persona natural o jurídica, pública o privada, que realiza el tratamiento de datos personales por cuenta del Responsable. La Empresa aunque es RESPONSABLE de datos personales, en determinados casos también podría ser también empresa ENCARGADA de datos personales.
<b>Habeas Data</b>	Derecho fundamental (Art. 15 de la Constitución Política de Colombia) que permite a toda persona conocer, actualizar y rectificar la información recogida sobre ella en bases de datos públicas o privadas.
<b>Incidente de Seguridad</b>	Evento que afecta la confidencialidad, integridad o disponibilidad de los datos personales, incluyendo accesos no autorizados, pérdida o divulgación indebida.
<b>Matriz de riesgos por protección de datos personales</b>	Herramienta de gestión que permite <b>identificar, analizar, evaluar y priorizar los riesgos</b> asociados al tratamiento de datos personales dentro de una organización, con el fin de prevenir incidentes como filtraciones, accesos no autorizados o uso indebido de la información.

<b>Oficial PDP (PDP: Protección de Datos Personales) - OPD</b>	Persona con conocimientos especializados que lidera el cumplimiento de la Ley 1581 de 2012 con respaldo de la Alta Dirección. No podrá tener conflicto de intereses con la organización.
<b>Responsable del Tratamiento</b>	Persona natural o jurídica, pública o privada, que decide sobre la base de datos y/o el tratamiento de los datos personales.
<b>RNBD</b>	Registro Nacional de Bases de Datos. Sistema de información de la SIC donde se inscribe anualmente el inventario de bases de datos con datos personales.
<b>SIC, Superintendencia de Industria y Comercio o Súper Industria.</b>	SIC, conocida como la Superintendencia de Industria y Comercio (también llamada informalmente “Súper Industria”), es una entidad del Estado colombiano encargada de vigilar, controlar y proteger los derechos de los consumidores, la libre competencia y la protección de datos personales.
<b>Titular del dato</b>	Persona natural cuyos datos personales son objeto de tratamiento.
<b>Transferencia</b>	Envío de datos personales a un receptor en Colombia o en el exterior que asume calidad de Responsable del Tratamiento.
<b>Transmisión</b>	Comunicación de datos personales a un Encargado, dentro o fuera de Colombia, para que realice el tratamiento por cuenta del Responsable, mediante contrato. Las partes deben hacer un contrato de transmisión de datos personales para establecer el objetivo, las condiciones y obligaciones de las partes respecto del uso de los datos.
<b>Tratamiento de datos</b>	Cualquier operación sobre datos personales: recolección, almacenamiento, uso, circulación, supresión, actualización, entre otras.

## 5. PRINCIPIOS RECTORES PARA EL TRATAMIENTO DE DATOS PERSONALES

URRÁ aplica de manera armónica e integral los principios del Título II, Artículo 4° de la Ley 1581 de 2012:

- **Legalidad:** El tratamiento es una actividad reglada sujeta a la Ley 1581 de 2012 y demás normas que la desarrollen.
- **Finalidad:** El tratamiento obedece a una finalidad legítima, constitucional y legal, informada al Titular.
- **Libertad:** El tratamiento solo puede ejercerse con consentimiento previo, expreso e informado del Titular, salvo mandato legal o judicial.
- **Veracidad o Calidad:** La información debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales o que induzcan a error.
- **Transparencia:** El Titular puede obtener del Responsable o del Encargado, en cualquier momento y sin restricciones, información sobre sus datos.
- **Acceso y Circulación Restringida:** El tratamiento solo lo pueden hacer personas autorizadas por el Titular o la ley. Los datos no pueden estar disponibles en internet salvo acceso técnicamente controlado.
- **Seguridad:** Los datos deben manejarse con medidas técnicas, humanas y administrativas que eviten adulteración, pérdida, acceso no autorizado o fraudulento.

- **Confidencialidad:** Quienes intervienen en el tratamiento están obligados a garantizar la reserva de la información, incluso después de finalizada su relación laboral o contractual con URRÁ.

## 6. CATEGORÍAS ESPECIALES DE DATOS

### 6.1 Tratamiento de Datos Sensibles

Son datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar discriminación (Ley 1581 de 2012, Art. 5°): origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos u organizaciones de derechos humanos, datos de salud, vida sexual y datos biométricos.

Se PROHÍBE el tratamiento de datos sensibles, excepto cuando:

- El Titular otorgue autorización explícita, salvo que la ley no lo exija.
- Sea necesario para salvaguardar el interés vital del Titular incapacitado física o jurídicamente (con autorización del representante legal).
- Lo efectúe una fundación, ONG o asociación sin ánimo de lucro con finalidad política, filosófica, religiosa o sindical, para sus miembros, sin suministrar datos a terceros sin autorización.
- Se requieran para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Tengan finalidad histórica, estadística o científica, adoptando medidas de supresión de identidad.

**Casos en los que URRÁ tratará datos sensibles:** identificación biométrica, videovigilancia, control de acceso, registros fotográficos y audiovisuales, teletrabajo, videoconferencias. En el ámbito de Seguridad y Salud en el Trabajo (SST): datos de salud, exámenes médicos, incapacidades, control de temperatura y medidas gubernamentales de salud pública. También para cumplimiento de contratos laborales y comerciales. En todos los casos se solicitará autorización expresa del Titular.

### 6.2 Derechos de los Niños, Niñas y Adolescentes

Queda prohibido el tratamiento de datos de menores de edad, salvo datos de naturaleza pública o cuando el tratamiento respete el interés superior del menor y sus derechos fundamentales. La autorización la otorga el representante legal, previo derecho del menor a ser escuchado según su madurez y capacidad. Todo Responsable o Encargado que trate datos de menores deberá garantizar su uso adecuado conforme a la Ley 1581 de 2012.

## 7. DERECHOS DE LOS TITULARES DE DATOS PERSONALES

Conforme al Título IV, Artículo 8° de la Ley 1581 de 2012, el Titular tiene derecho a:

- Conocer, actualizar y rectificar sus datos personales frente al Responsable o Encargado, incluso cuando sean parciales, inexactos, incompletos o induzcan a error.
- Solicitar prueba de la autorización otorgada al Responsable, salvo que la ley la exceptúe.
- Ser informado sobre el uso dado a sus datos personales, previa solicitud.
- Presentar quejas ante la SIC por infracciones a la Ley 1581 de 2012.
- Revocar la autorización y/o solicitar la supresión de sus datos cuando el tratamiento no respete los principios y derechos constitucionales y legales.
- Acceder gratuitamente a sus datos personales que hayan sido objeto de tratamiento.

URRÁ garantiza el ejercicio efectivo de estos derechos a través de sus canales de atención establecidos en el numeral 15 de esta Política.

## 8. AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

Sin perjuicio de las excepciones legales, el tratamiento requiere autorización previa, expresa e informada del Titular, obtenida por cualquier medio que permita su consulta posterior (Ley 1581 de 2012, Arts. 9° y 10°). URRÁ captará la autorización en medios físicos, digitales o electrónicos: firma física, aceptación electrónica, verbal con constancia, video, señal biométrica u otros. La autorización también puede otorgarse por conducta inequívoca del Titular, excepto para datos sensibles o de menores de edad.

### Casos en los que NO es necesaria la autorización:

- Información requerida por entidad pública o administrativa en ejercicio de sus funciones legales, o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil.

URRÁ conservará la documentación que acredite la autorización obtenida, conforme al literal b) del artículo 17 de la Ley 1581 de 2012. Esta obligación es de especial relevancia frente a las sanciones de la SIC, que ha impuesto multas por la ausencia de mecanismos verificables de autorización.

## 9. AVISO DE PRIVACIDAD

Conforme al Decreto 1074 de 2015, Capítulo 25, URRÁ emite Avisos de Privacidad diferenciados según el grupo de Titulares, en el momento de la recolección de datos. El Aviso de Privacidad informa al Titular sobre:

- La identidad, domicilio y datos de contacto del Responsable.
- El tipo de datos que se recolectan.
- Las finalidades del tratamiento.
- Los derechos que le asisten como Titular.
- Los mecanismos para conocer la Política de Tratamiento de Datos Personales.
- El carácter facultativo u obligatorio de suministrar datos sensibles.

Cuando la recolección se realice en formularios físicos o digitales, el Aviso de Privacidad estará disponible de manera visible y accesible para el Titular. La Política de Tratamiento de Datos Personales vigente está siempre disponible en [www.urra.com.co](http://www.urra.com.co) y a través de nuestros canales de atención.

## 10. FINALIDADES DEL TRATAMIENTO

El uso de los datos personales dependerá del tipo de Titular y su relación con URRÁ:

### 10.1 Titulares Empleados, Colaboradores y/o Candidatos

EMPRESA URRÁ S.A. E.S.P. | NIT 800.175.746-9 **Versión 04 | Marzo 2026**

El Tratamiento de estos datos tiene como finalidad cumplir a cabalidad los procesos de selección y/o vinculación laboral lo cual implica, según sea el caso, verificación de identidad, actualización de datos de contacto y ubicación, solicitud de autorización de tratamiento de datos personales, análisis de hoja de vida, verificación de referencias, verificación de información, procesos de selección, exámenes de conocimientos (cuando aplique), control de acceso y control de acceso biométrico (si aplica), seguridad, registro en plataformas tecnológicas, comunicación, encuestas, entrenamiento, seguimiento a funciones, actividades y responsabilidades laborales, análisis del desempeño laboral, pagos de nómina, cumplimiento de requisitos relacionados con el Sistema General de Seguridad Social, vinculación a cuentas de nómina y demás obligaciones que surjan del contrato laboral, así como la gestión del expediente laboral.

Además se cubren las actividades necesarias para el cumplimiento de la normatividad vigente de Seguridad y Salud en el Trabajo (SST); atención y prevención en salud. Servicios de alimentación y transporte (cuando aplique), actividades de bienestar, actividades lúdicas o deportivas, programación de viajes, auxilios y seguros.

También usaremos los datos para la coordinación y cubrimiento audiovisual cuando haya participación del talento humano en representación la EMPRESA en actividades locales o internacionales. Para comunicación, publicaciones y producciones audiovisuales y para informes oficiales a entidades públicas para el cumplimiento normativo.

El Responsable usará los datos de los hijos de los EMPLEADOS para hacer las afiliaciones que exige la ley a servicios de salud, caja de compensación familiar, entre otros. También podría usarlos para invitaciones y cubrimiento audiovisual a actividades de entretenimiento, lúdicas, artísticas, deportivas, entre otras que desarrolle en pro del bienestar de su equipo humano.

Las FINALIDADES del tratamiento de datos de EX EMPLEADOS serán las requeridas para garantizar el suministro de información que la normatividad laboral exija para atender certificaciones laborales, reclamos laborales o derecho a la pensión.

También conservaremos datos con fines históricos, por buenas prácticas empresariales o por otras normas legales.

### 10.2 Titulares Contratistas y Proveedores

Verificación de identidad, actualización de datos, comunicación para procesos de selección y gestión comercial, coordinación de pedidos y proyectos, verificación de referencias, control de acceso y videovigilancia (si aplica), pagos, gestión de garantías, cumplimiento tributario, solicitud de autorización de tratamiento, reporte en el RNBD como Encargados (cuando aplique) y demás obligaciones legales y contractuales.

### 10.3 Titulares Clientes

Verificación de identidad, solicitud de autorización de tratamiento de datos, actualización de datos personales, mercadeo y comunicación, servicio al cliente, cotizaciones, gestión comercial, firma y cumplimiento de contratos, facturación, cobro de cartera, cumplimiento tributario, control de acceso biométrico si aplica, seguridad y videovigilancia (si aplica). La empresa podrá categorizar clientes como potenciales, activos e inactivos con finalidades apropiadas para cada grupo.

### 10.4 Titulares Comunidades

URRÁ apoya el bienestar de las comunidades de la región. Las finalidades comprenden divulgación, organización de actividades deportivas, lúdicas y de capacitación, gestión social y ambiental, y comunicación institucional con comunidades del área de influencia.

### 10.5 Otros Titulares

Las finalidades corresponden a la naturaleza de la relación EMPRESA-TITULAR: cumplimiento de obligaciones entre las partes, seguridad, videovigilancia y comunicaciones. Se recolectarán únicamente los datos necesarios para cada finalidad declarada (principio de minimización de datos).

## 11. TEMPORALIDAD: DURACIÓN DEL TRATAMIENTO DE DATOS

Los datos personales se conservarán por el tiempo necesario según las finalidades del tratamiento y conforme a:

- Normatividad laboral vigente (expedientes laborales: mínimo 20 años tras la terminación del contrato, para efectos pensionales).
- Obligaciones contractuales, contables y fiscales (mínimo 10 años según Código de Comercio).
- Procesos jurídicos en curso.
- Normas de calidad y buenas prácticas empresariales.
- Finalidades históricas, estadísticas o científicas, con anonimización de datos.
- Gestión Documental: según lo establecido en las tablas de retención documental.

Cumplida la finalidad del tratamiento, URRÁ procederá a la supresión o anonimización de los datos personales, salvo obligación legal de conservación. Los plazos de conservación por categoría de base de datos están documentados en el Inventario de Bases de Datos de URRÁ.

## 12. ENCARGADOS DEL TRATAMIENTO

El Encargado es la persona natural o jurídica que realiza el tratamiento de datos por cuenta de URRÁ como Responsable. URRÁ podrá compartir datos personales con Encargados para la correcta operación empresarial, siempre que exista un contrato de transmisión de datos que establezca:

- El alcance y las finalidades del tratamiento encomendado.
- Las obligaciones del Encargado frente al Titular y al Responsable.
- Las medidas de seguridad exigibles.
- La prohibición de usar los datos para fines distintos a los autorizados.
- La obligación de suprimir o devolver los datos al término del encargo.

URRÁ exigirá a los Encargados demostración de su cumplimiento de la Ley 1581 de 2012 (Responsabilidad Demostrada) y realizará verificaciones periódicas. En caso de que URRÁ actúe como Encargado de otro Responsable, aplicará las mismas obligaciones establecidas en el Título VI de la Ley 1581 de 2012.

## 13. TRANSMISIÓN Y TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

URRÁ podrá transmitir o transferir datos a terceros (proveedores, contratistas, socios) para el cumplimiento de su misión o por exigencia legal. En todos los casos solicitará el cumplimiento de los principios de protección de datos y de esta Política.

**Conforme al Artículo 26 de la Ley 1581 de 2012, se PROHÍBE la transferencia a países que no proporcionen niveles adecuados de protección, salvo:**

- Autorización expresa e inequívoca del Titular.
- Intercambio de datos médicos por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles conforme a la legislación aplicable.
- Transferencias en el marco de tratados internacionales en que Colombia sea parte.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable, con autorización del Titular.
- Transferencias legalmente exigidas para salvaguardar el interés público o para el reconocimiento, ejercicio o defensa de un derecho en proceso judicial.

En casos no exceptuados, URRÁ gestionará la Declaratoria de Conformidad de la SIC antes de realizar la transferencia internacional.

Las transmisiones internacionales entre Responsable y Encargado no requieren informar al Titular si existe contrato de transmisión conforme al Decreto 1074 de 2015.

Estas disposiciones serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008 referente a Habeas Data financiero.

## 14. REPORTE DE INCIDENTES DE SEGURIDAD

URRÁ ha establecido un protocolo de gestión de incidentes de seguridad de datos personales que incluye:

- Identificación y contención inmediata del incidente.
- Evaluación del impacto sobre los derechos de los Titulares.
- Notificación a la SIC cuando se presenten violaciones a los códigos de seguridad o riesgos graves en la administración de la información (Ley 1581 de 2012, Art. 17, lit. n y Art. 18, lit. k).
- Notificación a los Titulares afectados cuando el incidente pueda afectar gravemente sus derechos o generar perjuicios significativos.
- Registro del incidente en el RNBD como novedad, conforme a la Circular Externa 001 de 2016 de la SIC.
- Implementación de medidas correctivas y preventivas.

El incumplimiento de la obligación de reporte de incidentes es una de las causales de sanción identificadas reiteradamente por la SIC en sus resoluciones de los últimos años. Urrá cumple su Política de Seguridad de Información.

## 15. CANALES DE ATENCIÓN DE CONSULTAS Y RECLAMOS

**Responsable de Atención:** Oficial de Protección de Datos Personales (OPD) – URRÁ S.A. E.S.P.

**Correo Electrónico:** protecciondedatos@urra.com.co

**Teléfono:** 604 784 8991 Ext. 533 y 542

**Dirección:** Cra 2 # 48-08 Esq., Montería, Córdoba

**Horario de Atención:** Lunes a viernes: 7:30 a.m. – 12:00 m. y 2:00 p.m. – 5:00 p.m.

**IMPORTANTE:** Las redes sociales **NO SON UN CANAL HABILITADO** para radicar consultas y reclamos de Protección de Datos Personales.

**La solicitud debe contener como mínimo:**

- Nombres y apellidos del Titular y/o su representante legal o causahabiente.
- Descripción clara y completa de la consulta o reclamo.
- Documentos de soporte adjuntos.
- Datos de identificación y contacto: nombre, número de documento, correo electrónico, dirección y teléfono.
- Relación del Titular con URRÁ (ej.: ex empleado, cliente, contratista).
- Firma del documento (o equivalente electrónico para solicitudes digitales).
- Copia del documento de identidad del titular del dato y de su apoderado, representante legal o causahabiente.

## 16. PROCEDIMIENTO Y PLAZOS PARA ATENDER LOS DERECHOS DE LOS TITULARES

Las consultas y reclamos serán recibidas y atendidas conforme lo establece la Ley. En su trámite y respuesta intervendrán la persona cargo dentro de la organización, Oficiales de Datos Personales en outsourcing u otros asesores cuando la Empresa lo considere necesario y el Comité de PDP.

El procedimiento propio del proceso está disponible en el Manual interno respectivo.

### 16.1 Consultas

Las consultas serán atendidas en un término máximo de diez (10) días hábiles desde la fecha de recepción. Si no es posible responder en ese plazo, URRÁ informará al interesado los motivos antes del vencimiento y solicitará hasta cinco (5) días hábiles adicionales.

### 16.2 Reclamos

El término máximo para atender el reclamo es de quince (15) días hábiles desde el día siguiente al recibo. Si no es posible responder en ese plazo, se informarán los motivos y se indicará nueva fecha, que no podrá superar ocho (8) días hábiles adicionales.

Dentro de los dos (2) días hábiles siguientes al recibo del reclamo, URRÁ anotará en la base de datos la leyenda "Reclamo en Trámite" con el motivo, hasta que el proceso concluya.

### 16.3 Requisito de Procedibilidad

Conforme al Artículo 16 de la Ley 1581 de 2012, el Titular o causahabiente solo podrá elevar queja ante la SIC una vez haya agotado el trámite de consulta o reclamo ante URRÁ. El incumplimiento de los plazos de respuesta es una de las infracciones sancionadas de manera reiterada por la SIC.

## 17. REGISTRO NACIONAL DE BASES DE DATOS (RNBD)

En cumplimiento del artículo 25 de la Ley 1581 de 2012 y el Capítulo 26 del Decreto 1074 de 2015, URRÁ inscribe en el RNBD las bases de datos sobre las que es Responsable del Tratamiento, incluyendo:

- Identificación y descripción de cada base de datos.

EMPRESA URRÁ S.A. E.S.P. | NIT 800.175.746-9 **Versión 04 | Marzo 2026**

- Finalidades del tratamiento.
- Política de Tratamiento de Datos Personales vigente.
- Identificación de Encargados del Tratamiento cuando aplique.
- Información sobre transferencias o transmisiones nacionales e internacionales.
- Reporte de novedades: reclamos presentados por Titulares e incidentes de seguridad.

URRÁ actualiza el RNBD de manera oportuna ante cualquier novedad relevante. La omisión de registro o la desactualización del RNBD constituyen infracciones sancionables por la SIC.

## 18. RESPONSABILIDAD DEMOSTRADA (ACCOUNTABILITY)

Conforme al Decreto 1074 de 2015 (Arts. 2.2.2.25.6.1 y 2.2.2.25.6.2, compilatorio del Decreto 1377 de 2013), URRÁ debe estar en capacidad de demostrar a la SIC que ha implementado medidas apropiadas y efectivas para el cumplimiento de la Ley 1581 de 2012. Dichas medidas incluyen:

- Estructura administrativa con un Oficial de Protección de Datos (OPD) con respaldo de la Alta Dirección.
- Programa integral de capacitación y concientización para el talento humano.
- Mecanismos internos para la atención de consultas y reclamos.
- Inventario y clasificación de bases de datos con datos personales.
- Evaluaciones periódicas de riesgo sobre el tratamiento de datos.
- Procedimientos de gestión de incidentes de seguridad.
- Contratos de transmisión con Encargados.
- Auditorías internas de cumplimiento de protección de datos.
- Conservación de evidencias de autorizaciones obtenidas de los Titulares.

La Responsabilidad Demostrada implica no solo el cumplimiento formal de la ley, sino la capacidad de probarlo. La ausencia de documentación y evidencias es un factor agravante en los procesos sancionatorios de la SIC.

## 19. DEBERES DEL RESPONSABLE Y DE LOS ENCARGADOS DEL TRATAMIENTO

### 19.1 Deberes del Responsable (Ley 1581 de 2012, Art. 17)

URRÁ, como Responsable, debe:

- Garantizar al Titular el pleno ejercicio del derecho de Habeas Data.
- Solicitar y conservar copia de la autorización otorgada por el Titular.
- Informar debidamente al Titular sobre la finalidad y los derechos que le asisten.
- Conservar la información bajo condiciones de seguridad que impidan su adulteración, pérdida o acceso no autorizado.
- Garantizar que la información suministrada al Encargado sea veraz, completa, exacta y actualizada.
- Actualizar la información y comunicar oportunamente las novedades al Encargado.
- Rectificar la información cuando sea incorrecta y comunicarlo al Encargado.
- Suministrar al Encargado únicamente datos cuyo tratamiento esté previamente autorizado.
- Exigir al Encargado en todo momento el respeto a las condiciones de seguridad y privacidad.
- Tramitar consultas y reclamos en los términos legales.
- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley.

EMPRESA URRÁ S.A. E.S.P. | NIT 800.175.746-9 Versión 04 | Marzo 2026

- Informar al Encargado cuando determinada información esté en discusión por parte del Titular.
- Informar a la SIC sobre violaciones a los códigos de seguridad y riesgos en la administración de datos.
- Cumplir las instrucciones y requerimientos de la SIC.

### 19.2 Deberes de los Encargados (Ley 1581 de 2012, Art. 18)

Los Encargados contratados por URRÁ deben:

- Garantizar al Titular el pleno ejercicio del derecho de Habeas Data.
- Conservar la información bajo condiciones de seguridad adecuadas.
- Actualizar, rectificar o suprimir datos en los términos de la ley.
- Actualizar la información reportada por URRÁ dentro de los cinco (5) días hábiles siguientes a su recibo.
- Tramitar consultas y reclamos de los Titulares en los términos legales.
- Adoptar manual interno de políticas y procedimientos para el cumplimiento de la ley.
- Registrar la leyenda "Reclamo en Trámite" en la base de datos.
- Insertar "Información en Discusión Judicial" cuando sea notificado por autoridad competente.
- Abstenerse de circular información controvertida por el Titular cuyo bloqueo haya sido ordenado por la SIC.
- Permitir el acceso a la información únicamente a personas autorizadas.
- Informar a la SIC sobre violaciones a los códigos de seguridad.
- Cumplir las instrucciones y requerimientos de la SIC.

## 20. CAPACITACIÓN DEL TALENTO HUMANO

URRÁ realizará sesiones de capacitación y concientización en Protección de Datos Personales con las siguientes características:

- Frecuencia mínima: una vez al año para todo el personal.
- Capacitación obligatoria para todo nuevo empleado durante el proceso de inducción.
- Capacitación específica para las áreas que traten datos sensibles o volúmenes significativos de datos personales, áreas estrategias con datos personales relevantes para la operación.
- Registro de asistentes a cada sesión de capacitación.
- Evaluación de conocimientos al menos una vez al año.
- Inclusión en el plan de capacitación de cambios normativos y lecciones aprendidas de incidentes.

La capacitación es un elemento clave de la Responsabilidad Demostrada. La ausencia de programas de entrenamiento verificables ha sido identificada por la SIC como factor agravante en procesos sancionatorios.

## 21. SEGURIDAD DE LA INFORMACIÓN

URRÁ implementa su Política de Seguridad de la Información con medidas técnicas, administrativas y humanas para proteger los datos personales, que incluyen:

- Cifrado de información en tránsito y en reposo para datos sensibles.
- Control de acceso a sistemas de información basado en roles y responsabilidades.
- Autenticación mediante contraseñas seguras y, cuando aplique, doble factor de autenticación.
- Copias de respaldo periódicas y verificadas.
- Prácticas seguras de desarrollo e implementación de software.
- Gestión de vulnerabilidades y actualizaciones de seguridad.



EMPRESA URRÁ S.A. E.S.P. | NIT 800.175.746-9 **Versión 04 | Marzo 2026**

- Acuerdos de confidencialidad con empleados, colaboradores y terceros que accedan a datos personales.
- Procedimientos de destrucción segura de datos y medios de almacenamiento al final de su ciclo de vida.

Las medidas de seguridad son objeto de revisión y fortalecimiento continuo. URRÁ documenta las medidas implementadas como parte de su Responsabilidad Demostrada frente a la SIC.

## 22. ENTREGA DE DATOS A AUTORIDADES

Cuando una autoridad pública o administrativa, en ejercicio de sus funciones legales o con orden judicial, solicite datos personales de Titulares, URRÁ los entregará conforme al Artículo 10° de la Ley 1581 de 2012. Previo a la entrega, URRÁ:

- Verificará que la solicitud sea auténtica, esté dentro de las competencias del solicitante y corresponda a las finalidades indicadas.
- Levantará un acta de entrega donde consten los detalles de la solicitud, los datos entregados y el compromiso de la entidad receptora con la protección de los mismos.
- Conservará copia del acta y la solicitud en los archivos de gestión de URRÁ.

## 23. VIGENCIA Y ACTUALIZACIÓN DE LA POLÍTICA

Esta versión de la Política está vigente desde marzo de 2026 y reemplaza la versión anterior (V03 de marzo de 2024). Cuando se produzcan cambios sustanciales en la Política, URRÁ informará a los Titulares a través de sus canales de comunicación y actualizará la versión publicada en [www.urra.com.co](http://www.urra.com.co).

Se consideran cambios sustanciales: modificaciones en las finalidades del tratamiento, en los datos tratados, en los Encargados, en los períodos de conservación o en los derechos de los Titulares. Cambios no sustanciales (datos de contacto, correcciones de estilo) podrán realizarse sin notificación previa a los Titulares.

URRÁ revisará y actualizará esta Política al menos una vez al año o cuando existan cambios normativos relevantes, con el apoyo del Oficial de Protección de Datos Personales.

## 24. RESUMEN DE CAMBIOS RESPECTO A LA VERSIÓN ANTERIOR

SECCIÓN	CAMBIO INCORPORADO (V04 vs V03)
<b>Sección 3: Marco Legal</b>	Se incorpora el Decreto 255 de 2022 sobre Normas Corporativas Vinculantes.
<b>Sección 4. Definiciones</b>	Se incorporan: Aviso de Privacidad, Incidente de Seguridad, Oficial PDP, entre otros conceptos.
<b>Sección 8. Autorización</b>	Se refuerza la obligación de conservar evidencia de la autorización como medida de mitigación de riesgo frente a sanciones SIC.
<b>Sección 9. Aviso de Privacidad</b>	Sección nueva. Se formaliza el Aviso de Privacidad como documento independiente a la Política, conforme al Decreto 1074 de 2015.

EMPRESA URRÁ S.A. E.S.P. | NIT 800.175.746-9 **Versión 04 | Marzo 2026**

<b>Sección 14. Incidentes de Seguridad</b>	Sección nueva. Se incluye protocolo de reporte de incidentes a la SIC y a los Titulares, conforme a obligaciones de los Arts. 17 y 18 de la Ley 1581 de 2012.
<b>Sección 18. Responsabilidad Demostrada</b>	Sección nueva. Se desarrolla el principio de Accountability (Decreto 1074 de 2015, Arts. 2.2.2.25.6.1 y 2.2.2.25.6.2).
<b>Sección 11. Temporalidad</b>	Ampliada con plazos concretos por tipo de dato (laboral, contable, jurídico).
<b>Sección 12. Encargados</b>	Se incluyen los elementos mínimos del contrato de transmisión de datos.
<b>Sección 13. Transferencia Internacional</b>	Se aclara el régimen de transmisiones internacionales sin necesidad de informar al Titular (con contrato).
<b>Sección 17. RNBD</b>	Se detallan los elementos a inscribir, incluyendo novedades y reporte de incidentes.

*Documento actualizado por Eliana Salgado de Data & Business Risk SAS para la Empresa Urrá SA, con base en la Ley 1581 de 2012, el Decreto 1074 de 2015 (Cap. 25 y 26), la Guía OPD SuperIndustria 2023 y jurisprudencia sancionatoria de la SIC 2022-2026.*

Esta Política de Tratamiento de datos ha sido estructurada y/o actualizada por Data & Business Risk SAS para EMPRESA URRÁ S.A. ESP y no debe ser usada por otras entidades sin autorización expresa de Data & Business Risk.