

**Política de Tratamiento y Protección de Datos Personales de Pedro Baracutao
García**
(con base en la Ley 1581 de 2012)

Tabla de contenido

<i>1. Introducción y Contexto</i>	<i>1</i>
1.1 Justificación política y legal	1
1.2 Marco jurídico aplicable	2
1.3 Compromiso con la protección de datos personales	2
<i>2. Identificación del Responsable del Tratamiento</i>	<i>3</i>
2.1 Datos del Responsable	3
2.2 Encargados del Tratamiento	3
2.3 Autoridad de Control	4
2.4 Principio de responsabilidad demostrada en la identificación	5
<i>3. Objeto y Alcance de la Política</i>	<i>5</i>
3.1 Objeto	5
3.2 Alcance material	5
3.3 Alcance territorial	6
3.4 Exclusiones legales	6
3.5 Principio de integralidad en el alcance	7
<i>4. Definiciones</i>	<i>7</i>
4.1 Definiciones legales aplicables (Ley 1581/2012 y reglamentación)	7
4.2 Definiciones adaptadas al contexto político, comunitario y electoral	8
4.3 Glosario técnico complementario	9
<i>5. Principios Rectores del Tratamiento de Datos Personales</i>	<i>9</i>

5.1 Principio de legalidad	9
5.2 Principio de finalidad	9
5.3 Principio de libertad	10
5.4 Principio de veracidad o calidad	10
5.5 Principio de transparencia	10
5.6 Principio de acceso y circulación restringida	10
5.7 Principio de seguridad	10
5.8 Principio de confidencialidad	10
5.9 Principio de responsabilidad demostrada (Accountability)	11
6. Categorías especiales de datos	11
6.1 Datos sensibles (incluida la orientación y opinión política)	11
6.2 Datos personales de niños, niñas y adolescentes (NNA)	12
6.3 Procedimientos y controles reforzados	13
6.4 Prohibiciones y restricciones específicas	13
6.5 Derechos reforzados y canales preferentes	13
7. Finalidades del Tratamiento	13
7.1 Finalidades políticas y comunitarias	14
7.2 Finalidades administrativas y legales	14
7.3 Finalidades de comunicación y marketing político	14
7.4 Finalidades estadísticas e investigativas	14
8. Autorización del Titular	15
8.1 Modalidades de obtención	15
8.2 Prueba y conservación de la autorización	15
8.3 Revocatoria y supresión de datos	16
9. Derechos de los Titulares	16
9.1 Conocer, actualizar y rectificar	16
9.2 Ser informado	16

9.3 Revocar y/o suprimir	16
9.4 Acceso gratuito	17
10. Deberes del Responsable y Encargados	17
10.1 Deberes generales del Responsable	17
10.2 Deberes de los Encargados	17
10.3 Contratos de encargo	18
11. Procedimientos para el Ejercicio de Derechos	18
11.1 Procedimiento de consultas	18
11.2 Procedimiento de reclamos	18
11.3 Tiempos de respuesta	19
12. Medidas de Seguridad	19
12.1 Seguridad física	19
12.2 Seguridad lógica y digital	19
12.3 Controles de acceso	20
12.4 Plan de respuesta a incidentes	20
13. Transferencia y Transmisión de Datos	20
13.1 Nacionales	20
13.2 Internacionales	21
13.3 Condiciones y cláusulas contractuales	21
14. Registro Nacional de Bases de Datos (RNBD)	21
14.1 Obligación y condiciones de registro	21
14.2 Reportes y actualizaciones	22
15. Cookies y Tecnologías de Seguimiento	22
15.1 Uso en sitios web y redes sociales	22
15.2 Finalidad y control	22
16. Videovigilancia y Registro de Eventos	23

16.1 Uso de cámaras y registro audiovisual	23
16.2 Avisos y finalidades	23
17. Vigencia de la Política	24
17.1 Fecha de entrada en vigor	24
17.2 Cambios y actualizaciones	24
18. Anexos	24
18.1 Formato de autorización	24
18.2 Aviso de privacidad	25
18.3 Procedimientos internos	25

1. Introducción y Contexto

1.1 Justificación política y legal

El tratamiento de datos personales en el marco de la actividad política y electoral, incluyendo la recolección, almacenamiento, uso, circulación y supresión de información de simpatizantes, líderes comunitarios, electores potenciales, organizaciones sociales y otros actores de interés, se encuentra regulado por un conjunto de normas de orden constitucional, legal y reglamentario que reconocen el derecho fundamental al hábeas data y establecen obligaciones estrictas para su garantía.

En Colombia, el artículo 15 de la Constitución Política reconoce el derecho de todas las personas a conocer, actualizar y rectificar la información que sobre ellas se haya recogido en bases de datos o archivos, así como el derecho a la intimidad y a exigir el respeto de la misma. Dicho precepto constitucional encuentra desarrollo en la Ley Estatutaria 1581 de 2012, que establece las disposiciones generales para la protección de datos personales, y en el Decreto 1377 de 2013 (hoy compilado en el Decreto Único 1074 de 2015), que reglamenta parcialmente su aplicación.

El uso de datos personales con fines de proselitismo político, marketing electoral, segmentación de mensajes, invitaciones a eventos y coordinación de actividades partidistas constituye una actividad reglada sujeta a estrictos principios, obligaciones y responsabilidades, como lo ha precisado la Superintendencia de Industria y Comercio (SIC) en múltiples pronunciamientos y circulares, en especial la Circular Externa 001 de 2018 y la Circular Externa 001 de 2022, que fijan lineamientos específicos para el tratamiento de datos en campañas políticas, referendos, consultas populares y demás mecanismos de participación ciudadana.

Por su parte, la jurisprudencia constitucional ha sostenido que el hábeas data no se limita a la protección frente a abusos comerciales, sino que también se extiende a ámbitos como el electoral y el político, donde el riesgo de uso indebido de la información personal puede afectar derechos fundamentales como la intimidad, la libertad de expresión, la libertad de conciencia y la libertad política. La Sentencia C-748 de 2011, en el control previo de constitucionalidad de la Ley 1581 de 2012, precisó que el tratamiento de datos personales es legítimo únicamente si respeta los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

En este contexto, Pedro Baracutao García, en su calidad de líder político, representante electo y aspirante a nuevos cargos de elección popular, reconoce la obligación de adoptar una Política de Tratamiento y Protección de Datos Personales como instrumento normativo interno y de cara a la ciudadanía, garantizando así el ejercicio pleno de los derechos de los titulares y la conformidad con la regulación aplicable.

1.2 Marco jurídico aplicable

La presente política se fundamenta en las siguientes normas y criterios:

- Constitución Política de Colombia

- Artículo 15: derecho a la intimidad, al buen nombre y al hábeas data.
 - Artículo 20: derecho a recibir información veraz e imparcial.
 - Artículo 40: derechos políticos y participación ciudadana.
- Leyes estatutarias y ordinarias
 - Ley 1581 de 2012: disposiciones generales para la protección de datos personales.
 - Ley 1266 de 2008: régimen de protección de datos financieros, crediticios, comerciales y de servicios.
 - Ley 1712 de 2014: ley de transparencia y del derecho de acceso a la información pública nacional.
 - Ley 1755 de 2015: derecho de petición.
 - Ley 996 de 2005: régimen de garantías electorales.
 - Ley 1475 de 2011: organización y funcionamiento de los partidos y movimientos políticos.
- Decretos reglamentarios
 - Decreto 1377 de 2013 y Decreto Único Reglamentario 1074 de 2015 (Título 2, Capítulo 25): reglamentación parcial de la Ley 1581 de 2012.
- Circulares de la Superintendencia de Industria y Comercio (SIC)
 - Circular Externa 001 de 2018: tratamiento de datos en campañas políticas.
 - Circular Externa 001 de 2022: directrices para el tratamiento de datos con fines políticos y electorales.
 - Circular Única de la SIC: procedimientos para el registro, reporte y atención de quejas.
- Jurisprudencia relevante
 - Corte Constitucional, Sentencia C-748 de 2011: principios rectores del tratamiento de datos.
 - Corte Constitucional, Sentencia T-729 de 2002: autodeterminación informativa como expresión del derecho a la intimidad.

- Corte Constitucional, Sentencia SU-082 de 1995 y SU-056 de 2023: alcance del hábeas data y control judicial de su ejercicio.
- Consejo de Estado, Sección Quinta, múltiples sentencias sobre uso indebido de bases de datos en campañas políticas.

1.3 Compromiso con la protección de datos personales

Pedro Baracutao García, en su rol de actor político y representante ciudadano, asume el compromiso de:

- Cumplir estrictamente las disposiciones legales, reglamentarias y jurisprudenciales sobre protección de datos personales.
- Garantizar que todo tratamiento de datos personales esté precedido de autorización previa, expresa e informada del titular, salvo las excepciones previstas en la ley.
- Aplicar medidas técnicas, jurídicas y organizativas para prevenir el acceso no autorizado, la pérdida, alteración o uso indebido de la información.
- Implementar el principio de **responsabilidad demostrada** (*accountability*), manteniendo evidencias documentales del cumplimiento normativo.
- Respetar, en el tratamiento de datos con fines políticos, la dignidad humana, la no discriminación y el pluralismo político, asegurando que la información no sea utilizada para manipulación ilícita, persecución o exclusión.

2. Identificación del Responsable del Tratamiento

2.1 Datos del Responsable

En cumplimiento del artículo 17 de la Ley 1581 de 2012 y el artículo 2.2.2.25.3.1 del Decreto 1074 de 2015, se informa que el Responsable del Tratamiento de Datos Personales es:

- Nombre completo: Pedro Baracutao García Ospina
- Calidad: Representante a la Cámara – Circunscripción Territorial de Antioquia (Período 2022–2026) y líder político en ejercicio.
- Documento de identidad: 71054740

- Dirección sede legislativa: Carrera 7 # 8-62, Oficina 341B, Edificio Nuevo del Congreso, Bogotá D.C.
- Teléfonos de contacto: (+57) 301 566 9175 – (incluir línea fija si aplica).
- Correo electrónico oficial de contacto en materia de datos personales: pedro.garcia@camara.gov.co
- Página web oficial: www.pedrobaracutao.com
- Canales adicionales habilitados: formulario de contacto web, redes sociales oficiales (Facebook, Instagram, X/Twitter, YouTube).

El Responsable, en su calidad de persona natural que actúa en ejercicio de actividades políticas y de representación ciudadana, adopta la presente política como instrumento vinculante para todo el personal de campaña, colaboradores, contratistas, voluntarios y terceros que participen en actividades que involucren el tratamiento de datos personales bajo su dirección.

2.2 Encargados del Tratamiento

Para el cumplimiento de los fines descritos en esta política, el Responsable podrá delegar el tratamiento de datos personales a Encargados del Tratamiento, que pueden ser personas naturales o jurídicas, públicas o privadas, quienes actuarán siguiendo instrucciones documentadas y bajo contratos o acuerdos de confidencialidad y seguridad de la información.

Se consideran Encargados de forma enunciativa, no limitativa:

- Empresas proveedoras de servicios de call center o contact center para llamadas y envío de mensajes de texto.
- Plataformas tecnológicas de envíos masivos de correo electrónico y SMS.
- Agencias o consultores de marketing político y comunicación digital.
- Proveedores de servicios de hosting, cloud computing y administración de bases de datos.

- Proveedores de servicios logísticos para eventos (registro de asistentes, acreditaciones, control de accesos).

Obligaciones de los Encargados (art. 18 Ley 1581/2012 y art. 2.2.2.25.4.2 Decreto 1074/2015):

1. Garantizar al titular el ejercicio de sus derechos.
2. Conservar prueba de la autorización otorgada.
3. Actualizar la información conforme a solicitudes legítimas del titular.
4. Adoptar medidas de seguridad para impedir adulteración, pérdida, consulta o uso no autorizado.
5. Tratar la información únicamente para las finalidades autorizadas.

2.3 Autoridad de Control

La autoridad competente para velar por el cumplimiento de las disposiciones sobre protección de datos personales en Colombia es la:

Superintendencia de Industria y Comercio – Delegatura para la Protección de Datos Personales

- Dirección: Carrera 13 No. 27-00, Pisos 1, 3, 4 y 10, Bogotá D.C., Colombia.
- Página web: www.sic.gov.co
- Teléfono conmutador: (+57)(1) 587 0000.
- Correo electrónico para protección de datos personales: habeasdata@sic.gov.co

Los titulares podrán presentar ante esta autoridad quejas por infracciones a la normativa, previo agotamiento del trámite de consulta o reclamo ante el Responsable o Encargado.

2.4 Principio de responsabilidad demostrada en la identificación

En aplicación del principio de accountability (Decreto 1377 de 2013 y criterios de la SIC), el Responsable mantendrá un registro documental y trazable que permita:

- Demostrar la cadena de responsabilidad sobre cada base de datos.
- Identificar de forma inequívoca a los Encargados que intervienen en el tratamiento.
- Incorporar cláusulas contractuales de protección de datos en todos los contratos de prestación de servicios, alianzas políticas y convenios.
- Documentar los canales y medios de contacto disponibles para los titulares.

3. Objeto y Alcance de la Política

3.1 Objeto

La presente Política de Tratamiento y Protección de Datos Personales tiene como propósito establecer los lineamientos, procedimientos y principios que regirán el tratamiento de datos personales realizado por Pedro Baracutao García, en su calidad de Responsable del Tratamiento, en el desarrollo de sus actividades políticas, legislativas, comunitarias, electorales, de comunicación y relacionamiento social.

En virtud de la Ley Estatutaria 1581 de 2012, el Decreto 1377 de 2013 (compilado en el Decreto Único 1074 de 2015), y las circulares de la Superintendencia de Industria y Comercio (SIC), esta política constituye un instrumento normativo interno y público que garantiza el respeto de los derechos fundamentales al hábeas data, intimidad, buen nombre, libertad política y libertad de expresión, tanto de ciudadanos simpatizantes como de cualquier persona natural cuyos datos personales sean tratados por el Responsable.

Esta política es obligatoria para todo el personal vinculado formal o informalmente al equipo político, incluidas las estructuras de voluntariado, comités de campaña, contratistas, proveedores y aliados estratégicos que accedan o traten datos por cuenta del Responsable.

3.2 Alcance material

La política aplica a todo tratamiento de datos personales efectuado en el marco de las siguientes actividades, enunciadas de manera no limitativa:

1. Actividades políticas y electorales
 - Organización y ejecución de campañas políticas.
 - Envío de información electoral, programas, propuestas y mensajes de interés público.
 - Convocatoria y registro de participación en eventos políticos, foros y audiencias.
 - Realización de encuestas, sondeos y segmentación de mensajes.
 - Gestión de listas de apoyo, redes de simpatizantes y contactos de líderes comunitarios.
2. Actividades legislativas y de representación ciudadana
 - Recepción y gestión de peticiones, quejas, reclamos y sugerencias de la ciudadanía.
 - Coordinación de agendas legislativas y comunitarias.
 - Comunicación institucional y política con sectores sociales.
3. Actividades comunitarias y de gestión social
 - Organización de reuniones, jornadas de trabajo comunitario, brigadas sociales y eventos cívicos.
 - Registro de asistencia y control de acceso.
 - Interacción con organizaciones sociales, ONGs, sindicatos y colectivos ciudadanos.
4. Actividades de comunicación y marketing político
 - Gestión de redes sociales y páginas web.
 - Envío de boletines electrónicos, mensajes de texto, llamadas telefónicas y mensajería instantánea.

- Producción y difusión de material audiovisual, fotográfico y escrito.

5. Actividades administrativas

- Contratación de personal, proveedores y prestadores de servicios.
- Gestión de relaciones con medios de comunicación y periodistas.
- Administración de bases de datos de contactos, clientes y proveedores.

3.3 Alcance territorial

Esta política se aplicará al tratamiento de datos personales realizado:

- Dentro del territorio colombiano, independientemente de que los datos sean almacenados en medios físicos o digitales.
- Fuera del territorio colombiano, cuando la información sea tratada por Encargados o subencargados contratados por el Responsable, incluyendo servicios de almacenamiento en la nube (cloud computing) y plataformas tecnológicas radicadas en el exterior, conforme a las reglas de transferencia internacional de datos previstas en la Ley 1581 de 2012 y el Decreto 1074 de 2015.

3.4 Exclusiones legales

De acuerdo con la Ley 1581 de 2012, esta política no se aplica a:

- Bases de datos o archivos mantenidos con fines exclusivamente personales o domésticos.
- Bases de datos que tengan como fin la seguridad y defensa nacional o la prevención, detección, monitoreo y control del lavado de activos y financiamiento del terrorismo.
- Bases de datos que contengan información periodística u otros contenidos protegidos por el derecho a la libertad de prensa.

- Bases de datos de naturaleza histórica, estadística o científica, cuando se apliquen medidas de disociación.

3.5 Principio de integralidad en el alcance

Esta política se interpreta de manera armónica con:

- Los estatutos, reglamentos internos y directrices de la campaña o estructura política del Responsable.
- Los lineamientos de protección de datos emitidos por la SIC.
- Las decisiones jurisprudenciales que delimiten el alcance de los derechos de los titulares y las obligaciones del Responsable.

4. Definiciones

4.1 Definiciones legales aplicables (Ley 1581/2012 y reglamentación)

A continuación, se adoptan –con redacción sustancialmente equivalente– las definiciones de uso obligatorio en Colombia para el tratamiento de datos personales:

- Titular: persona natural cuyos datos personales sean objeto de tratamiento.
- Tratamiento: cualquier operación u operaciones sobre datos personales (recolección, almacenamiento, uso, circulación o supresión).
- Responsable del tratamiento: persona natural o jurídica, pública o privada, que decide sobre la base de datos y/o el tratamiento de los datos.
- Encargado del tratamiento: persona natural o jurídica, pública o privada, que realiza tratamiento por cuenta del responsable.
- Base de datos: conjunto organizado de datos personales, en archivos físicos o electrónicos.
- Autorización: consentimiento previo, expreso e informado del titular para efectuar el tratamiento.
- Dato personal: información vinculada o asociable a una o varias personas naturales determinadas o determinables.

- Dato público: información que no es privada, semiprivada o sensible; incluye, entre otros, estado civil, profesión u oficio y calidad de comerciante o servidor público.
- Dato privado: información de naturaleza íntima o reservada, relevante solo para el titular.
- Dato semiprivado: información que no es íntima, reservada ni pública y cuyo conocimiento puede interesar a un sector o a la sociedad (p. ej., datos financieros o crediticios).
- Datos sensibles (categorías especiales): datos que afectan la intimidad o cuya utilización indebida puede generar discriminación; incluyen, entre otros, origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos u organizaciones sociales, datos relativos a la salud, vida sexual y datos biométricos.
- Datos personales de niños, niñas y adolescentes: su tratamiento solo procede si responde al interés superior y respeta sus derechos prevalentes (conforme a C-748/2011).
- Transferencia internacional de datos: envío de datos por un responsable o encargado ubicado en Colombia a un receptor que es responsable en otro país (o dentro del país).
- Transmisión de datos: comunicación de datos a un encargado para su tratamiento por cuenta del responsable, dentro o fuera de Colombia.

Notas complementarias de interpretación (alineadas con guías institucionales):

- Principios de legalidad, finalidad, libertad, veracidad/calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad guían toda la política.
- La confidencialidad obliga inclusive después de terminada la relación con actividades de tratamiento.

4.2 Definiciones adaptadas al contexto político, comunitario y electoral

Para efectos de esta Política —y sin contradecir la normatividad vigente— se adoptan las siguientes definiciones operativas, propias de la actividad política de Pedro Baracutao García:

- Prospección política: conjunto de actividades lícitas destinadas a identificar y contactar ciudadanos para informar, invitar a eventos, escuchar necesidades y promover participación política, con base en autorización válida del titular.
- Segmentación y perfilamiento político: organización de bases de datos en grupos (p. ej., territorio, temas de interés, disponibilidad para voluntariado) con fines de comunicación política transparente y acorde con las finalidades informadas; no incluye decisiones automatizadas con efectos jurídicos sin intervención humana.
- Contactabilidad: condición por la cual un registro cuenta con autorización vigente y medios válidos de contacto (teléfono, correo, mensajería), con trazabilidad de la prueba del consentimiento.
- Voluntariado político: conjunto de titulares que han manifestado su voluntad de colaborar en actividades de campaña o trabajo comunitario, previa autorización para tratamiento de sus datos.
- Base de datos electoral/comunitaria: base de datos que almacena datos personales de ciudadanos, líderes sociales o simpatizantes vinculados a actividades de participación, representación o campaña, con finalidades informadas (comunicación, invitaciones, logística, encuestas, rendición de cuentas), sometida a los principios y medidas de seguridad de esta Política.
- Incidente de seguridad de datos personales: evento que compromete la confidencialidad, integridad o disponibilidad de datos personales (pérdida, acceso o divulgación no autorizada), que activa el plan de respuesta e, incluso, los deberes de notificación cuando corresponda, conforme a lineamientos de la SIC.
- Pseudonimización / anonimización: técnicas de reducción de riesgo que sustituyen o suprimen identificadores directos para limitar la identificación del titular cuando se realicen análisis estadísticos o de impacto de políticas públicas; no alteran los derechos del titular cuando el dato sigue siendo personal.

Estas definiciones operativas se incorporan para asegurar claridad en los procesos internos de campaña y relacionamiento comunitario. Cuando exista tensión interpretativa, prevalecerá la definición legal citada en el numeral 4.1.

4.3 Glosario técnico complementario

- Confidencialidad: propiedad de seguridad que limita el acceso a la información a personas y condiciones autorizadas.
- Acceso y circulación restringida: solo el personal autorizado puede tratar la información; los datos personales (salvo los públicos) no estarán disponibles en Internet u otros medios masivos sin controles técnicos de acceso.
- Calidad del dato: la información debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- Información pública clasificada/reservada: categorías de acceso según régimen de transparencia y acceso a la información pública, relevantes para la gestión documental y respuesta a peticiones.
- Oficial/Área responsable de protección de datos (rol interno): instancia encargada de liderar, coordinar y evaluar el programa de protección de datos, inventariar bases, registrar en RNBD cuando aplique y revisar contratos de transmisión internacional. *(La denominación final del rol se precisará en el Título de Gobernanza de Datos de esta Política).*

5. Principios Rectores del Tratamiento de Datos Personales

El tratamiento de datos personales realizado por Pedro Baracutao García, en su calidad de Responsable, se sujetará estrictamente a los principios establecidos en la Ley 1581 de 2012, al Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015), así como a los desarrollos jurisprudenciales de la Corte Constitucional y a los lineamientos de la Superintendencia de Industria y Comercio (SIC). Estos principios son de obligatorio cumplimiento para todo el personal vinculado a las actividades políticas, comunitarias, legislativas y electorales del Responsable, así como para los Encargados del Tratamiento.

5.1 Principio de legalidad

El tratamiento de datos personales es una actividad reglada que debe ajustarse a lo dispuesto en la Constitución, la Ley 1581 de 2012, sus decretos reglamentarios, circulares y demás normas que regulen la materia. Ningún tratamiento podrá realizarse al margen de estas disposiciones.

5.2 Principio de finalidad

El tratamiento debe obedecer a una finalidad legítima, conforme a la Constitución y la ley, la cual debe ser informada al titular antes o al momento de la recolección de los datos. En el contexto político-electoral, las finalidades deberán ser claras y precisas, evitando expresiones ambiguas que permitan usos posteriores no autorizados, como lo ha señalado la Sentencia C-748 de 2011.

5.3 Principio de libertad

El tratamiento solo podrá realizarse con el consentimiento previo, expreso e informado del titular, salvo las excepciones legales. Ningún dato personal podrá ser obtenido o divulgado sin autorización o sin que medie mandato legal o judicial que releve de este requisito.

5.4 Principio de veracidad o calidad

La información objeto de tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Está prohibido el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error, especialmente en el caso de datos usados para segmentación de comunicaciones políticas.

5.5 Principio de transparencia

Se garantizará el derecho del titular a obtener, en cualquier momento y sin restricciones, información sobre la existencia y uso de sus datos, ya sea que el tratamiento lo realice directamente el Responsable o un Encargado.

5.6 Principio de acceso y circulación restringida

El tratamiento se sujeta a los límites derivados de la naturaleza de los datos, las disposiciones legales y la Constitución. Los datos personales no podrán estar disponibles en internet u otros medios de divulgación masiva sin control

técnico que limite el acceso únicamente a los titulares o a terceros autorizados por la ley.

5.7 Principio de seguridad

Se adoptarán medidas técnicas, humanas y administrativas necesarias para proteger los datos personales, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El nivel de seguridad deberá ser proporcional a la sensibilidad de la información, considerando especialmente el tratamiento de datos sensibles de opinión política.

5.8 Principio de confidencialidad

Todas las personas que intervengan en el tratamiento de datos personales, que no sean de carácter público, están obligadas a garantizar la reserva de la información, incluso después de finalizar su vínculo con el Responsable o el Encargado.

5.9 Principio de responsabilidad demostrada (Accountability)

El Responsable debe implementar medidas eficaces, apropiadas y verificables para cumplir con la normativa y poder demostrar dicho cumplimiento ante la autoridad de control. Esto implica mantener registros de tratamiento, pruebas de autorización, protocolos de seguridad, y realizar auditorías y capacitaciones periódicas.

6. Categorías especiales de datos

6.1 Datos sensibles (incluida la orientación y opinión política)

Definición y alcance. Son datos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación; incluyen, entre otros, el origen racial o étnico, la orientación u opinión política, convicciones religiosas o filosóficas, pertenencia a sindicatos u organizaciones sociales, datos relativos a la salud, vida sexual y datos biométricos.

Regla general. El tratamiento de datos sensibles está prohibido, salvo que concurra alguna de las excepciones legales y se cumplan salvaguardas reforzadas. Las excepciones admitidas por la Ley 1581/2012 (y desarrolladas en guías oficiales) son:

- a) Autorización explícita del titular;

- b) Salvaguarda del interés vital del titular cuando esté física o jurídicamente incapacitado (autorización por representantes);
- c) Tratamientos por fundaciones/ONG/organizaciones con finalidad política, filosófica, religiosa o sindical, respecto de sus miembros o contactos regulares, con debidas garantías y sin suministro a terceros sin autorización;
- d) Reconocimiento, ejercicio o defensa de derechos en proceso judicial;
- e) Finalidad histórica, estadística o científica, con supresión de identidad (anonimización efectiva).

Salvaguardas reforzadas obligatorias (campañas y actividad política):

1. Consentimiento expreso y específico para fines políticos (p. ej., recibir comunicaciones sobre agenda, propuestas, invitaciones, encuestas).
2. Carácter facultativo: ningún campo sensible será obligatorio para acceder a actividades o servicios; el titular siempre puede continuar sin aportarlo.
3. Minimización y proporcionalidad: recolectar solo lo estrictamente necesario para finalidades informadas.
4. Segmentación y perfilamiento político únicamente con base en finalidades y autorizaciones informadas; prohibido utilizar datos sensibles para discriminación o exclusión.
5. Registro y trazabilidad de la autorización (copias, metadatos, logs) y prueba de las finalidades comunicadas.
6. Seguridad reforzada: controles de acceso, cifrado en reposo y tránsito, acuerdos de confidencialidad, gestión de proveedores y de subencargados.
7. Evaluación de impacto (PIA/DPIA) cuando existan tratamientos de alto riesgo (p. ej., microsegmentación masiva, combinación de fuentes, transferencia internacional).
8. Transparencia y opción de oposición/supresión para cesar envíos o llamadas políticas, con canales expeditos.

Cláusula modelo de consentimiento para datos sensibles (uso político-comunicacional):

“Autorizo de manera expresa y específica a Pedro Baracutao García para tratar datos que puedan revelar mi opinión u orientación política con la finalidad de

enviarme información, invitaciones y encuestas relacionadas con su actividad política y comunitaria. He sido informado de que el suministro de datos sensibles es facultativo, que puedo revocar esta autorización en cualquier momento y que mis datos serán tratados bajo medidas reforzadas de seguridad.”

Nota: Aun tratándose de datos públicos, su tratamiento debe sujetarse a los principios de finalidad, necesidad, transparencia, seguridad y circulación restringida.

6.2 Datos personales de niños, niñas y adolescentes (NNA)

Regla especial. El tratamiento de datos personales de NNA está proscrito, salvo que (i) se trate de datos de naturaleza pública, y (ii) el tratamiento responda al interés superior y asegure el respeto de sus derechos fundamentales. La Corte Constitucional (C-748/2011) precisó que, independientemente de la naturaleza del dato, el tratamiento es posible si se garantiza interés superior y derechos prevalentes.

Autorización y participación del menor. Cumplidos los requisitos, la autorización la otorga el representante legal, previo ejercicio del derecho del menor a ser escuchado, valorando su madurez y autonomía.

Política interna estricta para la actividad política:

- Prohibido realizar prospección o marketing político dirigido a NNA, incluso cuando se obtenga consentimiento del representante, salvo actividades pedagógicas o institucionales de participación juvenil avaladas por sus responsables y con salvaguardas reforzadas.
- Si por razones logísticas (p. ej., eventos familiares) se recabaran datos de NNA no públicos, se aplicará anonimización o supresión inmediata cuando no sea indispensable.
- Se reforzarán medidas de seguridad, acotación de finalidades y revocatoria preferente.

6.3 Procedimientos y controles reforzados

1. Doble capa informativa: aviso breve (finalidad sensible, carácter facultativo, canales de derechos) + política íntegra disponible. (Modelo de la autoridad de control).

2. Registros: evidencia de autorizaciones, matriz de tratamientos, evaluaciones de riesgo, contratos de transmisión/transferencia, bitácoras de incidentes.
3. Gestión de incidentes: activación inmediata del plan de respuesta; evaluación de impacto; medidas de contención; notificación a titulares y, cuando corresponda, a autoridad de control. (Buenas prácticas recogidas en políticas modelo del sector público).
4. Encargados y subencargados: cláusulas de confidencialidad, instrucciones documentadas, no reutilización ni suministro a terceros, y controles para envío masivo (SMS, correo, llamadas).
5. Transferencias/transmisiones (incluido cloud): solo con garantías equivalentes y mismas finalidades informadas; en fines históricos/estadísticos/científicos, con supresión de identidad.
6. Segmentación responsable: se permite agrupar/segmentar ciudadanos para fines informados, recordando el carácter facultativo de los datos sensibles y evitando decisiones automatizadas con efectos desfavorables sin intervención humana.

6.4 Prohibiciones y restricciones específicas

- No condicionamiento de servicios, participación en eventos o recepción de información a la entrega de datos sensibles. (Carácter facultativo).
- No discriminación ni perfilamiento excluyente por razones ideológicas, religiosas, sindicales, de salud, orientación o identidad.
- No recolección masiva de datos sensibles desde fuentes abiertas sin finalidad legítima y proporcional claramente informada.
- No suministro de datos sensibles a terceros sin autorización del titular o sin base legal expresa.

6.5 Derechos reforzados y canales preferentes

Pedro Baracutao garantizará canales expeditos para:

- Revocar autorizaciones sobre datos sensibles y solicitar supresión inmediata;
- Limitar el uso para comunicaciones políticas;
- Acceso y portabilidad en formatos comprensibles;

- Atención prioritaria a reclamos relacionados con datos sensibles y NNA (términos legales de consulta/reclamo). (Estructura alineada con políticas oficiales).

7. Finalidades del Tratamiento

El tratamiento de datos personales realizado por **Pedro Baracutao García**, en calidad de Responsable, se ajustará a las finalidades legítimas e informadas al titular en el momento de la recolección, en los términos de los artículos 4 y 9 de la Ley 1581 de 2012 y sus normas reglamentarias.

7.1 Finalidades políticas y comunitarias

El tratamiento de datos personales con este propósito tendrá como objetivos:

- Gestionar bases de datos de ciudadanos, líderes sociales, organizaciones comunitarias y simpatizantes con el fin de promover la participación política, ciudadana y comunitaria.
- Convocar a eventos políticos, comunitarios y sociales, foros, cabildos, reuniones barriales y audiencias públicas.
- Realizar encuestas y consultas sobre asuntos de interés político y comunitario.
- Coordinar redes de voluntarios y activistas para actividades de trabajo social, comunitario o electoral.
- Facilitar procesos de rendición de cuentas y de comunicación directa con la ciudadanía.

7.2 Finalidades administrativas y legales

- Gestionar relaciones contractuales con proveedores, aliados y prestadores de servicios.
- Cumplir obligaciones legales, contables, tributarias y administrativas aplicables a la actividad política y organizacional.
- Administrar procesos de contratación de personal y voluntarios, así como la gestión de sus datos para fines internos.
- Atender peticiones, quejas, reclamos y sugerencias (PQRs) formuladas por titulares o por autoridades competentes.
- Dar respuesta a requerimientos judiciales, administrativos o de entes de control.

7.3 Finalidades de comunicación y marketing político

- Enviar mensajes informativos, boletines, noticias, invitaciones y material audiovisual relacionado con la agenda política, legislativa y comunitaria del Responsable.
- Gestionar campañas de comunicación a través de correo electrónico, SMS, llamadas telefónicas, mensajería instantánea y redes sociales.
- Implementar estrategias de segmentación para personalizar la comunicación, siempre que exista autorización previa y específica.
- Realizar sondeos de opinión y retroalimentación sobre la percepción ciudadana de la gestión política.

7.4 Finalidades estadísticas e investigativas

- Elaborar estudios internos, informes estadísticos y análisis de impacto social o político.
- Desarrollar investigaciones sobre comportamiento electoral, necesidades comunitarias y políticas públicas, utilizando datos anonimizados cuando sea posible.
- Mantener registros históricos para fines de archivo y memoria institucional, respetando las disposiciones legales sobre conservación y supresión de datos.

8. Autorización del Titular

En cumplimiento de los artículos 9, 12 y 13 de la Ley 1581 de 2012 y del Decreto 1074 de 2015, el tratamiento de datos personales por parte de **Pedro Baracutao García** se realizará únicamente cuando el titular haya otorgado una autorización previa, expresa e informada, salvo en los casos exceptuados por la ley.

8.1 Modalidades de obtención

La autorización podrá obtenerse por cualquiera de los siguientes medios, siempre que permita conservar prueba de su otorgamiento:

- **Escrita:** mediante formularios físicos, encuestas, planillas de registro en eventos o contratos.
- **Verbal grabada:** en llamadas telefónicas o entrevistas presenciales, dejando registro auditivo que incluya la finalidad y aceptación.

- **Electrónica:** a través de formularios web, correo electrónico, mensajes de texto, aplicaciones de mensajería o sistemas de registro digital, utilizando mecanismos de validación y trazabilidad.

En todos los casos, el Responsable informará al titular:

- a) El tratamiento al cual serán sometidos sus datos y la finalidad específica.
- b) El carácter facultativo de responder preguntas sobre datos sensibles o de menores de edad.
- c) Los derechos que le asisten como titular.
- d) La identificación y datos de contacto del Responsable.

8.2 Prueba y conservación de la autorización

Pedro Baracutao García conservará prueba documental, digital o audiovisual de la autorización otorgada por el titular, garantizando su integridad y disponibilidad para consulta posterior por parte del titular o de la autoridad competente.

Las evidencias se almacenarán mientras dure la relación con el titular y por el tiempo necesario para el cumplimiento de las obligaciones legales y contractuales derivadas del tratamiento, sin exceder los plazos de conservación establecidos en la ley.

8.3 Revocatoria y supresión de datos

El titular podrá revocar, en cualquier momento, la autorización otorgada y/o solicitar la supresión de sus datos personales, mediante los canales habilitados, salvo cuando exista un deber legal o contractual que impida su eliminación inmediata.

Cuando la revocatoria o supresión proceda:

- Se eliminarán los datos de las bases activas.
- Se dejará constancia del cumplimiento de la solicitud.
- Se informará al titular sobre el cierre del proceso.

9. Derechos de los Titulares

En cumplimiento de lo dispuesto en el artículo 8 de la Ley 1581 de 2012, el artículo 2.2.2.25.4.1 del Decreto 1074 de 2015 y demás normas concordantes, **Pedro Baracutao García**, como Responsable del Tratamiento, garantiza a los titulares de los datos personales los siguientes derechos:

9.1 Conocer, actualizar y rectificar

Los titulares tienen derecho a acceder a la información personal que repose en las bases de datos del Responsable y a actualizarla o rectificarla cuando sea incorrecta, incompleta, fraccionada, inducida a error o cuyo tratamiento esté prohibido o no haya sido autorizado. Este derecho incluye la corrección de errores tipográficos, actualización de direcciones, teléfonos y correos electrónicos, así como la inclusión de información omitida.

9.2 Ser informado

El titular podrá solicitar, en cualquier momento, información sobre el uso y destino que se ha dado a sus datos personales.

El Responsable deberá responder de manera clara, precisa y completa, indicando:

- Finalidades aplicadas.
- Categorías de datos tratados.
- Encargados y terceros a quienes se han transmitido o transferido datos.

9.3 Revocar y/o suprimir

El titular puede revocar, en cualquier momento, la autorización otorgada para el tratamiento de sus datos o solicitar la supresión de los mismos, siempre que no exista un deber legal o contractual que impida su eliminación.

La supresión implica la eliminación total o parcial de los datos de las bases del Responsable.

9.4 Acceso gratuito

El acceso a la información del titular será gratuito:

- Al menos una vez al mes sin costo alguno.
- En caso de solicitudes adicionales dentro del mismo mes, podrán cobrarse los gastos de reproducción y envío.
- En ningún caso se podrán realizar cobros que desincentiven o limiten el ejercicio de los derechos.

10. Deberes del Responsable y Encargados

10.1 Deberes generales del Responsable

En calidad de **Responsable del Tratamiento**, **Pedro Baracutao García** cumplirá, como mínimo, con las obligaciones establecidas en la Ley 1581 de 2012 y el artículo 2.2.2.25.4.1 del Decreto 1074 de 2015:

1. Garantizar al titular, en todo momento, el ejercicio pleno y efectivo del derecho de hábeas data.
2. Solicitar y conservar copia de la autorización otorgada por el titular, cuando se requiera.
3. Informar de manera clara y suficiente sobre la finalidad de la recolección y los derechos que le asisten.
4. Conservar la información bajo condiciones de seguridad que impidan su pérdida, adulteración, consulta, uso o acceso no autorizado.
5. Actualizar la información, comunicando de forma oportuna a los Encargados todas las novedades.
6. Rectificar datos cuando sean incorrectos, e informar de ello al Encargado.
7. Tramitar consultas y reclamos en los términos legales.
8. Cumplir con las instrucciones y requerimientos de la Superintendencia de Industria y Comercio.
9. Informar a la autoridad de protección de datos sobre incidentes de seguridad que comprometan la información tratada.
10. Adoptar un **Programa Integral de Gestión de Datos Personales** que incluya procedimientos, medidas técnicas y capacitación del personal.

10.2 Deberes de los Encargados

Los Encargados del Tratamiento deberán cumplir con los deberes establecidos en el artículo 18 de la Ley 1581 de 2012 y demás normas aplicables:

1. Garantizar al titular el ejercicio de sus derechos.
2. Conservar prueba de la autorización otorgada por el titular cuando actúen por cuenta del Responsable.
3. Actualizar la información de acuerdo con las instrucciones del Responsable.
4. Adoptar medidas de seguridad para la protección de los datos.

5. Abstenerse de circular información a terceros no autorizados.
6. Cumplir las instrucciones documentadas del Responsable.

10.3 Contratos de encargo

Todo contrato de **transmisión** de datos personales incluirá, como mínimo:

- Finalidad específica del tratamiento.
- Obligaciones de confidencialidad.
- Medidas de seguridad exigidas.
- Prohibición de reutilización de la información para fines distintos a los contratados.
- Procedimientos para atender incidentes y reclamos de titulares.
- Obligación de eliminación o devolución de datos al finalizar la relación contractual.

11. Procedimientos para el Ejercicio de Derechos

Con el fin de garantizar el derecho de hábeas data consagrado en el artículo 15 de la Constitución Política, en la Ley 1581 de 2012 y el Decreto 1074 de 2015, Pedro Baracutao García establece los siguientes procedimientos para que los titulares puedan ejercer sus derechos de conocer, actualizar, rectificar, suprimir datos o revocar la autorización.

11.1 Procedimiento de consultas

- Objeto: Permite al titular conocer los datos personales que reposan en las bases de datos del Responsable y obtener información sobre su tratamiento.
- Canales habilitados:
 - Correo electrónico institucional.
 - Formulario web en el portal oficial.
 - Dirección física para atención presencial.
- Requisitos mínimos:
 - Identificación del titular o representante.
 - Descripción clara de la solicitud.
 - Datos de contacto para la respuesta.
- Término de respuesta: Máximo 10 días hábiles desde la recepción. Si no es posible responder en este plazo, se informará al titular antes de su

vencimiento, explicando el motivo y señalando la nueva fecha de respuesta, que no podrá exceder de 5 días hábiles adicionales.

11.2 Procedimiento de reclamos

- Objeto: Procede cuando el titular considere que la información debe ser corregida, actualizada o suprimida, o cuando advierta un presunto incumplimiento de la ley o de la presente Política.
- Requisitos mínimos:
 - Identificación del titular o representante.
 - Descripción precisa de los hechos que dan lugar al reclamo.
 - Pruebas y documentos que respalden la solicitud.
 - Dirección y datos de contacto.
- Etapas:
 0. Recepción y registro del reclamo.
 1. Verificación de requisitos: si está incompleto, se requerirá subsanación en máximo 5 días hábiles; si no se atiende, se entenderá desistido.
 2. Inclusión en la base de datos de la leyenda “reclamo en trámite”.
 3. Investigación y respuesta dentro del término legal.
- Término de respuesta: Máximo 15 días hábiles desde la recepción. Si no es posible responder en este plazo, se notificará al titular antes del vencimiento, explicando el motivo y señalando una nueva fecha de respuesta, que no podrá exceder de 8 días hábiles adicionales.

11.3 Tiempos de respuesta

- Consultas: 10 días hábiles (+5 días adicionales con justificación).
- Reclamos: 15 días hábiles (+8 días adicionales con justificación).
- El cómputo inicia el día hábil siguiente a la recepción de la solicitud.

12. Medidas de Seguridad

En cumplimiento del principio de seguridad (artículo 4, Ley 1581 de 2012) y las recomendaciones de la Superintendencia de Industria y Comercio, el Responsable adoptará medidas técnicas, humanas, organizativas y jurídicas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales, especialmente de aquellos considerados sensibles.

12.1 Seguridad física

- Control de acceso a instalaciones donde se almacenen soportes físicos (archivos, expedientes, formularios de recolección).
- Sistemas de cierre seguro, custodia por personal autorizado y vigilancia.
- Prohibición de acceso a personas no autorizadas a áreas de archivo.
- Destrucción segura de documentos físicos mediante trituración o incineración, garantizando la imposibilidad de reconstrucción.

12.2 Seguridad lógica y digital

- Uso de contraseñas robustas y autenticación de doble factor en sistemas de información.
- Cifrado de bases de datos y de la información transmitida por medios electrónicos.
- Firewalls, antivirus y sistemas de detección de intrusiones.
- Copias de seguridad periódicas, con almacenamiento en entornos seguros.
- Actualización constante de software y parches de seguridad.

12.3 Controles de acceso

- Asignación de credenciales de usuario individualizadas.
- Principio de mínimos privilegios: acceso únicamente a la información necesaria según el rol.
- Registro (logs) de acceso, modificación y eliminación de datos personales.
- Revisión periódica de perfiles de usuario y revocación de accesos no justificados.

12.4 Plan de respuesta a incidentes

- Identificación y clasificación de incidentes de seguridad (acceso no autorizado, pérdida, robo, divulgación indebida).
- Contención y mitigación inmediata para evitar daños mayores.
- Notificación a los titulares afectados y, cuando corresponda, a la Superintendencia de Industria y Comercio, siguiendo la Guía de Gestión de Incidentes de Seguridad.

- Documentación de cada incidente y medidas correctivas.
- Entrenamiento regular del personal en detección y manejo de incidentes.

13. Transferencia y Transmisión de Datos

El tratamiento de datos personales por parte de Pedro Baracutao García podrá implicar su transferencia o transmisión a terceros, dentro o fuera del territorio nacional, únicamente cuando:

- Exista autorización previa, expresa e informada del titular, o cuando se configure alguna de las excepciones previstas en la Ley 1581 de 2012 y normas complementarias.
- El tercero receptor garantice el cumplimiento de estándares equivalentes o superiores de protección de datos personales.
- Se suscriban los contratos o instrumentos jurídicos que exija la ley para salvaguardar la información.

13.1 Nacionales

Se podrán realizar transmisiones o transferencias a entidades y personas ubicadas en Colombia que actúen como:

- Encargados del tratamiento, para ejecutar actividades por cuenta del Responsable (p. ej., proveedores de servicios de mensajería, call centers, encuestadoras, plataformas de gestión).
- Aliados estratégicos o contratistas, con los cuales exista relación legítima y finalidades compatibles con las informadas al titular.

En todos los casos se exigirán obligaciones contractuales de confidencialidad, seguridad y uso limitado.

13.2 Internacionales

La transferencia internacional de datos personales se regirá por el artículo 26 de la Ley 1581 de 2012 y estará permitida únicamente cuando:

1. El país receptor proporcione niveles adecuados de protección de datos (según listado de la SIC) o exista una cláusula contractual aprobada.
2. Se cuente con autorización expresa del titular para la transferencia.
3. La transferencia sea necesaria para la ejecución de un contrato en interés del titular, o para el reconocimiento, ejercicio o defensa de un derecho en proceso judicial.

4. Sea requerida por autoridad competente en el marco de sus funciones. Cuando el tratamiento internacional se realice mediante transmisión, el receptor actuará como Encargado y deberá sujetarse a las instrucciones documentadas del Responsable.

13.3 Condiciones y cláusulas contractuales

Todo contrato o instrumento que soporte la transmisión o transferencia de datos incluirá, como mínimo:

- Identificación de las partes y su rol (Responsable/Encargado/Receptor).
- Finalidades específicas del tratamiento.
- Obligación de aplicar medidas técnicas, jurídicas y organizativas para garantizar la seguridad de la información.
- Prohibición de usar los datos para fines distintos a los pactados.
- Procedimientos para atender consultas, reclamos e incidentes de seguridad.
- Obligación de devolver o suprimir los datos una vez finalice la relación contractual.
- Mecanismos de verificación y auditoría por parte del Responsable.

14. Registro Nacional de Bases de Datos (RNBD)

El Registro Nacional de Bases de Datos (RNBD) es el directorio público administrado por la Superintendencia de Industria y Comercio (SIC), en el que se inscriben las bases de datos sujetas a tratamiento por responsables y encargados en el territorio colombiano.

14.1 Obligación y condiciones de registro

Pedro Baracutao García, en su calidad de Responsable del Tratamiento, se obliga a registrar las bases de datos que administre ante el RNBD cuando le aplique esta obligación conforme a la Ley 1581 de 2012, el Decreto 1074 de 2015 y la Circular Única de la SIC.

El registro se efectuará cuando:

- El Responsable cumpla con los topes y condiciones establecidos por la SIC para personas naturales o jurídicas.
- La base de datos contenga información personal sujeta a tratamiento permanente o semipermanente.

- Se administren datos sensibles o de menores de edad, aunque no se superen topes económicos, cuando así lo disponga la autoridad de control.

14.2 Reportes y actualizaciones

Una vez inscrita la base de datos, el Responsable deberá:

- Mantener la información del registro actualizada en caso de cambios sustanciales (finalidades, canales de atención, medidas de seguridad, encargados, transferencias internacionales, etc.).
- Cumplir con los reportes periódicos exigidos por la SIC, como incidentes de seguridad, reclamos de titulares y novedades en la administración de las bases de datos.
- Realizar la renovación o confirmación anual del registro en los plazos fijados por la autoridad.

El incumplimiento de estas obligaciones puede dar lugar a sanciones administrativas previstas en el artículo 23 de la Ley 1581 de 2012.

15. Cookies y Tecnologías de Seguimiento

15.1 Uso en sitios web y redes sociales

El sitio web oficial de Pedro Baracutao García y sus canales digitales pueden utilizar cookies y tecnologías similares (como píxeles, etiquetas, scripts o identificadores de dispositivo) con el fin de:

- Facilitar la navegación y recordar las preferencias del usuario.
- Mejorar la experiencia y personalizar contenidos.
- Analizar el tráfico y la interacción con el sitio.
- Medir la efectividad de campañas informativas o políticas.
- Integrar funcionalidades de redes sociales y terceros proveedores.

Las cookies pueden ser propias o de terceros, temporales (de sesión) o permanentes, y se instalarán únicamente cuando el usuario lo permita, salvo aquellas estrictamente necesarias para el funcionamiento básico del sitio.

15.2 Finalidad y control

Las cookies y tecnologías de seguimiento se usarán para:

1. Analítica web: medir número de visitas, páginas más consultadas y patrones de navegación.

2. Optimización del sitio: adaptar el contenido y la estructura en función del uso real.
3. Segmentación de comunicación política: mostrar contenidos o invitaciones relevantes según la interacción previa del usuario (con autorización previa y expresa).
4. Integración con redes sociales: permitir compartir contenido y registrar interacciones.

Control por parte del titular:

- En el primer acceso, se mostrará un aviso de cookies con información clara sobre su uso y un mecanismo para aceptar, rechazar o configurar las cookies no esenciales.
- El titular podrá modificar su configuración o revocar el consentimiento en cualquier momento desde el sitio web.
- Podrá borrar las cookies desde las opciones de su navegador, sin que ello impida el acceso a contenidos esenciales.

16. Videovigilancia y Registro de Eventos

16.1 Uso de cámaras y registro audiovisual

Pedro Baracutao García podrá utilizar sistemas de videovigilancia en sedes, oficinas, eventos y actividades públicas o privadas relacionadas con su actividad política, comunitaria o administrativa, con fines de:

- Seguridad de las personas, bienes e instalaciones.
- Registro documental de eventos, reuniones, foros, asambleas o actos de campaña.
- Producción de material audiovisual para difusión en medios propios o terceros, siempre con sujeción a las finalidades informadas y autorizaciones correspondientes.

Las imágenes y grabaciones podrán ser almacenadas en medios físicos o digitales bajo medidas de seguridad apropiadas, y se conservarán únicamente por el tiempo necesario para cumplir la finalidad que motivó su recolección, salvo requerimiento legal o judicial que exija su conservación por mayor plazo.

16.2 Avisos y finalidades

- En las zonas y eventos con videograbación o registro audiovisual se colocarán avisos visibles informando que se está realizando el registro, la finalidad del mismo, y los datos de contacto del Responsable.
- Cuando se realicen transmisiones en vivo, se advertirá previamente a los asistentes.
- Si las imágenes o grabaciones van a ser usadas para fines diferentes a la seguridad (por ejemplo, difusión política), se solicitará la autorización expresa de las personas identificables, salvo que se trate de eventos en espacios públicos o con fines periodísticos, culturales o de interés general conforme a la ley.

17. Vigencia de la Política

17.1 Fecha de entrada en vigor

La presente Política de Tratamiento y Protección de Datos Personales entra en vigor a partir del [indicar fecha exacta de aprobación o publicación] y permanecerá vigente mientras Pedro Baracutao García ejerza actividades que impliquen el tratamiento de datos personales, o mientras sea necesario para cumplir con las finalidades informadas y las obligaciones legales derivadas de dicho tratamiento.

17.2 Cambios y actualizaciones

Pedro Baracutao García se reserva el derecho de modificar o actualizar esta política en cualquier momento, con el fin de:

- Atender cambios normativos o regulatorios.
- Incorporar instrucciones de la autoridad de protección de datos (Superintendencia de Industria y Comercio).
- Ajustar procedimientos internos o medidas de seguridad.
- Reflejar modificaciones en las finalidades o en las prácticas de tratamiento.

Cualquier cambio sustancial será comunicado a los titulares mediante:

- Publicación en el sitio web oficial y redes sociales.
- Avisos físicos en sedes y puntos de atención.
- Otros medios electrónicos o físicos que aseguren su conocimiento.

En los casos en que el cambio implique nuevas finalidades o tipos de tratamiento, se solicitará nuevamente la autorización del titular, salvo que la ley disponga lo contrario.

18. Anexos

Los anexos forman parte integral de la presente política y contienen modelos y procedimientos que facilitan su implementación práctica y el cumplimiento de la normativa vigente.

18.1 Formato de autorización

Documento mediante el cual el titular otorga a Pedro Baracutao García su autorización previa, expresa e informada para el tratamiento de datos personales, con mención específica de:

- Identificación del titular.
- Finalidades precisas del tratamiento (políticas, comunitarias, administrativas, de comunicación, etc.).
- Carácter facultativo de la entrega de datos sensibles y de menores de edad.
- Derechos que le asisten y canales de contacto.
- Firma del titular o validación digital que garantice autenticidad.

Este formato podrá existir en versión física o electrónica, y deberá conservarse como prueba del consentimiento otorgado.

18.2 Aviso de privacidad

Comunicación verbal o escrita dirigida al titular en el momento de la recolección de sus datos, que contiene como mínimo:

- Identidad y datos de contacto del Responsable.
- Finalidades del tratamiento.
- Derechos del titular y cómo ejercerlos.
- Indicación de dónde consultar la política completa.

El aviso de privacidad se usará en situaciones donde no sea posible poner a disposición del titular la política completa en el mismo momento de la recolección (por ejemplo, en eventos masivos, formularios breves o interacciones rápidas en medios digitales).

18.3 Procedimientos internos

Protocolos y lineamientos internos que todo el personal y contratistas deben seguir para garantizar:

- Recolección lícita y transparente de datos.
- Registro y conservación de autorizaciones.
- Actualización, rectificación y supresión de información.
- Respuesta a consultas y reclamos dentro de los plazos legales.
- Manejo seguro de soportes físicos y digitales.
- Notificación y gestión de incidentes de seguridad.
- Capacitación periódica en protección de datos personales.

Estos procedimientos deberán ser revisados y actualizados periódicamente, alineándose con las directrices de la Superintendencia de Industria y Comercio y las mejores prácticas en gestión de la información.