

INDICE

Artículo	Descripción	Página
	OBJETIVO	3
	INTEGRACIÓN NORMATIVA Y DOCUMENTOS COMPLEMENTARIOS	3
	GENERALIDADES	4
1	IDENTIFICACIÓN	4
2	DEFINICIONES	4
3	ÁMBITO DE APLICACIÓN	6
4	PRINCIPIOS	6
5	EFFECTOS DE LA NEGATIVA EN ETAPA PRECONTRACTUAL	7
6	AUTORIZACIÓN Y PRUEBA DE LA AUTORIZACIÓN	7
	PARÁGRAFO 1. Manifestación de la autorización	7
	PARÁGRAFO 2. Conservación y custodia de la autorización	7
	PARÁGRAFO 3. Prueba de la autorización	8
	PARÁGRAFO 4. Tratamiento de Datos Personales de Personas Naturales Vinculadas a Personas Jurídicas Clientes	8
7	CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN	8
8	AUTORIZACIONES A TERCEROS	9
9	TRATAMIENTO DE DATOS DE MENORES DE EDAD	9
10	DATOS SENSIBLES	9
11	FINALIDADES DEL TRATAMIENTO DE LOS DATOS	10
	PARÁGRAFO 1. Aceptación de finalidades y ejercicio de derechos del titular	12
	PARÁGRAFO 2. Tratamiento directo y a través de encargados del tratamiento	12
12	TRATAMIENTO DE DATOS EN SERVICIOS DE SOPORTE, MESA DE AYUDA Y CANALES DE ATENCIÓN MULTICANAL	12
	PARÁGRAFO 1. Grabación de llamadas	13
	PARÁGRAFO 2. Mensajería instantánea	13
	➔ Exclusión de responsabilidad por canales no oficiales	13
	PARÁGRAFO 3. Evidencias técnicas	13
13	DERECHOS DEL TITULAR DE LOS DATOS PERSONALES	13
	PARÁGRAFO. Prueba de la autorización	13
14	DEBERES DEL RESPONSABLE DEL TRATAMIENTO DE LOS DATOS PERSONALES	13
15	DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO	14
16	OFICIAL DE PROTECCIÓN DE DATOS PERSONALES	14
	PROCEDIMIENTO PARA CONSULTA, QUEJAS, RECLAMACIONES Y REVOCATORIAS DE AUTORIZACIONES	14
17	ACCESO A LA INFORMACIÓN	14
18	PERSONA / GRUPO RESPONSABLE / CANAL INSTITUCIONAL DE ATENCIÓN DE PETICIONES, CONSULTAS, RECLAMOS Y DENUNCIAS	14
19	TÉRMINO PARA LA ATENCIÓN DE CONSULTAS	15
20	RECLAMOS	15
21	TÉRMINO PARA LA ATENCIÓN DE RECLAMOS	15
22	RECTIFICACIÓN, ACTUALIZACIÓN, CANCELACIÓN O SUPRESIÓN DE DATOS	15
23	SUPRESIÓN DE DATOS	15
24	REVOCATORIA DE LA AUTORIZACIÓN	16
25	REQUISITOS PARA ATENDER CONSULTAS, QUEJAS O RECLAMOS	16
	CAPTURA DE IMÁGENES POR CÁMARAS DE VIDEOVIGILANCIA	16
26	TRATAMIENTO DE DATOS PERSONALES EN SISTEMAS DE VIDEOVIGILANCIA	16
	PARÁGRAFO 1. Zonas excluidas	17
	PARÁGRAFO 2. Transmisión de datos personales	17

	PARÁGRAFO 3. Control por el Oficial de Protección de Datos Personales	17
	TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES	17
27	TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES	17
	PARÁGRAFO. Control y reporte de transmisiones de datos personales	18
28	TRANSMISIÓN DE DATOS PERSONALES A TERCEROS EN EL DESARROLLO DE LAS OPERACIONES	18
	PARÁGRAFO 1. Plataformas tecnológicas y servicios en la nube	18
	PARÁGRAFO 2. Prohibición de uso autónomo de la información	18
	PARÁGRAFO 3. Control interno	18
29	VIGENCIA DE LAS BASES DE DATOS	18
30	TEMPORALIDAD DEL TRATAMIENTO DEL DATO	19
	AVISO DE PRIVACIDAD	19
31	AVISO DE PRIVACIDAD	19
	MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES SENSIBLES, BIOMÉTRICOS Y AUDIOVISUALES	19
32	ALCANCE DE LAS MEDIDAS DE SEGURIDAD	19
33	TRATAMIENTO DE DOCUMENTOS FÍSICOS CON DATOS BIOMÉTRICOS	20
34	REGISTRO, CIRCULACIÓN Y CONSULTA DE DOCUMENTOS FÍSICOS SENSIBLES	20
35	CUSTODIA Y ARCHIVO DE DOCUMENTOS FÍSICOS SENSIBLES	20
36	DIGITALIZACIÓN DE DOCUMENTOS FÍSICOS CON FIRMA Y/O HUELLA	20
37	ACCESO A REGISTROS DIGITALES SENSIBLES	21
38	ALMACENAMIENTO Y CONSERVACIÓN DE REGISTROS BIOMÉTRICOS Y AUDIOVISUALES	21
39	PROHIBICIONES EXPRESAS	21
40	RESPONSABILIDAD EN LA APLICACIÓN DE LAS MEDIDAS	21
41	INCUMPLIMIENTO	21
42	INCIDENTES DE SEGURIDAD	21
	ANEXO 1: AVISO DE PRIVACIDAD	23
	Firmas	24
	Registro de Conocimiento, Notificación y Aceptación	25

	POLÍTICA DE TRATAMIENTO DE INFORMACIÓN Y PROTECCIÓN DE LOS DATOS PERSONALES, BIOMÉTRICOS Y AUDIOVISUALES	Código: PL-0010-GE Versión: 2.0 13-Feb-2026 Dominio: USO PÚBLICO Página 3 de 40
---	---	--

<i>Responsabilidad institucional:</i>	La presente política es adoptada y aprobada por la Gerencia de LA EMPRESA, en su calidad de responsable del tratamiento de datos personales.
<i>Administración y ejecución:</i>	La implementación, aplicación operativa, custodia y actualización de los procedimientos derivados de la presente política estará a cargo del área de Talento Organizacional .

SAIMYR S.A.S, en adelante LA EMPRESA, mediante la publicación de este documento, comunica a sus grupos de interés la *Política de tratamiento y protección de datos personales, biométricos y audiovisuales* en cumplimiento de lo establecido en la Ley 1581 de 2012, el Decreto 1074 de 2015 y las demás normas que la regulan.

OBJETIVO

La presente política de tratamiento y protección de datos personales, biométricos y audiovisuales tiene como propósito establecer los parámetros generales para la gestión, manejo, uso, supresión y protección de los datos de carácter personal recolectados, tratados o almacenados en cualquier base de datos administrada o de propiedad de **LA EMPRESA**, quien actuará como responsable del Tratamiento salvo indicación expresa en contrario.

INTEGRACIÓN NORMATIVA Y DOCUMENTOS COMPLEMENTARIOS

La presente Política se aplica y se interpreta de manera armónica con los demás instrumentos normativos y documentales adoptados por LA EMPRESA, los cuales desarrollan aspectos específicos relacionados con el tratamiento de la información, la gestión documental, las relaciones laborales y el ejercicio de los derechos de los titulares.

En particular, esta política se integra y complementa con los siguientes documentos de USO PÚBLICO:

- La Autorización **"FO-0010-GE: Autorización para el Tratamiento de Datos Personales, Biométricos y Audiovisuales"**, mediante la cual LA EMPRESA obtiene el consentimiento previo, expreso, informado y libremente otorgado por los titulares, cuando este resulte exigible de conformidad con la normatividad vigente.
- El Acuerdo **"FO-0020-GE: Acuerdo de Confidencialidad, Protección de la Información y Secretos Empresariales"**, es un documento de carácter vinculante mediante el cual el trabajador o tercero reconoce, acepta y se obliga a proteger la información confidencial, los datos personales, sensibles, biométricos y audiovisuales, los secretos empresariales, la propiedad intelectual y demás activos informacionales de LA EMPRESA y de terceros bajo su custodia, comprometiéndose a su uso limitado, custodia, no divulgación y cumplimiento de las medidas técnicas, humanas y administrativas establecidas, durante la vigencia de la relación y con posterioridad a su terminación. Este acuerdo no sustituye ni reemplaza la autorización para el tratamiento de datos personales cuando esta sea legalmente exigible.

Asimismo, se complementa con los siguientes documentos de uso interno (privado) de LA EMPRESA:

- El Reglamento **"Reglamento Interno de Trabajo"**, aplicable exclusivamente respecto de los trabajadores vinculados laboralmente con LA EMPRESA, en lo relacionado con el tratamiento de datos personales en el marco de la relación laboral, el uso de medios tecnológicos institucionales, los mecanismos de vigilancia, supervisión y control, y la utilización de la información como medio de prueba en procesos internos, disciplinarios o judiciales, conforme a la legislación laboral y de protección de datos vigente, respetando en todo caso los derechos fundamentales del trabajador, en especial la dignidad humana, la intimidad y el debido proceso.

El Reglamento Interno de Trabajo no será aplicable a contratistas, proveedores, aspirantes, visitantes u otros terceros, quienes se registrarán por los acuerdos, contratos, autorizaciones y documentos que resulten aplicables según la naturaleza de su relación con LA EMPRESA.

- d) La Política **"PL-0020-GE: Política para el Manejo de los Documentos y Comunicaciones Institucionales"**, que constituye la política marco y sistema de referencia obligatorio, regula el ciclo de vida integral de los documentos institucionales de LA EMPRESA, incluyendo su emisión, elaboración, aprobación, socialización, notificación, validez, exigibilidad, gestión, custodia, conservación, acceso, actualización, trazabilidad, control y seguimiento; así como el control de los documentos y registros que contengan datos personales, biométricos o audiovisuales, y la implementación y gestión del **"Registro de Conocimiento, Notificación y Aceptación"**, garantizando la integridad de la información, su valor probatorio y la seguridad jurídica institucional.

GENERALIDADES

LA EMPRESA manifiesta su compromiso y respeto por los principios fundamentales establecidos en la Constitución Política y en la ley, para garantizar los derechos a la privacidad, intimidad, buen nombre, en el tratamiento de los datos personales recolectados, tratados y almacenados en sus bases de datos, en el desarrollo de su objeto social, en calidad de responsable del tratamiento, directamente o a través de terceros debidamente autorizados.

ARTÍCULO 1. IDENTIFICACIÓN: Nombre o razón social, domicilio, dirección, sitio web:

Razón social:	SAIMYR S.A.S
NIT:	811029572-1
Dirección – Domicilio:	Cl. 37 # 59 105 (Rionegro, Antioquia)
Sitio Web:	https://saimyr.co/politicas-de-tratamiento-de-datos
Correo y teléfono:	privacidad@saimyr.com.co (+574) 444 65 60

ARTÍCULO 2. DEFINICIONES. Las siguientes definiciones, permiten una correcta y apropiada aplicación e interpretación de las disposiciones legales sobre protección de datos personales:

Titular de la información o Titular: Es la persona natural cuyos datos son objeto de tratamiento, por ejemplo: trabajador, contratista, proveedor, candidato, visitante o cualquier otro tercero. En el caso de relaciones comerciales o contractuales con personas jurídicas, se entenderán como titulares los empleados, funcionarios, representantes, contratistas o usuarios autorizados que actúen en nombre, por cuenta o en interés de la persona jurídica (cliente).

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales; es la base primordial de la protección de datos personales, por regla general, no se podrán tratar los datos personales sin su consentimiento, salvo las excepciones expresamente previstas en la ley.

Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Base de datos personales: Es todo conjunto organizado (manual o automatizado) de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Consulta: Solicitud del titular del dato o las personas autorizadas por éste o por la ley para acceder a la información que repose en cualquier base de datos de LA EMPRESA.

Datos personales: Es cualquier información vinculada o que pueda asociarse a una o a varias personas naturales, determinadas o determinables.

Dato privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato público: Es el dato que no sea semiprivado, privado o sensible. 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. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento y divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas, o a la sociedad en general, como el dato financiero y crediticio.

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como:

- Aquellos que revelen el origen racial o étnico.
- La orientación política.
- Las convicciones religiosas o filosóficas.
- La pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición.
- Los datos relativos a la salud, a la vida sexual.
- Los datos biométricos: Son aquellos datos personales sensibles obtenidos a partir de características físicas, fisiológicas o conductuales de una persona natural que permiten o confirman su identificación, tales como la huella dactilar y la firma.

Los datos audiovisuales (imagen, audio y video) podrán tener carácter sensible y, en determinados contextos, carácter biométrico, cuando permitan la identificación del titular, y serán tratados conforme a las finalidades documentales, laborales, de seguridad y probatorias definidas en la presente política.

Encargado del tratamiento: Es el tercero que por designación realiza el tratamiento de datos personales por cuenta del responsable.

Oficial de protección de datos: Persona, área o unidad designada por LA EMPRESA para coordinar y supervisar el cumplimiento del régimen de protección de datos personales y las quejas, solicitudes o reclamos que los titulares formulen.

Reclamo: Solicitud del titular del dato o de las personas autorizadas por éste o por la ley para corregir, actualizar o suprimir sus datos personales o para revocar la autorización en los casos establecidos en la ley.

Tratamiento: Conjunto de operaciones sobre datos personales, tales como: la recolección, almacenamiento, actualización, uso, circulación, cancelación o supresión.

Responsable del tratamiento: LA EMPRESA, como persona jurídica, es la responsable del tratamiento de los datos personales contenidos en las bases de datos de su propiedad o administración, en los términos de la Ley 1581 de 2012. Las personas naturales que, en virtud de su cargo, funciones o relación contractual, tengan acceso a consultar, recolectar o realizar cualquier tipo de tratamiento de datos personales, actuarán por cuenta y bajo las instrucciones de LA EMPRESA, y estarán obligadas a dar estricto cumplimiento a la presente Política, siendo responsables a título personal por el uso indebido, no autorizado o contrario a la ley y a las políticas internas. Lo anterior se entiende sin perjuicio del régimen de responsabilidad laboral y disciplinaria aplicable.

Transferencia de datos: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

Transmisión de datos: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia, cuando tenga por objeto la realización de un tratamiento por el encargado o por cuenta del responsable.

Incidente de seguridad: Para efectos del presente Acuerdo y de las políticas internas de LA EMPRESA, se entiende por Incidente de Seguridad de la Información todo evento, situación, acción u omisión, real o potencial, intencional o accidental, que comprometa o pueda comprometer la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la Información Confidencial, de los datos personales, datos sensibles, datos biométricos o datos audiovisuales, propios de LA EMPRESA o de terceros bajo su custodia.

ARTÍCULO 3. ÁMBITO DE APLICACIÓN. La presente política aplicará a los datos personales de personas naturales consignados en cualquier base de datos administrada o de propiedad de LA EMPRESA, como responsable del tratamiento o, de manera excepcional, como encargado de este, cuando así se pacte expresamente.

La presente política aplica exclusivamente al tratamiento de datos personales que sean recolectados, tratados, almacenados o transmitidos por LA EMPRESA a través de sus canales oficiales, institucionales y autorizados, tales como correos electrónicos corporativos, líneas telefónicas institucionales, plataformas de atención, sistemas de información, aplicaciones de mensajería autorizadas, sitios web, formularios oficiales y demás medios definidos y comunicados por LA EMPRESA.

LA EMPRESA no será responsable por el tratamiento de datos personales que los titulares suministren de manera voluntaria, espontánea o informal a través de canales no oficiales, tales como correos electrónicos personales, números telefónicos personales, cuentas privadas de mensajería instantánea o redes sociales de trabajadores, contratistas o terceros, aun cuando exista relación comercial o contractual con LA EMPRESA.

En consecuencia, LA EMPRESA podrá abstenerse de atender solicitudes, requerimientos o prestar servicios de soporte cuando estos se formulen a través de canales no oficiales, o requerir al titular para que formalice la solicitud a través de los canales institucionales definidos.

ARTÍCULO 4. PRINCIPIOS. LA EMPRESA hace suyos los siguientes principios, a los que deberá ajustar la recolección, la custodia y el tratamiento de datos de carácter personal:

- a) *De legalidad:* El tratamiento se ajustará a lo establecido en la ley.
- b) *De finalidad:* El tratamiento obedecerá a una finalidad legítima y debidamente enunciada en esta política y comunicada al titular.
- c) *De libertad:* El tratamiento sólo se realizará con el consentimiento: previo, expreso e informado del titular.

- d) *De veracidad o calidad*: La información sujeta a tratamiento deberá ser: veraz, completa, exacta, actualizada, comprobable y comprensible.
- e) *De transparencia*: En el tratamiento se garantizará el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le concierne.
- f) *De acceso y circulación restringida*: El tratamiento se sujetará a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y de la Constitución; en este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el responsable y/o por las personas previstas en la ley.
- g) *De seguridad*: La información sujeta a tratamiento por el responsable o encargado deberá manejarse con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros **evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.**
- h) *De confidencialidad*: Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos, están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento.

ARTÍCULO 5. EFECTOS DE LA NEGATIVA EN ETAPA PRECONTRACTUAL: La negativa del titular a otorgar la autorización para el tratamiento de sus datos personales, datos sensibles, biométricos o audiovisuales, o a suscribir los documentos que resulten necesarios para habilitar dicho tratamiento, tales como:

- La autorización "**FO-0010-GE: Autorización para el Tratamiento de Datos Personales, Biométricos y Audiovisuales**"
- el acuerdo "**FO-0020-GE: Acuerdo de Confidencialidad, Protección de la Información y Secretos Empresariales**"
- O cualquier otro documento habilitante requerido razonablemente en la etapa precontractual,

podrá dar lugar a la imposibilidad de continuar con el proceso precontractual o de selección, sin que ello constituya sanción, discriminación ni genere obligación alguna de vinculación para LA EMPRESA, en la medida en que esta no se encontraría legalmente habilitada para realizar el tratamiento de la información requerido para dicha etapa.

En todo caso, dicha decisión se fundamenta exclusivamente en la imposibilidad jurídica de adelantar el tratamiento de datos sin la autorización correspondiente, conforme a la Ley 1581 de 2012 y normas concordantes.

ARTÍCULO 6. AUTORIZACIÓN Y PRUEBA DE LA AUTORIZACIÓN: LA EMPRESA solo recolectará, almacenará, usará y circulará los datos personales que sean pertinentes y adecuados para las finalidades señaladas en la presente política, para lo cual contará con el consentimiento previo, expreso e informado del titular, el cual podrá ser otorgado a través de cualquier medio válido, ya sea físico, electrónico o tecnológico, que permita garantizar su posterior consulta y verificación.

PARÁGRAFO 1. Manifestación de la autorización: La autorización para el tratamiento de los datos personales podrá ser otorgada únicamente por:

- a) El titular de la información.
- b) Los causahabientes del titular.
- c) El representante legal o apoderado del titular.
- d) Terceros debidamente autorizados por el titular o por la ley.

PARÁGRAFO 2. Conservación y custodia de la autorización: LA EMPRESA adoptará las medidas necesarias, pertinentes y razonables para guardar, custodiar y conservar las autorizaciones otorgadas por los titulares, las cuales podrán reposar en archivos físicos o electrónicos, de manera directa o por medio

de terceros contratados para el manejo de la información, quienes deberán cumplir con los requisitos legales, técnicos y de seguridad exigidos por la normativa vigente.

PARÁGRAFO 3. Prueba de la autorización: LA EMPRESA podrá acreditar la existencia y validez de la autorización otorgada por el titular cuando así lo requiera este, o cuando sea solicitada por la Superintendencia de Industria y Comercio o cualquier autoridad competente, en los términos establecidos en la Ley 1581 de 2012 y demás normas que la reglamenten o complementen.

PARÁGRAFO 4. Tratamiento de Datos Personales de Personas Naturales Vinculadas a Personas Jurídicas Clientes: En el marco de las relaciones contractuales o precontractuales celebradas con personas jurídicas, LA EMPRESA podrá tratar datos personales de personas naturales vinculadas, designadas o autorizadas por una persona jurídica cliente, incluidos sus empleados, funcionarios, representantes, contratistas o usuarios autorizados, que se comuniquen con **LA EMPRESA** para la ejecución, desarrollo, control y cumplimiento de la relación contractual o precontractual existente con dicha persona jurídica, así como para la prestación de los servicios a través de la mesa de ayuda, los canales de soporte técnico o de atención al cliente, incluyendo solicitudes de soporte, mantenimiento, gestión de incidencias o desarrollo de nuevos requerimientos sobre los sistemas o servicios contratados, siempre que el tratamiento:

- ✓ Sea estrictamente necesario y proporcional para dichas finalidades, y
- ✓ Se realice exclusivamente a través de los canales oficiales, institucionales y autorizados definidos por **LA EMPRESA**,

Sin perjuicio del ejercicio de los derechos de revocatoria y supresión por parte del titular, en los términos y con las limitaciones previstas en los artículos 23 y 24 de la presente política.

Esta autorización: tratamiento de datos personales de personas vinculadas a personas jurídicas clientes, se realizará conforme a la regla general de autorización previa, expresa e informada del titular, en los términos del artículo 9 de la Ley 1581 de 2012.

Dicha autorización podrá ser otorgada directamente por el titular a través de la persona jurídica cliente con la cual el titular mantenga una relación laboral, contractual, funcional o de representación, siempre que el tratamiento resulte estrictamente necesario y proporcional para la ejecución, desarrollo, control o cumplimiento de la relación contractual o precontractual existente entre dicha persona jurídica y LA EMPRESA.

En estos casos, LA EMPRESA tratará exclusivamente los datos personales necesarios para las finalidades autorizadas, en especial aquellas relacionadas con la prestación de servicios, soporte técnico, mesa de ayuda o atención al cliente, y únicamente a través de los canales oficiales, institucionales y autorizados definidos por LA EMPRESA.

En ningún caso el presente literal constituye una excepción a la obligación de contar con autorización del titular ni se asimila a los supuestos previstos en el artículo 10 de la Ley 1581 de 2012.

En estos supuestos, LA EMPRESA actúa como encargado o responsable del tratamiento según corresponda, bajo la presunción de que la persona jurídica cliente ha informado y obtenido del titular la autorización prevista en el artículo 9 de la Ley 1581 de 2012.

ARTÍCULO 7. CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN. La autorización del titular no será necesaria en los siguientes casos:

- a) Cuando la información sea requerida por una entidad pública o administrativa, en ejercicio de sus funciones legales, o por orden judicial, siempre y cuando la motivación de la solicitud de información esté basada en una clara y específica competencia funcional de la entidad que solicita

la información y se garantice al titular, los derechos fundamentales previstos en la Constitución Política y en las normas sobre datos personales.

- b) Cuando los datos sean de naturaleza pública, según lo establecido en la Constitución Política y en la jurisprudencia constitucional.
- c) En casos de urgencia médica o sanitaria.
- d) Información autorizada por la ley para fines históricos, estadísticos o científicos.
- e) Datos relacionados con el estado civil de las personas.

ARTÍCULO 8. AUTORIZACIONES A TERCEROS: Se establece que los derechos de los titulares de la información podrán ser ejercidos a través de terceras personas, previa acreditación de la representación o apoderamiento. En virtud de lo anterior, **LA EMPRESA** informa a los titulares los requisitos mínimos que deberá contener la autorización de terceros, así:

- a) Identificación del titular de la información que autoriza.
- b) Copia de la cédula de ciudadanía o documento de identificación del titular de la información.
- c) Nombre, datos de identificación y copia de la cédula o documento de identificación del tercero autorizado.
- d) Tiempo de la autorización a través de la cual puede consultar, actualizar o rectificar la información (solo una vez, por un año, por la duración de la relación jurídica, o hasta nueva orden, etc.).
- e) Manifestación libre y voluntaria de la autorización al tercero.

El titular de la información deberá entregar la anterior autorización a LA EMPRESA, en la cual autoriza a un tercero para que consulte, actualice o rectifique su información.

Esta autorización tiene como fin proteger y restringir el acceso de la información a terceros no autorizados.

ARTÍCULO 9. TRATAMIENTO DE DATOS DE MENORES DE EDAD: El tratamiento de datos personales de niños, niñas y adolescentes se realizará respetando su interés superior y sus derechos fundamentales, conforme a la ley, y únicamente cuando sea necesario para el desarrollo del objeto social de LA EMPRESA y con la autorización del representante legal.

ARTÍCULO 10. DATOS SENSIBLES. La ley prevé una categoría de datos denominada “datos sensibles”, cuyo tratamiento está restringido y sometido a requisitos especiales. Cuando el tratamiento de los datos sensibles sea posible conforme a lo establecido en la ley, se deberá informar al titular de forma explícita y previa cuáles de los datos se consideran sensibles y la finalidad del tratamiento para obtener su consentimiento expreso (informándole que no está obligado a autorizar su tratamiento).

En el contexto de la relación laboral y documental, el tratamiento de datos sensibles por parte de LA EMPRESA podrá resultar necesario, proporcional y razonable, según la finalidad específica (por ejemplo: el cumplimiento de obligaciones legales, contractuales, de seguridad, control de acceso, gestión documental, soporte probatorio, etc.) y conforme al principio de minimización de datos.

Tipos de Datos Sensibles:

Los datos definidos por la ley como sensibles, es decir, los que afecten la intimidad del titular, o cuyo uso indebido pueda generar su discriminación, podrán ser objeto de tratamiento y solicitados por **LA EMPRESA**, únicamente en los siguientes casos:

- a) El titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
- b) El Tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;

- c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;
- d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
- e) Cuando el tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

ARTÍCULO 11. FINALIDADES DEL TRATAMIENTO DE LOS DATOS: LA EMPRESA, en el desarrollo de su objeto social y de sus actividades administrativas, operativas, contractuales, laborales, comerciales, formativas, disciplinarias y de control, recopila, consulta, utiliza, almacena, archiva, circula, transmite y, en general, trata datos personales de manera responsable, segura y confidencial, conforme a los principios y disposiciones legales aplicables.

Las finalidades aquí descritas se interpretan de manera sistemática e integral, y comprenden, de forma expresa, la gestión documental institucional, el soporte probatorio de las actuaciones laborales, contractuales y disciplinarias, la conservación de la historia laboral y la garantía de la seguridad jurídica de LA EMPRESA.

1. Los datos personales podrán ser tratados para las siguientes finalidades sobre la Gestión documental, probatoria e historia laboral:
 - a) Gestionar, administrar, custodiar, conservar y controlar los Documentos Institucionales, independientemente de su formato o medio, garantizando su integridad, trazabilidad, disponibilidad, autenticidad y conservación.
 - b) Constituir, conservar y administrar el soporte probatorio de las actuaciones administrativas, contractuales, laborales, disciplinarias, formativas y de control, incluyendo notificaciones, aceptaciones, constancias, comunicaciones y evidencias digitales o físicas.
 - c) Conservar la historia laboral, contractual, formativa y disciplinaria de los trabajadores y demás titulares, conforme a las disposiciones legales, reglamentarias y documentales aplicables.
 - d) Garantizar la seguridad jurídica de LA EMPRESA, de sus decisiones, actuaciones, procesos internos y relaciones con los titulares de la información.
2. Los datos personales podrán ser tratados para las siguientes finalidades sobre la gestión, ejecución, control y conservación de la relación laboral, contractual y reglamentaria:
 - a) Ejecutar, mantener, desarrollar y dar cumplimiento a la relación contractual, legal o reglamentaria existente con clientes, proveedores, trabajadores, contratistas y demás titulares, incluida la gestión y pago de obligaciones contractuales y legales.
 - b) Propiciar el seguimiento, acompañamiento, cumplimiento, control y evaluación de los compromisos contractuales, reglamentarios o del vínculo existente entre el titular y LA EMPRESA.
 - c) Consultar, verificar, actualizar, rectificar y mantener actualizada la información personal de los titulares, para el adecuado desarrollo de las finalidades inicialmente previstas.
3. Los datos personales podrán ser tratados para las siguientes finalidades sobre servicios, clientes y actividad comercial:

- a) Proveer los servicios y/o productos requeridos por los usuarios, clientes o aliados de LA EMPRESA.
 - b) Informar sobre nuevos productos, servicios, programas, capacitaciones o cambios en los mismos.
 - c) Comunicar información empresarial, institucional, organizacional, promocional o relacionada con la actividad de LA EMPRESA a través de correos electrónicos, redes sociales, plataformas digitales, llamadas telefónicas u otros canales de comunicación autorizados. El titular **podrá manifestar su oposición** a recibir estas comunicaciones en cualquier momento, a través de los canales que LA EMPRESA tenga habilitadas para tal fin.
 - d) Establecer contacto con los titulares mediante llamadas telefónicas, mensajes de texto, aplicaciones de mensajería instantánea, redes sociales y/o correos electrónicos, con el fin de realizar asesorías, acompañamientos o gestiones relacionadas con los servicios o productos ofrecidos por LA EMPRESA. El titular **podrá manifestar su oposición** a recibir estas comunicaciones en cualquier momento, a través de los canales que LA EMPRESA tenga habilitadas para tal fin.
 - e) Comunicar a los grupos de interés información relacionada con bienes, servicios, actividades empresariales, actualidad corporativa, tecnológica o publicidad asociada a la actividad de LA EMPRESA, de manera directa o a través de terceros o aliados.
4. Los datos personales podrán ser tratados para las siguientes finalidades sobre las comunicaciones y PQRS:
- a) Enviar información institucional, operativa, administrativa, contractual, formativa, comercial o informativa al correo físico, electrónico, número de contacto, dispositivo móvil o a través de cualquier medio físico o digital de comunicación, incluyendo mensajes de texto, aplicaciones de mensajería instantánea, plataformas virtuales o medios tecnológicos presentes o futuros. El titular **podrá manifestar su oposición** a recibir estas comunicaciones en cualquier momento, a través de los canales que LA EMPRESA tenga habilitadas para tal fin.
 - b) Atender, gestionar y dar respuesta a peticiones, quejas, reclamos, solicitudes, felicitaciones o requerimientos (PQRS-F) presentados por los titulares.
5. Los datos personales podrán ser tratados para las siguientes finalidades sobre la transferencia y encargados: Suministrar, compartir, transmitir o entregar datos personales a empresas filiales, aliadas, proveedores o colaboradores de LA EMPRESA, ubicados en Colombia o en el exterior, cuando ello sea necesario para el cumplimiento de las finalidades aquí descritas y conforme a la normativa vigente
6. Los datos personales podrán ser tratados para las siguientes finalidades sobre la seguridad, control y biometría: Controlar el ingreso, permanencia y salida de las instalaciones físicas o virtuales de LA EMPRESA mediante mecanismos de identificación biométrica, fotográfica, filmica o tecnológica, así como garantizar la seguridad de las instalaciones, de los trabajadores, visitantes y bienes, mediante sistemas de videovigilancia; estos datos pueden servir como prueba y para control institucional
7. Los datos personales podrán ser tratados para las siguientes finalidades sobre la información financiera y riesgo: Realizar consultas en centrales de información, riesgo crediticio, operadores de bases de datos o entidades autorizadas, cuando sea necesario para evaluar comportamientos financieros, comerciales o de servicios, conforme a la normatividad aplicable

8. Finalidad residual: Cualquier otra finalidad estrictamente necesaria, directamente relacionada y compatible con las aquí descritas, debidamente informada al titular.

Las disposiciones contenidas en los siguientes incisos aplican de manera transversal a todas las finalidades previstas en el presente artículo:

Las finalidades previstas en el presente artículo comprenden, de manera expresa, la gestión documental institucional y la incorporación de firmas autógrafas, huellas dactilares y demás datos personales o biométricos en registros institucionales únicos, incluidos registros colectivos, destinados a dejar constancia del conocimiento, notificación, aceptación, cumplimiento y trazabilidad de las actuaciones de LA EMPRESA.

Dichos registros se rigen por los principios de integridad documental, autenticidad, trazabilidad, conservación y valor probatorio definidos en la Política para **"PL-0020-GE: Política para el Manejo de los Documentos y Comunicaciones Institucionales"**, y constituyen soporte probatorio válido para la conservación de la historia laboral, contractual, formativa y disciplinaria, así como para la garantía de la seguridad jurídica de LA EMPRESA.

En consecuencia, la supresión individual de firmas, huellas o datos biométricos incorporados en dichos registros no será procedente cuando afecte la validez del documento, los derechos de terceros o el cumplimiento de obligaciones legales, contractuales o probatorias, por tratarse de datos que forman parte inseparable del documento y que no son técnica ni jurídicamente dissociables sin comprometer su integridad, validez y eficacia probatoria, conforme a los principios de integridad documental, autenticidad y valor probatorio reconocidos por la legislación civil, laboral y probatoria vigente.

PARÁGRAFO 1. Aceptación de finalidades y ejercicio de derechos del titular: Se entenderá que las finalidades aquí descritas han sido informadas y aceptadas por el titular con la autorización para el tratamiento de sus datos personales, sin perjuicio del derecho que le asiste de ejercer los derechos consagrados en la ley.

PARÁGRAFO 2. Tratamiento directo y a través de encargados del tratamiento: LA EMPRESA podrá realizar el tratamiento de los datos personales de manera directa o a través de terceros encargados, mediante contratos o convenios que garanticen el cumplimiento de esta política y de las normas de protección de datos personales.

ARTÍCULO 12. TRATAMIENTO DE DATOS EN SERVICIOS DE SOPORTE, MESA DE AYUDA Y CANALES DE ATENCIÓN MULTICANAL. En desarrollo de su objeto social y de la prestación de servicios de soporte técnico, atención al cliente y mesa de ayuda (helpdesk), a través de sus canales oficiales, institucionales y debidamente autorizados, LA EMPRESA podrá recolectar, tratar, almacenar, grabar, conservar y utilizar datos personales suministrados por los titulares mediante distintos canales de comunicación, tales como, sin limitarse a: líneas telefónicas institucionales, telefonía móvil corporativa, aplicaciones de mensajería instantánea autorizadas (incluido WhatsApp corporativo), correos electrónicos corporativos, chats, plataformas digitales, sistemas de tickets, videollamadas u otros medios tecnológicos presentes o futuros definidos oficialmente por LA EMPRESA.

El tratamiento de dichos datos tendrá, entre otras, las siguientes finalidades específicas:

- a) Atender, gestionar, documentar y dar solución a solicitudes de soporte técnico, incidencias, requerimientos, PQRS-F y comunicaciones relacionadas con los servicios prestados.
- b) Registrar, documentar y conservar las interacciones como soporte probatorio de la atención brindada, de las instrucciones recibidas y de las actuaciones realizadas.
- c) Garantizar la trazabilidad, calidad, continuidad y mejora del servicio.
- d) Servir como medio de prueba en procesos contractuales, administrativos, disciplinarios o judiciales.
- e) Cumplir obligaciones legales, contractuales y de seguridad de la información.

LA EMPRESA se reserva el derecho de redirigir o exigir que las solicitudes sean canalizadas exclusivamente por los medios y canales establecidos por la empresa, considerados: medios oficiales.

PARÁGRAFO 1. Grabación de llamadas: Las llamadas telefónicas realizadas o recibidas por LA EMPRESA a través de sus líneas institucionales o canales oficiales de atención en el marco de los servicios de soporte, atención o mesa de ayuda podrán ser grabadas, previo aviso de privacidad, con fines de calidad, seguridad, trazabilidad, control, soporte probatorio y cumplimiento legal.

El uso continuado del canal por parte del titular se entenderá como aceptación del tratamiento informado, cuando dicho tratamiento se encuentre amparado en una autorización previa, en una excepción legal a la autorización o en una relación contractual o legal vigente, sin perjuicio del ejercicio posterior de los derechos legales.

PARÁGRAFO 2. Mensajería instantánea: Los mensajes, audios, archivos, imágenes, capturas de pantalla y demás contenidos enviados voluntariamente por el titular a través de aplicaciones de mensajería instantánea autorizadas por LA EMPRESA serán tratados conforme a esta política y podrán ser conservados como parte del registro de atención, soporte técnico y evidencia probatoria.

Exclusión de responsabilidad por canales no oficiales: LA EMPRESA no asume responsabilidad por el tratamiento de datos personales que sean compartidos por los titulares a través de cuentas personales, números privados, correos electrónicos no institucionales o canales no oficiales, aun cuando correspondan a trabajadores, contratistas o terceros vinculados.

PARÁGRAFO 3. Evidencias técnicas: En el desarrollo del soporte técnico prestado por canales oficiales, LA EMPRESA podrá tratar datos visibles de manera incidental en capturas de pantalla, registros técnicos, logs o accesos temporales, limitando dicho tratamiento estrictamente a la finalidad de soporte, aplicando el principio de minimización de datos y las medidas de seguridad correspondientes.

ARTÍCULO 13. DERECHOS DEL TITULAR DE LOS DATOS PERSONALES:

- a) Conocer, actualizar, rectificar, cancelar y suprimir sus datos personales frente a los responsables o encargados del tratamiento, a través de los medios definidos y comunicados por LA EMPRESA.
- b) Solicitar prueba de la autorización a LA EMPRESA, como responsable del tratamiento.
- c) Solicitar a LA EMPRESA información sobre el uso que le ha dado a sus datos personales.
- d) Presentar ante la Superintendencia de Industria y Comercio, quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y demás disposiciones que lo reglamentan o complementan.
- e) Revocar la autorización y/o solicitar la supresión del dato cuando ello resulte procedente conforme a la ley, siempre que no exista un deber legal, contractual o probatorio que impida su eliminación.
- f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

PARÁGRAFO. Prueba de la autorización: La prueba de la autorización para el tratamiento de datos personales podrá constar en documentos físicos o electrónicos, mensajes de datos, grabaciones de voz, registros de aceptación por medios digitales, comunicaciones escritas, formularios electrónicos, registros de sistemas de información, o cualquier otro medio que permita demostrar de manera objetiva que el titular otorgó una autorización previa, expresa e informada, conforme a la ley, cuando ello resulte exigible conforme a la naturaleza del tratamiento y al rol asumido por LA EMPRESA.

ARTÍCULO 14. DEBERES DEL RESPONSABLE DEL TRATAMIENTO DE LOS DATOS PERSONALES: LA EMPRESA, en su calidad de responsable del tratamiento de datos personales, deberá cumplir, entre otros, los siguientes deberes:

- a) Garantizar en todo momento el pleno y efectivo ejercicio del derecho de hábeas data de los titulares.

- b) Solicitar, conservar y custodiar la autorización otorgada por el titular, cuando esta sea requerida conforme a la ley, en medios físicos o electrónicos que permitan su consulta posterior.
- c) Informar de manera clara, suficiente y oportuna al titular sobre las finalidades del tratamiento y los derechos que le asisten.
- d) Adoptar y mantener medidas técnicas, humanas y administrativas razonables para garantizar la seguridad, integridad, confidencialidad y disponibilidad de los datos personales, evitando su adulteración, pérdida, uso o acceso no autorizado.
- e) Garantizar que la información tratada sea veraz, completa, exacta, actualizada, comprobable y comprensible, y realizar oportunamente su actualización o rectificación cuando sea necesario.
- f) Garantizar mecanismos idóneos y efectivos para la atención de consultas, reclamos y solicitudes de los titulares, conforme a la ley y a esta política.
- g) Informar al titular, cuando este lo solicite, sobre el uso dado a sus datos personales.
- h) Exigir a los encargados del tratamiento el cumplimiento de las condiciones de seguridad, confidencialidad y protección de los datos personales, conforme a esta política y a la normativa vigente.
- i) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

ARTÍCULO 15. DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO: Los encargados del tratamiento de datos personales deberán cumplir los deberes establecidos en la Ley 1581 de 2012, el Decreto 1377 de 2013 y las normas que los modifiquen o sustituyan, así como las instrucciones impartidas por LA EMPRESA en su calidad de responsable del tratamiento, en especial en materia de seguridad, confidencialidad, atención de consultas y reclamos, y protección de los derechos de los titulares.

ARTÍCULO 16. OFICIAL DE PROTECCIÓN DE DATOS PERSONALES. El Oficial de Datos podrá ser la persona(s), área(s) o unidad(es) designada por **LA EMPRESA** quien en conjunto con la Gerencia y la Dirección de Talento Organizacional se apoyará para ejercer de manera formal la función de coordinar y controlar el cumplimiento de la Ley 1581 de 2012, las quejas, solicitudes o reclamos que los titulares formulen, son quienes deberán velar por la implementación efectiva de las políticas y procedimientos que se requieran para dar cumplimiento a la normatividad vigente, así como de las buenas prácticas de gestión de datos personales para lo cual establecerá los controles, evaluaciones y revisiones pertinentes.

PROCEDIMIENTO PARA CONSULTA, QUEJAS, RECLAMACIONES Y REVOCATORIAS DE AUTORIZACIONES

ARTÍCULO 17. ACCESO A LA INFORMACIÓN: LA EMPRESA garantiza el derecho de acceso a los datos personales de la siguiente forma:

- a) El titular del dato personal puede conocer la existencia del tratamiento a que son sometidos sus datos personales.
- b) El titular puede tener acceso a sus datos personales.
- c) El titular tiene derecho a conocer las circunstancias esenciales del tratamiento, lo cual se traduce en el deber de **LA EMPRESA** de informar al titular sobre el tipo de datos personales tratados, y todas y cada una de las finalidades que justifican el tratamiento.

ARTÍCULO 18. PERSONA / GRUPO RESPONSABLE / CANAL INSTITUCIONAL DE ATENCIÓN DE PETICIONES, CONSULTAS, RECLAMOS Y DENUNCIAS: Los titulares o sus causahabientes podrán ejercer sus derechos a través de los siguientes medios:

- a) Correos electrónicos: privacidad@saimyr.com.co
- b) Página web: <https://saimyr.co/politicas-de-tratamiento-de-datos/>
- c) Consulta telefónica: (+604) 444 65 60
- d) Físicos: Cl. 37 # 59 105 (Rionegro, Antioquia)

ARTÍCULO 19. TÉRMINO PARA LA ATENCIÓN DE CONSULTAS. Las consultas serán atendidas en un término máximo de diez (10) días hábiles, contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los diez (10) días, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.

ARTÍCULO 20. RECLAMOS. El titular de la información contenida en la base de datos, o quien lo represente legalmente, podrá solicitar a **LA EMPRESA** la corrección, actualización o supresión de sus datos personales; también podrá presentar reclamos cuando advierta el presunto incumplimiento de cualquiera de los deberes contenidos en la ley 1581 de 2012 o las normas que lo complementan, el cual será tramitado bajo las siguientes reglas:

- a) Si el reclamo recibido no cuenta con información completa que permita darle trámite, esto es: con la identificación del titular, la descripción de los hechos que dan lugar al reclamo, la dirección y acompañando los documentos que se quiera hacer valer, se requerirá al interesado dentro de los cinco (5) días hábiles siguientes a su recepción para que subsane las fallas. Si transcurridos dos (2) meses desde la fecha del requerimiento el solicitante no presenta la información requerida, se entenderá que ha desistido del reclamo.
- b) Si por alguna circunstancia quien recibe el reclamo no es el competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.
- c) Una vez recibido el reclamo completo, se incluirá en la base de datos con los siguientes datos: como "reclamo en trámite" y el motivo del mismo; así deberá mantenerse hasta que el reclamo sea resuelto.

ARTÍCULO 21. TÉRMINO PARA LA ATENCIÓN DE RECLAMOS. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atenderlo dentro de dicho término, se informará al interesado antes del vencimiento del referido plazo los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

ARTÍCULO 22. RECTIFICACIÓN, ACTUALIZACIÓN, CANCELACIÓN O SUPRESIÓN DE DATOS: El TITULAR de la información, puede ejercer en cualquier momento estos derechos, para esto deberá presentar la solicitud correspondiente, por medio de los canales descritos en el artículo 18, en caso de que esta sea formulada por persona distinta del titular y no se acredite que la misma actúa en representación de aquél, se tendrá por no presentada.

ARTÍCULO 23. SUPRESIÓN DE DATOS: La supresión de datos personales no implica la eliminación de documentos, registros o soportes probatorios institucionales, cuando estos deban conservarse por mandato legal, contractual, documental o probatorio.

No procede la solicitud de supresión de datos (parcial o total) cuando:

- a) Se tenga con el titular un deber legal o contractual de permanecer en la base de datos.
- b) Cuando se obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
- c) Cuando los datos sean necesarios para proteger los intereses jurídicamente tutelados del titular; para realizar una acción en función del interés público o para cumplir con una obligación legalmente adquirida por el titular.
- d) Formen parte del "**Registro de Conocimiento, Notificación y Aceptación**" de los documentos institucionales.
- e) Sean necesarios para la historia laboral.
- f) Tengan valor probatorio, disciplinario o contractual.

En estos casos, el ejercicio del derecho de supresión se entenderá limitado al tratamiento futuro del dato, sin afectar la conservación de los documentos, registros o evidencias que deban mantenerse por razones legales, contractuales, documentales o probatorias.

En ningún caso el ejercicio de los derechos del titular podrá interpretarse como una facultad para exigir la alteración, eliminación o desnaturalización de documentos institucionales válidamente constituidos.

ARTÍCULO 24. REVOCATORIA DE LA AUTORIZACIÓN: Los titulares de los datos personales pueden revocar total o parcialmente su consentimiento para el tratamiento de sus datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal o contractual.

Habrán casos en que el consentimiento, por su carácter necesario por la relación del titular con **LA EMPRESA**, no podrá ser revocado mientras subsistan obligaciones legales o contractuales que lo justifiquen.

ARTÍCULO 25. REQUISITOS PARA ATENDER CONSULTAS, QUEJAS O RECLAMOS: Para la atención de consultas, quejas o reclamos, se deberán tener en cuenta las siguientes condiciones:

- a) El nombre del titular y sus datos de contacto (correo electrónico y otros) para comunicarle la respuesta a su solicitud.
- b) Documentos que acrediten la identidad del titular o, en su defecto, los documentos que lo acrediten como representante legal del titular.
- c) La descripción clara y precisa del motivo de consulta o inconformidad y los datos o registros respecto de los que se busca ejercer alguno de los derechos antes mencionados.
- d) Elementos o documentos que faciliten la localización de los datos personales. Para el caso de las solicitudes de rectificación de información, el titular deberá indicar las modificaciones a realizarse y aportar la documentación que sustente su petición.

PARÁGRAFO: El procedimiento para la atención de las consultas, quejas y reclamos, se realiza a través de los canales que disponga **LA EMPRESA**.

CAPTURA DE IMÁGENES POR CÁMARAS DE VIDEOVIGILANCIA

ARTÍCULO 26. TRATAMIENTO DE DATOS PERSONALES EN SISTEMAS DE VIDEOVIGILANCIA. LA EMPRESA, en su calidad de responsable del tratamiento, informa que, con el fin de garantizar la seguridad de las personas, bienes, instalaciones, activos de información, procesos y operaciones, podrá utilizar sistemas de videovigilancia en sus sedes, oficinas, centros de trabajo, áreas comunes, zonas de acceso y demás espacios debidamente señalizados.

La existencia de estos mecanismos será informada mediante avisos visibles de videovigilancia, los cuales indicarán, como mínimo, la existencia de cámaras, la finalidad del tratamiento, la identificación del responsable del tratamiento y el medio para consultar la Política de Tratamiento de la Información. Dichos avisos serán ubicados de manera estratégica para su fácil identificación.

Las imágenes y grabaciones obtenidas a través de los sistemas de videovigilancia tendrán, entre otras, las siguientes finalidades:

- a) Garantizar la seguridad de empleados, contratistas, clientes, proveedores y visitantes.
- b) Proteger los bienes, instalaciones, infraestructura tecnológica y activos de información de LA EMPRESA.
- c) Prevenir, detectar, investigar y documentar incidentes de seguridad, conductas irregulares, accesos no autorizados o hechos que puedan afectar a LA EMPRESA o a terceros.
- d) Servir como soporte probatorio en procesos administrativos, disciplinarios, contractuales, laborales, judiciales o extrajudiciales, conforme al Reglamento Interno de Trabajo y la normatividad aplicable, cuando resulte estrictamente necesario y proporcional.

- e) Dar cumplimiento a obligaciones legales, reglamentarias y a políticas internas de seguridad y control.

Las imágenes y grabaciones no serán utilizadas para fines distintos a los aquí previstos, ni para el monitoreo permanente del desempeño laboral, salvo cuando constituyan evidencia necesaria en procesos disciplinarios, de seguridad o judiciales, siempre que exista una causa objetiva, proporcional y debidamente justificada conforme a la ley.

LA EMPRESA adoptará las medidas técnicas, humanas y administrativas necesarias para garantizar la confidencialidad, integridad, disponibilidad y seguridad de las imágenes, restringiendo el acceso exclusivamente a personal autorizado y conservándolas únicamente por el tiempo necesario para cumplir las finalidades descritas o el exigido por la ley.

Las imágenes y grabaciones obtenidas a través de sistemas de video vigilancia se conservarán por el período prudencial que determine LA EMPRESA, sin embargo, si dichas imágenes son requeridas como evidencia o soporte en reclamaciones, quejas o procesos administrativos o judiciales, se mantendrán hasta la resolución definitiva de la controversia.

PARÁGRAFO 1. Zonas excluidas: Los sistemas de videovigilancia no serán instalados ni utilizados en áreas en las que prime la intimidad del titular, tales como baños, vestidores, zonas de lockers u otros espacios de naturaleza similar.

PARÁGRAFO 2. Transmisión de datos personales: Las imágenes y registros obtenidos a través de los sistemas de videovigilancia podrán ser transmitidos a encargados del tratamiento, proveedores de servicios tecnológicos o autoridades competentes, cuando sea necesario para el cumplimiento de las finalidades descritas, obligaciones legales o requerimientos administrativos o judiciales, siempre que dicha transmisión se encuentre amparada en un contrato, acuerdo o instrumento jurídico que garantice el cumplimiento de la presente política y de la normativa vigente.

PARÁGRAFO 3. Control por el Oficial de Protección de Datos Personales: Las transmisiones de datos personales derivadas de los sistemas de videovigilancia podrán ser registradas, documentadas y puestas en conocimiento del Oficial de Protección de Datos Personales de LA EMPRESA, con fines de control, seguimiento, evaluación de riesgos y verificación del cumplimiento del principio de responsabilidad demostrada.

TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

ARTÍCULO 27. TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES. LA EMPRESA podrá realizar la transferencia y/o transmisión de datos personales a terceros, dentro o fuera del territorio nacional, cuando ello resulte necesario para el cumplimiento de su objeto social, la ejecución de relaciones contractuales o precontractuales, el desarrollo de sus operaciones, la prestación de servicios, el cumplimiento de obligaciones legales o la defensa de sus intereses, siempre en observancia de la Ley 1581 de 2012, el Decreto 1074 de 2015 y demás normas que los modifiquen o sustituyan.

En particular, LA EMPRESA podrá transferir datos personales en los siguientes supuestos:

- a) Cuando el titular haya otorgado su autorización previa, expresa e inequívoca para la transferencia.
- b) Cuando la transferencia se encuentre establecida o determinada en tratados internacionales en los que el Estado Colombiano sea parte, con fundamento en el principio de reciprocidad.
- c) Cuando la transferencia sea necesaria para el desarrollo de un contrato celebrado entre el titular y LA EMPRESA, o para la ejecución de medidas precontractuales solicitadas por el titular, siempre que se cuente con la autorización correspondiente o que la ley la permita.
- d) Cuando la transferencia sea legalmente exigida para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, administrativo o arbitral.

La transferencia o transmisión de datos personales se realizará únicamente para las finalidades autorizadas por el titular o permitidas por la ley, garantizando en todo momento el respeto de los principios de legalidad, finalidad, necesidad, proporcionalidad, seguridad y confidencialidad.

En todo caso, LA EMPRESA exigirá que la transferencia o transmisión de datos personales se encuentre amparada en un contrato, acuerdo o instrumento jurídico vinculante, en el cual se establezcan de manera expresa las obligaciones del tercero respecto al tratamiento de los datos, la adopción de medidas técnicas, humanas y administrativas adecuadas, y la prohibición de utilizar la información para fines distintos a los autorizados.

La transmisión no implicará en ningún caso cambio de responsable del tratamiento, el cual permanecerá en cabeza de LA EMPRESA

PARÁGRAFO. Control y reporte de transmisiones de datos personales: Toda transmisión de datos personales que realice LA EMPRESA a encargados del tratamiento, ubicados dentro o fuera del territorio nacional, deberá encontrarse amparada en un contrato, acuerdo o instrumento jurídico que garantice el cumplimiento de la presente política y de la normatividad vigente.

Así mismo, dichas transmisiones podrán ser registradas, documentadas y puestas en conocimiento del Oficial de Protección de Datos Personales de LA EMPRESA, con el fin de ejercer funciones de control, seguimiento, evaluación de riesgos y verificación del cumplimiento del principio de responsabilidad demostrada.

ARTÍCULO 28. TRANSMISIÓN DE DATOS PERSONALES A TERCEROS EN EL DESARROLLO DE LAS OPERACIONES: En desarrollo de sus actividades y operaciones, LA EMPRESA podrá transmitir datos personales a terceros que actúen en calidad de encargados del tratamiento, tales como proveedores de servicios tecnológicos, plataformas de información, sistemas de soporte, servicios en la nube, servicios de seguridad, firmas de auditoría, asesores profesionales, aliados estratégicos u otros terceros que resulten necesarios para la ejecución de su objeto social.

Dicha transmisión se realizará exclusivamente para el cumplimiento de las finalidades autorizadas, conforme a lo dispuesto en el Artículo 27 de la presente política, y bajo las instrucciones de LA EMPRESA, sin que los terceros puedan utilizar la información para fines distintos ni asumir la calidad de responsables del tratamiento.

Los terceros que actúen como encargados del tratamiento deberán garantizar la adopción de medidas técnicas, humanas y administrativas adecuadas para la protección de los datos personales, así como el cumplimiento de los principios de confidencialidad, seguridad y responsabilidad demostrada.

PARÁGRAFO 1. Plataformas tecnológicas y servicios en la nube: Cuando la transmisión de datos personales implique el uso de plataformas tecnológicas, aplicaciones, sistemas de información o servicios en la nube, LA EMPRESA verificará que dichos proveedores ofrezcan niveles adecuados de seguridad de la información y protección de datos personales, sin perjuicio de las obligaciones contractuales correspondientes.

PARÁGRAFO 2. Prohibición de uso autónomo de la información: Los encargados del tratamiento no podrán subcontratar, ceder, transferir ni reutilizar los datos personales transmitidos, salvo autorización expresa y previa de LA EMPRESA o disposición legal en contrario.

PARÁGRAFO 3. Control interno: Las transmisiones de datos personales realizadas en desarrollo del presente artículo podrán ser registradas, documentadas y puestas en conocimiento del Oficial de Protección de Datos Personales, en los términos previstos en el Artículo 27 de la presente política.

ARTÍCULO 29. VIGENCIA DE LAS BASES DE DATOS: La información personal contenida en las bases de datos de LA EMPRESA será conservada durante el tiempo que sea necesario para

cumplir las finalidades para las cuales fue recolectada, y posteriormente por el término que exijan las disposiciones legales, documentales, contractuales, contables, probatorias o administrativas aplicables, de acuerdo con el tipo de relación o vinculación con el titular.

El ejercicio del derecho de supresión procederá únicamente cuando no exista un deber legal, contractual o probatorio que obligue a LA EMPRESA a conservar dicha información, conforme a lo dispuesto en la Ley 1581 de 2012.

ARTÍCULO 30. TEMPORALIDAD DEL TRATAMIENTO DEL DATO. Los datos personales serán tratados y conservados únicamente durante el tiempo que resulte razonablemente necesario para cumplir las finalidades para las cuales fueron recolectados, atendiendo a la naturaleza del dato, la finalidad del tratamiento y las obligaciones legales, contractuales, administrativas, contables o judiciales a cargo de LA EMPRESA.

En todo caso, los datos personales podrán conservarse por un período adicional cuando sea necesario para:

- a) El cumplimiento de obligaciones legales o regulatorias.
- b) La ejecución, desarrollo, terminación y liquidación de relaciones contractuales o laborales.
- c) La atención de requerimientos de autoridades competentes.
- d) La defensa judicial, administrativa o extrajudicial de los intereses de LA EMPRESA.
- e) El cumplimiento de términos de prescripción legal de acciones.

Una vez desaparecida la finalidad que dio origen al tratamiento y siempre que no exista un deber legal o contractual que exija su conservación, los datos personales serán suprimidos, anonimizados o bloqueados, según corresponda, sin perjuicio del ejercicio de los derechos de revocatoria o supresión por parte del titular, cuando estos resulten procedentes conforme a la ley.

AVISO DE PRIVACIDAD

ARTÍCULO 31. AVISO DE PRIVACIDAD. El aviso de privacidad es la comunicación breve mediante la cual LA EMPRESA informa a los titulares la existencia del tratamiento de sus datos personales, las finalidades del mismo, los derechos que les asisten y el medio para consultar la Política de Tratamiento de Datos Personales.

LA EMPRESA podrá publicar y difundir el aviso de privacidad a través de medios físicos o electrónicos, tales como la cartelera institucional, avisos visibles en las instalaciones, formularios físicos o digitales, plataformas internas, correos electrónicos o mediante su página web oficial, indicando de forma clara la dirección URL donde se encuentre disponible la Política de Tratamiento de Datos Personales.

LA EMPRESA podrá modificar, revisar o actualizar la presente política en cualquier momento. Dichos cambios serán informados a los titulares mediante la actualización del aviso de privacidad, a través de los medios antes señalados, de manera oportuna.

El Anexo 1 de la presente política contiene el modelo de Aviso de Privacidad, el cual será utilizado por LA EMPRESA como mecanismo de información a los titulares, de conformidad con la Ley 1581 de 2012 y normas concordantes.

MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES SENSIBLES, BIOMÉTRICOS Y AUDIOVISUALES

ARTÍCULO 32. ALCANCE DE LAS MEDIDAS DE SEGURIDAD: Las disposiciones del presente capítulo establecen las medidas técnicas, humanas y administrativas para la protección de los datos personales,

incluidos los datos sensibles de carácter biométrico y audiovisual, tratados por LA EMPRESA, con el fin de evitar su adulteración, pérdida, consulta, uso, circulación o acceso no autorizado o fraudulento.

Estas medidas serán de obligatorio cumplimiento para todo trabajador, contratista o tercero que, por razón de sus funciones, tenga acceso directo o indirecto a dicha información.

DOCUMENTOS FÍSICOS CON FIRMA AUTÓGRAFA Y/O HUELLA DACTILAR:

ARTÍCULO 33. TRATAMIENTO DE DOCUMENTOS FÍSICOS CON DATOS BIOMÉTRICOS: Los documentos físicos que contengan firmas autógrafas, huellas dactilares u otros datos biométricos se clasificarán como documentos sensibles de alta protección, y estarán sujetos a medidas reforzadas de custodia, acceso, circulación, consulta y conservación, en atención a los riesgos asociados a la exposición, copia o uso indebido de dichos datos.

ARTÍCULO 34. REGISTRO, CIRCULACIÓN Y CONSULTA DE DOCUMENTOS FÍSICOS SENSIBLES: Los documentos físicos que contengan firmas autógrafas y/o huellas dactilares se regirán por las siguientes reglas obligatorias:

- a) La impresión, estampado o registro de la firma y/o huella solo podrá realizarse en presencia del responsable de la custodia del documento, de la persona que realizó la socialización o administración del mismo, o de quien esta delegue expresamente.
- b) La consulta de estos documentos únicamente podrá efectuarse en presencia del responsable de su custodia, de la persona que socializó o administró el documento, o de quien esta delegue.
- c) Se prohíbe su circulación libre, tanto dentro como fuera de LA EMPRESA.
- d) Se prohíbe de manera expresa su reproducción, copia, fotografía, escaneo o captura, por cualquier medio, sin autorización previa, expresa y escrita del responsable autorizado.
- e) Toda consulta deberá realizarse exclusivamente para fines legítimos, necesarios y previamente autorizados, conforme a la finalidad del documento y a la normatividad vigente.

Estas medidas tienen como finalidad evitar que, por circulación indebida, descuido o falta de supervisión, los datos sensibles puedan ser fotografiados, copiados, escaneados o reutilizados sin autorización.

ARTÍCULO 35. CUSTODIA Y ARCHIVO DE DOCUMENTOS FÍSICOS SENSIBLES: Los documentos físicos que contengan firmas autógrafas, huellas dactilares u otros datos biométricos deberán cumplir, como mínimo, con las siguientes medidas de custodia:

- a) Ser archivados y conservados en muebles, archivadores o contenedores cerrados bajo llave.
- b) Permanecer bajo la custodia directa de la Dirección de Talento Organizacional, o de quien esta delegue expresamente y por escrito.
- c) No estar disponibles ni accesibles en áreas de acceso público, común o no controlado.
- d) Contar, cuando aplique, con un registro de control de acceso, que permita identificar las consultas realizadas.
- e) Cuando sea necesaria la consulta por parte de un tercero autorizado, esta deberá realizarse de manera obligatoria en presencia del responsable de la custodia.

ARTÍCULO 36. DIGITALIZACIÓN DE DOCUMENTOS FÍSICOS CON FIRMA Y/O HUELLA: Cuando resulte necesario digitalizar documentos físicos que contengan firmas autógrafas y/o huellas dactilares, se aplicarán de manera estricta las siguientes reglas:

- a) La digitalización se realizará únicamente para fines administrativos, probatorios, de respaldo o conservación, conforme a las finalidades autorizadas.
- b) Cuando el archivo digital incluya firmas, huellas u otros datos biométricos —ya sea como respaldo, histórico o prueba— este deberá:

- ✓ Estar protegido con mecanismos de seguridad digital, como contraseña o cifrado.
 - ✓ Ser almacenado en un repositorio seguro de acceso restringido, limitado exclusivamente a la Dirección de Talento Organizacional o a quien esta delegue expresamente.
- c) Cuando el documento digitalizado esté destinado a consulta pública o a circulación interna o externa, no deberán incluirse las páginas o secciones que contengan firmas, huellas o datos biométricos, salvo que su inclusión sea estrictamente necesaria por razones legales o probatorias.

En estos casos excepcionales, las firmas y huellas deberán ser enmascaradas, cubiertas, ocultadas o pixeladas, garantizando que no puedan ser reproducidas, copiadas o reutilizadas.

- d) El documento físico original, o el archivo digital íntegro que contenga la firma y/o huella, conservará pleno valor probatorio y será considerado el respaldo principal del registro.

MEDIDAS SOBRE REGISTROS DIGITALES, BIOMÉTRICOS Y AUDIOVISUALES

ARTÍCULO 37. ACCESO A REGISTROS DIGITALES SENSIBLES: El acceso a bases de datos, sistemas, repositorios o plataformas que contengan datos personales sensibles estará sujeto a:

- a) Perfiles de usuario diferenciados, según funciones.
- b) Credenciales personales e intransferibles.
- c) Principio de mínimo privilegio (solo acceso a lo estrictamente necesario).
- d) Registro de accesos, cuando sea técnicamente viable.

ARTÍCULO 38. ALMACENAMIENTO Y CONSERVACIÓN DE REGISTROS BIOMÉTRICOS Y AUDIOVISUALES: Los registros biométricos (huella digital, firma digitalizada) y audiovisuales (videograbaciones, imágenes, audios):

- a) Serán almacenados en medios seguros, físicos o electrónicos.
- b) No podrán ser almacenados en dispositivos personales no autorizados.
- c) Deberán contar con mecanismos de respaldo y control de integridad.
- d) Serán conservados únicamente por el tiempo necesario según su finalidad y obligaciones legales.

ARTÍCULO 39. PROHIBICIONES EXPRESAS: Se prohíbe expresamente:

- a) El uso de firmas, huellas o registros biométricos para fines distintos a los autorizados.
- b) La reproducción, reutilización o transferencia no autorizada de datos biométricos.
- c) El envío de este tipo de información por medios no seguros.
- d) La captura de imágenes, audios o videos sin autorización previa cuando aplique.

RESPONSABILIDADES Y CONTROL

ARTÍCULO 40. RESPONSABILIDAD EN LA APLICACIÓN DE LAS MEDIDAS: La responsabilidad por la aplicación, control y cumplimiento de las medidas previstas en el presente capítulo recaerá en el responsable y/o encargado del tratamiento, según corresponda, sin perjuicio de las responsabilidades individuales derivadas de usos indebidos o negligentes.

ARTÍCULO 41. INCUMPLIMIENTO: El incumplimiento de las disposiciones de este capítulo constituirá una falta grave a las políticas internas de LA EMPRESA y dará lugar a las acciones disciplinarias, contractuales, administrativas o legales correspondientes.

ARTÍCULO 42. INCIDENTES DE SEGURIDAD: se consideran incidentes de seguridad, sin limitarse a, los siguientes:

- a) El acceso, consulta, visualización, uso o divulgación de información sin autorización o excediendo los permisos otorgados.
- b) La pérdida, extravío, robo o hurto de documentos físicos, dispositivos, equipos, medios de almacenamiento o credenciales que contengan o permitan acceder a información protegida.
- c) La copia, reproducción, descarga, transferencia, envío o almacenamiento de información por medios no autorizados, incluidos correos personales, dispositivos externos, nubes públicas o herramientas de inteligencia artificial no aprobadas por LA EMPRESA.
- d) La alteración, destrucción, eliminación, corrupción o modificación no autorizada de información o registros.
- e) El uso de contraseñas compartidas, débiles, expuestas o comprometidas, así como la suplantación de identidad digital.
- f) La captura no autorizada de imágenes, videos, audios, firmas, huellas o cualquier otro dato biométrico o audiovisual.
- g) La divulgación verbal, escrita, gráfica o visual de información confidencial a personas no autorizadas, incluso de manera informal o negligente.
- h) El acceso a información por error, exceso de permisos o fallas de control, aun cuando no se haya hecho uso posterior de la misma.
- i) Cualquier falla, vulnerabilidad, amenaza, intento de intrusión, malware, phishing, ransomware o evento tecnológico que afecte o pueda afectar la seguridad de la información.
- j) La omisión de reportar oportunamente cualquiera de los eventos anteriores.

La ocurrencia o sospecha de un Incidente de Seguridad deberá ser reportada de manera inmediata a LA EMPRESA, conforme a los canales y procedimientos internos establecidos, sin que sea necesario que el daño se haya materializado.

LA EMPRESA mantendrá en reserva la información de sus bases de datos confidenciales.

(Pasa a la siguiente página).

ANEXO 1

AVISO DE PRIVACIDAD

SAIMYR S.A.S., en adelante **LA EMPRESA**, informa que, en desarrollo de sus actividades, realiza el tratamiento de datos personales de trabajadores, exempleados, candidatos, clientes, proveedores, contratistas, visitantes y demás grupos de interés, conforme a la Ley 1581 de 2012 y normas concordantes.

Los datos personales recolectados podrán incluir datos de identificación, contacto, laborales, académicos, biométricos, imágenes, audios y demás información necesaria, y serán tratados para finalidades administrativas, laborales, contractuales, comerciales, formativas, de seguridad, control de acceso, cumplimiento normativo, gestión documental y soporte probatorio.

El tratamiento de datos sensibles se realizará con observancia de las garantías legales y únicamente cuando sea estrictamente necesario.

Los titulares podrán ejercer sus derechos de conocer, actualizar, rectificar y solicitar la supresión de sus datos personales, así como revocar la autorización, conforme a la Política de Tratamiento de Datos Personales de LA EMPRESA, disponible en:

<https://saimyr.co/politicas-de-tratamiento-de-datos>

Para mayor información sobre el tratamiento de sus datos y el ejercicio de derechos, podrá consultar los canales de atención definidos en dicha política.

(Pasa a la siguiente página).



**POLÍTICA DE TRATAMIENTO DE INFORMACIÓN Y
PROTECCIÓN DE LOS DATOS PERSONALES,
BIOMÉTRICOS Y AUDIOVISUALES**

Código: PL-0010-GE
Versión: 2.0
13-Feb-2026
Dominio: USO PÚBLICO
Página 24 de 40

Esta política de tratamiento de información y protección de los datos personales, biométricos y audiovisuales reemplaza la anterior; ha sido elaborada, revisada, conocida, aceptada y aprobada integralmente, en representación de **LA EMPRESA** a los 13 días del mes febrero del año 2026, por:

Nombre:	Juan Felipe Isaza Arango	Firma y huella
Cargo:	Gerente	
Fecha:		

Nombre:	Yaritza María Marín Ocampo	Firma y huella
Cargo:	Directora de Talento Organizacional	
Fecha:		

Nombre:	Yamilacé Hernández Ríos	Firma y huella
Cargo:	Directora de Relacionamento	
Fecha:		

Nombre:	Carlos Andrés Álvarez Mejía	Firma y huella
Cargo:	Líder de Desarrollo	
Fecha:		

Nombre:	Daniela Espinosa Noreña	Firma y huella
Cargo:	Líder de Mesa de Ayuda	
Fecha:		

Nombre:	Yudy Alexandra Valencia Noreña	Firma y huella
Cargo:	Coordinadora de Sala	
Fecha:		

Nombre:	Reined de Jesús Hernández Agudelo	Firma y huella
Cargo:	Coordinador de Sala	
Fecha:		

Registro de Conocimiento, Notificación y Aceptación

Las firmas autógrafas y, cuando aplique, las huellas dactilares de la(s) persona(s) aquí consignada(s), constituyen autorización expresa, previa e informada para el tratamiento de sus datos personales y datos sensibles de carácter biométrico, conforme a las finalidades previstas en la Política "**PL-0010-GE: Política de Tratamiento de Información y Protección de los Datos Personales, Biométricos y Audiovisuales**" y en la autorización "**FO-0010-GE: Autorización para el Tratamiento de Datos Personales, Biométricos y Audiovisuales**" de LA EMPRESA, documentos que declara conocer, haber recibido, leído, comprendido y aceptado en su totalidad, entendiendo que dichos datos forman parte inseparable del documento, y que la supresión individual de los datos del titular no será procedente en aquellos eventos en que dicha supresión no resulte legalmente exigible, por afectar la integridad, validez, o eficacia probatoria del registro, los derechos de terceros o el cumplimiento de obligaciones legales, contractuales o probatorias de LA EMPRESA.

Cada persona declara, bajo la gravedad del juramento y con pleno conocimiento de sus efectos legales, que su consentimiento ha sido otorgado de manera libre, voluntaria, informada y sin vicio alguno, y que tuvo la oportunidad de formular preguntas y solicitar las aclaraciones que estimó necesarias.

Cada persona autoriza expresamente que el presente registro sea utilizado como medio de prueba en actuaciones internas, disciplinarias (cuando aplique), administrativas o judiciales, y que, en el caso de trabajadores, sea incorporado al expediente laboral, contractual, administrativo o documental que corresponda; en consecuencia, la falta de lectura, el desconocimiento posterior, la omisión o la interpretación personal de su contenido no eximen a ninguna persona de su cumplimiento ni de las responsabilidades legales, contractuales, administrativas o disciplinarias que puedan derivarse, de acuerdo con la naturaleza de la relación jurídica con LA EMPRESA y la normatividad vigente.

La negativa la(s) persona(s) aquí consignada(s) a firmar y/o registrar su huella dactilar no suspende ni invalida la vigencia u obligatoriedad del presente documento, salvo imposibilidad física, médica o legal debidamente acreditada. En tales casos, LA EMPRESA dejará constancia escrita mediante el diligenciamiento del documento "**FO-0001-GE: Constancia de Negativa o Imposibilidad de Firma**", el cual será archivado como evidencia de la notificación y puesta en conocimiento.

Lo anterior se entenderá igualmente aplicable cuando la notificación, aceptación o autorización se realice mediante medios electrónicos oficiales, conforme a los términos y condiciones definidos en la Política "**PL-0020-GE: Política para el Manejo de los Documentos y Comunicaciones Institucionales**".

Funcionario responsable de la socialización y notificación		FIRMADO EN DOCUMENTO ORIGINAL
Nombre:		
Cargo:		
Fecha:		
		Firma y huella

NOTA ACLARATORIA: En caso de que la(s) persona(s) aquí consignada(s) asista(n) a la socialización de manera virtual, el responsable de la socialización deberá diligenciar los campos: "Virtual" (indicando Sí), "# Dcto. Id" y "Nombre", como constancia de dicha asistencia. La firma, fecha y huella dactilar, cuando sean exigibles conforme a la naturaleza del documento, deberán ser diligenciadas posteriormente, una vez la(s) persona(s) aquí consignada(s) se presente(n) de manera presencial ante LA EMPRESA.

#	Virtual	# Dcto. Id.	Nombre	Fecha	Firma y Huella
1.					