

Contenido

POLITICA DE PRIVACIDAD, TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES	3
1. OBJETIVO.....	3
2. ALCANCE.....	3
3. RESPONSABLE DEL TRATAMIENTO DE DATOS.....	3
4. DESTINATARIOS DE LA POLÍTICA DE TRATAMIENTO DE DATOS.....	3
5. DISPOSICIONES NORMATIVAS.....	4
6. DEFINICIONES.....	4
7. OBLIGACIONES.....	6
8. ESTRUCTURA ADMINISTRATIVA SOBRE PROTECCIÓN Y TRATAMIENTO DE DATOS.....	6
8.1 Órgano Superior del SGSDP	6
8.2 Responsables de Áreas Claves del SGSDP:.....	7
8.2.1 Responsable de Base Documental, es el Trabajador que maneja y/o administra bases de datos.....	7
8.2.2 Responsable de Cumplimiento Legal, asesor jurídico de INSURCOL y/o abogado de INSURCOL:	7
8.3 Responsable de TIC, será el Ingeniero de Sistemas, para las tareas administrativas y documentales, contará con el apoyo del Ingeniero Informático.....	7
8.4 Responsable de Locaciones Físicas/ Ingeniero de sistemas:.....	7
9. TRATAMIENTO Y FINALIDAD DE LAS BASES DE DATOS.....	7
9.1 Tratamiento de Datos de Clientes.....	8
9.2 Tratamiento de Datos de Proveedores.....	9
9.3 Tratamiento de Datos de Trabajadores.....	10
9.4 Tratamiento de Datos de Accionistas.....	12
9.5 Tratamiento de Datos de Contratistas.....	13
9.6 Tratamiento de Datos de Aspirantes a Trabajadores.....	14
9.7 Tratamiento de Datos de Visitantes.....	15
9.8 Tratamiento de Datos de la Comunidad.....	16
9.9 Tratamiento de Datos de Extrabajadores.....	17
10. ATENCIÓN DE CONSULTAS, QUEJAS Y RECLAMOS DEL TITULAR DE LA INFORMACIÓN	19
10.1 Procedimientos para la recepción y resolución de consultas y reclamos.....	20
10.1.1 Opciones para presentar la consulta:.....	20
10.1.1.1 Presencial:.....	20
10.1.1.2 Escrita:	20
10.1.1.3 Digital:.....	20
10.1.2 Plazo de Respuesta:.....	20
10.2 Procedimientos para reclamos.....	20
10.2.1 Requisitos del Reclamo:.....	21
10.2.2 Proceso de Trámite del Reclamo:.....	21

10.3	Procedimiento para Supresión de Almacenamiento de Datos Personales en Físicos:	21
11	REQUISITO DE PROCEDIBILIDAD:	21
12	CASOS EN LOS QUE, NO ES NECESARIA LA AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES:	22
13	AUTORIZACIÓN PARA TRATAMIENTO DE DATOS SENSIBLES:	22
13.1	Autorización para tratamiento de datos de niños, niñas y adolescentes (NNA):	22
14	PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES:	22
14.1	PRINCIPIOS RELACIONADOS CON LA RECOLECCIÓN DE DATOS PERSONALES:	22
14.2	PRINCIPIOS GENERALES PARA LA RECOLECCIÓN DE DATOS:	23
14.2.1	PRINCIPIO DE DIGNIDAD:	23
14.3	PRINCIPIOS RELACIONADOS CON EL USO DE DATOS PERSONALES:	23
14.3.1	PRINCIPIO DE LEGALIDAD:	23
14.3.2	PRINCIPIO DE LIBERTAD:	24
14.4	PRINCIPIOS RELACIONADOS CON LA CALIDAD DE LA INFORMACIÓN:	24
14.4.1	PRINCIPIO DE INTEGRIDAD:	24
14.5	PRINCIPIOS RELACIONADOS CON LA PROTECCIÓN, EL ACCESO Y CIRCULACIÓN DE DATOS PERSONALES:	24
14.6	PRINCIPIOS RELACIONADOS CON LA TRANSFERENCIA Y TRANSMISIÓN DE DATOS:	24
15	ALMACENAMIENTO DE DATOS PERSONALES:	25
16	MEDIDAS DE SEGURIDAD: INSURCOL:	25
17	DERECHOS DE LOS TITULARES: INSURCOL:	25
18	MEDIDAS DE PREVENCIÓN PARA GARANTIZAR LOS PRINCIPIOS BÁSICOS DE LA INFORMACIÓN:	26
19	TRATAMIENTO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:	26
20	PROCEDIMIENTO PARA EL EJERCICIO DEL DERECHO DE HABEAS DATA:	26
21	VIGENCIA:	27
22	CAMBIOS EN LA POLÍTICA DE PRIVACIDAD:	27
23	LEGISLACIÓN VIGENTE:	27

POLÍTICA DE PRIVACIDAD, TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

INSURCOL SAS, persona jurídica identificada con Nit. 800.042.972-6, con domicilio en la Calle 41 No 21-32 barrio Bolívar, Bucaramanga, Santander, y constituida de conformidad con las leyes de la República de Colombia, establece la presente política de tratamiento de datos personales en cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios, incluyendo el Decreto 1377 de 2013, el Decreto 886 de 2014 y la Circular 003 de 2024 de la SIC.

1. OBJETIVO

Establecer las directrices y procedimientos que regulan la recolección, almacenamiento, uso, circulación, transferencia y supresión de los datos personales gestionados por INSURCOL SAS, garantizando el respeto por los derechos fundamentales de los titulares y el cumplimiento de la normativa aplicable. Asimismo, esta política integra principios de cultura de calidad, conducta ética, sostenibilidad, gestión del conocimiento y fortalecimiento de la seguridad de la información, así como la identificación, evaluación y control de riesgos tecnológicos, reputacionales y de ciberseguridad asociados al tratamiento de datos personales.

2. ALCANCE

Esta política aplica a todas las bases de datos y archivos físicos y digitales que contengan información personal recolectada, almacenada, utilizada, procesada o compartida por INSURCOL SAS, en el ejercicio de su objeto social.

INSURCOL SAS, se compromete a implementar medidas técnicas, administrativas y organizativas que garanticen la seguridad y confidencialidad de los datos personales, conforme a la Ley 1581 de 2012, el Decreto 1377 de 2013, el Decreto 886 de 2014 y demás disposiciones reglamentarias. A su mismo, en cumplimiento de la Circular 003 de 2024 de la SIC, la empresa mantendrá actualizadas sus bases de datos en el RNBD y facilitará a los titulares el ejercicio de sus derechos.

Al otorgar su autorización para el tratamiento de datos personales, el titular acepta los términos y condiciones establecidos en la presente política.

INSURCOL SAS respeta y protege la privacidad de los datos personales proporcionados por clientes, empleados, aspirantes a trabajar, proveedores, accionistas, visitantes y demás grupos de interés. Esta política define las finalidades del tratamiento, las medidas de protección y los mecanismos para que los titulares puedan conocer, actualizar, rectificar, suprimir sus datos o revocar la autorización otorgada.

3. RESPONSABLE DEL TRATAMIENTO DE DATOS.

El responsable del tratamiento de datos personales es **INSURCOL SAS**, identificada con NIT. 800042972-6, quien actúa como responsable del manejo, almacenamiento y protección de la información personal recolectada en el ejercicio de su actividad:

- a. Domicilio principal: Bucaramanga
- b. Dirección: Calle 41 No 21-32
- c. Correo electrónico: datospersonales@insurcol.com
- d. Número de teléfono: 300 2052430
- e. Página web: www.insurcol.com

4. DESTINATARIOS DE LA POLÍTICA DE TRATAMIENTO DE DATOS.

La presente política está dirigida a todas las personas naturales cuyos datos personales se encuentran en las bases de datos de **INSURCOL SAS**, incluyendo, pero sin limitarse a, clientes, empleados, aspirantes a trabajador, proveedores, contratistas, accionistas, aliados comerciales y cualquier otra persona con la que la empresa tenga una relación comercial, laboral o contractual.

Asimismo, esta política es de cumplimiento obligatorio para todos los empleados, directivos y terceros que tengan acceso a información personal en calidad de responsables, encargados o colaboradores, garantizando el cumplimiento de las disposiciones legales sobre protección de datos.

La presente política está dirigida a todas las personas naturales cuyos datos personales se encuentran en las bases de datos de INSURCOL SAS, incluyendo, pero sin limitarse a, clientes, empleados, aspirantes a trabajador,

proveedores, contratistas, accionistas, aliados comerciales y cualquier otra persona con la que la empresa tenga una relación comercial, laboral o contractual.

Asimismo, esta política es de cumplimiento obligatorio para todos los empleados, directivos y terceros que tengan acceso a información personal en calidad de responsables, encargados o colaboradores, garantizando el cumplimiento de las disposiciones legales sobre protección de datos, así mismo esta política también se dirige a todas las partes interesadas internas y externas que, directa o indirectamente, puedan influir en el tratamiento de los datos personales o verse afectadas por él. Esto incluye a entidades y personas involucradas en procesos asociados a tecnologías de la información, digitalización, ciberseguridad y gestión del conocimiento, así como a aliados estratégicos que participan en la cadena de valor o en actividades que comportan riesgos tecnológicos, operacionales o reputacionales.

5. DISPOSICIONES NORMATIVAS.

Esta política se desarrolla en el marco del régimen de protección de datos personales en Colombia, conforme a las siguientes disposiciones:

El artículo 15 de la Constitución Política de Colombia protege los derechos a la intimidad, buen nombre y al habeas data. De esta disposición constitucional, se desprenden las demás normas que reglamentan la protección de datos en Colombia.

La Ley Estatutaria 1581 del 17 de octubre de 2012 establece las condiciones mínimas para realizar tratamiento legítimo de los datos personales de los Titulares de la información personal.

El Decreto 1074 del 2015, que incorporó los Decretos 1377 de 2013, 886 de 2014, entre otros; los cuales definieron aspectos puntuales frente a la recolección de datos personales, el contenido de la política de tratamiento de la información y el Registro Nacional de Base de Datos, entre otros de los puntos tratados.

La Circular Externa 002 del 3 de noviembre de 2015 de la Superintendencia de Industria y Comercio.

Circular 003 de 2024 de la Superintendencia de Industria y Comercio (SIC): Esta circular reitera la importancia de cumplir con las obligaciones de registro y actualización de bases de datos en el RNBD, y establece medidas específicas para asegurar la protección de los datos personales.

6. DEFINICIONES

Para efectos de la interpretación y aplicación de la presente política, se deben considerar los siguientes conceptos:

- **AUTORIZACIÓN:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
- **CONSULTA:** Solicitud del Titular del dato o de las personas autorizadas por éste o por la ley, para conocer la información que reposa sobre él en bases de datos o archivos de INSURCOL S.A.S.
- **RECLAMO:** Solicitud del Titular del dato o 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.
- **BASE DE DATOS:** Conjunto organizado de datos personales que sea objeto de Tratamiento.
- **DATOS PERSONALES.** La información objeto de tratamiento por parte de **INSURCOL**, en adelante en este documento "Datos personales", es aquella que suministran los Titulares, cuando acceden a sus bienes y/o servicios, o con ocasión de los mismos, tales como: nombre, apellidos, identificación, edad, sexo, teléfono, dirección física y electrónica, número telefónico, país, ciudad, información financiera y/o contable, profesión, oficio, experiencia comercial y/o laboral, formación académica, datos familiares, y demás datos necesarios que le sean solicitados en el proceso de registro. Igualmente, **INSURCOL** tratará datos personales obtenidos a través de sus sistemas de video vigilancia. La recolección de datos personales a través de sistemas de video vigilancia en INSURCOL se realizará a través de cámaras de seguridad instaladas en cada una de sus sedes y en los predios que por seguridad así lo disponga la empresa.
- **DATO PERSONAL PRIVADO:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para la persona Titular del dato. Ejemplos: información extraída a partir de la inspección del domicilio, número telefónico siempre y cuando no se encuentre en bases públicas o el salario. También lo son los datos que reposen en los archivos de la Registraduría, referentes a la identidad de las personas, cómo son sus datos biográficos, su filiación y fórmula dactiloscópica.
- **DATO PERSONAL SENSIBLE:** Información que afecta la intimidad de la persona o cuyo uso indebido puede generar su discriminación, tales como por ejemplo 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, así como los datos relativos a la salud, a la vida sexual y los datos biométricos (huellas dactilares, fotos).

- **DATO PERSONAL SEMIPRIVADO:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general, como, entre otros, el dato referente al cumplimiento o incumplimiento de las obligaciones financieras o los datos relativos a las relaciones con las entidades de la seguridad social.
- **DATO PERSONAL PÚBLICO:** Es el dato calificado como tal por ley o la Constitución Política o el que no sea privado, semiprivado o sensible. Son públicos, entre otros, el nombre, el número de identificación, fecha y lugar de expedición del documento de identificación, la profesión u oficio y la calidad de comerciante o de servidor público, los datos contenidos en el Registro Único nacional de Tránsito - RUNT o los datos contenidos en el registro público mercantil de las Cámaras de Comercio, entre otros.
- **ENCARGADO DEL TRATAMIENTO:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.
- **RESPONSABLE DEL TRATAMIENTO:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
- **SUBENCARGADO DEL TRATAMIENTO:** Persona que realiza el tratamiento de datos por cuenta de un Encargado del tratamiento.
- **TITULAR:** Persona natural: clientes, consumidores, empleados, ex- empleados, proveedores, entre otros, cuyos datos personales sean objeto de Tratamiento.
- **TRANSFERENCIA:** actividad en la cual 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:** tratamiento de los 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 por cuenta del responsable;
- **SGPDP:** Sistema de gestión de protección de datos personales.
- **PDP:** Protección de datos personales.
- **INCIDENTES:** Pueden ser Ataques Informáticos o pérdida de Bases de datos por motivos internos.
- **SISTEMA DE VIDEO VIGILANCIA:** Los Sistemas de Video vigilancia (CCTV) o cámaras de seguridad implementadas con la finalidad de garantizar la seguridad de bienes o personas en un lugar determinado han venido incrementando su presencia al ser considerados como un medio idóneo para realizar el monitoreo y la observación de actividades en escenarios domésticos, empresariales, laborales y públicos.
- **SAGRILAF:** Sistema de Autocontrol y Gestión del Riesgo Integral de Lavado de Activos, Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva.
- **NNA:** Hace referencia a los menores de 18 años, y corresponde a la sigla de Niños, Niñas y Adolescentes.
- **TIC:** Tecnologías de la Información y la Comunicación
- **CAUSAHABIENTE** El causahabiente, en Derecho, es aquella persona física o jurídica que se ha sucedido o sustituido a otra, el causante, por cualquier título jurídico en el derecho de otra. La sucesión o sustitución puede haberse producido por acto entre vivos inter vivos o por causa de muerte mortis causa.
- **ADECUACIÓN:** Se refiere a que los datos personales deben ser tratados de manera que se garantice un nivel adecuado de protección, conforme a las normativas vigentes. Esto implica que los datos solo pueden ser transferidos a países o entidades que ofrezcan un nivel de protección adecuado, reconocido por las autoridades competentes
- **PERTINENCIA:** Este principio establece que los datos personales recolectados y tratados deben ser pertinentes y adecuados en relación con las finalidades específicas para las cuales fueron obtenidos. Es decir, solo se deben recolectar y utilizar los datos necesarios para cumplir con los objetivos del tratamiento
- **PROPORCIONALIDAD** Este principio implica que el tratamiento de datos personales debe ser proporcional a las finalidades para las cuales se recolectan. Esto significa que solo se deben tratar los datos estrictamente necesarios para la finalidad, explícita lícita, legítima que justifica su tratamiento. y durante el tiempo necesario para cumplir con dichas finalidades, evitando cualquier exceso o uso indebido,
- **CIBERSEGURIDAD:** Conjunto de prácticas, controles, tecnologías y medidas orientadas a proteger los datos personales y demás activos de información frente a accesos no autorizados, ataques informáticos, fugas de información, alteraciones o cualquier riesgo derivado del uso de sistemas digitales.
- **RIESGO TECNOLÓGICO:** Posibilidad de que un evento relacionado con fallas tecnológicas, vulnerabilidades digitales, ciberataques, errores de software o interrupciones en los sistemas de información afecte la seguridad, disponibilidad, integridad o confidencialidad de los datos personales.

- **INFORMACIÓN CONFIDENCIAL:** Toda información, incluidos los datos personales, que no es pública y cuyo acceso, uso o divulgación no autorizados pueden generar un riesgo o impacto para los titulares o para INSURCOL SAS.
- **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Evento adverso, sospechoso o confirmado, relacionado con la pérdida, alteración, destrucción, robo, divulgación no autorizada o acceso indebido de datos personales o información bajo custodia de INSURCOL SAS. Incluye ataques informáticos, errores operativos, fallas tecnológicas y accesos indebidos.
- **TRANSFORMACIÓN DIGITAL:** Proceso mediante el cual INSURCOL SAS adopta tecnologías digitales para mejorar la gestión, protección y procesamiento de los datos personales, incorporando prácticas seguras, éticas y eficientes.
- **ACTIVOS DE INFORMACIÓN:** Elementos que permiten el tratamiento de datos personales, tales como bases de datos, sistemas, aplicaciones, soportes magnéticos, documentos físicos, infraestructura tecnológica y recursos humanos asociados al procesamiento de información.

7. OBLIGACIONES.

Esta política es de **obligatorio y estricto cumplimiento para INSURCOL SAS**, para todos y cada uno de los sus empleados, contratistas, aliados estratégicos y cualquier tercero que tenga acceso a datos personales en calidad de **responsable, Encargado o Sub encargado del tratamiento**. Todos los involucrados en el tratamiento de datos personales deberán cumplir con las disposiciones establecidas en esta política durante el desarrollo de sus funciones, actividades y ejecuciones contractuales. Este compromiso se mantiene incluso después de finalizada la relación laboral, contractual o comercial con INSURCOL SAS.

Así mismo, cualquier persona que acceda, gestione o trate datos personales por disposición de INSURCOL SAS está obligada a mantener **estricta confidencialidad y reserva** respecto de la información, garantizando su adecuada protección y evitando su divulgación no autorizada. Esta obligación incluye la adopción de comportamientos éticos, el cumplimiento de las medidas de ciberseguridad, la atención de los riesgos tecnológicos y el manejo responsable de la información conforme a los lineamientos del Sistema de Gestión de la Calidad.

El incumplimiento de estas obligaciones constituye una **falta gravísima** y puede dar lugar a sanciones disciplinarias, contractuales o legales según corresponda.

Adicionalmente, INSURCOL SAS podrá implementar acciones preventivas y correctivas derivadas del enfoque basado en riesgos, cuando se evidencien vulneraciones, amenazas o debilidades relacionadas con el tratamiento de datos personales.

Cualquier incidente, irregularidad o incumplimiento relacionado con el tratamiento de datos personales debe ser reportado de inmediato a través de los siguientes canales:

- **Correo electrónico:** datospersonales@insurcol.com
- **Dirección física:** Calle 41 No 21-32, Barrio Bolívar, Bucaramanga, Santander, Colombia

INSURCOL SAS tomará las acciones correspondientes para garantizar el cumplimiento de la normativa vigente y la protección de los derechos de los titulares de los datos, incluyendo la investigación de incidentes, la aplicación de medidas correctivas y la mejora continua del Sistema de Gestión de Protección de Datos Personales (SGPDP), en concordancia con las prácticas de calidad, sostenibilidad y seguridad de la información contempladas.

8. ESTRUCTURA ADMINISTRATIVA SOBRE PROTECCIÓN Y TRATAMIENTO DE DATOS

INSURCOL SAS, ha definido la siguiente estructura de gobierno para el **Sistema de Gestión de Seguridad de Datos Personales (SGSDP)**, con el propósito de garantizar la adecuada protección y tratamiento de los datos personales conforme a la normativa vigente.

Órganos de Gobierno del SGSDP.

8.1 Órgano Superior del SGSDP

- Será la **Gerente general** de INSURCOL SAS o el órgano de dirección que la empresa designe.
- Tendrá la responsabilidad de supervisar la implementación, cumplimiento y mejora continua del SGSDP.
- Se apoyará en el **Comité del SGSDP** y en los demás responsables asignados para garantizar el adecuado funcionamiento del sistema.

El Ingeniero informático asumirá el rol de presidente del SGSDP y será responsable del Apoyo Técnico. Para las tareas administrativas y documentales, contará con el apoyo del Ingeniero de sistemas

- Actuará como **canal de comunicación** entre los diferentes órganos y miembros del SGSDP.
- Será el encargado de coordinar la atención de **consultas, quejas y reclamos** presentados por los titulares de los datos personales.

Coordinadores y/o subcoordinadores de área, conformarán el Comité del Sistema de Gestión de Seguridad de Datos Personales (SGSDP)

- Será el **órgano encargado de la implementación, mantenimiento y mejora** del SGSDP.
- Coordinará las estrategias de protección de datos y supervisará la ejecución de políticas y protocolos.

8.2 Responsables de Áreas Claves del SGSDP:

8.2.1 Responsable de Base Documental, es el Trabajador que maneja y/o administra bases de datos

- Designado por la **Gerente General** a través del manual de cargos.
- Responsable de velar por la implementación, cumplimiento y actualización de las políticas y protocolos relacionados con la **gestión documental** y el almacenamiento seguro de datos personales.

8.2.2 Responsable de Cumplimiento Legal, asesor jurídico de INSURCOL y/o abogado de INSURCOL:

- Designado por la **Gerente General**, a través del rol del cargo y/o Manual de funciones.
- Garantiza que INSURCOL SAS cumpla con la normatividad vigente en protección de datos personales y mantiene actualizados los protocolos jurídicos.

8.3 Responsable de TIC, será el Ingeniero informático, para las tareas administrativas y documentales, contará con el apoyo del Ingeniero de sistemas.

- Designado por la **Gerente General**.
- Garantiza la **seguridad digital** de los datos personales, asegurando la correcta implementación de políticas de ciberseguridad, acceso y protección en medios electrónicos.

8.4 Responsable de Locaciones Físicas/ Ingeniero informático:

- Designado por la **Gerente General**, a través del rol del cargo y/o Manual de funciones.
- Supervisa la seguridad en **espacios físicos**, garantizando la correcta protección de documentos e información en medios no digitales.

9 TRATAMIENTO Y FINALIDAD DE LAS BASES DE DATOS.

INSURCOL SAS recolectará, almacenará, usará, circulará y suprimirá los datos personales conforme a esta política, limitándose a aquellos datos que sean pertinentes y adecuados para la finalidad específica de su tratamiento, de acuerdo con la normatividad vigente.

Este tratamiento se realizará garantizando la seguridad, integridad, disponibilidad y confidencialidad de la información, incorporando controles asociados a riesgos tecnológicos, ciberseguridad y manejo de información digital.

La información requerida a clientes, proveedores, trabajadores, accionistas, contratistas, aspirantes a trabajar y visitantes dependerá de la finalidad para la cual sea solicitada.

INSURCOL SAS también tendrá en cuenta criterios de sostenibilidad, gestión del conocimiento, cumplimiento ético y necesidades de partes interesadas relevantes para determinar los datos estrictamente necesarios para el tratamiento.

Para el cumplimiento de su misión, compromisos organizacionales y obligaciones adquiridas, INSURCOL SAS realiza el tratamiento de datos personales para los siguientes fines:

9.1 Tratamiento de Datos de Clientes

INSURCOL SAS recopilará y tratará los datos personales de sus clientes con los siguientes propósitos:

A. Relación Comercial y Contractual

- Gestionar las relaciones comerciales y contractuales establecidas con los clientes, garantizando que las actividades relacionadas se ejecuten conforme a principios de transparencia, ética, calidad y trazabilidad de la información.
- Cumplir con el Sistema de Autocontrol y Gestión del Riesgo integral de Lavado de Activos, Financiación del terrorismo y financiamiento de la proliferación de armas de destrucción Masiva (SAGRILAF) y Programa de transparencia y ética empresarial (PTEE), de obligatorio cumplimiento para la organización según la normatividad colombiana vigente, incluyendo consultas masivas de manera directa o a través de terceros en fuentes de información nacional y listas restrictivas (OFAC, ONU, Clinton, etc.).
- Mantener evidencia documental sobre la entrega de documentos, inducciones, entrenamientos, charlas, reuniones y otras actividades de la empresa.
- Enviar facturas y comunicaciones relacionadas con los contratos celebrados entre las partes.

B. Comunicación y Contacto.

- Informar sobre los productos y servicios ofrecidos por la organización.
- Establecer comunicación con los clientes a través de llamadas, mensajes de texto, correos electrónicos, documentos físicos y aplicaciones corporativas, garantizando la protección de la información documentada
- Enviar información sobre eventos, cambios organizacionales, políticas y proyectos de INSURCOL SAS.
- Contactar a los titulares para encuestas de satisfacción, estudios de mercado y segmentación de clientes.

C. Gestión Administrativa y Operativa.

- Realizar auditorías, análisis y estudios de datos para diseñar, implementar y desarrollar programas, proyectos y eventos.
- Gestionar solicitudes, quejas y reclamos presentados por los clientes.
- Contactar a los titulares a través de medios telefónicos o electrónicos para encuestas y confirmación de datos personales.
- Enviar estados de cuenta, facturas y demás información relacionada con las obligaciones contractuales.
- Prestar los servicios ofrecidos por INSURCOL SAS y aceptados en los contratos suscritos.
- Incorporar herramientas tecnológicas bajo criterios de seguridad, calidad y gestión del riesgo, asegurando el correcto tratamiento de datos dentro de los procesos operativos.

D. Protección y Cumplimiento Normativo.

- Cumplir con leyes, regulaciones o procesos legales que exijan la divulgación de información.
- Implementar medidas para prevenir fraudes, ataques a la seguridad o problemas técnicos que afecten a INSURCOL SAS o a terceros.
- Suministrar información de contacto a terceros con los cuales INSURCOL SAS tenga vínculos contractuales, cuando sea necesario para el cumplimiento de sus obligaciones.
- Dar trámite a procesos perjuicios y jurídicos relacionados con el cobro de cartera o cumplimiento contractual.

E. Otros Usos Legales y Empresariales

- Ofrecer productos y servicios adicionales.
- Evaluar hábitos de consumo, analizar tendencias y realizar estudios estadísticos.
- Solicitar retroalimentación sobre los productos y servicios.
- Los demás usos descritos en la presente política o permitidos por la ley.
- Utilizar la información para procesos de análisis organizacional y mejora continua, garantizando siempre la minimización de datos y su pertinencia frente a la finalidad.

En todo caso, la información no será objeto de tratamiento por un periodo superior al tiempo que dure la relación del cliente con la empresa, y el tiempo adicional que se requiera de acuerdo con las circunstancias legales o contractuales que hagan necesario el manejo de la información del cliente.

En particular, y sin perjuicio de lo anterior, los datos personales contenidos en documentos que soporten operaciones comerciales serán conservados por un término de **diez (10) años**, contados a partir de la fecha del último asiento, documento o comprobante, conforme lo establece el artículo 60 del código de comercio colombiano.

INSURCOL SAS garantizará que la conservación se realice bajo medidas adecuadas de seguridad, almacenamiento y control de acceso, incluyendo tecnologías que eviten pérdida, alteración o uso indebido.

9.2 Tratamiento de Datos de Proveedores

INSURCOL SAS recopilará y tratará la información de sus proveedores con el objetivo de gestionar eficientemente la relación comercial y contractual, garantizando el cumplimiento normativo y la seguridad en el tratamiento de datos personales.

Este tratamiento se realizará bajo criterios de ética, transparencia, gestión del riesgo y calidad, incorporando controles para proteger la información frente a riesgos tecnológicos, ciberseguridad y uso indebido de datos.

A. Relación Comercial y Contractual

- Seleccionar, evaluar y reevaluar proveedores, así como gestionar invitaciones a cotizar y
- realizar adquisiciones de bienes y servicios.
- Efectuar pagos derivados de obligaciones contractuales.
- Enviar correspondencia relacionada con contratos y otros asuntos comerciales.
- Garantizar la trazabilidad y cumplimiento de los contratos celebrados.
- Verificar el cumplimiento ético y de calidad de los proveedores, conforme a los principios de transparencia, conducta responsable y cultura organizacional

B. Comunicación y Contacto

- Mantener contacto con proveedores a través de llamadas, mensajes de texto, correos electrónicos y documentos físicos para gestionar cotizaciones y desarrollar negocios, asegurando que los mecanismos de comunicación utilicen canales seguros que minimicen riesgos tecnológicos y garanticen la integridad y confidencialidad de la información intercambiada.
- Establecer comunicación con los proveedores sobre cualquier aspecto relacionado con las finalidades de esta política.
- Contactar a los proveedores para realizar encuestas, estudios o confirmación de datos personales necesarios para la ejecución de una relación contractual.

C. Cumplimiento Normativo y Seguridad

- Cumplir con el Sistema de Autocontrol y Gestión del Riesgo integral de Lavado de Activos, financiación del Terrorismo, y Financiamiento de la Proliferación de Armas de Destrucción Masiva (SAGRILAF) y Programa de transparencia y ética empresarial (PTEE), de obligatorio cumplimiento a la organización, según la normatividad colombiana vigente, incluyendo consultas masivas de manera directa o a través de terceros en fuentes de información nacional y listas restrictivas (OFAC, ONU, Clinton, etc.).
- Atender requerimientos de entidades públicas, administrativas y/o judiciales.
- Asegurar la correcta vinculación de proveedores en cumplimiento de las normativas vigentes.
- Implementar medidas de control, seguimiento, monitoreo y vigilancia en la contratación de bienes y servicios.
- Cumplir con leyes, regulaciones o procesos legales que exijan la divulgación de información.
- Prevenir fraudes, ataques a la seguridad, problemas técnicos o cualquier situación que pueda afectar a INSURCOL SAS o a terceros.
- Dar trámite a procesos prejurídicos y jurídicos relacionados con cumplimiento contractual.
- Incorporar análisis de riesgos tecnológicos, reputacionales y operativos en la gestión de proveedores, garantizando la protección de la información y la continuidad operativa

D. Gestión Administrativa y Operativa

- Auditar, estudiar, analizar y utilizar la información de la base de datos para diseñar, implementar y desarrollar programas, proyectos y eventos, incorporando herramientas tecnológicas que permitan un manejo seguro, eficiente y trazable de la información, garantizando el cumplimiento de los requisitos de calidad, seguridad y protección de datos.
- Socializar políticas, proyectos, programas, resultados y cambios organizacionales.
- Gestionar trámites administrativos, solicitudes, quejas y reclamos.
- Suministrar información a la fuerza comercial y/o red de distribución, telemarketing, investigación de mercados y cualquier tercero con el cual INSURCOL SAS tenga un vínculo contractual.
- Contactar a los proveedores a través de SMS, chat o correo electrónico para el envío de información sobre campañas de mejora de servicio.
- Enviar estados de cuenta, facturas y demás información relacionada con obligaciones contractuales.
- Gestionar la entrega de documentos, registro de inducciones, entrenamientos, charlas y reuniones como evidencia de cumplimiento contractual.

E. Confidencialidad y Protección de Datos

- La información suministrada por INSURCOL SAS a los proveedores es confidencial y deberá ser protegida conforme a las disposiciones de la Ley 1581 de 2012 y las normas que la reglamentan.
- Los proveedores de INSURCOL SAS deberán implementar medidas adecuadas para garantizar la seguridad y protección de los datos personales tratados.
- Los proveedores deberán adoptar prácticas éticas, controles de ciberseguridad, políticas internas de protección de datos y mecanismos de prevención de fugas, alteraciones o accesos indebidos, en coherencia con los estándares de seguridad y calidad exigidos por INSURCOL SAS.

En todo caso, la información no será objeto de tratamiento por un periodo superior al tiempo que dure la relación del proveedor con la empresa, y el tiempo adicional que se requiera de acuerdo con las circunstancias legales o contractuales que hagan necesario el manejo de la información el proveedor.

En particular, y sin perjuicio de lo anterior, los datos personales contenidos en documentos que soporten operaciones comerciales serán conservados por un término de **diez (10) años**, contados a partir de la fecha del último asiento, documento o comprobante, conforme lo establece el artículo 60 del código de comercio colombiano.

Durante este periodo, INSURCOL SAS aplicará controles de seguridad, acceso restringido y monitoreo para garantizar la integridad y protección de la información almacenada.

9.3 Tratamiento de Datos de Trabajadores

INSURCOL SAS almacenará los documentos y datos personales de cada trabajador tanto en formato digital como físico, en carpetas individuales accesibles únicamente por el Departamento de Recursos Humanos, HSE&RSE, nómina, calidad. El tratamiento de esta información se realiza con el propósito exclusivo de cumplir y ejecutar la relación laboral entre el trabajador e INSURCOL SAS.

Este tratamiento se realizará bajo criterios de ética, transparencia, seguridad de la información, gestión del riesgo y cultura de calidad, incorporando medidas técnicas y administrativas para prevenir accesos no autorizados, alteraciones, pérdida o uso indebido de la información laboral.

A. Relación contractual y obligaciones legales

- Formalizar el contrato de trabajo.
- Ejecutar el objeto del contrato.
- Cumplir con los deberes legales, como afiliaciones al Sistema General de Seguridad Social Integral (EPS, Fondo de Pensiones, ARL, Caja de Compensación Familiar).
- Realizar el pago de salarios, prestaciones y beneficios extralegales no constitutivos de salario, mediante transferencias electrónicas.
- Llevar control de las condiciones del contrato y de las que se deriven de él.
- Determinar las condiciones de salud del trabajador para su ingreso y retiro.
- Expedir certificaciones laborales.

- Confirmar referencias laborales.
- Mantener un historial de los trabajadores.
- Asegurar que todas las actividades contractuales se realicen con trazabilidad, integridad documental y protección de la información en coherencia con los principios éticos y de calidad.

B. Gestión administrativa y operativa

- Gestionar la elaboración del carné de identificación.
- Gestionar la apertura de cuentas de nómina.
- Gestionar el retiro de cesantías, la adquisición de libranzas y descuentos a cuentas AFC.
- Gestionar la adquisición de tiquetes aéreos.
- Gestionar anticipos de gastos de viajes.
- Realizar reportes de novedades a las pólizas colectivas.
- Gestionar la asignación de usuarios para las diferentes plataformas tecnológicas, implementando controles de seguridad digital para garantizar que los accesos a plataformas y sistemas tecnológicos asignados a los trabajadores sean protegidos adecuadamente y utilizados bajo criterios de seguridad y ciberseguridad.

C. Control y monitoreo del cumplimiento contractual

- Proporcionar información solicitada por clientes, gestorías y/o interventorías para verificar el perfil profesional y competencias del trabajador necesarias para la ejecución del contrato.
- Remitir información a los clientes de INSURCOL SAS para ejecutar el control, seguimiento, monitoreo y vigilancia del cumplimiento de la vinculación de mano de obra local, atender requerimientos de entidades públicas, administrativas y/o judiciales, realizar validaciones en listas restrictivas de entidades públicas o monitoreo preventivo de conocimiento de contrapartes y realizar análisis estadísticos de contratación de mano de obra calificada y no calificada.

D. Seguridad y salud en el trabajo

- Registrar, seguir y controlar la historia médica ocupacional del trabajador.
- Atender asuntos relacionados con la historia clínica médica ocupacional frente a las obligaciones, derechos y deberes en seguridad y salud en el trabajo, tanto del trabajador como de la Empresa.
- Implementar medidas de protección para datos sensibles relacionados con salud, garantizando confidencialidad y controles de acceso estrictos conforme a buenas prácticas de seguridad de la información.

E. Cumplimiento normativo y auditorías

- Atender auditorías internas y externas.
- Atender requerimientos y/o acciones judiciales y extrajudiciales.
- Atender asuntos administrativos, judiciales y extrajudiciales.
- Incorporar análisis de riesgos y acciones preventivas/correctivas cuando los procesos de auditoría identifiquen vulnerabilidades o brechas relacionadas con el tratamiento de datos personales.

F. Registro y evidencias de actividades

- Servir como prueba de entrega de documentos, registro de inducciones, entrenamientos, charlas, reuniones y diferentes actividades de la empresa.
- Evidenciar cualquier tipo de trámite, procedimiento y/o constancia que requiera la Compañía.
- Garantizar la trazabilidad, integridad y custodia adecuada de las evidencias documentales, tanto físicas como digitales, asegurando su conservación bajo estándares de seguridad y calidad.

Adicionalmente, INSURCOL S.A.S podrá:

A. Gestión de información del trabajador

- Obtener datos de contacto, formación y demás información relevante necesaria durante los procesos de selección y eventuales relaciones laborales.
- Efectuar las gestiones pertinentes para el desarrollo del objeto social de la compañía, en cumplimiento del contrato celebrado con el Titular de la información.

- Gestionar trámites administrativos como solicitudes, quejas y reclamos.

B. Comunicación y notificaciones

- Contactar al Titular a través de medios telefónicos para realizar encuestas, estudios y/o confirmación de datos personales necesarios para la ejecución de una relación contractual
- Contactar al Titular a través de medios electrónicos – SMS, aplicativos de los teléfonos corporativos o chat para el envío de noticias relacionadas con campañas de mejora de servicio.
- Contactar al Titular a través de correo electrónico o aplicativos de los teléfonos corporativos para el envío de cualquier tipo de información, estados de cuenta o facturas en relación con las obligaciones derivadas del contrato celebrado entre las partes, garantizando la protección de datos laborales.

C. Cumplimiento de obligaciones y beneficios

- Dar cumplimiento a las obligaciones contraídas por INSURCOL SAS con el Titular de la Información, en relación con el pago de salarios, prestaciones sociales y demás retribuciones consagradas en el contrato de trabajo o según lo disponga la ley
- Ofrecer programas de bienestar corporativo y planificar actividades empresariales para el Titular y sus beneficiarios (hijos, cónyuge, compañero permanente).
- Asegurar que los programas y beneficios sean comunicados y gestionados cumpliendo criterios de transparencia, ética y protección de datos.

D. Seguridad y cumplimiento legal

- Revelar la información cuando sea necesario para cumplir con leyes, regulaciones o procesos legales, asegurar el cumplimiento de términos y condiciones, detener o prevenir fraudes, ataques a la seguridad de INSURCOL SAS o de terceros, prevenir problemas técnicos o proteger los derechos de terceros según la ley.
- Las demás finalidades descritas en la presente política o en la Ley.
- Cumplir con el Sistema de Autocontrol y Gestión del Riesgo integral de Lavado de Activos, financiación del Terrorismo, y Financiamiento de la Proliferación de Armas de Destrucción Masiva (SAGRILAF) y Programa de transparencia y ética empresarial (PTEE), de obligatorio cumplimiento a la organización, según la normatividad colombiana vigente, incluyendo consultas masivas de manera directa o a través de terceros en fuentes de información nacional y listas restrictivas (OFAC, ONU, Clinton, etc.).

En todo caso, la información laboral del colaborador será conservada por la organización después de finalizada la relación laboral, así: (i) la información del Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST) hasta por veinte (20) años contados desde la terminación de la relación laboral y en los términos del Decreto 1072 de 2015, (ii) la información de la historia de la relación laboral por un término de hasta ochenta (80) años contados a partir de la terminación de la relación laboral.

Durante estos periodos, INSURCOL SAS garantizará controles adecuados de seguridad, acceso restringido, integridad y almacenamiento seguro, incluyendo soportes digitales protegidos contra alteración, pérdida o acceso no autorizado.

9.4 Tratamiento de Datos de Accionistas

INSURCOL SAS, utilizará los datos personales de los accionistas exclusivamente para los fines relacionados con su calidad de socios de la empresa, garantizando el cumplimiento de las normativas aplicables y bajo los criterios de transparencia, ética, seguridad de la información y gestión de riesgo y la confidencialidad de la información, asegurando la protección frente a riesgos tecnológicos, ciberseguridad y uso indebido de datos.

A. Gestión financiera y administrativa

- Realizar el pago de las utilidades.
- Mantener un registro de las reuniones realizadas y validar la asistencia de sus miembros, asegurando la trazabilidad, integridad y disponibilidad de la información financiera mediante controles documentales y tecnológicos alineados con el Sistema de Gestión de la Calidad.

B. Convocatorias y comunicación

- Convocar a la Junta Directiva de Accionistas.
- Convocar a las reuniones de la Asamblea General de Accionistas.
- Enviar correspondencia a los accionistas.
- Utilizar mecanismos de comunicación seguros y confiables que garanticen la confidencialidad de la información y minimicen riesgos tecnológicos o ciberataques.

C. Cumplimiento normativo y jurídico

- Atender asuntos administrativos, judiciales y extrajudiciales.
- Proporcionar información a clientes y/o terceros con los que se pretenda iniciar relaciones contractuales y/o jurídicas, para certificar la composición accionaria de INSURCOL SAS.
- Proporcionar información a clientes y/o sus contratistas designados para validaciones en listas restrictivas o monitoreo preventivo de contrapartes dentro de los programas de SAGRILAF y Ética y Transparencia Empresarial (PTEE).
- Cumplir con el Sistema de Autocontrol y Gestión del Riesgo Integral de Lavado de Activos, Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (SAGRILAF) y Programa de transparencia y ética empresarial (PTEE), de obligatorio cumplimiento para la organización según la normatividad colombiana vigente, incluyendo consultas masivas de manera directa o a través de terceros en fuentes de información nacional y listas restrictivas (OFAC, ONU, Clinton, etc.).
- Incorporar análisis de riesgos legales, reputacionales y tecnológicos cuando se procese información de accionistas, garantizando decisiones responsables y alineadas con la cultura de integridad y ética empresarial.

D. Registro y evidencias de actividades

- Servir como prueba de entrega de documentos, registro de inducciones, entrenamientos, charlas, reuniones y diferentes actividades de la empresa.
- Evidenciar cualquier tipo de trámite, procedimiento y/o constancia que requiera la Compañía.
- Implementar medidas de conservación segura, preservación digital y control de acceso para proteger las evidencias documentales, asegurando su integridad y disponibilidad.

9.5 Tratamiento de Datos de Contratistas

INSURCOL SAS recolectará y tratará los datos personales de los contratistas con el propósito de gestionar adecuadamente las relaciones comerciales y contractuales que se establezcan, garantizando el cumplimiento de las normativas aplicables y la protección de la información, conforme a criterios de ética, transparencia, calidad, gestión del riesgo y seguridad de la información, incorporando medidas para prevenir accesos no autorizados, fugas de información, riesgos tecnológicos o vulneraciones de ciberseguridad.

A. Gestión contractual y administrativa

- Ejecutar el objeto del contrato u orden y cumplir con las demás prestaciones asumidas.
- Controlar y supervisar las condiciones del contrato y de las que se deriven de este.
- Realizar el pago de las obligaciones mediante transferencias electrónicas.
- Expedir certificaciones a solicitud del titular.

B. Evaluaciones y auditorías

- Atención de auditorías internas y externas.
- Evaluar el desempeño de los contratistas de la Empresa.
- Implementar acciones preventivas y correctivas derivadas del análisis de riesgos y de los hallazgos de auditoría, especialmente cuando involucren el manejo de datos personales o información crítica.

C. Comunicación y correspondencia

- Envío de correspondencia o comunicaciones relacionadas con el objeto del contrato.
- Presentación y autorizaciones ante contratantes de la Empresa.

- Utilizar medios de comunicación seguros que mitiguen riesgos tecnológicos y garanticen la confidencialidad e integridad de la información compartida con los contratistas.

D. Cumplimiento normativo y jurídico

- Atención de asuntos administrativos, judiciales y extrajudiciales.
- Cumplir con lineamientos de integridad, transparencia y prevención de riesgos, incluidos aquellos derivados del SAGRILAF y del Programa de Ética Empresarial, aplicando verificaciones en listas restrictivas cuando sea necesario para proteger la organización.

E. Registro y evidencias de actividades

- Servir como prueba de entrega de documentos, registro de inducciones, entrenamientos, charlas, reuniones y diferentes actividades de la empresa.
- Evidenciar cualquier tipo de trámite, procedimiento y/o constancia que requiera la Compañía, garantizando que las evidencias documentales, físicas o digitales, sean almacenadas bajo medidas de seguridad, control de acceso y conservación adecuada.

En todo caso, la información no será objeto de tratamiento por un período superior al tiempo que dure la relación del contratista con la empresa, y el tiempo adicional que se requiera de acuerdo con las circunstancias legales o contractuales que hagan necesario el manejo de la información del contratista.

En particular, y sin perjuicio de lo anterior, los datos personales contenidos en documentos que soporten operaciones comerciales serán conservados por un término de **diez (10) años**, contados a partir de la fecha del último asiento, documento o comprobante, conforme lo establece el artículo 60 del Código de Comercio colombiano.

Durante este período, INSURCOL SAS aplicará medidas de protección física y digital que garanticen la integridad, disponibilidad y confidencialidad de la información.

9.6 Tratamiento de Datos de Aspirantes a Trabajadores

INSURCOL SAS recolectará y almacenará los datos personales de los aspirantes a trabajadores durante los procesos de selección, tanto en formato físico como digital. Estos datos serán gestionados exclusivamente por el Departamento de Recursos Humanos, garantizando la implementación de medidas de seguridad, principios de ética, transparencia, gestión del riesgo, seguridad de la información, protección de datos sensibles y cultura de calidad adecuadas para la protección de su confidencialidad.

A. Verificación y Evaluación del Candidato

- Verificar la información del titular con empresas, centros de formación y capacitación, y autoridades, para comprobar antecedentes judiciales, disciplinarios, fiscales e infracciones de tránsito.
- Asegurar que el perfil del candidato se ajuste al puesto al que se postula, en términos de formación, experiencia y competencias.
- Realizar evaluaciones psico-técnicas.
- Implementar mecanismos de validación seguros, éticos y transparentes, garantizando la confidencialidad de los datos obtenidos y la protección de información sensible durante el proceso de selección.

B. Registro y Seguimiento

- Mantener un registro histórico de los aspirantes a ser vinculados a la Empresa.
- Cumplir con el Sistema de Autocontrol y Gestión del Riesgo Integral de Lavado de Activos, Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (SAGRILAF) y Programa de transparencia y ética empresarial (PTEE), de obligatorio cumplimiento para la organización según la normatividad colombiana vigente, incluyendo consultas masivas de manera directa o a través de terceros en fuentes de información nacional y listas restrictivas (OFAC, ONU, Clinton, etc.).
- Conservar la trazabilidad digital y documental del proceso de selección, garantizando el adecuado tratamiento de la información en plataformas tecnológicas y minimizando riesgos tecnológicos conforme a los estándares de seguridad de la información.

C. Cumplimiento Normativo y Evidencias

- Atender asuntos administrativos, judiciales y extrajudiciales.
- Servir como prueba de entrega de documentos, registro de inducciones, entrenamientos, charlas, reuniones y diferentes actividades de la empresa.
- Evidenciar cualquier tipo de trámite, procedimiento y/o constancia que requiera la Compañía.
- Implementar medidas de protección, control de acceso y conservación segura de las evidencias obtenidas durante el proceso de selección, incorporando controles de integridad, disponibilidad y confidencialidad de la información.

La información de los aspirantes será tratada durante el proceso de selección y:

- a) Aspirantes no seleccionados:** Los datos se conservarán por **seis (6) meses** después de finalizado el proceso de selección, para cubrir eventuales vacantes similares y atender posibles reclamaciones. Con consentimiento expreso, podrán conservarse hasta por **dos (2) años** en base de datos de talento para futuros procesos. Durante este período, INSURCOL SAS garantizará medidas de seguridad física y digital que prevengan accesos no autorizados, fugas de información o alteraciones.
- b) Aspirantes seleccionados:** Los datos pasarán a formar parte de la historia laboral y se sujetarán a los términos de vigencia establecidos para la información de colaboradores. Este proceso será documentado y gestionado conforme a las prácticas de trazabilidad, protección de datos sensibles y gestión del conocimiento.

9.7 Tratamiento de Datos de Visitantes

INSURCOL SAS recolectará y almacenará los datos personales de los visitantes con el propósito de gestionar su acceso a las instalaciones y garantizar la seguridad del personal, los bienes y la infraestructura de INSURCOL. El tratamiento de esta información se realizará bajo criterios de seguridad, ética, gestión del riesgo, ciberseguridad y cultura de calidad implementando medidas de control que prevengan accesos no autorizados, fugas de información o riesgos asociados al uso de tecnologías de vigilancia y control.

A. Control de Acceso y Seguridad

- Permitir y gestionar el acceso a las instalaciones.
- Mantener un registro de visitantes para la protección y control de ingreso y salida.
- Garantizar la seguridad del personal, los bienes y la infraestructura de INSURCOL.
- Validar la información de los visitantes mediante mecanismos seguros, digitales o físicos, que garanticen la integridad, exactitud y disponibilidad de los datos utilizados en el proceso de control de acceso.
- Aplicar controles de gestión del riesgo para identificar amenazas o eventos que puedan comprometer la seguridad física o digital de la organización.

La información de visitantes registrada en las planillas de ingreso a las instalaciones se conservará por el período que la empresa determine según sus políticas internas de seguridad, el cual no podrá ser inferior a **un (1) mes** ni superior a **seis (6) meses** contados desde la fecha de la visita.

Si el visitante está involucrado en un incidente de seguridad o situación que requiera investigación, los datos se conservarán por el tiempo adicional necesario hasta la resolución del asunto.

Transcurrido el plazo establecido, los datos serán eliminados, salvo obligación legal o requerimiento de autoridad competente.

Durante los periodos de conservación, INSURCOL SAS garantizará medidas de seguridad física y digital que eviten accesos no autorizados, alteración o pérdida de información,

B. Uso de Sistemas de Vigilancia

Capturar imágenes, voz y videos mediante el sistema de vigilancia para:

- Proteger al personal, los bienes y la infraestructura ante posibles amenazas o incidentes.
- Monitorear y registrar quién entra y sale de las instalaciones, asegurando que solo personas autorizadas tengan acceso.
- Disuadir actividades delictivas y facilitar la identificación de personas involucradas en incidente.

- Proporcionar evidencia visual en caso de investigaciones administrativas, judiciales o extrajudiciales.
- Cumplir con normativas de seguridad y protección establecidas por la ley.
- Asegurar que los sistemas de videovigilancia operen bajo controles de ciberseguridad que eviten accesos indebidos a las imágenes, manipulación de grabaciones o riesgos tecnológicos derivados de dispositivos conectados.

Los datos recolectados por los Sistemas de Video vigilancia de INSURCOL en cada una de sus sedes, son utilizadas con las siguientes finalidades:

- a) Garantizar la seguridad de bienes y personas que hacen parte de la organización.
- b) Velar por el cumplimiento de las obligaciones laborales de visitantes los trabajadores de INSURCOL.
- c) Tener un registro temporal de las imágenes para ser utilizadas en investigaciones disciplinarias.
- d) Ser utilizadas en eventuales procesos judiciales y/o extrajudiciales en los que se vea involucrada INSURCOL.
- e) Contribuir a la gestión del riesgo, incluyendo la detección de amenazas, fallas operativas y situaciones críticas que puedan afectar la continuidad del negocio.

Como prueba de entrega de documentos, registro de inducciones, entrenamientos, charlas, reuniones y diferentes actividades de la empresa, así como para evidenciar cualquier tipo de trámite, procedimiento y/o constancia que requiera la Compañía.

Las imágenes captadas por el sistema de circuito cerrado de televisión (CCTV) se conservarán por un periodo de (4) días, determinado según la capacidad de almacenamiento de los dispositivos de grabación (DVR) de la empresa. Las grabaciones serán sobrescritas automáticamente una vez cumplido este periodo, siguiendo un sistema de rotación continua. Durante este lapso, INSURCOL SAS implementará medidas de seguridad para garantizar la confidencialidad e integridad de las grabaciones.

Si las imágenes están relacionadas con un incidente de seguridad, investigación interna, proceso judicial o requerimiento de autoridad competente, se conservarán por el tiempo necesario hasta la resolución definitiva del asunto. El acceso a las grabaciones está restringido al personal autorizado y su tratamiento se limita a finalidades de seguridad, protección de bienes y personas, y cumplimiento de obligaciones legales. El acceso a las grabaciones estará estrictamente restringido al personal autorizado, bajo medidas de trazabilidad, control de acceso y de uso, asegurando su tratamiento conforme a principios éticos y de calidad.

9.8 Tratamiento de Datos de la Comunidad

INSURCOL SAS, en el desarrollo de su objeto social y dentro del marco de sus acciones de Responsabilidad Social Empresarial, podrá recolectar y tratar datos personales de miembros de la comunidad con el propósito de gestionar solicitudes y garantizar el cumplimiento de normativas:

El tratamiento de estos datos se realizará de acuerdo con los principios de ética, transparencia, gestión del riesgo, cultura de calidad y seguridad de la información, asegurando la protección frente a riesgos tecnológicos, accesos no autorizados, alteración o uso indebido de datos.

A. Atención de Solicitudes y Gestión de PQRS

- Atender peticiones, quejas y reclamos (PQRS) presentados por miembros de la comunidad.
- Garantizar una comunicación efectiva con la comunidad para resolver inquietudes y facilitar la gestión de trámites.
- Implementar canales de atención seguros - físicos y digitales - que garanticen la confidencialidad, disponibilidad e integridad de la información suministrada por la comunidad.

B. Validaciones y Cumplimiento Normativo

- Realizar validaciones en listas restrictivas, de entidades públicas o llevar a cabo monitoreos preventivos de conocimiento de contrapartes, en caso de aplicar.
- Atender asuntos administrativos, judiciales y extrajudiciales relacionados con la comunidad.
- Aplicar criterios de análisis de riesgos reputacionales, sociales y tecnológicos en la interacción con miembros de la comunidad.

C. Registro y Evidencia de Actividades

- Mantener un registro de la entrega de documentos, inducciones, entrenamientos, charlas, reuniones y demás actividades de la empresa.
- Evidenciar cualquier tipo de trámite, procedimiento o constancia que requiera la compañía en sus relaciones con la comunidad.
- La información de miembros de la comunidad (PQRS, registros de actividades, validaciones y demás interacciones) se conservará por un período de (2 años) años contados desde la fecha del último registro o interacción con el titular. La información podrá conservarse por períodos adicionales cuando sea requerida para atender asuntos administrativos, judiciales o extrajudiciales en curso, o cuando exista obligación legal específica de conservación.
- Garantizar que las evidencias documentales, físicas o digitales, sean almacenadas con controles de acceso, trazabilidad y conservación adecuada, implementando medidas de seguridad.

9.9 Tratamiento de Datos de Extrabajadores

INSURCOL SAS, almacenará y tratará la información personal de todas las personas con quienes ha suscrito contratos de trabajo, con el propósito de garantizar el cumplimiento de obligaciones legales, administrativas y laborales posteriores a la finalización de la relación contractual.

El tratamiento de estos datos se realizará bajo criterios de ética, transparencia, gestión del riesgo, seguridad de la información y cultura de calidad, garantizando la protección frente a riesgos tecnológicos, accesos no autorizados o uso indebido de información.

A. Registro y Certificación

- Mantener un registro histórico de los extrabajadores, incluyendo las condiciones de su vinculación y retiro.
- Expedir certificaciones sobre la relación laboral que existió.
- Preservar la integridad, exactitud y disponibilidad del historial laboral, asegurando controles adecuados para evitar alteraciones o pérdida de información.

B. Cumplimiento de Requerimientos Legales

- Atender requerimientos de entidades judiciales, públicas y administrativas.

C. Gestión de la Historia Médica Ocupacional

- Registrar, seguir y controlar la historia médica ocupacional del trabajador.
- Atender asuntos relacionados con la historia clínica médica ocupacional en el marco de los derechos, deberes y obligaciones en seguridad y salud en el trabajo, tanto del trabajador como de la empresa.
- Atender requerimientos y/o acciones judiciales, extrajudiciales e investigaciones administrativas que requieran el uso de la historia médica ocupacional del trabajador para la defensa de la Compañía.
- Aplicar medidas reforzadas de seguridad y confidencialidad, dada la naturaleza sensible de estas historias clínicas, garantizando controles estrictos de acceso y trazabilidad en cumplimiento de estándares de seguridad de la información.

D. Evidencia y Control de Actividades

- Atender asuntos administrativos, judiciales y extrajudiciales.
- Mantener registros como prueba de entrega de documentos, inducciones, entrenamientos, charlas, reuniones y otras actividades realizadas en la empresa.
- Evidenciar cualquier trámite, procedimiento o constancia que requiera la Compañía.
- Implementar medidas de conservación segura y registro trazable de documentos históricos, garantizando su integridad digital y física, y su uso exclusivo para fines autorizados por la normatividad vigente.

La información de extrabajadores se conservará conforme a los términos de vigencia establecidos en el numeral de Colaboradores de la presente política.

Los datos se conservarán por tiempo adicional cuando sean necesarios para la atención de requerimientos legales o la defensa de intereses del RESPONSABLE en procesos judiciales o administrativos.

Durante estos períodos, INSURCOL SAS garantizará medidas de seguridad física y digital, controles de acceso, almacenamiento seguro, monitoreo, trazabilidad y protección contra riesgos tecnológicos, asegurando la continuidad, confidencialidad e integridad de la información.

9.10 Tratamiento de datos personales de Páginas Web, redes sociales y eventos:

INSURCOL SAS recolecta datos personales privados de terceros a través de su página web, redes sociales y demás eventos físicos o digitales en los que participa la empresa de manera directa o en virtud de alianzas comerciales. Dichos datos personales son almacenados en una base de datos la cual es calificada por la compañía como de reserva, y solo será revelada con la expresa autorización del titular o cuando una Autoridad Competente lo solicite.

El tratamiento se realizará bajo criterios de ética, transparencia, seguridad de la información, protección de datos en entornos digitales, gestión del riesgo y cultura de calidad, incorporando controles de ciberseguridad y uso responsable de plataformas tecnológicas.

Las finalidades para las cuales son utilizados los datos personales que son recopilados a través de la página web serán:

- Permite la comunicación con los clientes o terceros mediante la sección de contacto o peticiones, quejas y reclamos disponible en la página web.
- Recepcionar y dar trámite a las quejas y reclamos de los terceros.
- Fines legales, contables y administrativos.
- Dar a conocer el portafolio de productos y servicios que son comercializados por parte de la Empresa.
- Resolver las peticiones, consultas o solicitudes que son gestionadas a través de dichos medios.
- Enviar publicidad o material de interés
- Desarrollar actividades comerciales y de mercadeo, tales como; análisis de uso, perfilamiento de clientes, trazabilidad de marca, envío de beneficios, publicidad, promociones, ofertas, novedades, descuentos, programas de fidelización de clientes, investigación de mercado, generación de campañas y eventos y demás noticias de interés.
- Garantizar que las actividades de mercadeo se realicen conforme a criterios de proporcionalidad, minimización del dato y gestión del riesgo, respetando la privacidad de los titulares.
- Implementar controles de seguridad digital para proteger la información recolectada mediante formularios web, cookies, herramientas analíticas, plataformas de eventos y redes sociales, incluyendo la prevención de accesos indebidos o vulnerabilidades tecnológicas.
- Asegurar la trazabilidad digital y la integridad de la información recopilada en entornos virtuales, evitando su alteración, pérdida o divulgación no autorizada.

En todo caso, la información no será objeto de tratamiento por un período superior a 2 años, y de acuerdo con las circunstancias legales o contractuales que hacen necesario el manejo de la información.

Durante ese período, INSURCOL SAS garantizará medidas adecuadas de seguridad digital, almacenamiento seguro, control de acceso, monitoreo de riesgos tecnológicos y protección de la información conforme a los lineamientos de gestión del riesgo y seguridad de la información

9.11 Tratamiento de Datos de Aprendices SENA

INSURCOL SAS recolectará y tratará los datos personales de los aprendices SENA en cumplimiento de la Ley 789 de 2002 y demás normatividad del contrato de aprendizaje.

Todo tratamiento se realizará bajo criterios de ética, transparencia, cultura de calidad, seguridad de la información, gestión del riesgo y ciberseguridad, garantizando la protección frente a accesos no autorizados, alteración, pérdida o uso indebido de información.

A. Gestión del Contrato de Aprendizaje

- Formalizar y registrar el contrato en la plataforma SGVA del SENA
- Gestionar las etapas lectiva y productiva
- Pagar el apoyo de sostenimiento
- Expedir certificaciones de la relación de aprendizaje

- Asegurar la trazabilidad, integridad documental y disponibilidad de la información del aprendiz en todos los sistemas y plataformas utilizadas, implementando controles de seguridad digital y prevención de riesgos tecnológicos.

B. Obligaciones Legales

- Reportar novedades al SENA
- Cumplir la cuota de aprendices establecida por ley
- Atender auditorías y requerimientos del SENA
- Cumplir con los deberes legales, como afiliaciones al Sistema General de Seguridad Social Integral (EPS, Fondo de Pensiones, ARL, Caja de Compensación Familiar).
- Cumplir con el Sistema de Autocontrol y Gestión del Riesgo Integral de Lavado de Activos, Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (SAGRILAF) y PTEE, de obligatorio cumplimiento para la organización según la normatividad colombiana vigente, incluyendo consultas masivas de manera directa o a través de terceros en fuentes de información nacional y listas restrictivas (OFAC, ONU, Clinton, etc.).
- Implementar acciones preventivas y correctivas cuando se identifiquen riesgos legales, tecnológicos o reputacionales asociados al tratamiento de datos personales de aprendices.

C. Formación y Seguridad

- Asignar funciones acordes al programa de formación
- Realizar evaluaciones médicas ocupacionales
- Capacitar en seguridad y salud en el trabajo
- Cumplir con validaciones SAGRILAF
- Garantizar la protección de datos sensibles del aprendiz (como información médica, evaluaciones, desempeño y seguimiento), mediante controles de acceso, confidencialidad y trazabilidad.
- Asegurar que las capacitaciones y registros de formación sean gestionados como parte del conocimiento organizacional, manteniendo su integridad y disponibilidad.

D. Vigencia del Tratamiento

- Conforme a la normatividad laboral vigente y la reforma laboral, la información de los aprendices SENA se conservará bajo los mismos términos establecidos para los trabajadores en el numeral 9.3 de esta política:
- **Sistema de Gestión de SST:** Hasta veinte (20) años desde la terminación del contrato de aprendizaje
- **Historia de la relación de aprendizaje:** Hasta ochenta (80) años desde la terminación del contrato

Durante estos períodos, INSURCOL SAS implementará medidas de seguridad física y digital, controles de acceso, monitoreo, protección contra riesgos tecnológicos y conservación adecuada de los registros, asegurando la integridad, disponibilidad y confidencialidad de la información almacenada.

10 ATENCIÓN DE CONSULTAS, QUEJAS Y RECLAMOS DEL TITULAR DE LA INFORMACIÓN

INSURCOL SAS, en cumplimiento de la Ley 1581 de 2012 y los Decretos 1377 de 2013 y 1074 de 2015, atenderá cualquier consulta, queja o reclamo relacionado con el manejo de datos personales a través del área de Sistemas. Los titulares de la información pueden presentar sus solicitudes en:

- **Sede Administrativa:** Calle 41 No. 21-32, Barrio Bolívar, Bucaramanga - Colombia., **Ingeniero de Sistemas, igualmente se podrá contar con el apoyo del Ingeniero Informático.**
- **Correo electrónico:** datospersonales@insurcol.com

INSURCOL SAS garantizará que todos los canales de atención operen bajo criterios de seguridad de la información, ciberseguridad, trazabilidad, confidencialidad y cultura de calidad. Asimismo, se implementarán controles para evitar accesos no autorizados, manipulación de solicitudes o pérdida de información durante el proceso de atención.

10.1 Procedimientos para la recepción y resolución de consultas y reclamos

El Titular de la información, sus causahabientes, representante y/o apoderado podrán presentar consultas de manera presencial, escrita o digital, asegurando la protección y confidencialidad de los datos personales.

Todas las consultas serán registradas, clasificadas, gestionadas y archivadas bajo criterios de trazabilidad, integridad y disponibilidad, como parte del Sistema de Gestión de la Calidad.

10.1.1 Opciones para presentar la consulta:

10.1.1.1 Presencial:

- Acudir a la sede administrativa de INSURCOL SAS con documento de identificación.
- En caso de ser presentada por un representante o apoderado, se debe presentar un Poder escrito debidamente firmado, adjuntando la copia del documento de identificación del titular y del apoderado.
- Solicitar dialogar con el Ingeniero de sistemas, quien atenderá la consulta o reclamo a presentar.
- Una vez se ha entrevistado con el ingeniero de sistemas, Este, procede a registrar la consulta en los formatos establecidos por INSURCOL, dentro del sistema de gestión integral y dar continuidad al procedimiento de atención.
- Todo el proceso presencial se realizará bajo controles de seguridad física y documental, garantizando la confidencialidad de la información entregada.

10.1.1.2 Escrita:

- Presentación del relato de la petición o reclamo a realiza, este documento debe incluir la dirección de correspondencia o medio para recibir respuesta.
- Adjuntar una copia del documento de identificación del Titular o del apoderado (en este caso, incluir el poder autenticado).
- Los documentos físicos recibidos serán gestionados bajo prácticas de conservación segura, evitando exposición, deterioro o extravío.

10.1.1.3 Digital:

- Acceder a la página web www.insurcol.com en la sección PQR y diligenciar el formulario.
- Enviar un correo electrónico a datospersonales@insurcol.com.
- Las solicitudes enviadas por medios digitales serán protegidas mediante controles de ciberseguridad, evitando interceptación, pérdida o alteración de datos.
- El sistema registrará automáticamente la fecha, hora, canal y responsable de atención, garantizando trazabilidad completa.

10.1.2 Plazo de Respuesta:

- INSURCOL SAS atenderá la consulta en **un máximo de diez (10) días hábiles** a partir de su recepción.
- Si no es posible responder dentro de este plazo, se notificará al solicitante sobre la demora, explicando los motivos y señalando la fecha en que se resolverá la consulta, de acuerdo con lo establecido en la normativa de **Habeas Data**.
- INSURCOL SAS garantizará que el seguimiento y cierre de cada solicitud esté documentado, registrado y disponible para auditorías internas y externas, conforme a las prácticas de mejora continua del Sistema de Gestión de la Calidad.

10.2 Procedimientos para reclamos

El Titular de la información, sus causahabientes, representante y/o apoderado que consideren que los datos personales en una Base de Datos deben ser **corregida, actualizada o suprimida**, o que adviertan el presunto **incumplimiento** de los deberes establecidos en la Ley 1581 de 2012, podrán presentar un reclamo escrito ante el área responsable, siguiendo estos parámetros:

Todos los reclamos seguirán un proceso formal, documentado y trazable, con medidas de seguridad digital y física para proteger la información involucrada.

10.2.1 Requisitos del Reclamo:

El reclamo debe formularse mediante solicitud escrita dirigida al área de sistemas Ing. de sistemas (ver numeral 10 de la presente política) y debe contener:

- La identificación del Titular.
- La descripción y evidencia de los hechos que sustentan el reclamo.
- La dirección de correspondencia o medio para recibir respuesta
- INSURCOL SAS validará la identidad del solicitante, aplicando controles antifraude y de seguridad para evitar suplantaciones o accesos indebidos.

10.2.2 Proceso de Trámite del Reclamo:

- Si el reclamo está incompleto**, se solicitará al interesado que subsane la información dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo.
- Si el solicitante no responde en dos (2) meses, se entenderá que ha desistido del reclamo.
- Una vez recibido el reclamo completo, en un plazo máximo de cinco **(5) días hábiles**, se incluirá en la Base de Datos de reclamos una leyenda con la indicación **"reclamo en trámite"** y su motivo. Esta leyenda se mantendrá hasta que el reclamo sea resuelto.
- INSURCOL SAS atenderá el reclamo en un plazo máximo de quince (15) días hábiles, contados a partir del día siguiente a la fecha de su recepción.
- Si no es posible atender el reclamo dentro de este plazo**, se informará al interesado sobre la demora, indicando los motivos y la fecha de resolución, la cual no podrá superar los ocho (8) días hábiles posteriores al vencimiento del primer plazo.

Cada etapa del trámite será registrada en el Sistema de Gestión de la Calidad, garantizando trazabilidad, integridad y seguimiento obligatorio.

10.3 Procedimiento para Supresión de Almacenamiento de Datos Personales en Físicos:

Los datos personales almacenados en físicos por parte de INSURCOL SAS., deberán ser eliminados de acuerdo al control de documentos descrito en el **MANUAL DE ADMINISTRACIÓN DE BASES DE DATOS PERSONALES**. Este aplica únicamente para las siguientes finalidades:

- De acuerdo a la vigencia establecida en el manual
- Cuando el titular de los datos así los solicite.

11 REQUISITO DE PROCEDIBILIDAD

El titular de la información o su causahabiente sólo podrá presentar una queja ante la **Superintendencia de Industria y Comercio**, una vez haya agotado el trámite de consulta o reclamo ante INSURCOL SAS., de conformidad con lo establecido en la normativa vigente.

INSURCOL SAS garantizará que este trámite interno sea atendido bajo criterios de oportunidad, transparencia, ética, gestión del riesgo, seguridad de la información y cultura de calidad.

Durante el proceso de atención, la organización asegurará la trazabilidad de cada solicitud, la confidencialidad de la información suministrada y el registro adecuado en el Sistema de Gestión Integral, garantizando que no existan barreras indebidas para el ejercicio del derecho fundamental de Habeas Data.

Asimismo, INSURCOL SAS implementará controles que aseguren la correcta documentación, seguimiento y cierre de las solicitudes, permitiendo evidencia verificable para auditorías internas y externas, fortaleciendo la mejora continua del proceso y la gestión de riesgos legales y reputacionales.

12 CASOS EN LOS QUE, NO ES NECESARIA LA AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

De acuerdo con lo dispuesto en el artículo 10 de la ley 1581 de 2012, NO se requerirá la autorización del Titular para el tratamiento de sus datos personales en los siguientes casos:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública, según lo establecido en la ley
- Casos de urgencia médica o sanitaria, en los que se requiera el tratamiento de datos personales para proteger la salud y la vida del Titular.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

En todos los casos anteriores, INSURCOL SAS garantizará que el tratamiento se realice bajo criterios de ética, seguridad de la información, confidencialidad, gestión del riesgo y cultura de calidad, aplicando controles que eviten accesos no autorizados, divulgaciones indebidas o tratamientos excesivos de datos personales. Cualquier tratamiento realizado bajo estos supuestos deberá quedar documentado y ser verificable en auditorías internas o externas, como parte de los mecanismos de control, transparencia y mejora continua del Sistema de Gestión Integral.

13 AUTORIZACIÓN PARA TRATAMIENTO DE DATOS SENSIBLES:

Para la recolección y tratamiento de datos sensibles, se deben cumplir los siguientes requisitos

- Obtener una autorización explícita, previa o concomitante a la recolección.
- Informar al Titular que no está obligado a suministrar estos datos
- Implementar medidas de seguridad especiales como cifrado de bases de datos, control de accesos y copias de seguridad en ubicaciones seguras.
- Garantizar la aplicación de medidas reforzadas de seguridad de la información y ciberseguridad, considerando el alto nivel de riesgo asociado al tratamiento de este tipo de datos,
- Aplicar estrictamente los principios de confidencialidad y trazabilidad durante todo el ciclo de vida de los datos sensibles.
- Documentar y registrar todas las actividades de tratamiento, incluyendo accesos, modificaciones, almacenamiento y eliminación, garantizando evidencia verificable para auditorías internas y externas.

13.1 Autorización para tratamiento de datos de niños, niñas y adolescentes (NNA):

INSURCO SAS, no realiza de forma directa el tratamiento de datos personales de menores de edad; sin embargo, de forma particular la Empresa recolecta y trata los datos personales de los hijos menores de edad de sus trabajadores o aprendices SENA, con la única finalidad de cumplir con las obligaciones que impone la Ley a los empleadores en relación con las afiliaciones a sistema de seguridad social y parafiscales, así como el cumplimiento de la jornada familiar (Ley 1857 de 2017), y en particular para permitir el disfrute de los derechos fundamentales de los niños a la salud, la recreación y el derecho a la familia.

En todo caso, recolectará cuando corresponda la respectiva autorización a sus representantes legales para su tratamiento, teniendo siempre de presente el interés superior del menor y el respeto de los derechos prevalentes de los niños, niñas y adolescentes consagrados en el artículo 44 de la constitución política de Colombia.

14 PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES:

En el desarrollo, interpretación y aplicación de la presente política, se aplicarán, de manera armónica e integral, los siguientes principios:

14.1 PRINCIPIOS RELACIONADOS CON LA RECOLECCIÓN DE DATOS PERSONALES.

La recolección y tratamiento de datos personales debe realizarse con fines lícitos, bajo principios éticos, transparencia y cultura de calidad, asegurando que el titular comprenda la finalidad del tratamiento, y en cumplimiento de la normatividad vigente, Los datos personales solo se podrán recolectar y tratar cuando sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para

las que se hayan obtenido, aplicando el enfoque basado en riesgos para identificar y mitigar riesgos asociados a la recolección de datos (tecnológicos, operativos, reputacionales y legales).

Los datos personales serán tratados de manera justa y legal y transparente. NO podrán utilizarse para fines incompatibles con aquellos para los que fueron recolectados. Salvo para propósitos históricos, estadísticos o científicos, siempre que se adopten medidas de seguridad adecuadas.

Los datos personales serán exactos y actualizados. Si se determinan que son inexactos o incompletos, se procederá a su actualización, rectificación o supresión conforme a lo solicitud del titular o por iniciativa de la organización. Solo se recolectarán los datos personales estrictamente necesarios para cumplir con las finalidades del tratamiento, prohibiéndose el registro y divulgación de datos irrelevantes. Se aplicará el principio de minimización de datos para garantizar que el procesamiento de información sea el mínimo necesario para el cumplimiento de los fines previstos.

14.2 PRINCIPIOS GENERALES PARA LA RECOLECCIÓN DE DATOS:

La Organización tendrá en cuenta los siguientes principios para la recolección de datos:

- **Adecuación:** Los datos deben ser adecuados para las finalidades previstas.
- **Pertinencia:** Los datos deben ser pertinentes para los fines del tratamiento.
- **Proporcionalidad:** Los datos deben ser acordes con las finalidades para las cuales fueron previstos.

Se aplicarán mecanismos de seguridad informática y controles documentales para proteger la información desde el momento de su recolección.

14.2.1 PRINCIPIO DE DIGNIDAD:

Toda acción u omisión relacionada con el tratamiento de datos personales debe ejecutarse siempre salvaguardando la dignidad del Titular y respetando sus derechos constitucionales. Esto incluye, de manera especial, el derecho al buen nombre, a la honra, a la intimidad y el derecho a la información. La protección de la dignidad del Titular implica que cualquier manejo de sus datos personales debe realizarse con respeto y consideración, evitando cualquier forma de abuso o maltrato.

INSURCOL SAS adoptará un enfoque ético en el manejo de datos, garantizando que los procesos estén alineados con la cultura organizacional.

14.3 PRINCIPIOS RELACIONADOS CON EL USO DE DATOS PERSONALES.

- **FINALIDAD:** Los datos deben ser tratados para propósitos explícitos, informados y legítimos.
- **TEMPORALIDAD:** Se conservarán solo por el tiempo necesario para el cumplimiento de sus fines y obligaciones legales
- **NO DISCRIMINACIÓN:** Está prohibido realizar actos discriminatorios con base en la información recolectada.

INSURCOL SAS garantizará que el uso de los datos se realice bajo métricas de calidad, trazabilidad y control documental, evitando cualquier uso indebido, exceso o riesgo operacional.

14.3.1 PRINCIPIO DE LEGALIDAD:

El tratamiento de datos personales es una actividad regulada que debe cumplir estrictamente con todas las disposiciones legales y normativas aplicables. Según la Ley 1581 de 2012, esta actividad debe enmarcarse dentro de los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

INSURCOL SAS implementará procedimientos documentados que aseguren el cumplimiento normativo, la evaluación constante del contexto regulatorio y la mitigación de riesgos legales

14.3.2 PRINCIPIO DE LIBERTAD:

El tratamiento de datos personales solo puede llevarse a cabo con el consentimiento previo, expreso e informado del Titular. Esto significa que el Titular debe ser claramente informado sobre las finalidades específicas para las cuales se recolectarán y utilizarán sus datos, y debe otorgar su autorización de manera libre y consciente. Todo procedimiento de autorización será trazable, verificable y gestionado mediante controles que garanticen la integridad, disponibilidad y autenticidad.

14.4 PRINCIPIOS RELACIONADOS CON LA CALIDAD DE LA INFORMACIÓN.

- **VERACIDAD O CALIDAD:** La información debe ser exacta, completa, actualizada y comprobable. Se prohíbe el tratamiento de datos parciales, inexactos o que induzcan a error.

14.4.1 PRINCIPIO DE INTEGRIDAD:

En el tratamiento de datos personales, se debe garantizar el derecho del Titular a obtener información del responsable o del Encargado del Tratamiento sobre la existencia de datos que le conciernan, en cualquier momento y sin restricciones.

INSURCOL SAS aplicará controles para asegurar la integridad digital y documental, evitando alteraciones, manipulaciones o pérdidas de información.

14.5 PRINCIPIOS RELACIONADOS CON LA PROTECCIÓN, EL ACCESO Y CIRCULACIÓN DE DATOS PERSONALES.

- **SEGURIDAD:** Se implementarán medidas técnicas y administrativas para evitar acceso no autorizado, pérdida o uso indebido de la información.
- **TRANSPARENCIA:** El titular tiene derecho a obtener información sobre sus datos en cualquier momento.
- **ACCESO RESTRINGIDO:** Sólo podrán acceder a los datos:
 - ✓ Titular del dato.
 - ✓ Personas autorizadas por el Titular.
 - ✓ Autoridades por mandato legal
- **CIRCULACIÓN RESTRINGIDA:** La información solo se suministrará a:
 - ✓ Titular del dato, sus causahabientes o sus representantes legales.
 - ✓ Personas autorizadas por la ley o por el Titular
 - ✓ Entidades públicas en ejercicio de sus funciones, bajo medidas de protección adecuadas.
- **CONFIDENCIALIDAD:** Todas las personas que intervengan en el tratamiento de datos personales deben garantizar la reserva de la información, adoptará controles de ciberseguridad, gestión del riesgo, auditorías internas y monitoreo continuo para asegurar la circulación segura de datos.
 - ✓ incluso después de finalizada su relación con la Organización.

14.6 PRINCIPIOS RELACIONADOS CON LA TRANSFERENCIA Y TRANSMISIÓN DE DATOS

- **Transferencia internacional:** Solo se podrán transferir datos personales a países que garanticen un nivel adecuado de protección.
- **Contrato de transmisión:** Cuando los datos sean transmitidos a encargados del tratamiento, se suscribirá un contrato que garantice su protección.

Estos principios aseguran que el tratamiento de los datos personales se realice conforme a las mejores prácticas y en cumplimiento de la normativa vigente.

Actualmente la Empresa no realiza transferencia ni transmisión Internacional de datos personales relacionados con información contenida en sus bases de datos. En caso de que **INSURCOL SAS** requiera realizar dicha transferencia, verificará que el país de destino reúna los estándares que garantizan un nivel adecuado de protección de datos personales, lo anterior de acuerdo con el numeral 3.2. del Capítulo tercero, del Título V de la Circular Única 005 del 10 de agosto de 2017 de la Superintendencia de Industria y Comercio.

Adicionalmente, en caso de que **INSURCOL SAS** realice Transmisión internacional de datos personales, además de contar con la autorización expresa e inequívoca por parte del Titular, se asegurará que la acción proporciona los niveles adecuados de protección de datos y atiende a los requisitos fijados en Colombia por el Régimen de Hábeas Data.

Por otro lado, cuando **INSURCOL SAS** decida realizar una Transferencia Internacional de datos podrá hacerlo sin autorización de los titulares, siempre y cuando garantice la seguridad de la información, confidencialidad y las condiciones que regulen el alcance del tratamiento de los datos, de acuerdo con lo establecido en el artículo 10 de la Ley 1581 de 2012.

15 TIPO DE TRATAMIENTO AL QUE SERAN SOMETIDOS LOS DATOS PERSONALES.

De conformidad con lo estipulado en los Decretos Reglamentarios, que regulan las Políticas de Tratamiento de Datos Personales, se informa a los Titulares, que su información, puede ser usada, almacenada y conservada en medios electrónicos como físicos.

El almacenamiento de la información digital y física se realiza en medios o ambientes que cuentan con adecuados controles para la protección de los datos, implementando medidas de ciberseguridad, autenticación, registro de accesos y monitoreo continuo para garantizar la trazabilidad, integridad, disponibilidad y confidencialidad de la información. Lo anterior conlleva controles de seguridad física e informática, tecnológicos y de tipo ambiental en todas las áreas de la compañía, tanto en instalaciones propias, centros de cómputo y sitios para el almacenamiento documental.

De conformidad con el principio de transparencia, los Titulares tienen acceso en todo momento (previa solicitud escrita o verbal) a la información almacenada, como también, sus causahabientes que acrediten su calidad, el representante y/o apoderado del Titular, por una autoridad competente y por estipulación a favor de otro o para otro.

Las finalidades o propósitos de su recolección, almacenamiento, uso y disposición se regulan de conformidad con lo estipulado en la ley 1581 de 2012, sus decretos reglamentarios y la presente Política.

16 ALMACENAMIENTO DE DATOS PERSONALES.

El Titular otorga su consentimiento expreso a **INSURCOL** para que almacene sus datos personales de la manera que considere más adecuada, siempre y cuando se cumplan con las medidas de seguridad necesarias para proteger dicha información. **INSURCOL** se compromete a implementar y mantener protocolos de seguridad robustos y actualizados, que incluyan tanto medidas técnicas como organizativas, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales. Estas medidas de seguridad están diseñadas para prevenir el acceso no autorizado, la pérdida, alteración o divulgación indebida de la información. Además, **INSURCOL** se asegurará de que el almacenamiento de los datos cumpla con todas las normativas legales y regulaciones aplicables, proporcionando así una protección integral y efectiva de los datos personales del Titular.

17 MEDIDAS DE SEGURIDAD: INSURCOL

INSURCOL S.A.S., se compromete al uso correcto y tratamiento de los datos personales, evitando el acceso no autorizado de terceros que permita conocer o vulnerar, modificar, divulgar y/o destruir la información que reposa en sus bases de datos. Por tal motivo, **INSURCOL** cuenta con protocolos de seguridad y acceso a sus sistemas de información, almacenamiento y procesamiento incluidas medidas físicas de control de riesgos de seguridad.

18 DERECHOS DE LOS TITULARES. INSURCOL

INSURCOL S.A.S., informa a los titulares que, conforme a la legislación vigente, estos tienen el derecho de conocer, actualizar, rectificar su información, y/o revocar la autorización para su tratamiento. En particular, son derechos de los titulares según se establece en el artículo 8 de la Ley 1581 de 2012:

- Conocer, actualizar y rectificar su información frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté prohibido o no haya sido autorizado.
- Solicitar prueba de la autorización otorgada para el tratamiento de sus datos.
- Ser informado, previa solicitud, respecto del uso que le ha dado a sus datos personales,
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley.
- Revocar la autorización y/o solicitar la supresión del dato, siempre que no exista un deber legal o contractual que impida eliminarlos.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

RUTA ARCHIVO: E:/ISO9000/7.APOYO/7.1.4 AMBIENTE PARA LA OPERACION DE LOS PROCESOS/IN-AZD56-F01 POLITICA DE TRATAMIENTO DE DATOS PERSONALES

"El presente documento es propiedad de Insurcol. Los derechos de uso y reproducción se limitan a la organización para fines empresariales. Está prohibido hacer cualquier tipo de reproducción parcial o total de este documento sin autorización escrita de Insurcol. Ninguna parte del documento podrá ser reproducido, copiado o transmitido digitalmente de acuerdo con las leyes que regulan los derechos de autor."

- g) Abstenerse de responder las preguntas sobre datos sensibles. Tendrá carácter facultativo las respuestas que versen sobre datos sensibles o sobre datos de las niñas y niños y adolescentes.
- h) INSURCOL SAS garantizará atención oportuna, trazabilidad de solicitudes, registro documental y mecanismos seguros para validar identidad del solicitante.

19 MEDIDAS DE PREVENCIÓN PARA GARANTIZAR LOS PRINCIPIOS BÁSICOS DE LA INFORMACIÓN

- Informar y capacitar al personal de la empresa, para garantizar la adecuada recolección, manejo, uso, tratamiento, almacenamiento e intercambio de la información personal.
- Incluir acuerdos de confidencialidad de la información para todos los trabajadores de la compañía en sus contratos de trabajo.
- Implementar formación periódica en seguridad digital, ética, cultura de calidad, ciberseguridad y gestión del riesgo.
- Registrar evidencia de capacitaciones como parte del Sistema de Gestión de la Calidad y del conocimiento organizacional.
- Realizar monitoreos preventivos y auditorías internas para identificar brechas y oportunidades de mejora.

20 TRATAMIENTO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Cuando se tenga conocimiento de pérdida de información física y/o ataque cibernéticos que ponga en riesgo la protección de los datos personales recopilados en las bases de datos de la Compañía, El oficial de cumplimiento de la Empresa informará oportunamente a la Superintendencia de Industria y Comercio y a los titulares de la información sobre lo ocurrido.

Una vez reportado el incidente y establecida su causa, se implementará un plan de acción para evitar que la situación vuelva a ocurrir.

INSURCOL SAS activará un protocolo de respuesta a incidentes basado en análisis de riesgo, contención, mitigación, recuperación y mejora continua.

Todos los incidentes serán documentados, trazados y evaluados como entrada para el análisis de riesgos del Sistema de Gestión de la Calidad.

21 PROCEDIMIENTO PARA EL EJERCICIO DEL DERECHO DE HABEAS DATA

- a. En caso de que desee ejercer sus derechos, el titular deberá enviar un correo electrónico o físico a las siguientes direcciones de contacto

Dirección: Calle 41 No 21-32

Correo electrónico: datospersonales@insurcol.com

- b. **Peticiones y Consultas Sobre Datos Personales.** Cuando el titular de los datos o sus causahabientes deseen consultar la información que reposa en la base de datos, **INSURCOL** responderá la solicitud en plazo de máximo diez (10) días. En cumplimiento a lo dispuesto en la Ley 1581 de 2012, cuando no fuere posible atender la consulta dentro de dicho término, se informará al usuario, se le expresará los motivos de la demora y se le señalará la fecha en que se atenderá su consulta, la cual no podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

- c. **Revocación de autorización, retiro o supresión de la Base de Datos y reclamos Sobre Datos Personales.** Cuando el titular de los datos o sus causahabientes consideren que la información contenida en las bases de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1581 de 2012, podrán presentar un reclamo ante **INSURCOL**, el cual será tramitado bajo las siguientes reglas:

- d. El reclamo se formulará mediante solicitud dirigida a **INSURCOL**. Para la radicación y atención de su solicitud le solicitamos suministrar la siguiente información:

- I. Nombre completo y apellidos
- II. Datos de contacto (Dirección física y/o electrónica y teléfonos de contacto),
- III. Medios para recibir respuesta a su solicitud,
- IV. Motivo(s)/hecho(s) que dan lugar al reclamo con una breve descripción del derecho que desea ejercer (conocer, actualizar, rectificar, solicitar prueba de la autorización otorgada, revocarla, suprimir, acceder a la información)
- V. Firma (si aplica) y número de identificación.
- VI. Anexos de los documentos que se quieran hacer valer.

RUTA ARCHIVO: E:/ISO9000/7.APOYO / 7.1.4 AMBIENTE PARA LA OPERACIÓN DE LOS PROCESOS /IN-AZD56-F01 POLITICA DE TRATAMIENTO DE DATOS PERSONALES

"El presente documento es propiedad de Insurcol. Los derechos de uso y reproducción se limitan a la organización para fines empresariales. Está prohibido hacer cualquier tipo de reproducción parcial o total de este documento sin autorización escrita de Insurcol. Ninguna parte del documento podrá ser reproducido, copiado o transmitido digitalmente de acuerdo con las leyes que regulan los derechos de autor."

Si el reclamo resulta incompleto, INSURCOL podrá requerir al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo. En caso de que **INSURCOL** no sea competente para resolver el reclamo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al Titular, con lo cual quedará relevada de cualquier reclamación o responsabilidad por el uso, rectificación o supresión de los datos.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

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 atender el reclamo dentro de dicho término, se informará al Titular 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.

INSURCOL SAS garantizará que todos los procedimientos sean trazables, auditables y registrados dentro del Sistema Integrado de Gestión.

- Los procesos serán ejecutados bajo criterios de transparencia, ética, veracidad, seguridad digital y control documental.
- Se incorporará análisis de riesgos para prevenir suplantaciones, errores, accesos indebidos o manipulación de información durante la atención.

22 VIGENCIA

Los datos personales incorporados en la Base de Datos estarán vigentes durante el plazo necesario para cumplir sus finalidades.

Las bases de datos en las que se registrarán los datos personales tendrán una vigencia igual al tiempo en que se mantenga y utilice la información para las finalidades descritas en esta política. Una vez se cumpla(n) esa(s) finalidad(es) y siempre que no exista un deber legal o contractual de conservar su información, sus datos serán eliminados de nuestras bases de datos.

23 CAMBIOS EN LA POLITICA DE PRIVACIDAD.

Cualquier cambio sustancial en las políticas de Tratamiento, será comunicado oportunamente a los Titulares mediante la publicación en nuestros portales web.

INSURCOL SAS mantendrá control documental de versiones, historial de cambios, trazabilidad normativa y evidencia de divulgación a los titulares.

- La organización aplicará revisión periódica de esta política como parte del ciclo de mejora continua.

24 LEGISLACIÓN VIGENTE.

La legislación nacional vigente en materia de protección de datos personales está contenida en la Ley 1581 de 2012, el Decreto 1377 de 2013 y la Ley 1266 de 2008 y las normas que lo modifiquen o complementen.



CLAUDIA MARCELA MARTINEZ SILVA
Subgerente / Representante legal suplente

Fecha de última revisión: 27 de diciembre de 2025

Fecha de Revisión Actual: 13 de marzo de 2026

Se actualizó en la página web: SI ☒ NO ☐

Fecha de actualización en la página web: 13 de marzo de 2026