POLÍTICA DE TRATAMIENTO DE DATOS

OBJETIVO GENERAL

El propósito de la presente Política es garantizar el cumplimiento de las disposiciones legales en materia de protección de datos personales, estableciendo directrices claras para el adecuado manejo de la información recolectada, almacenada, usada, transmitida y/o suprimida por la Empresa. De esta manera, se busca salvaguardar los derechos de los titulares, minimizar riesgos asociados al uso indebido de la información y prevenir eventuales conflictos legales derivados de un tratamiento inadecuado de los datos.

La Empresa informa que todos los datos personales obtenidos en el marco de sus operaciones serán tratados de conformidad con los principios, derechos y obligaciones previstos en la Ley 1581 de 2012, sus decretos reglamentarios y demás normas que regulen la materia.

ALCANCE

La presente Política es aplicable a todas las bases de datos y archivos que contengan información personal y que sean objeto de tratamiento por parte de la Empresa, en su calidad de responsable o encargado del tratamiento.

En consecuencia, todos los funcionarios, colaboradores, contratistas, proveedores y terceros que, en virtud de su relación con la Empresa, tengan acceso o realicen cualquier operación de tratamiento sobre datos personales, deberán dar estricto cumplimiento a lo aquí dispuesto, así como a los procedimientos internos adoptados para garantizar la seguridad, confidencialidad y legalidad en el manejo de la información.

MARCO NORMATIVO

Seguridad Jano Ltda.**,** consagra las disposiciones generales para la protección de datos personales a las cuales se acoge y adopta la política de tratamiento de datos personales para garantizar el adecuado cumplimiento normativo. Teniendo en cuenta las disposiciones contenidas en los artículos 15 y 20 de la Constitución Política de Colombia, y en virtud de lo establecido en la Ley 1581 de 17 de octubre de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”, el Decreto 1377 de 2013 “Por el cual se reglamenta parcialmente la Ley 1581 de 2012” y el Decreto 886 de 2014, “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos”, y todas las demás normas que complementen o sustituyan las anteriores.

FINALIDAD CON LA QUE SE EFECTÚA LA RECOLECCIÓN DE DATOS PERSONALES Y TRATAMIENTO DE LOS MISMOS

Seguridad Jano Ltda., podrá hacer uso de los datos personales para:

- Ejecutar la relación contractual existente con sus clientes, proveedores y trabajadores. incluida el pago de obligaciones contractuales.
- Proveer los servicios y/o los productos requeridos por sus usuarios.
- Informar sobre nuevos productos o servicios y/o sobre cambios en los mismos.
- Evaluar la calidad del servicio.
- Realizar estudios internos sobre hábitos de consumo.
- Enviar al correo físico, electrónico, celular o dispositivo móvil, vía mensajes de texto (SMS y/o MMS) o a través de cualquier otro medio análogo y/o digital de comunicación creado o por crearse, información comercial, publicitaria o promocional sobre los productos y/o servicios, eventos y/o promociones de tipo comercial o no de estas, con el fin de impulsar, invitar, dirigir, ejecutar, informar y de manera general, llevar a cabo campañas, promociones o concursos de carácter comercial o publicitario, adelantados por Seguridad Jano Ltda., y/o por terceras personas.
- Desarrollar el proceso de selección, evaluación, y vinculación laboral.
- Soportar procesos de auditoría interna o externa.
- Registrar la información de empleados y/o pensionados (activos e inactivos) en las bases de datos de Seguridad Jano Ltda.
- Los indicados en la autorización otorgada por el titular del dato o descritos en el aviso de privacidad respectivo, según sea el caso.
- Suministrar, compartir, enviar o entregar sus datos personales a empresas filiales, vinculadas, o subordinadas de Seguridad Jano Ltda., ubicadas en Colombia o cualquier otro país en el evento que dichas compañías requieran la información para los fines aquí indicados.

Respecto de los datos recolectados directamente por funcionarios de Seguridad Jano Ltda., en puestos de trabajo, y durante la realización de funciones propias de su actividad económica y que sean tomadas de los documentos o que suministran las partes interesadas, a Seguridad Jano Ltda., y obtenidos de los registros fotográficos y de las videograbaciones que se realizan dentro o fuera de las instalaciones, éstos se utilizarán para fines de seguridad de las personas naturales y jurídicas, los bienes e instalaciones y podrán ser utilizados como prueba en cualquier clase de investigación judicial, fiscal, administrativa y disciplinaria, y por tanto, Seguridad Jano Ltda., no procederá a vender, licenciar, transmitir, o divulgar la misma, salvo que:

- Exista autorización expresa para hacerlo por parte de la autoridad competente.
- Sea necesario para permitir a los contratistas o agentes prestar los servicios encomendados.
- Sea necesario con el fin de proveer nuestros servicios y/o productos.
- Sea necesario divulgarla a las entidades que prestan servicios de mercadeo en nombre de Seguridad Jano Ltda., y/o a otras entidades con las cuales se tengan acuerdos de mercado conjunto, y la información tenga relación con una fusión, consolidación, adquisición, desinversión, u otro proceso de restructuración de la sociedad.
- Que sea requerido mediante orden judicial, y/o entidad competente.

- Seguridad Jano Ltda., podrá subcontratar a terceros para el procesamiento de determinadas funciones o información.
- Cuando efectivamente se subcontrate con terceros el procesamiento de información personal o se proporcione información personal a terceros prestadores de servicios, Seguridad Jano Ltda., advierte a dichos terceros sobre la necesidad de proteger dicha información personal con medidas de seguridad apropiadas, se prohíbe el uso de la información para fines propios y se solicite que no se divulgue la información personal a otros.

DEFINICIONES

Las siguientes definiciones, tomadas de la Ley 1581 de 2012, sus decretos reglamentarios y normas complementarias, constituyen la base para la interpretación y aplicación de la presente Política:

A. Aviso de privacidad: Comunicación verbal o escrita generada por el responsable del tratamiento, dirigida al titular para informarle sobre la existencia de las políticas de tratamiento de información, la forma de acceder a ellas y la finalidad del tratamiento de sus datos personales.
B. Confidencialidad: Propiedad de la información que impide su divulgación a personas, procesos o sistemas no autorizados.
C. Dato Privado: Información de carácter íntimo o reservado que solo es relevante para el titular.
D. Dato Público: Información calificada como tal por la Ley o la Constitución Política, así como aquella que no es semiprivada o privada. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales ejecutoriadas no sometidas a reserva y los relativos al estado civil de las personas.
E. Dato Semiprivado: Información que no es de naturaleza íntima ni pública, y cuyo conocimiento o divulgación interesa tanto a su titular como a un grupo determinado de personas o a la sociedad en general. Ejemplo: información financiera, crediticia, comercial o de servicios.
F. Datos Sensibles: Información que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación, como datos sobre origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos, organizaciones sociales o de derechos humanos, así como datos relativos a la salud, la vida sexual o biométricos. Su tratamiento está prohibido, salvo las excepciones previstas en el artículo 6 de la Ley 1581 de 2012.
G. Disponibilidad: Cualidad de la información de estar accesible y utilizable por personas, procesos o aplicaciones autorizadas cuando se requiera.
H. Política: Declaración formal de intenciones y lineamientos de la organización en materia de protección de datos personales, expresada por la alta dirección.

I. Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que decide sobre la recolección y tratamiento de los datos personales.
J. Seguridad de la Información: Conjunto de medidas y prácticas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, garantizando la continuidad del negocio, minimizando riesgos y reduciendo pérdidas por daños.
K. Titular: Persona natural cuyos datos personales son objeto de tratamiento.
L. Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, como recolección, almacenamiento, uso, circulación o supresión.
M. Definiciones adicionales que podrías incluir para robustecer el documento:
N. Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que realiza el tratamiento de datos personales por cuenta del responsable.
O. Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de sus datos personales.
P. Causahabiente: Persona que ha sucedido o se ha subrogado por cualquier título en el derecho de otra u otras.

PRINCIPIOS

Los principios que se establecen a continuación, constituyen los parámetros generales que serán respetados por Seguridad Jano Ltda. En los procesos de recolección, uso y tratamiento de datos personales.

1. **Principio de Legalidad en materia de tratamiento de datos personales:** El tratamiento de los datos personales es una actividad reglada que debe sujetarse a lo establecido en la legislación colombiana, especialmente a lo consagrado en la Ley 1581 de 2012 y demás disposiciones que reglamenten, modifiquen o adicionen la materia.
2. **Principio de Finalidad:** El tratamiento de los datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución colombiana y la Ley, la cual debe ser comunicada al titular de la información.
3. **Principio de Libertad:** El Tratamiento sólo puede llevarse a cabo con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
4. **Principio de Veracidad o Calidad**: La información personal sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y compresible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
5. **Principio de Transparencia:** En el tratamiento de los datos personales debe garantizarse a los titulares el derecho de acceso y conocimiento de su información de carácter personal en cualquier momento y sin restricciones.
6. **Principio de Acceso y Circulación Restringida:** El tratamiento de los datos personales está sujeto a los límites de la naturaleza de los mismos, de las disposiciones legales vigentes, de la Constitución y a las disposiciones del presente manual. En este sentido, solo podrán tener

acceso a los datos personales los responsables y/o encargados del tratamiento, previa autorización expresa del titular de la información. Los datos personales, excepto la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo previa autorización expresa del titular de la información personal y que este acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados.

7. **Principio de Seguridad:** La información personal sujeta a tratamiento por parte de Seguridad Jano Ltda., debe ser manejada con las medidas técnicas, humanas y administrativas necesarias para otorgar la seguridad pertinente a los registros, evitando así su adulteración, perdida, consulta, uso o acceso no autorizado y/o fraudulento.
8. **Principio de Confidencialidad:** Todas las personas que intervengan en el tratamiento de datos personales, que no tengan la naturaleza de públicos, están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento de la información personal, pudiendo sólo suministrar o comunicar los datos personales cuando ello corresponda al desarrollo de las actividades autorizadas por la Ley colombiana y en los términos definidos por la misma.

DERECHOS DE LOS TITULARES

Los Titulares de datos personales que reposen en las bases de datos de la Empresa, tienen los siguientes derechos:

a) Derecho a conocer, actualizar y rectificar sus datos personales: Los titulares de datos personales podrán ejercer este derecho frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

b) Derecho a solicitar prueba de la autorización: Los titulares de datos personales podrán solicitar prueba de la autorización otorgada para el tratamiento de sus datos, de conformidad con lo previsto en el artículo 9 de la Ley 1581 de 2012. Se exceptúan de esta obligación los datos señalados en el artículo 10 de esta Ley.

c) Derecho a ser informado frente al uso que se le ha dado a sus datos personales: Los titulares de datos personales tienen derecho a conocer en cualquier momento el uso que se les ha dado a sus datos personales previa solicitud dirigida al responsable del Tratamiento.

d) Derecho a revocar la autorización y/o a solicitar la supresión del dato: Los titulares de datos personales podrán revocar la autorización otorgada a la Empresa para el Tratamiento de sus datos personales, si evidencian que no han sido respetados los principios, derechos y garantías constitucionales y legales.

e) Derecho a acceder a sus datos personales: Los titulares de datos personales podrán acceder de forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

DEBERES DEL RESPONSABLE DE TRATAMIENTO

En cumplimiento de lo dispuesto en el artículo 17 de la Ley 1581 de 2012, la Empresa, en calidad de responsable del Tratamiento de datos personales, deberá cumplir con los siguientes deberes:

a) Garantizar al titular, en todo momento, el pleno y efectivo ejercicio del derecho de hábeas data.
b) Solicitar y conservar copia de la autorización otorgada por el titular para el tratamiento de sus datos, en los casos en que la Ley lo requiera.
c) Informar de manera clara y previa al titular la finalidad para la cual se recolectan sus datos y los derechos que le asisten en virtud de la autorización concedida.
d) Conservar la información bajo condiciones de seguridad adecuadas, a fin de impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
e) Garantizar que la información suministrada al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
f) Actualizar oportunamente la información, comunicando al encargado del tratamiento todas las novedades respecto de los datos previamente suministrados.
g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.
h) Suministrar al encargado del tratamiento, cuando corresponda, únicamente los datos cuyo tratamiento haya sido previamente autorizado, conforme a lo dispuesto en la Ley 1581 de 2012.
i) Exigir al encargado del tratamiento el cumplimiento de las condiciones de seguridad y privacidad de la información del titular.
j) Tramitar consultas, peticiones y reclamos formulados por los titulares en los términos establecidos en la Ley.
k) Adoptar procedimientos internos que garanticen el cumplimiento de la normativa vigente en materia de protección de datos, especialmente en lo relacionado con la atención de consultas y reclamos.
l) Informar al encargado del tratamiento cuando determinada información se encuentre en discusión por parte del titular, una vez se haya presentado la reclamación y no se haya resuelto el trámite respectivo.
m) Informar a la autoridad de protección de datos (Superintendencia de Industria y Comercio) cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
o) Respetar y garantizar, en todo momento, los principios rectores del tratamiento de datos personales establecidos en la legislación vigente.

TRATAMIENTO DE LA INFORMACIÓN DE LOS DATOS PERSONALES

Seguridad Jano Ltda., no vende ni alquila a terceros las bases de datos personales que obtiene en desarrollo de su objeto social, esta información solo será tratada para los fines autorizados por los titulares de la información, garantizando a los titulares de la misma mantenerla con un alto grado de privacidad, seguridad y confidencialidad. Toda la información recopilada por Seguridad Jano Ltda., se encuentra protegida en archivos físicos y digitales, en servidores propios, internos y externos los cuales se encuentran debidamente resguardados.

La información recogida y suministrada por los titulares de la información, cuenta con accesos restringidos para el personal de Seguridad Jano Ltda. Y se encuentra protegida por medio de usuarios y contraseñas de administrador.

Toda la información de datos personales, de los titulares de la información que recoge Seguridad Jano Ltda., para su tratamiento, podrá ser transferida total o parcialmente al exterior, siempre dando cumplimiento a los requerimientos legales para la realización de dicha transferencia. De igual forma, la información seguirá manteniéndose con la misma privacidad y seguridad con la que se mantenía en Seguridad Jano Ltda., y solo será tratada para los fines autorizados por el titular de la información.

PROCEDIMIENTO PARA ATENCIÓN Y RESPUESTA A PETICIONES, CONSULTAS, QUEJAS Y RECLAMOS DE LOS TITULARES DE DATOS PERSONALES

Los titulares de los datos personales que estén siendo recolectados, almacenados, procesados, usados y transmitidos o transferidos por la Empresa, podrán ejercer en cualquier momento sus derechos a conocer, actualizar y rectificar la información. Para el efecto, se seguirá el siguiente procedimiento:

- El titular, sus causahabientes o representantes legales que consideren que la información contenida en la base de datos debe ser objeto de rectificación, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la de Ley de Protección de Datos Personales, podrán presentar la reclamación.

- La radicación de solicitudes de Consulta y/o Reclamaciones de datos personales, el titular o sus causahabientes o sus representantes legales, puede utilizar los siguientes canales habilitados para la atención de quejas y soluciones:

    a. Aquellos que se presenten en físico se encuentra disponible la ventanilla de Correspondencia - Carrera 40ª #16-05 - Barrio Villamaría (Villavicencio - Meta).

    b. Aquellos que se presenten en formato digital, deberán ser remitidos a través del siguiente correo: servicioalcliente@seguridadjano.com.

- Las solicitudes deberán, como mínimo, cumplir con los siguientes requisitos:

    1) Los nombres y apellidos completos del solicitante y de su representante o apoderado si es el caso, con indicación del documento de identidad, la dirección donde recibirá la correspondencia. El peticionario podrá agregar el número de teléfono o correo electrónico.
    2) El objeto de la petición.
    3) Las razones en las que fundamenta su petición.
    4) La relación de los documentos que desee presentar para iniciar el trámite.
    5) La firma del peticionario, representante o apoderado cuando fuere el caso.

Las solicitudes serán tramitadas y contestadas de acuerdo a los términos establecidos en la Ley 1755 de 2015.

CLASIFICACIÓN DE LA INFORMACIÓN

De acuerdo a los lineamientos desarrollados por la Corte Constitucional en la jurisprudencia, específicamente las sentencias T-729 de 2002, C-337 de 2007 y T-238 de 2018, la información se clasifica así:

1. **Información pública:** Es aquella que, según los mandatos de la ley o de la Constitución, puede ser obtenida y ofrecida sin reserva alguna y sin importar si se trata de información general, privada o personal. Se trata por ejemplo de los documentos públicos, las providencias judiciales debidamente ejecutoriadas, los datos sobre el estado civil de las personas o sobre la conformación de la familia. Este tipo de información se puede solicitar por cualquier persona de manera directa y no existe el deber de satisfacer algún requisito para obtenerla.

   Para la empresa de vigilancia y seguridad privada, la información pública comprende los datos que pueden ser consultados por cualquier ciudadano sin restricción, relacionados con el registro legal de la compañía, licencias de funcionamiento expedidas por la Superintendencia de Vigilancia y Seguridad Privada, certificaciones de cumplimiento normativo, o políticas institucionales publicadas en la página web.

   Ejemplos:

   - Licencia de funcionamiento vigente emitida por la Supervigilancia.
   - Certificados de cumplimiento del Sistema de Gestión.
   - Políticas institucionales publicadas en medios oficiales de la empresa.

2. **Información semiprivada:** Son los datos que versan sobre información personal o impersonal que no está comprendida en la regla general anterior, porque para su acceso y

conocimiento presenta un grado mínimo de limitación, de tal forma que sólo puede ser obtenida y ofrecida por orden de autoridad administrativa o judicial en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales.

Corresponde a la información que, si bien no es estrictamente privada, requiere autorización o control para su uso, pues hace parte de la operación interna de la empresa. Incluye datos de desempeño, registros de asistencia, evaluaciones del servicio, información de proveedores o contratistas, y reportes operativos que contienen datos no sensibles de los trabajadores o del servicio.

Ejemplos:

- Listados de personal asignado a los servicios (sin datos sensibles).
- Informes mensuales de supervisión.
- Resultados y gestión de indicadores.

3. **Información privada:** Es aquella que por versar sobre información personal y por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, los documentos privados, las historias clínicas y la información extraída a partir de la inspección del domicilio.

   En la empresa, la información privada incluye los datos personales del personal operativo y administrativo que no son de acceso público y cuya utilización requiere autorización del titular. Comprende información operativa, financiera, contractual o relacionada con evaluaciones de desempeño individual. Esta información solo puede ser tratada con fines legítimos y conforme a las normas de protección de datos personales.

   Ejemplos:

   - Hoja de vida y documentos de vinculación laboral.
   - Contratos de trabajo o prestación de servicios.
   - Registros de nómina y afiliaciones al sistema de seguridad social.

   El suministro de la misma a terceros está sujeta a la autorización del superior jerárquico.

4. **Información reservada:** Versa sobre información personal y guarda estrecha relación con los derechos fundamentales del titular a la dignidad, a la intimidad y a la libertad, motivo por el cual se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. Cabría mencionar aquí la información genética, y los llamados "datos sensibles" o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc.”

El suministro de la misma no podrá efectuarse bajo ningún escenario, únicamente podrá hacerlo el titular del derecho.

PROCEDIMIENTO PARA EL SUMINISTRO DE LA INFORMACIÓN A TERCEROS

Con el fin de garantizar el cumplimiento de los principios de legalidad, confidencialidad, finalidad y circulación restringida en el tratamiento de información y datos personales, Seguridad Jano Ltda., establece el siguiente procedimiento para el suministro de información a terceros, sean estos personas naturales, jurídicas o autoridades competentes:

1. **Recepción de la solicitud:**

Toda solicitud de información presentada por un tercero deberá ser remitida al canal oficial de atención al cliente (correo electrónico: servicioalcliente@seguridadjano.com). En caso de que la solicitud sea recibida por otro medio o funcionario, este deberá trasladarla de inmediato al canal oficial, con el fin de que se surta el trámite formal, registro y asignación correspondiente.

2. **Asignación del trámite:**

Una vez el requerimiento sea recibido por el área competente, el director o responsable designado asignará el funcionario encargado de evaluar y gestionar la solicitud. Dicha asignación deberá quedar registrada internamente para efectos de trazabilidad y control.

3. **Análisis de la naturaleza de la información:**

El funcionario responsable deberá determinar la clasificación de la información solicitada (pública, semiprivada, privada o reservada), conforme a lo dispuesto en este manual y la normativa vigente sobre protección de datos.

Este análisis permitirá definir si la información puede ser compartida, si requiere autorización previa del titular o si está restringida.

4. **Determinación y validación de procedencia:**

Si el funcionario no logra establecer con certeza la naturaleza de la información o las condiciones para su entrega, deberá consultar al superior inmediato o al área jurídica/relaciones laborales, quienes determinarán:

- Si procede o no el suministro de la información.
- Bajo qué condiciones puede compartirse.
- El alcance y las limitaciones del acceso.

5. **Entrega y registro:**

Una vez autorizada la entrega, el funcionario responsable deberá:

- Asegurar que la información se suministre únicamente a la persona o entidad solicitante, en los términos aprobados.

- Registrar la fecha, el responsable y el motivo de la entrega en el control interno de solicitudes de información.

- Garantizar que se conserven las evidencias documentales del proceso (correo, oficio, acta o soporte de entrega).

6. **Confidencialidad y protección:**

En todos los casos, el personal deberá abstenerse de divulgar, copiar o utilizar la información para fines distintos a los autorizados, observando las políticas de confidencialidad y los principios de protección de datos personales aplicables a la empresa.

CONSECUENCIAS POR INCUMPLIMIENTO A LA POLÍTICA

El incumplimiento de las disposiciones contenidas en la presente Política constituye una falta grave y podrá generar las sanciones correspondientes conforme al Reglamento Interno de Trabajo. La comisión de tales faltas podrá acarrear, según la gravedad del caso, llamados de atención, suspensiones o incluso la terminación del contrato de trabajo.

De igual manera, el incumplimiento por parte de contratistas, proveedores o aliados estratégicos podrá dar lugar a sanciones contractuales, suspensión de la relación comercial o terminación anticipada del contrato, sin perjuicio de las acciones legales que correspondan.

Asimismo, la empresa podrá informar a las autoridades competentes cualquier conducta que configure infracción a la legislación sobre protección de datos personales o vulneración de derechos de los titulares.

VIGENCIA

La presente Política de Tratamiento y Protección de Datos Personales entrará en vigor a partir de la fecha de su aprobación por la Empresa. Su contenido será objeto de revisión, modificación o actualización en caso de que se expidan nuevas disposiciones legales, lineamientos internos o externos, o cuando se identifique la necesidad de fortalecer las medidas de gestión de la información.

La Política será divulgada a través de los medios oficiales, incluyendo el portal web y el sistema integrado de gestión de la Empresa, garantizando así su conocimiento por parte de los funcionarios, contratistas, proveedores, estudiantes y demás partes interesadas.

LUIS FERNANDO SERRANO TASCON
GERENTE GENERAL

VERSIÓN: 2
FECHA DE VIGENCIA: 01/09/2025

Seguridad JANO