



POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Habeas Data



1. Introducción

En JP Seguros recolectamos y administramos datos personales de quienes asesoramos en la adquisición de cualquier tipo de seguro, como requisito de las aseguradoras que nos respaldan para analizar los riesgos y presentar propuestas de protección.

La protección de los datos personales es un derecho fundamental en Colombia, consagrado en el artículo 15 de la Constitución Política.

Los Asesores de seguros, en su labor diaria, acceden a información sensible de sus clientes, como datos financieros, de salud, identificación y ubicación.

JP Seguros tiene el deber de dar cumplimiento a la normativa vigente sobre el tratamiento de datos personales, cuyo alcance está delimitado por las finalidades que han sido informadas y autorizadas por el Titular.

La vigencia y duración del Tratamiento de Datos Personales será el término en el que el Titular de la información tenga vigente el producto, servicio, contrato o relación, más el término que establezca la ley, adicionalmente los datos se conservarán de acuerdo con los principios de necesidad y razonabilidad





2. Objeto



El Habeas Data para los intermediarios de seguros opera como un mecanismo de protección de datos personales, otorgando a los titulares el derecho a conocer, actualizar y rectificar la información que se ha recopilado sobre ellos en el marco de las actividades de seguros.

Los Agentes de seguros, las Agencias y los Corredores, tenemos el deber de cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y la Ley 1266 de 2008, que regulan la protección de datos personales y seguir los lineamientos que se han definido con el fin de proteger esa información de los Titulares con los cuales se relaciona, las finalidades del tratamiento de la información, la atención de quejas y reclamos, y los procedimientos que se deben tener en cuenta para que los titulares puedan ejercer su derecho a conocer, actualizar, rectificar y suprimir la información, así como los canales a través de los cuales pueden ejercerlos.



3. Aplicación y Alcance

La política se aplica a las bases de datos y archivos físicos y digitales que contengan datos personales y que estén bajo la administración de JP Seguros, en virtud de las relaciones comerciales con las Aseguradoras que nos respaldan.

La política aplica cuando el tratamiento de los datos se dé en territorio colombiano. En aquellos casos en que el tratamiento suponga la participación de un encargado no establecido en Colombia, se buscará que sus estándares y políticas permitan cumplir al responsable con los deberes fundamentales que tiene bajo el marco legal colombiano.

La presente Política, está dirigida a nuestros clientes y exclientes, candidatos, empleados, exempleados, proveedores, aliados y en general, los grupos de interés sobre los cuales JP Seguros realiza tratamiento de información personal.

Todos los funcionarios de JP Seguros deben cumplir esta política y en tal sentido adelantamos las campañas pedagógicas y de capacitación que requieran para que las áreas con mayor nivel de interacción con la administración de datos personales conozcan la ley y las disposiciones adoptadas por nosotros para asegurar su cumplimiento.





4. Definiciones



AUTORIZACIÓN: Consentimiento previo, expreso e informado que da el Titular para llevar a cabo el tratamiento de sus datos personales.

DATO PERSONAL: Cualquier información que pueda asociar o identificar a una persona determinada (como su nombre o número de identificación) o determinable (como sus rasgos físicos).

DATO PÚBLICO: Son los datos o la información (como estado civil, profesión u oficio) que puede estar contenida en registros o documentos públicos, tales como: gacetas, boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

DATO SEMIPRIVADO: Cualquier información 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 el dato financiero y crediticio de actividad comercial o de servicios.

DATO SENSIBLE: Son aquellos que afectan la intimidad del Titular o pueden dar lugar a que lo discriminen; revelan su origen racial o étnico, su orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, así como los datos relativos a la salud, a la vida sexual y los datos biométricos, entre otros.

BASE DE DATOS: Se entiende como base de datos un conjunto de información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Datos personales), la cual está ordenada de modo sistemático para su posterior recuperación, análisis y/o transmisión.

ENCARGADO DEL TRATAMIENTO: Son todos los externos ya sean personas naturales o jurídicas que LAS COMPAÑÍAS han delegado para el tratamiento del dato personal de sus Grupos de Interés de acuerdo a lo definido en el objeto del contrato.

GRUPOS DE INTERÉS: Para efectos del presente documento, se ha definido por Grupo de Interés todas aquellas personas que en conjunto son parte de LAS COMPAÑÍAS, o que se vinculan con las actuaciones de éstas, y cuyas características comunes permiten considerarlos como beneficiarios de las reglas de Gobierno Corporativo. Bajo esta orientación, se pueden establecer tres tipos de Grupos de Interés a saber: Grupos de Interés Internos, Grupos de Interés Vinculados y Grupos de Interés Externos (Código de Gobierno Corporativo).

RESPONSABLE DEL TRATAMIENTO: Es la persona natural o jurídica, pública o privada que decide sobre la finalidad de las bases de datos y/o el tratamiento de los mismos.

TITULAR: Es la persona natural cuyos datos personales son objeto de tratamiento.

TRATAMIENTO: Es cualquier conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

PETICIÓN, QUEJA O RECLAMO (PQR'S): Es la manifestación de inconformidad expresada por un Titular de la información respecto de un servicio adquirido, ofrecido o prestado por JP Seguros o por las Aseguradora, puesta en conocimiento de éstos, de la Superintendencia de Industria y Comercio e instituciones competentes, según corresponda. Así mismo, es la manera establecida por la ley para hacer efectivos los derechos de los Titulares de conocer, rectificar, actualizar o suprimir su información contenida en las bases de datos.



5. Principios

Para JP Seguros es un compromiso entender y desarrollar de manera armónica los principios establecidos en la Ley General.

1. PRINCIPIO DE LEGALIDAD EN MATERIA DE TRATAMIENTO DE DATOS: El tratamiento a que se refiere esta ley es una actividad regulada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

2. PRINCIPIO DE FINALIDAD: El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley y debe ser informada al Titular.

3. PRINCIPIO DE LIBERTAD: El tratamiento sólo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no pueden 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 sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

5. PRINCIPIO DE TRANSPARENCIA: En el tratamiento debe garantizarse el derecho del Titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

6. PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales y de las disposiciones de la presente ley y la Constitución. En este sentido, el tratamiento sólo puede estar a cargo de personas autorizadas por el Titular y/o por las personas previstas en esta ley. Los datos personales, salvo la información pública, no pueden estar disponibles en internet ni en otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la Ley General.

7. PRINCIPIO DE SEGURIDAD: La información sujeta a tratamiento se debe manejar con las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

8. PRINCIPIO DE NECESIDAD Y PROPORCIONALIDAD: Los datos personales registrados en una base de datos deben ser los estrictamente necesarios para el cumplimiento de la finalidad del tratamiento, la cual debe ser comunicada al Titular. Deben ser adecuados, pertinentes y acordes con esa finalidad.

9. 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, pudiendo sólo realizar suministro o comunicación de datos personales cuando corresponda al desarrollo de las actividades autorizadas en la Ley General y en los términos de ésta.

10. PRINCIPIO DE TEMPORALIDAD O CADUCIDAD: El periodo de conservación de los datos personales será el necesario que permita alcanzar la finalidad para la cual se han recolectado.





6. Tratamiento

1. TRATAMIENTO DE DATOS SENSIBLES

La información referida al estado de salud del titular tiene esta naturaleza de dato sensible y opera para los ramos de salud, vida y riesgos laborales. “Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles, salvo que los mismos sean indispensables para el tratamiento para el cual se pretende la autorización”, de acuerdo con lo expresado en la Ley.

En JP Seguros, respetando los derechos que tienen los Titulares de la información, se indicará cuando corresponda, que las preguntas relacionadas con el estado de salud son de naturaleza sensible y que el Titular goza de libertad para responderlas, dejando claro que en atención a la naturaleza del seguro a ser contratado.

Esto, de conformidad con el Artículo 1058 del Código de Comercio, que señala: “el Tomador está obligado a declarar sinceramente los hechos o circunstancias que determinan el estado del riesgo, según el cuestionario que le sea propuesto por el asegurador”. En el evento en que el tomador es diferente del asegurado, le corresponderá a este último declarar en forma fidedigna sobre su estado de salud e historia médica.

Los datos biométricos, tales como la foto, huella o los demás que determine la Ley General, que se soliciten, tienen por finalidad garantizar la identidad del cliente frente a las Aseguradoras, prevenir situaciones de fraude por suplantación de identidad y garantizar un servicio más eficiente.

A través de JP Seguros como Intermediarios, Aseguradoras ponen a disposición de sus clientes diferentes aplicaciones móviles Apps y/o plataformas tecnológicas en las cuales los clientes pueden acceder a información acerca de los productos y servicios contratados, y a distintas funcionalidades adicionales y complementarias acordes a su vinculación y relacionamiento con éstas.

Teniendo en cuenta que ciertas funcionalidades de las Aplicaciones y/o Plataformas tecnológicas pueden requerir que los usuarios proporcionen datos personales que pueden ser considerados de carácter sensible, tales como: estado de salud, estilo de vida, hábitos, valores y antecedentes médicos, estado de ánimo, fotografías o imágenes en las que el Titular aparezca, ubicación, geolocalización, georreferenciación y/o bluetooth; Cuando haya lugar a dicho Tratamiento, JP Seguros deberá cumplir con las obligaciones expresadas previamente. Así mismo, ninguna actividad podrá condicionarse a que el Titular suministre Datos Personales Sensibles. Si éste no desea hacerlo y los datos corresponden o se requieren para acceder a las facilidades o servicios de las Apps o plataformas digitales, se entenderá que el Titular que manifiesta su negativa no está dispuesto a suscribirse y en consecuencia no se conservará ningún dato de éste.

2. Tratamiento de datos de niños, niñas y adolescentes

Los datos de niños, niñas y adolescentes que sean recolectados por JP Seguros en atención a que éstos tengan la calidad de asegurado o beneficiario de un contrato de seguro o de capitalización, o sean usuarios de las páginas web educativas creadas por las Aseguradoras, serán los pertinentes y adecuados para dicho contrato o para dicho uso, según corresponda, procurando el respeto de los derechos fundamentales que les asisten. Así mismo, JP Seguros y las Aseguradoras velarán porque la información personal de carácter sensible suministrada por los asegurados, tomadores y beneficiarios se utilice exclusivamente para la finalidad señalada en el contrato, de manera que sólo pueda ser accedida por los terceros autorizados por la ley.



7. Finalidades del tratamiento de datos





EN RELACIÓN CON LOS CLIENTES

1. Utilizar bases de datos de clientes para la debida prestación del servicio o del producto adquirido por el Titular.
2. Desarrollar actividades propias de los contratos celebrados, entre ellas el envío de información relevante.
3. Medir nivel de satisfacción respecto del(los) producto(s) y/o servicio(s) contratados(s).
4. Realizar campañas comerciales y actividades de mercadeo.
5. Realizar actividades de analítica, procesamiento, investigación y análisis estadístico, con el fin de identificar, generar conocimientos encaminados a mejorar los productos y/o servicios ofrecidos, actuales o futuros, así como mi experiencia del Titular para posibles ofertas de valor, bienes, productos y/o servicios.
6. Contactar a la finalización del(los) contrato(s) suscrito(s) con las Aseguradoras, con el fin único y específico de informar sobre productos y/o servicios que le puedan interesar y que permitan reactivar el vínculo comercial.

EN RELACIÓN CON LOS EXCLIENTES

La información de exclientes se conservará durante 5 años posterior a su desvinculación, de acuerdo con lo previsto el Art. 96 del Estatuto Orgánico del Sistema Financiero que regula la conservación de los archivos y documentos que soporten sus operaciones y demás normatividad vigente que le resulte aplicable o aquella que la modifique o derogue.

EN RELACIÓN CON LOS EMPLEADOS:

1. Capacitar a los empleados de JP Seguros en la Política de Tratamiento de Datos. El suministro de la información sensible es de carácter facultativo; y la de los menores de edad solamente podrá ser suministrada por sus representantes legales atendiendo al interés superior del menor.
2. Validar la información que ha suministrado para su vinculación.
3. Control, seguimiento y cumplimiento de las obligaciones como empleador y de las obligaciones a cargo de los empleados.
4. Establecer acciones para implementar garantías de seguridad, protección, bienestar, centro de trabajo, condiciones de salud, prevención de riesgos laborales, promoción y selección de empleados, control de exámenes médicos, estado de salud y condiciones del trabajador.
5. Cumplir con el proceso de archivo, de actualización de los sistemas, de protección y custodia de información y de las bases de datos creadas con fines de gestión del recurso humano.
6. Llevar un historial de los empleados para la expedición de certificaciones.
7. Llevar el control de las afiliaciones al Sistema de Seguridad Social.
8. Conocer información personal con el ánimo de contactar a familiares en caso de emergencias que se presenten en el ejercicio de las labores desarrolladas por el empleado.
9. Adelantar las labores de monitoreo y auditoría de los equipos y dispositivos suministrados para el cumplimiento de sus funciones, así como del uso que hagan de las redes, plataformas y demás infraestructura física y tecnológica suministrada o puesta a su disposición por LAS COMPAÑÍAS.
10. Realizar los registros contables, tributarios y demás requeridos por la ley.



8. Derechos del Titular



El derecho de Habeas Data para JP Seguros opera como un mecanismo de protección de datos personales, otorgando a los titulares el derecho a conocer, actualizar y rectificar la información que se ha recopilado sobre ellos en el marco de las actividades de seguros. Los intermediarios de seguros, como agencias aseguradoras, agentes y corredores, deben cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y la Ley 1266 de 2008, que regulan la protección de datos personales. El habeas data para los intermediarios de seguros implica lo siguiente:

Los titulares de datos personales tienen derecho a:

1. Conocer la información que se ha recolectado sobre ellos.
2. Actualizar la información, solicitando que se modifiquen o rectifiquen datos inexactos o incompletos.
3. Rectificar la información, solicitando la corrección de datos incorrectos.
4. Exigir la eliminación de datos cuando la información sea inexacta o incompleta, o cuando se haya obtenido sin consentimiento.



9. Obligaciones de JP Seguros

JP Seguros tiene la obligación de:

1. Obtener el consentimiento previo, expreso, informado e inequívoco del titular de los datos antes de procesar la información.
2. Mantener una política de tratamiento de datos personales que cumpla con los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
3. Garantizar la seguridad de los datos personales y tomar medidas técnicas y administrativas para evitar su pérdida, uso o acceso no autorizado.
4. Atender las solicitudes de los titulares de datos en un plazo máximo de 15 días hábiles.
10. Informar al titular de los datos sobre cualquier modificación o corrección realizada a sus datos personales.
5. Proceso para ejercer el habeas data:
6. El titular de los datos debe formular una solicitud escrita a la entidad aseguradora o al intermediario de seguros, indicando la naturaleza de la solicitud y la información que desea conocer, actualizar o rectificar.
7. La entidad aseguradora o el intermediario de seguros debe responder a la solicitud en un plazo máximo de 15 días hábiles.
8. Si la solicitud es aceptada, la entidad aseguradora o el intermediario de seguros debe cumplir con la solicitud y realizar las modificaciones o correcciones necesarias en los datos personales.
9. Si la solicitud es rechazada, la entidad aseguradora o el intermediario de seguros debe informar al titular de los datos sobre las razones de la negativa.

En resumen, el habeas data para los intermediarios de seguros es un mecanismo fundamental para proteger los derechos de los titulares de datos y garantizar la transparencia y seguridad en el manejo de la información personal en el marco de las actividades de seguros. Los intermediarios de seguros deben cumplir con sus obligaciones legales y éticas para garantizar la protección de los derechos de los usuarios.





10. Canales para ejercer los --- Derechos del Titular



JP Seguros ha dispuesto los siguientes canales de atención para garantizar el ejercicio de los derechos del Titular a conocer, actualizar, corregir y suprimir su información; esto último cuando no medie un deber legal o contractual que lo impida:

Todos los Titulares podrán ejercer sus derechos a través de los siguientes canales:

Telefónico y WhatsApp:

Linea 1: 3147052796

Linea 2: 3116178600

Linea 3: 3137480204

www.jpseguros.co