



**MANUAL DE PROCEDIMIENTOS PARA LA GESTIÓN Y TRASLADO DE  
SOLICITUDES DE TITULARES DE DATOS PERSONALES DE LA  
HERRAMIENTA SIRIEST**

PCM-002

<b>Fecha de aprobación</b>	20 de marzo de 2023	
<b>Elaborado por</b> (Área Legal)	<b>Revisado por</b> (Sebastián Cepeda)	<b>Aprobado por</b> (Mariano Sánchez)

## CONTROL DE VERSIONES

VERSIÓN	FECHA MODIFICACIÓN	COMENTARIO – JUSTIFICACIÓN
1	20 de marzo 2023	Primera Versión
2	27 de Junio 2025	Inclusión normativa MGE-002; PCM: Ley 1581 de 2012; Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015); Sentencias de la Corte Constitucional: C-748 de 2011, C-1011 de 2008

*Toda la información del presente documento tiene carácter confidencial, comprometiéndose el receptor a impedir su divulgación a terceros, limitándose el uso formal de su publicación.*

*El receptor del presente documento se compromete a no copiarlo ni reproducirlo, por sí mismo o por terceras personas, cualquiera que sea el medio o fin al que se destine, sin obtener permiso escrito de RISKS INTERNATIONAL.*

## **1. OBJETIVO**

Establecer los lineamientos y procedimientos internos que permiten garantizar:

El derecho de los titulares de datos personales a solicitar y obtener información clara, precisa y suficiente sobre el uso de sus datos personales en SISCOM que hace parte de SIRIEST.

El trámite, traslado y gestión oportuna de las solicitudes que eleven los titulares ante RISKS INTERNATIONAL SAS, conforme a la Ley 1581 de 2012 y demás normas concordantes. Nuestro compromiso fundamental en RISKS INTERNATIONAL SAS es salvaguardar los derechos de los titulares de datos personales. Para ello, hemos implementado un marco robusto de directrices y procedimientos internos, diseñado para asegurar la transparencia, la accesibilidad y la gestión eficiente de la información personal.

En primer lugar, nos enfocamos en facilitar el ejercicio del derecho de los titulares a solicitar y recibir información. Esto implica proporcionar detalles claros, precisos y suficientes sobre cómo sus datos personales son utilizados dentro del componente SISCOM, que forma parte integral de SIRIEST. Creemos firmemente que la información accesible es clave para que los individuos comprendan y controlen el manejo de su información.

En segundo lugar, hemos establecido un proceso meticuloso para el trámite, transferencia y gestión oportuna de todas las solicitudes presentadas por los titulares. Este proceso se adhiere estrictamente a los principios y requisitos establecidos en la Ley 1581 de 2012, así como a todas las demás normativas aplicables en materia de protección de datos personales en Colombia. Esto incluye, pero no se limita a, solicitudes de acceso, rectificación, cancelación y oposición (Derechos ARCO).

Nuestro objetivo es garantizar que cada solicitud sea manejada con la mayor diligencia y en el menor tiempo posible, manteniendo siempre la integridad y confidencialidad de la información.

## **2. ALCANCE**

Este procedimiento aplica a todas las solicitudes presentadas por los titulares, sus representantes legales o apoderados, en relación con el tratamiento de sus datos personales, específicamente cuando RISKS INTERNATIONAL actúe en calidad de **encargado del tratamiento**, y que deban ser trasladadas al **responsable del tratamiento**

El presente manual, realiza un procedimiento diseñado y establecido para regular de manera exhaustiva y transparente todas las acciones y etapas relacionadas con la gestión de solicitudes que versen sobre el tratamiento de datos personales. Su aplicación es de carácter obligatorio para la totalidad de las peticiones que, en este ámbito, sean presentadas, ya sea directamente por los titulares de los datos personales afectados o por sus respectivos representantes legales debidamente acreditados.

Es crucial destacar que la aplicabilidad específica de este Manual se activa en aquellos escenarios en los que RISKS INTERNATIONAL ostenta la calidad jurídica de **encargado del tratamiento** de los datos personales en la herramienta SIRIEST. En esta capacidad, la responsabilidad primordial de RISKS INTERNATIONAL radica en la recepción, documentación y, lo más importante, la pronta y diligente retransmisión o traslado de dichas solicitudes al **responsable del tratamiento**. Ello se fundamenta en la necesidad de garantizar que sea la entidad o persona jurídica Suscriptora del servicio, quien define los fines y medios del tratamiento de los datos asumiendo la obligación de dar una respuesta sustantiva y conforme a la normativa vigente a la solicitud planteada por el titular o su representante.

Este manual asegura la trazabilidad y la correcta canalización de las peticiones, minimizando los riesgos de incumplimiento de la normativa de protección de datos personales y salvaguardando los derechos de los individuos. Adicionalmente, establece los mecanismos internos para la identificación, clasificación y priorización de las solicitudes, así como los protocolos de comunicación interna necesarios para una coordinación eficiente entre RISKS INTERNATIONAL como encargado en la herramienta SIRIEST y el responsable del tratamiento.

### **3. BASE LEGAL**

La protección de datos personales en Colombia se encuentra sólidamente fundamentada en un marco normativo que busca garantizar el derecho fundamental al *habeas data*. Este derecho permite a los ciudadanos conocer, actualizar y rectificar la información que sobre ellos se haya recogido en bases de datos o archivos de entidades públicas y privadas. A continuación, se detallan los pilares de esta regulación:

- **Ley 1581 de 2012 - Ley General de Protección de Datos Personales:** Esta es la norma principal y rectora en materia de protección de datos en Colombia. Establece

los principios y definiciones aplicables al tratamiento de datos personales, los derechos de los titulares de la información, las obligaciones de los responsables y encargados del tratamiento, y el régimen de sanciones. Su objetivo es desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan sido recogidas sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales relacionados con la recopilación, tratamiento y circulación de datos personales.

- **Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015) - Decreto Reglamentario de la Ley 1581 de 2012:** Este decreto reglamenta aspectos específicos de la Ley 1581 de 2012, detallando procedimientos, requisitos y obligaciones para la implementación de la ley. Por ejemplo, establece las condiciones para la obtención de la autorización del titular, las medidas de seguridad que deben adoptar los responsables y encargados del tratamiento, el Registro Nacional de Bases de Datos, y los procedimientos para el ejercicio de los derechos de los titulares. Es importante destacar que este decreto fue compilado en el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, el Decreto 1074 de 2015, lo que facilita su consulta y aplicación en el contexto empresarial.
- **Sentencias de la Corte Constitucional:** La jurisprudencia de la Corte Constitucional ha sido fundamental en la interpretación y desarrollo del derecho al *habeas data* y la protección de datos personales. Entre las sentencias más relevantes se encuentran:
  - **Sentencia C-748 de 2011:** Esta sentencia es crucial porque declaró la exequibilidad condicionada de varios artículos de la Ley 1581 de 2012, definiendo aspectos clave sobre la naturaleza del derecho al *habeas data* como derecho fundamental autónomo y las garantías que lo rodean. También precisó la aplicación de la ley a entidades de naturaleza privada.
  - **Sentencia C-1011 de 2008:** Aunque anterior a la Ley 1581 de 2012, esta sentencia sentó las bases para el desarrollo legislativo posterior al establecer principios constitucionales sobre el tratamiento de datos personales, como el principio de finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
- **Directrices de la Superintendencia de Industria y Comercio (SIC):** La Superintendencia de Industria y Comercio es la autoridad de control en materia de protección de datos personales en Colombia. A través de sus directrices, circulares y conceptos, la SIC orienta a los responsables y encargados del tratamiento sobre el correcto cumplimiento de la normativa. Estas directrices abordan temas como la implementación de políticas de tratamiento de datos, la gestión de incidentes de seguridad, la respuesta a las solicitudes de los titulares, y la aplicación de sanciones en caso de incumplimiento. La SIC también administra el Registro Nacional de Bases de Datos (RNBD), herramienta esencial para el control y supervisión del tratamiento de datos.

Este conjunto de normas y la interpretación jurisprudencial y administrativa conforman un robusto andamiaje legal que busca garantizar la privacidad y el control de los ciudadanos sobre su información personal en un entorno cada vez más digitalizado.

#### **4. DEFINICIONES**

- **Titular:** Se refiere a la persona natural, debidamente identificada o identificable, a quien corresponden los datos personales que son objeto de tratamiento. Esta persona es el eje central de la normativa de protección de datos, ya que posee el derecho fundamental sobre su información personal.
- **Responsable del Tratamiento:** Es la persona natural o jurídica, de naturaleza pública o privada, que por sí misma o en asocio con otros, tiene la capacidad de decidir sobre la base de datos y/o el Tratamiento de los datos. Esto implica que es quien define los fines, los medios y, en general, todos los aspectos sustanciales relacionados con el manejo de la información personal.
- **Encargado del Tratamiento:** Es la persona natural o jurídica, pública o privada, que, por sí misma o en asocio con otros, realiza el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. Su actuación está supeditada a las instrucciones y directrices que le imparta el Responsable, y no tiene capacidad de decisión sobre el propósito o el contenido del tratamiento.
- **Oficial de Protección de Datos (OPD):** Es la persona designada dentro de la organización o entidad, encargada de coordinar y supervisar la implementación y el cumplimiento de las políticas y procedimientos relacionados con la gestión y protección de datos personales. Su rol es crucial para asegurar la observancia de la normativa vigente y para facilitar la comunicación entre los titulares, el responsable y las autoridades de control.
- **Solicitud de Información:** Es cualquier requerimiento o petición que realiza el titular de datos personales con el fin de conocer la existencia de sus datos, el uso que se les está dando, y los fines para los cuales fueron recolectados. Esta solicitud busca garantizar la transparencia y el derecho de los titulares a estar informados sobre el manejo de su información.
- **Consulta:** Se refiere específicamente a la solicitud que presenta el titular de datos personales con el propósito de acceder a la totalidad de su información personal que se encuentra en posesión del Responsable del Tratamiento. A través de la consulta, el titular puede verificar la exactitud de sus datos y la legitimidad de su tratamiento.
- **Reclamo:** Es la solicitud formal que un titular de datos personales interpone ante el Responsable del Tratamiento para ejercer sus derechos de corrección, actualización, supresión de datos, o para revocar la autorización previamente otorgada para el tratamiento de su información. Este mecanismo busca proteger los derechos del titular frente a posibles inexactitudes, omisiones, tratamientos

indebidos o la necesidad de retirar su consentimiento.

- **Suscriptor:** Se refiere a la entidad o empresa que ha formalizado un acuerdo contractual con RISKS INTERNATIONAL SAS. En dicho contrato se establecen los términos y condiciones bajo los cuales RISKS INTERNATIONAL SAS proporcionará sus servicios, y el Suscriptor se compromete a cumplir con las obligaciones y responsabilidades estipuladas en dicho acuerdo. La relación entre ambas partes se rige por este marco legal, que puede incluir aspectos como la prestación de servicios de consultoría, gestión de riesgos, aseguramiento, u otros servicios especializados ofrecidos por RISKS INTERNATIONAL SAS.

## 5. PROCEDIMIENTO

### 5.1 Recepción de la Solicitud

El titular puede presentar su solicitud a través de cualquiera de los siguientes canales oficiales:

- **Correo electrónico:** [habeasdata@risksint.com](mailto:habeasdata@risksint.com)
- **Formulario web:** <https://www.risksint.com/habeas-data/>

La solicitud debe contener como mínimo:

- Nombre completo del titular
- Tipo y número de documento
- Descripción clara de la solicitud
- Evidencias o pruebas (si aplica)
- Medio de respuesta (física o electrónica)
- Firma (si es en físico)

### 5.2 Radicación y Acuse de Recibo

- Se asignará un número de radicado de conformidad a orden fecha y hora de radicación.
- En caso de que no se allegue documento de identidad, se solicitará para evitar suplantaciones conforme la normatividad (Decreto 1377 de 2013, art. 20, núm.. 1 y 3 y Ley 1755 de 2015).
- Adicionalmente, se requerirá autorización del tratamiento de datos, para la consulta en la herramienta y poder emitir respuesta.

### 5.3 Verificación de Identidad

Se verificará que:

- La solicitud haya sido presentada por el titular o su representante legal, debidamente acreditado.
- En caso de representación de una persona jurídica, se exigirá copia del poder, certificación de cámara de comercio o documento equivalente.
- Persona natural que obre mediante apoderado judicial, deberá presentar el correspondiente poder judicial.

#### **5.4 Análisis Interno y Clasificación**

El Oficial de Protección de Datos revisará:

- La naturaleza y/o tipo de dato.
- Si los datos solicitados están siendo tratados por RISKS INTERNATIONAL SAS.
- Si RISKS INTERNATIONAL SAS en ese caso actúa como **responsable** o **encargado** del tratamiento.
- Si la solicitud requiere traslado al responsable del tratamiento.

#### **5.5 Trámite y Traslado**

##### **a) Cuando RISKS es Responsable del Tratamiento:**

- Se da respuesta directa al titular conforme a la Ley 1581 de 2012 y el MANUAL DE POLÍTICAS Y PROCEDIMIENTOS PARA EL TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES, MGE-002, V2; ENERO DE 2018.

##### **b) Cuando RISKS es Encargado del Tratamiento:**

- Se tramita la solicitud dando cumplimiento al artículo 4 de la ley 1581 de 2012.
- De conformidad al artículo 15 de la Ley 1581 de 2012, si la solicitud lo requiere se **traslada dentro del término de dos (2) días hábiles al responsable del tratamiento** para que sea este quien la resuelva, en los términos de ley.
- Se informa al titular sobre el traslado, incluyendo:
  - Fecha del traslado
  - Nombre del responsable
  - Medio de contacto

#### **5.6 Plazos para la Gestión**

- **Consultas:**
  - Máximo 10 días hábiles para respuesta.
  - Prórroga hasta 8 días hábiles, previo aviso al titular.
- **Reclamos:**

- Máximo 15 días hábiles para respuesta.
- Prórroga hasta 8 días hábiles, informando previamente.

### 5.7 Registro y Trazabilidad

- Toda solicitud debe registrarse con:
  - Fecha de ingreso
  - Medio de ingreso
  - Nombre del titular
  - Tipo de solicitud
  - Fecha de respuesta
  - Estado (en trámite, resuelto, traslado)
  
- Si la solicitud es un reclamo, debe incluirse en la base de datos la leyenda:
  - **“Reclamo en trámite” conforme al artículo 15 numeral 2 de la ley 1581 de 2012.**

### 5.8 Respuesta al Titular

- La respuesta será clara, precisa, completa y redactada en lenguaje comprensible.
- Se enviará por el medio indicado por el titular.
- El encargado, si actúa por cuenta del responsable, debe asegurar que la respuesta se entregue **dentro de los plazos legales.**

## 6. RESPONSABILIDADES

<b>Cargo</b>	<b>Responsabilidad</b>
Oficial de Protección de Datos	Recibir, clasificar, tramitar y/o trasladar solicitudes; coordinar respuesta.
Área Jurídica	Asesoría legal en casos particulares.
Área de Tecnología	Acceso y apoyo técnico a los registros de datos.
Todos los colaboradores	Cumplir los principios y deberes sobre protección de datos.

## 7. MEDIDAS DE CONTROL Y MEJORA

### 7.1. Auditorías internas anuales de cumplimiento

Se llevarán a cabo auditorías internas de forma anual para asegurar el cumplimiento continuo del presente manual, las políticas y procedimientos establecidos. Estas auditorías examinarán la eficacia de los controles implementados, la adherencia a los marcos

regulatorios y la identificación de áreas de mejora. Los resultados de estas auditorías serán documentados y presentados a la dirección para su revisión y la implementación de acciones correctivas cuando sea necesario. El objetivo principal es garantizar que todas las operaciones se realicen de acuerdo con los estándares internos y las regulaciones externas pertinentes.

## 7.2. Indicadores de gestión

Para monitorear y evaluar el desempeño de la gestión de solicitudes de datos personales, se establecerán los siguientes indicadores clave de gestión:

- **Número de solicitudes recibidas:** Este indicador registrará la cantidad total de solicitudes de titulares de datos personales recibidas en un período determinado. Permitirá comprender el volumen de trabajo y las tendencias en la demanda de gestión de datos.
- **Tiempo promedio de respuesta:** Se medirá el tiempo promedio que transcurre desde la recepción de una solicitud hasta la emisión de una respuesta final. Este indicador es crucial para evaluar la eficiencia operativa y la agilidad en la atención a los titulares de datos.
- **Porcentaje de cumplimiento en término legal:** Este indicador calculará la proporción de solicitudes que son respondidas dentro de los plazos establecidos por la normativa legal vigente. Es un indicador crítico para asegurar la conformidad legal y evitar posibles sanciones o reclamos para el cumplimiento de la normatividad vigente.

## 7.3. Revisión y actualización del procedimiento

El presente procedimiento será objeto de revisión y actualización obligatoria **cada año o cuando por actualización normativa se requiera**, independientemente de cambios externos. Esta revisión anual permitirá integrar las lecciones aprendidas de las auditorías internas, los indicadores de gestión y cualquier retroalimentación recibida. Adicionalmente, el procedimiento será revisado y actualizado de manera inmediata **cuando haya cambios normativos** significativos que afecten la gestión de datos personales. Esto asegura que el procedimiento se mantenga siempre alineado con las últimas disposiciones legales y las mejores prácticas en la protección de datos.

## 8. DIVULGACIÓN DEL PROCEDIMIENTO

- Este procedimiento se socializa internamente a través de capacitaciones, correos y en la página web de la compañía para conocimiento de los titulares de los datos personales.

- 
- Cualquier titular puede solicitar acceso al procedimiento a través de los canales de atención habilitados.