MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS SOBRE TRATAMIENTO DE PROTECCIÓN DE DATOS

MGE-006

Fecha de aprobación	Diciembre - 2025	
ORIGINAL FIRMADO Firma	ORIGINAL FIRMADO Firma	ORIGINAL FIRMADO Firma
Elaborado por Oficial de Protección de Datos	**Revisado por** Dirección Legal	**Aprobado por** Gerencia - CEO

CONTROL DE VERSIONES

VERSIÓN	FECHA MODIFICACIÓN	COMENTARIO – JUSTIFICACIÓN
1	Diciembre - 2025	Primera Versión - Mejora y unificación de otros manuales - Acreditación de Cumplimiento -

TABLA DE CONTENIDO

OBJETIVO DE ESTE MANUAL Y OBLIGATORIEDAD DE CUMPLIMIENTO

RISKS INTERNATIONAL S.A.S está comprometida con el respeto de los derechos de sus clientes, empleados, y cualquier persona. Por eso, adopta el manual interno de política y procedimientos para garantizar el debido tratamiento de los datos personales.

Este manual tiene como finalidad adoptar las políticas, orientaciones y procedimientos para para garantizar el adecuado cumplimiento de la ley 1581 de 2012 y demás regulaciones sobre tratamiento de datos personales y en especial, para la atención de consultas y reclamos.

Este manual es de obligatorio y estricto cumplimiento por parte de todos los empleados de RISKS INTERNATIONAL S.A.S, los contratistas y terceros que obran en nombre de RISKS INTERNATIONAL S.A.S.

Todos los empleados de RISKS INTERNATIONAL S.A.S deben leer y acatar lo que se ordena en este manual en cumplimiento de sus funciones. En los casos en que no exista vínculo laboral, se deberá incluir una cláusula contractual para que quienes obren en nombre de RISKS INTERNATIONAL S.A.S se obliguen a cumplir estas políticas y procedimientos.
El incumplimiento del mismo acarreará sanciones de tipo laboral o responsabilidad contractual según el caso. Lo anterior, sin perjuicio del deber de responder patrimonialmente por los daños y perjuicios que cause a los titulares de los datos o a RISKS INTERNATIONAL S.A.S por el incumplimiento de este manual o por el indebido tratamiento de datos personales.

MARCO JURÍDICO

El literal k) del artículo 17 de la Ley Estatutaria 1581 de 2012 ordena lo siguiente a los Responsables del Tratamiento: "Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;"
En línea con lo anterior, el decreto 1377 de 2013 reglamentó la citada ley y, entre otras establece lo que sigue a continuación

- "A solicitud de la Superintendencia de Industria y Comercio, los Responsables deberán proveer una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de información, como también la descripción de las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso."[1]
- "Los responsables y encargados del tratamiento deberán documentar los procedimientos para el Tratamiento, conservación y supresión de los datos personales"[2]
- " Los procedimientos de acceso, actualización, supresión y rectificación de datos personales y de revocatoria de la autorización deben darse a conocer o ser fácilmente accesibles a los Titulares de la información e incluirse en la política de tratamiento de la información."[3]
- "El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento."[4]
- Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca."[5]
- "El responsable y el encargado deben poner a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada."[6]

[1] Art 4, D 1377 de 2013
[2] Art. 11, D 1377 de 2013
[3] Art 18, D 1377 de 2013
[4] Art 5, D 1377 de 2013

[5] Art. 7, D 1377 de 2013
[6] Art. 9, D 1377 de 2013

DEL COMPROMISO DE TODOS (AS) PARA GARANTIZAR EL DEBIDO TRATAMIENTO DE LOS DATOS PERSONALES

TODO DEPENDE DE TODOS

En **RISKS INTERNATIONAL SAS** estamos comprometidos con el debido tratamiento de los datos personales.

Queremos fortalecer nuestra cultura empresarial de protección de datos en donde todo el equipo humano sea el principal protagonista.

Es fundamental el compromiso y la debida diligencia de todos (as) en el debido tratamiento de la información.

El debido tratamiento de datos personales es una tarea que nos involucra a todos (as).

PROCEDIMIENTO PARA OBTENER LA AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES E INFORMAR AL TITULAR LA INFORMACIÓN RECOLECTADA, ASÍ COMO TODAS LAS FINALIDADES ESPECÍFICAS DEL TRATAMIENTO PARA LAS CUALES SE OBTIENE EL CONSENTIMIENTO.

Las reglas de tratamiento de datos no aplican de la misma manera frente a todos los datos, ni a todos los sujetos obligados a cumplirlas

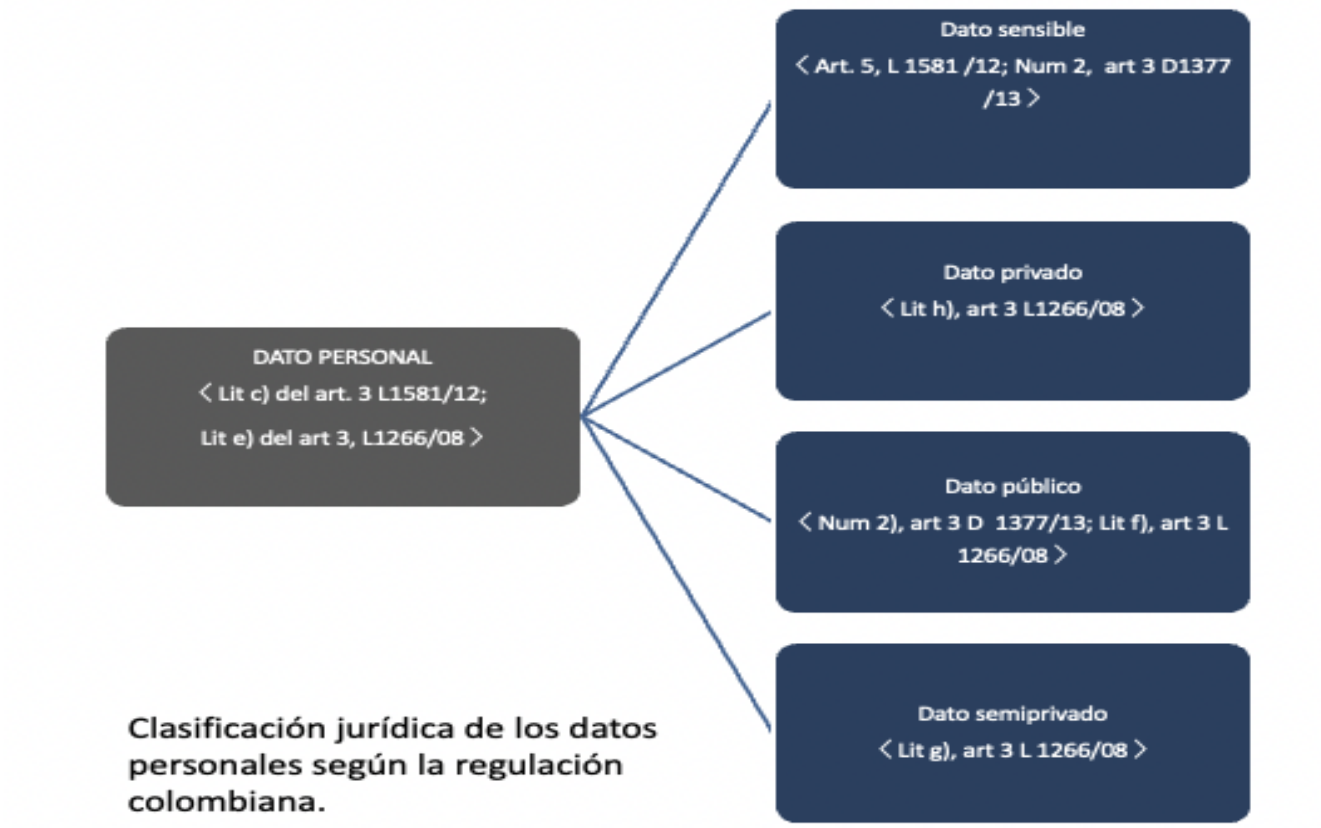
De conformidad con los artículos 6 (*lit -a-),* 8 (*lit -b-*), 9 y 10 de la ley 1581 de 2012, en concordancia con los artículos 3 (*num 2 y 3*), 4, 5 (*inciso 2*) para el tratamiento de datos personales no es necesaria la autorización en los siguientes casos:

	Entidad privada	Entidad pública o administrativa en el ejercicio de sus funciones
Dato sensible	**ROA**	NRA
Dato semiprivado	**ROA**	NRA
Datos privado	**ROA**	NRA
Dato de naturaleza pública	NRA	NRA

Siglas:

- ROA: Requiere Obtener Autorización
- NRA: No Requiere Autorización

En la siguiente gráfica se establece la clasificación de los datos personales y la fuente jurídica sobre cada categoría de dato personal.



Clasificación jurídica de los datos personales según la regulación colombiana.

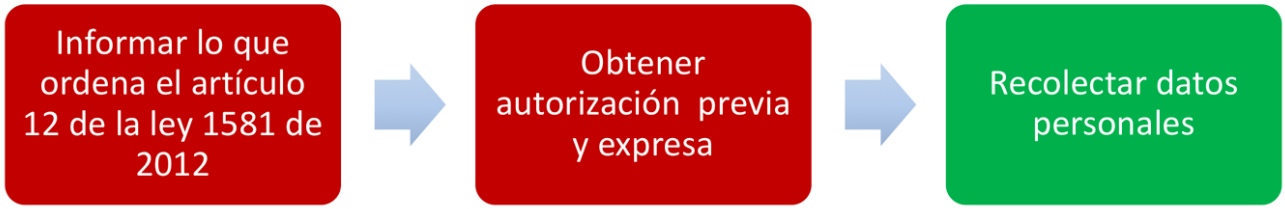
Los requisitos que debe cumplir la autorización depende del tipo de dato personas a tratar y de la regulación pertinente, tal y como se ilustra a continuación:

	Previa	Expresa	Informada	Informada especial
Ley 1266 de 2008	■	■		
Ley 1581 de 2012	■	■	■	
Datos sensibles	■	■	■	(Art 6 D 1377/13)

Requisitos jurídicos que debe cumplir la autorización

Pautas generales

La ley 1581 de 2012 exige que la autorización para recolectar datos personales (dirección de correo electrónico, teléfono, etc.) sea informada, previa y expresamente tal y como se ilustra a continuación:



Así las cosas, mediante mecanismos electrónicos (página web, app, entre otros) o físicos (formatos) se obtendrá de parte del titular su autorización previa, expresa e informada para recolectar y tratar sus datos personales. Para obtener la autorización se deberán seguir los siguientes pasos:

En primer lugar, antes de que la persona (Titular del dato) autorice, es necesario informarle de forma clara y expresa lo siguiente que ordena el artículo 12 de la Ley 1581 de 2012:

- La identificación, dirección física o electrónica y teléfono: RISKS INTERNATIONAL S.A.S **NIT**: 900352786-5; **Domicilio o dirección:** Calle 25 B 39A -30 **Correo electrónico**: habeasdata@risksint.com ; **Teléfono**: 6017941834
- El Tratamiento manual o automatizado al cual serán sometidos los datos personales
- Los datos que serán recolectados (nombre, identificación, número de identificación, información de contacto, etc)
- Las finalidades específicas del tratamiento de los datos; señalando las finalidades estrictamente necesarias y las finalidades accesorias.
- El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
- Los siguientes derechos del Titular establecidos en el artículo 8 de la mencionada ley:
    - Conocer, actualizar y rectificar sus datos personales. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;
    - Solicitar prueba de la autorización otorgada, salvo cuando expresamente se exceptúa como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la ley 1581 de 2012 u otras normas;

- Ser informado, previa solicitud, respecto del uso que se le ha dado a sus datos personales;
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;

  De conformidad con el artículo 9 del decreto 1377 de 2013, la solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos.

  Los Titulares podrán en todo momento solicitar la supresión de sus datos personales y/o revocar la autorización otorgada para el Tratamiento de los mismos, mediante la presentación de un reclamo, de acuerdo con lo establecido en el artículo 15 de la Ley 1581 de 2012 y como se señalará posteriormente. Se pondrá a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización otorgada.

  Si vencido el término legal respectivo, el responsable y/o el encargado, según fuera el caso, no hubieran eliminado los datos personales, el Titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización y/o la supresión de los datos personales. Para estos efectos se aplicará el procedimiento descrito en el artículo 22 de la Ley 1581 de 2012.

Se conservará prueba del cumplimiento del deber de informar lo previsto en el precitado artículo y, cuando el Titular lo solicite, se le entregará copia de esta.

En segundo lugar, obtendrá el consentimiento del titular a través de cualquier medio electrónico o físico que pueda ser objeto de consulta posterior.

Se deberá dejar prueba del cumplimiento de la obligación de informar y del consentimiento. Si el Titular solicita copia de estos se le deberá suministrar.

Autorización de datos sensibles y de menores de edad

Las personas obligadas al cumplimiento de este manual deben identificar los datos sensibles y de los niños, niñas y adolescentes (NNA) que eventualmente recolectan o almacenen con miras a:

- Implementar responsabilidad reforzada en el tratamiento de estos datos que se traduce en una exigencia mayor en términos de cumplimiento de los principios y los deberes.
- Aumentar los niveles de seguridad de esa información.
- Incrementar las restricciones de acceso y uso por parte del personal de RISKS INTERNATIONAL S.A.S y de terceros.
- Tener presente los requisitos legales y de esta política para su recolección.

Autorización mediante conductas inequívocas

La autorización también podrá obtenerse a partir de conductas inequívocas del Titular del Dato que permitan concluir de manera razonable que éste otorgó su consentimiento para el tratamiento de su información. Dicha(s) conducta(s) debe(n) ser muy clara(s) de manera que no admita(n) duda o equivocación sobre la voluntad de autorizar el tratamiento. En ningún caso, el silencio del Titular podrá considerarse como una conducta inequívoca.

En todo caso, se adoptarán medidas para informar al titular lo que ordena el artículo 12 de la Ley 1581 de 2012.

Personas legitimadas para dar el consentimiento

Se encuentran legitimados para otorgar el consentimiento:

a. El Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición RISKS INTERNATIONAL S.A.S.
b. Los causahabientes del Titular, quienes deberán acreditar tal calidad.
c. El(la) representante y/o apoderado (a) del Titular, previa acreditación de la representación o apoderamiento.

La autorización también podrá otorgarse cuando se den casos de estipulación a favor de otro o para otro.

Autorización para tratamiento de datos sensibles

Dato personal sensible: Información que afecta la intimidad de la persona o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, historia clínica la vida sexual y los datos biométricos (huellas dactilares, fotos).

Cuando se trate de la recolección de datos sensibles se deben cumplir los siguientes requisitos adicionales:

a. La autorización debe ser explícita.
b. Se debe informar al Titular que no está obligado a autorizar el tratamiento de dicha información.
c. Se debe informar de forma explícita y previa al Titular, cuáles de los datos que serán objeto de tratamiento son sensibles (datos relativos a la salud, biométricos, entre otros) y la finalidad del mismo.

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

Cuando se trate de la recolección y tratamiento de datos de niños, niñas y adolescentes se deben cumplir los siguientes requisitos:

a. La autorización debe ser otorgada por personas que estén facultadas para representar los NNA. El representante de los NNA deberá garantizarles el derecho a ser escuchados y valorar su opinión del tratamiento teniendo en cuenta la madurez, autonomía y capacidad de los NNA para entender el asunto.

b. Se debe informar que es facultativo responder preguntas sobre datos de los NNA.

c. El tratamiento debe respetar el interés superior de los NNA y asegurar el respeto de sus derechos fundamentales Se debe informar de forma explícita y previa al Titular cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del mismo.

Casos en que no es necesaria la autorización

De conformidad con el artículo 10 de la Ley 1581 de 2012, no es necesaria la autorización cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
- Datos de naturaleza pública;
- Casos de urgencia médica o sanitaria;
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
- Datos relacionados con el Registro Civil de las Personas.

En todo caso, sobre el tratamiento de estos datos se deberá cumplir las demás obligaciones o disposiciones previstas en la citada ley.

Descripción de las finalidades para las cuales la información es recolectada.

RISKS INTERNATIONAL S.A.S recolectará, usará y tratará los datos personales de manera leal y lícita para cumplir las actividades propias de su objeto social y en especial para prestar servicios como los siguientes:

- ✓ Prevención del Lavado de Activos y el financiamiento del terrorismo (LAFT).
- ✓ Validaciones para prevención de riesgos LAFT previas a cada despacho de transportes de carga o previas a cualquier vinculación contractual con clientes.
- ✓ Visitas domiciliarias y validación de arraigo de personas en procesos de selección.
- ✓ Validación y debida diligencia en materia de cumplimiento normativo para cumplir con normas nacionales e internacionales.
- ✓ Validación de debida diligencia ampliada, básica, intensificada y avanzada.
- ✓ Alimentar sistemas de información que permitan realizar debidas diligencias con información pública y compartida por parte de Suscriptores.
- ✓ Ayudar al control interno de los clientes, contrapartes.
- ✓ Cumplir con el objeto social y la actividad económica de las empresas para prevenir el Lavado de Activos y la Financiación del Terrorismo.
- ✓ Mantener actualizada la información de clientes, proveedores y trabajadores, contactarlos, verificar sus datos, realizar informes, análisis de información, búsqueda de tendencias en los servicios, enviar información, generar estadísticas, generar reportes a entidades externas y requerimientos internos de información.
- ✓ Efectuar labores de mercadeo y servicio al usuario.
- ✓ Conservar registros históricos de RISKS INTERNATIONAL S.A.S
- ✓ Cumplimiento de obligaciones o deberes contractuales.
- ✓ Contacto para asignación de operaciones de transporte, emisión de órdenes de carga, labores administrativas, de tráfico y seguridad y de cumplimiento normativo.

- ✓ Diligenciamiento de documentos exigidos por el Ministerio de Transporte, Superintendencia de Puertos y Transporte, autoridades de tránsito y demás entes de control.
- ✓ Validar de cualquier forma la identidad, antecedentes judiciales y penales, de comportamiento social, vínculos delictivos y demás información relevante, sea sensible o no, para efectos de conocimiento del cliente o contraparte, evaluación de riesgos, toma de decisiones de vinculación y debida diligencia SIPLAFT, SARLAFT, SAGRILAFT, SARO, SAR, OEA y BASC. Tratar mis datos contenidos en fuentes de información o bases de datos abiertas, centrales de riesgo, listas restrictivas, vinculantes, de sanciones, PEP, Noticias, incluyendo listas OFAC,ONU, INTERPOL, EU, y datos oficiales como la Rama Judicial, Policía Nacional, SIMIT, Procuraduría General de la Nación, entre otras.
- ✓ Consultar, validar, registrar, compartir o actualizar información noticiosa, señales de alerta, riesgos, faltantes, novedades y datos ante terceros SUSCRIPTORES, públicos o privados.
- ✓ Registrar cualquier novedad, sean datos sensibles o no, para realizar análisis de riesgos operativos, riesgos LAFT y seguridad, estadísticas, novedades de cumplimiento, reportando estos datos ante SIRIEST y SISCOM, para cumplir obligaciones de debida diligencia, gestión de riesgos, legales y operativos. También autorizo consultar y compartir mis datos personales con terceros SUSCRIPTORES o usuarios, a fin de mejorar la prevención de riesgos del sector, la seguridad y cumplir con las normas SIPLAFT o SARLAFT, SAGRILAFT, PESV, BASC y OEA.
- ✓ Innovar, crear, mejorar y proveer sistemas tecnológicos y modelos de inteligencia artificial para procesos de verificación, seguridad, prevención de riesgos asociados al Lavado de activos y financiación del terrorismo y delitos conexos y optimización administrativa u operativa.
- ✓ Contactar mediante cualquier medio físico, electrónico, telefónico o digital para la verificación de información, referencias personales, firma de documentos, apoyando a los clientes, sus departamentos de tráfico y seguridad, en la asignación de carga o de trabajo y validación contractual como terceros.
- ✓ Conservar la información en las bases de datos o sistemas de información durante el tiempo necesario para el cumplimiento de las finalidades aquí descritas.

FINALIDAD Y TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS PERSONALES DE LOS EMPLEADOS, COLABORADORES, CONTRATISTAS O PROVEEDORES DE RISKS INTERNATIONAL S.A.S

Los datos que se recolectan o almacenen sobre los empleados, contratistas o proveedores de RISKS INTERNATIONAL S.A.S mediante el diligenciamiento de formatos, inclusión de

reportes en la plataforma SIRIEST, redes sociales digitales, contratos, vía telefónica, correo electrónico o con la entrega de documentos (hojas de vida, anexos) serán tratados para todo lo relacionado con cuestiones laborales de orden legal o contractual según el caso.

En virtud de lo anterior, RISKS INTERNATIONAL S.A.S utilizará los datos personales para los siguientes fines respecto de los empleados:

- ✓ Dar cumplimiento a las leyes de derecho laboral, seguridad social, pensiones, riesgos profesionales, cajas de compensación familiar (Sistema Integral de Seguridad Social) e impuestos;
- ✓ Cumplir las instrucciones de las autoridades judiciales y administrativas competentes;
- ✓ Implementar las políticas y estrategias laborales y organizacionales
- ✓ Vincular personas a RISKS INTERNATIONAL S.A.S, generar reportes, obtener indicadores, pagar la nómina, la seguridad social, la ARL, proceso de cobro de incapacidades, procesos de certificaciones laborales o de prestación de servicios y generar información institucional.
- ✓ Realizar procesos de selección, procesos de bienestar del colaborador (empleado) y sus familias, procesos de compra de dotación, elementos de seguridad en el trabajo, procesos de contratación, nómina, seguridad social, proceso de cobro de incapacidades, procesos de certificaciones laborales o de prestación de servicios y en general, informes estadísticos, procesos de nóminas.
- ✓ Generar las evaluaciones de desempeño, actualizar información, conocer las personas activas y cargos actuales.
- ✓ Dar respuesta a requerimientos de autoridades competentes

En cuanto a los contratistas y proveedores, la información se utilizará para adelantar los procesos precontractuales, contractuales y post-contractuales pertinentes y mantener comunicación con los mismos para efectos contractuales y legales. Lo anterior incluye, entre otros, (i) inscribir el proveedor, llevar un control de los proveedores, solicitarles la presentación de ofertas, facturar los servicios o productos adquiridos, llevar control de pagos y de niveles de compras, y (ii) Cumplir lo pertinente de las obligaciones contractuales, enviar reportes a las autoridades tributarias, de conformidad con lo dispuesto en la normatividad colombiana.

En cuanto a todos los clientes que tengan acceso autorizado para incluir reportes en el componente del sistema de información compartida SISCOM, a través de la plataforma SIRIEST, sobre novedades o reportes relacionados con conductas consideradas riesgos o señales de alerta asociados al Lavado de Activos, la Financiación del Terrorismo y la financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM), la

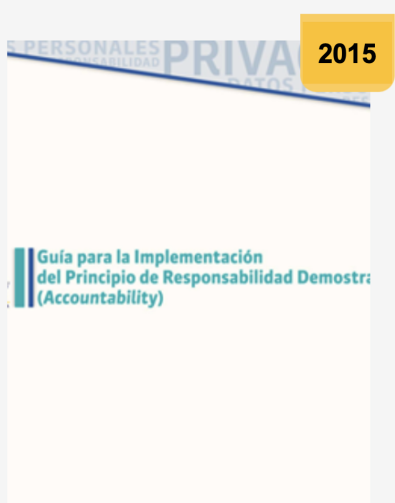
informacion se utilizara para el uso de esta misma herramienta por parte de los mismos clientes.

RESPONSABILIDAD DEMOSTRADA FRENTE AL TRATAMIENTO DE DATOS PERSONALES.

Este manual es parte de las estrategias, procedimientos y herramientas de RISKS INTERNATIONAL S.A.S para demostrar que ha implementado medidas apropiadas y efectivas para cumplir con sus obligaciones legales en todo lo relacionado con el tratamiento de datos personales. Dichas medidas serán consistentes con las instrucciones que para el efecto impacta la SIC y los mandatos de los artículos 26 y 27 del decreto 1377 de 2013.

Estas medidas serán objeto de monitoreo o auditorías con miras a establecer si funcionan correctamente y, en caso de ser necesario, mejorarlas.

Para el efecto, RISKS INTERNATIONAL SAS sigue las orientaciones de las dos siguientes guías de la SIC:



Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)

Guía para la implementación del principio de responsabilidad demostrada

Progresivamente, y en la medida que los recursos lo permitan, se procederá conforme se sintetiza a continuación:

I. Compromiso de la organización

A. Desde la alta gerencia:
(i) Designar persona o área responsable del cumplimiento de las normas sobre tratamiento de datos personales.(ii) Aprobar y monitorear el programa integral de gestión de datos personales (PIGDP); (iii) Informar periódicamente sobre la ejecución del PIGDP; (iv) Destinar recursos necesarios para el cumplimiento de la normativa sobre tratamiento de dato personales.

B. Presentación de informes a directivos:
(i) Seguimiento y ejecución del PIGDP; (ii) Auditorías internas sobre tratamiento de datos personales.

II. Controles del programa

(i) Diseñar e implantar procesos para cumplir las normas sobre tratamiento de datos personales; (ii) Realizar un inventario de bases de datos; (iii) Definir la política de tratamiento de datos personales y otras conexas como, entre otras, las de seguridad; (iv) Implantar herramientas de evaluación y riesgo del tratamiento de datos en la organización; (v) Formación y educación del equipo de colaboradores con miras a generar una cultura de tratamiento de datos personales y asegurar que respetarán las normas en el ejercicio de sus funciones; (vi) Tener previsto protocolos de respuesta a incidentes de seguridad.; (vii) Gestionar adecuadamente los procesos que impliquen recurrir a encargados de tratamiento o transmisiones y transferencias de datos (viii) Comunicación externa de sus políticas para conocimiento del público y los titulares de los datos

III. Evaluación y revisión permanente

Efectuar evaluaciones independientes respecto de las medidas que se han adoptado para garantizar un debido tratamiento de los datos personales

IV. Demostración de cumplimiento

Implantar mecanismos probatorios del cumplimiento de los deberes de la organización sobre tratamiento de datos personales.

Frente a cualquier tratamiento, se implementará un sistema de administración de riesgos de conformidad con las orientaciones de la SIC, las cuales, en términos generales, se resumen de la siguiente manera:

SISTEMA DE ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE DATOS PERSONALES

SIC (2015) "Guía para implementación del principio de responsabilidad demostrada (accountability)". Págs 16-18.

PROTECCIÓN DE DATOS PERSONALES DESDE EL DISEÑO Y POR DEFECTO (PRIVACY BY DESIGN AND BY DEFAULT)

Privacy by Design and by Default

RISKS INTERNATIONAL S.A.S.

Para garantizar el tratamiento lícito de los datos personales y evitar vulneraciones a los derechos de los titulares de esa información se hará uso de la privacidad desde el diseño y por defecto (*Privacy by Design and by Default*)

El debido tratamiento de datos es un elemento fundamental en nuestra organización. Por eso, desde antes de recolectar información y durante todo el ciclo de vida de la misma, adoptarán medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, ética y procedimental, entre otras) con el objeto de evitar vulneraciones a los derechos de las personas, así como fallas de

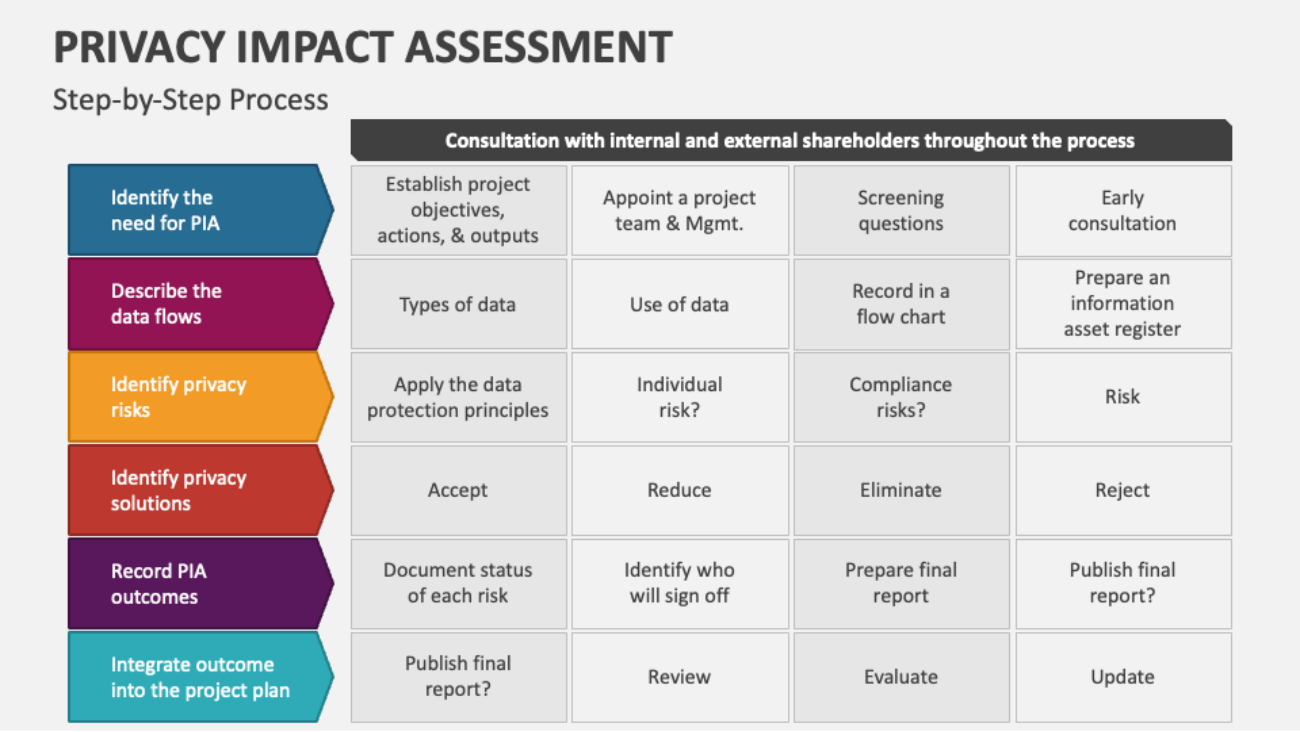
seguridad o indebidos Tratamientos de Datos Personales.

En el evento que surjan nuevos proyectos o actividades que involucre tratamiento de datos personales se aplicarán desde el inicio de los mismos medidas técnicas, organizativas y de cualquier otra índole, con miras a garantizar el tratamiento de datos personales conforme la ley.

Se implementarán medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos de la ley.

ESTUDIOS DE IMPACTO DE PRIVACIDAD (PRIVACY IMPACT ASSESSMENT - PIA).

Previo al diseño y desarrollo de proyectos o actividades que involucren tratamiento de datos personales, y en la medida en que sea probable que el mismo entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los Titulares, se efectuará una evaluación de impacto en la privacidad (*Privacy Impact Assessment - PIA* por sus siglas en inglés).



Se realizará esa evaluación con el fin de poner en funcionamiento un sistema efectivo de manejo de riesgos y controles internos, para garantizar que los datos se tratarán debidamente y conforme con la regulación existente.

Dicha evaluación debería incluir, como mínimo, lo siguiente:

- Una descripción detallada de las operaciones de Tratamiento de datos personales que involucran el proyecto o actividad.
- Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales. Se desarrollará y pondrá en marcha un sistema de administración de riesgos asociados al tratamiento de datos personales que les permita identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales.
- Las medidas previstas para afrontar los riesgos, incluidas garantías; medidas de seguridad; diseño de *software*; tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los Titulares de los datos y de otras personas eventualmente afectadas.

Los resultados de este estudio, junto con las medidas para mitigar los riesgos, hacen parte de la aplicación del principio de privacidad desde el diseño y por defecto.

FINALIDAD Y TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS PERSONALES DE LOS VISITANTES A LAS INSTALACIONES DE RISKS INTERNATIONAL S.A.S

Respecto de los datos (i) recolectados directamente en los puntos de seguridad, (ii) tomados de los documentos que suministran las personas al personal de seguridad y (iii) obtenidos de las videograbaciones que se realizan dentro o fuera de las instalaciones de RISKS INTERNATIONAL S.A.S, estos se utilizarán para fines de seguridad de las personas, los bienes e instalaciones de RISKS INTERNATIONAL S.A.S y podrán ser empleados como prueba en cualquier tipo de proceso.

FINALIDAD Y TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS PERSONALES DE LOS SOCIOS O ACCIONISTAS DE RISKS INTERNATIONAL S.A.S

El tratamiento de los datos de los accionistas tendrá como finalidad cumplir los deberes legales pertinentes como, entre otros, llevar los libros y papeles comerciales. De igual forma, la información se utilizará para efectuar todas las actividades relacionadas con los derechos

económicos y políticos, administrativos de los socios o accionistas. Adicionalmente, sus datos se emplearán para mantener comunicación con los mismos.

OTRAS FINALIDADES AL CUAL SERÁN SOMETIDOS LOS DATOS PERSONALES

RISKS INTERNATIONAL S.A.S también podrá tratar los datos personales para los siguientes fines:

- ✓ Efectuar las gestiones pertinentes para el desarrollo de la etapa precontractual, contractual y pos contractual de los titulares de los datos con RISKS INTERNATIONAL S.A.S., así como cualquiera de los contratos en los que hacen parte, y para dar cumplimiento a la ley colombiana o extranjera y a las órdenes de autoridades judiciales o administrativas.
- ✓ Dar a conocer, transferir y/o transmitir datos personales dentro del país a terceros a consecuencia de un contrato, ley o vínculo lícito que así lo requiera o para cumplir los contratos en que sea parte así como implementar servicios de computación en la nube o "big data".
- ✓ Implementar estrategias de CRM (customer relationship management), que comprende, entre otras, (i) un modelo de gestión de toda la organización, basada en la orientación al cliente y marketing relacional; (ii) Crear bases de datos o sistemas informáticos de apoyo a la gestión de las relaciones con los clientes, a la venta y al marketing.
- ✓ Realizar invitaciones a eventos, mejorar los servicios u ofertar nuevos, y todas aquellas actividades asociadas a la relación comercial o vínculo existente con RISKS INTERNATIONAL S.A.S , o aquel que llegare a tener.
- ✓ Gestionar trámites (solicitudes, quejas, reclamos), efectuar encuestas de satisfacción respecto de los bienes y servicios que ofrece .
- ✓ Suministrar información de contacto y documentos pertinentes a la fuerza comercial y/o red de distribución y telemercadeo.
- ✓ Ofrecer servicios y/o beneficios que buscan satisfacer las necesidades de los Titulares, o los productos y servicios de RISKS INTERNATIONAL S.A.S, lo cual pueden hacerse por medios físicos o a través de correos electrónicos y/o terminales móviles.
- ✓ Enviar la información a entidades gubernamentales por exigencia legal.
- ✓ Consultar información en las listas de control (Listas Nacionales e Internacionales) consulta a CIFIN, a las centrales de información, Lista Clinton, Procuraduría, Contraloría, Policía Nacional, DIJIN, y similares, con el fin de preservar la confianza y transparencia entre el Titular de los Datos y RISKS INTERNATIONAL S.A.S .
- ✓ Soportar procesos de auditoría externa e interna.
- ✓ Para la ejecución de procesos de índole judicial y extrajudicial.

- ✓ Registrar la información colaboradores, ex colaboradores, proveedores (activos e inactivos) y aliados en las bases de datos de RISKS INTERNATIONAL S.A.S, para el envío de información contractual, comercial y obligacional a que hubiere lugar.
- ✓ Para verificación de referencias de colaboradores, de ex colaboradores, proveedores (activos e inactivos) y aliados en las bases de datos.
- ✓ Respecto de la recolección y tratamiento de datos realizado mediante mecanismos automatizados con el objeto de generar registros de actividad de los visitantes de RISKS INTERNATIONAL S.A.S

Explicación sobre la necesidad de recolectar la información.

Según el caso, se recolectarán los datos estrictamente necesarios o razonables para cumplir cada una de las finalidades mencionadas. Para el efecto, se realizará un análisis para justificar la información requerida con miras a lograr lo anterior.

PROCEDIMIENTO PARA EL ALMACENAMIENTO DE DATOS PERSONALES

Una vez recolectados los datos, se almacenará la información en las bases de datos físicas o electrónicas con medidas técnicas, humanas y administrativas que establezca la empresa para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Los documentos, registros o informaciones serán almacenados o conservados en sistemas electrónicos que cumplan, por lo menos, las siguientes condiciones:

1. Que la información que contengan sea accesible para su posterior consulta.
2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y
3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

PROCEDIMIENTO PARA EL USO DE LOS DATOS PERSONALES

Los datos sólo podrán utilizarse, según el caso, para los fines autorizados por el Titular de la información o los permitidos por la ley. Para el efecto, antes de usar los datos se verificará si se puede o no utilizar la información.

Antes de usar la información, verifique en las autorizaciones o en la ley si podemos utilizarla para dichas finalidades

En el caso del uso de los datos para realizar campañas o actividades de publicidad o marketing la persona encargada de esa labor en la empresa deberá verificar previamente si se cuenta con la autorización necesaria para dicha labor. En caso de no contar con la misma, deberá abstenerse de utilizarla para ese propósito.

Uso de datos personales para el envío de comunicaciones electrónicas, telefónicas o cualquier otra naturaleza

Toda persona que utilice la dirección de correo corporativa de RISKS INTERNATIONAL S.A.S para remitir desde la misma mensajes o que emplee otros medios de comunicación (teléfono, chat, entre otros) deberá asegurarse de cumplir lo siguiente:

- Utilizar el correo electrónico y demás medios de comunicación sólo para fines lícitos e institucionales
- Los mensajes corporativos sólo pueden ser enviados por las personas previamente autorizadas por el (la) representante legal de RISKS INTERNATIONAL S.A.S. Por ejemplo, las campañas publicitarias o de marketing sólo pueden ser enviadas por quien esté previamente autorizado para dicho efecto y no por cualquier persona de RISKS INTERNATIONAL S.A.S.
- Únicamente remitir mensajes a personas respecto de las cuales se tenga autorización previa, expresa e informada para enviarle comunicaciones a su dirección de correo electrónico. Para el efecto, antes de enviar el mensaje se debe verificar si se cuenta con dicha autorización, salvo que se trate de direcciones de correo que son datos públicos como, entre otras, direcciones corporativas o relacionadas con la profesión u oficio de una persona.
- No se puede enviar correos a personas que no estén en la base de datos de RISKS INTERNATIONAL S.A.S., ni es permitido enviar comunicaciones a destinatarios (as) cuyos datos se hayan obtenido a título personal –no institucional- como, por ejemplo, amigos, ex-clientes, familiares, entre otros.

- Remitir el mensaje de manera que el destinatario sólo pueda ver su dirección de correo y no tenga acceso a las direcciones de correo de otros eventuales destinatarios de la misma comunicación.
- No puede enviarse información confidencial o privada de RISKS INTERNATIONAL S.A.S sin contar con la previa autorización de representante legal de la sociedad.
- La dirección de correo de RISKS INTERNATIONAL S.A.S es personal, intransferible y para uso institucional o corporativo. Por lo tanto está prohibido facilitar la cuenta de correo para el envío de información de usuarios externos o para actividades personales o diferentes a las autorizadas por el representante legal de RISKS INTERNATIONAL S.A.S.

Todo lo anterior también es aplicable a las comunicaciones que se realicen telefónicamente o por cualquier otro medio.

PROCEDIMIENTO PARA LA CIRCULACIÓN DE DATOS PERSONALES

Pautas generales

Está restringida la circulación o envío de datos personales a nivel interno o externo de la empresa. Solo se podrá compartir si se cuenta con la autorización para dicho efecto o en los términos previstos en la ley.

Antes de circular o enviar la información, verifique en las autorizaciones o en la ley si podemos enviarla a determinada persona o entidad

De conformidad con el artículo 13 de la Ley 1581 de 2012, los datos personales podrán suministrarse a las siguientes personas:

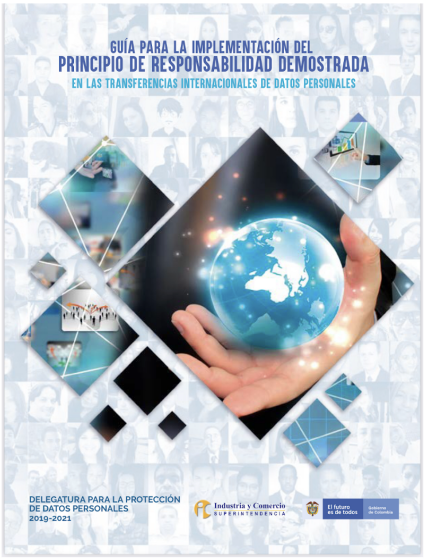
a) A los Titulares, sus causahabientes o sus representantes legales;
b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial;
c) A los terceros autorizados por el Titular o por la ley.
Dado lo anterior, en cada caso se verificará previamente si se puede

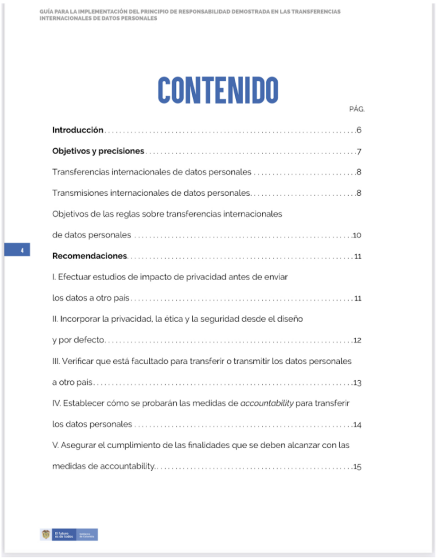
Transferencia internacional de datos personales

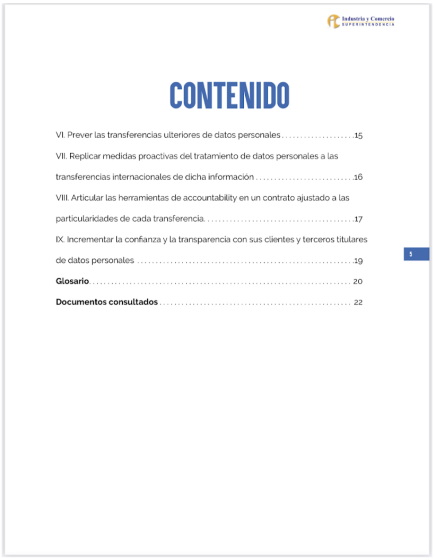
Cuando se envíen o transfieran datos a otro país será necesario contar con la autorización del Titular de la información que es objeto de transferencia. Salvo que la ley diga lo contrario o que Superintendencia de Industria y Comercio (SIC) ordene algo diferente, dicha autorización es prerrequisito para efectuar la circulación internacional de datos. En este sentido, antes de enviar datos personales a Responsables del Tratamiento ubicados en otro país, los obligados de cumplir esta política deberán verificar que se cuenta con la autorización previa, expresa e inequívoca del Titular que permita trasmitir sus datos personales.

Lo anterior, desde luego, siempre y cuando la autoridad de protección de datos no emita instrucciones diferentes, las cuales serán tenidas en cuenta al momento de circular transfronterizamente datos personales.

Para realizar la transferencia internacional de datos personales se revisará previamente las alternativas que ofrece la circular 5 de 2017 y la circular única de la SIC. Adicionalmente, se tendrá en cuenta la guía de accountability y transferencias internacionales de dicha entidad.



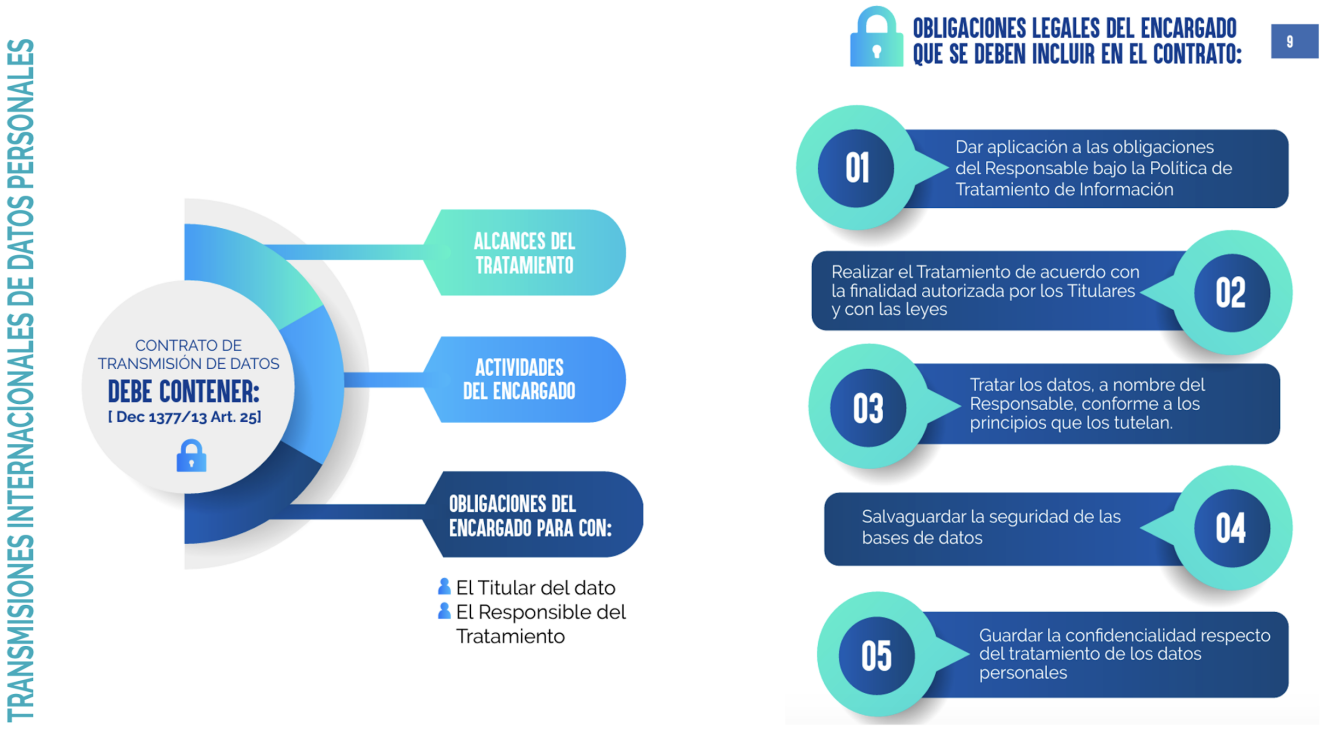




Transmisiones internacionales y nacionales de datos a Encargados

Cuando RISKS INTERNATIONAL S.A.S desee enviar o transmitir datos a uno o varios encargados ubicados dentro o fuera del territorio de la República de Colombia, deberá establecer mediante cláusulas contractuales o a través de un contrato de transmisión de datos personales, entre otros, lo siguiente:

(i) los alcances del tratamiento;
(ii) las actividades que el Encargado realizará en nombre de RISKS INTERNATIONAL S.A.S
(iii) las obligaciones que debe cumplir el Encargado respecto del Titular del dato y RISKS INTERNATIONAL S.A.S.
(iv) La obligación del Encargado de dar cumplimiento a las obligaciones del Responsable observando la presente política.
(v) El deber del Encargado de tratar los datos de acuerdo con la finalidad autorizada para el mismo y observando los principios establecidos en la ley colombiana y la presente política.
(vi) La obligación del Encargado de proteger adecuadamente los datos personales y las bases de datos así como de guardar confidencialidad respecto del tratamiento de los datos transmitidos.



*** Imagen tomada de la guía de accountability en las transferencias internacionales de la SIC

PROCEDIMIENTO DE ACCESO PARA REALIZAR LA CORRECCIÓN, ACTUALIZACIÓN, RECTIFICACIÓN O SUPRESIÓN DE LA INFORMACIÓN Y REVOCATORIA DE LA AUTORIZACIÓN REQUERIDOS POR EL TITULAR DE LA INFORMACIÓN.

A continuación, se detallan los procedimientos para que los titulares de los datos puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información o revocar la autorización.

Los derechos de los Titulares, podrán ejercerse por las siguientes personas legitimadas de conformidad con el artículo 20 del decreto 1377 de 2013:

a. Por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición RISKS INTERNATIONAL S.A.S.
b. Por sus causahabientes, quienes deberán acreditar tal calidad.
c. Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
d. Por estipulación a favor de otro o para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Todas las consultas y reclamos se canalizarán por medio de los mecanismos habilitados por RISKS INTERNATIONAL S.A.S., a través de comunicación escrita remitida a la Calle 25 B 39 A-30 en Bogotá teléfono: 6017981834 correo electrónico: habeasdata@risksint.com (Bogotá), quien adoptará mecanismos de prueba de la radicación y trámite de los mismos.

Esquema general

Estas son las pautas para atender consultas y reclamos:

	CONSULTAS	RECLAMOS
Objetivo	Que la persona (*Titular del dato*) conozca la información que poseen sobre ella las entidades públicas o privadas. *** Imprescindible verificar la identidad del Titular del dato (evitar suplantaciones o que personas no legitimadas presenten la consulta)*	Corregir, actualizar o suprimir la información. Colocar la "*Leyenda reclamo en trámite*" *** Indispensable verificar la identidad del Titular del dato (evitar suplantaciones o que personas no legitimadas presenten el reclamo)*
¿Ante quién se presenta?	Responsable o Encargado del tratamiento.	Responsable o Encargado del tratamiento.
Tiempo de respuesta	10 días hábiles (dh) a partir de la fecha de recibo. Prorrogables hasta 5 dh posteriores al vencimiento del primer término.	15 dh a partir del día siguiente de la fecha de recibo. Prorrogables hasta 8 dh posteriores al vencimiento del primer plazo.
Regulación	Art. 14 (Ley 1581/12)	Art. 15 (Ley 1581/12)

Consultas

Todas las consultas que realicen las personas legitimadas para conocer los datos personales que reposen en RISKS INTERNATIONAL S.A.S recolectados por medios físicos y/o, digitales que se encuentran en las bases de datos utilizadas por RISKS INTERNATIONAL S.A.S**.** para el desarrollo de sus actividades empresariales, se canalizarán a través de los canales que tiene RISKS INTERNATIONAL S.A.S para el efecto. En todo caso es necesario dejar prueba de lo siguiente:

- Fecha de recibo de la consulta
- Identidad del solicitante

Una vez verificada la identidad del Titular se le suministrarán los datos personales requeridos. La respuesta a la consulta deberá comunicarse al solicitante en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma.

Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Reclamos

Los reclamos tienen por objeto corregir, actualizar, o suprimir datos o elevar una queja por el presunto incumplimiento de cualquiera de los deberes contenidos en la ley 1581 de 2012 y en esta política.

El reclamo debe presentarse mediante solicitud dirigida a RISKS INTERNATIONAL S.A.S que contenga la siguiente información:

a. Nombre e identificación del titular del dato o la persona legitimada.
b. Descripción precisa y completa de los hechos que dan lugar al reclamo.
c. Dirección física o electrónica para remitir la respuesta e informar sobre el estado del trámite.
d. Documentos y demás pruebas pertinentes que quiera hacer valer.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días hábiles 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.

Si el reclamo está completo, se incluirá en la base de datos o sistema de información una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Ésta 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 interesado 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.

RISKS INTERNATIONAL S.A.S garantizará siempre en verificar que la respuesta dada al titular de la información sea de fondo e integralmente conforme a lo solicitado.

PROCEDIMIENTO PARA GARANTIZAR LA CALIDAD Y LA PLENA VERACIDAD DE LOS DATOS SUMINISTRADOS POR SUS SUSCRIPTORES, RESPECTO A LOS REPORTES QUE SOLICITAN INCLUIR EN EL HISTORIAL DEL TITULAR DE LA HERRAMIENTA SIRIEST COMPONENTE SISCOM.

Dentro de los servicios prestados por RISKS INTERNATIONAL SAS es apoyar a las empresas de transporte en la implementación de medidas que ayuden y permitan mitigar los riesgos asociados a piratería terrestre, mal manejo de anticipos, lavado de activos y financiación del terrorismo y proliferación de armas de destrucción masiva, hurto de mercancías, la receptación y las modalidades como el hurto de hidrocarburos, la contaminación de mercancía por narcotráfico, actos malintencionados de terceros y la informalidad en el sector logístico y de transporte.

RISKS INTERNATIONAL S.A.S ha desarrollado la herramienta SIRIEST y cuenta con un sistema de información compartida SISCOM que le permite atraer información de carácter público, de diferentes fuentes públicas para la mitigación del riesgo asociado a LAFT.

Una vez adquirido el servicio a través de la suscripción de un contrato y acuerdo de confidencialidad con el cliente, se le asigna un número determinado de usuarios, asignando un usuario a cada uno de ellos. Para el ingreso a SIRIEST, la persona debe cumplir las medidas de seguridad implementadas por RISKS INTERNATIONAL S.A.S, con el fin de asegurar el control, la seguridad en el uso y el acceso a la plataforma y a la información allí recopilada con estándares altos de protección informática.

Los usuarios creados serán anclados a un correo corporativo asignado a la persona que hará uso de la herramienta y para el cambio de los usuarios se debe realizar solicitud al área de soporte o al asesor comercial asignado, para que pueda brindar las credenciales de acceso al nuevo usuario una vez firmados los acuerdos de confidencialidad y posterior al bloqueo y/o elimine el usuario anterior.

Para el ingreso a la plataforma, cada usuario debe acceder a través del link correspondiente de acceso en la pestaña de Login, en donde se pedirán sus credenciales de acceso (usuario y contraseña), una vez validados los datos de ingreso, se enviará un código a la persona con

usuario asignado para habilitar el ingreso; el ingreso apoyado con código generado en línea, evita el uso simultáneo de acceso y el robo de usuario; así mismo, el sistema tiene implementado un cierre automático de sesión cuando se intenta abrir dos sesiones al mismo tiempo.

En el sistema SIRIEST se podrán realizar consultas y reportes sobre la información.

Consultas.

Se realizan ingresando a la plataforma en la cual se tendrá la opción de consultar por número de identificación de la persona, nombre o placa del vehículo.

Una vez introducida la opción, la plataforma le generará un informe en el cual podrá observar la información pública referente a la consulta realizada y en la parte superior podrá observar si se cuentan con datos en el sistema de información compartida SISCOM datos que son confidenciales, pues cumplen una función social, estadística y de mitigación para la prevención de riesgos para la prevención LAFT, corrupción, soborno transnacional entre otros del sector transporte.

Reportes

El cliente tiene la calidad de responsable del tratamiento de datos personales a luces de la ley 1581 de 2012 y sus decretos reglamentarios, entendiéndose como el encargado de definir sobre la finalidad del dato recolectado. Una vez indicado en la calidad en la que actúa el cliente, para poder reportar datos en el sistema de información compartida, SISCOM cuenta con dos opciones:

Reporte escalado:

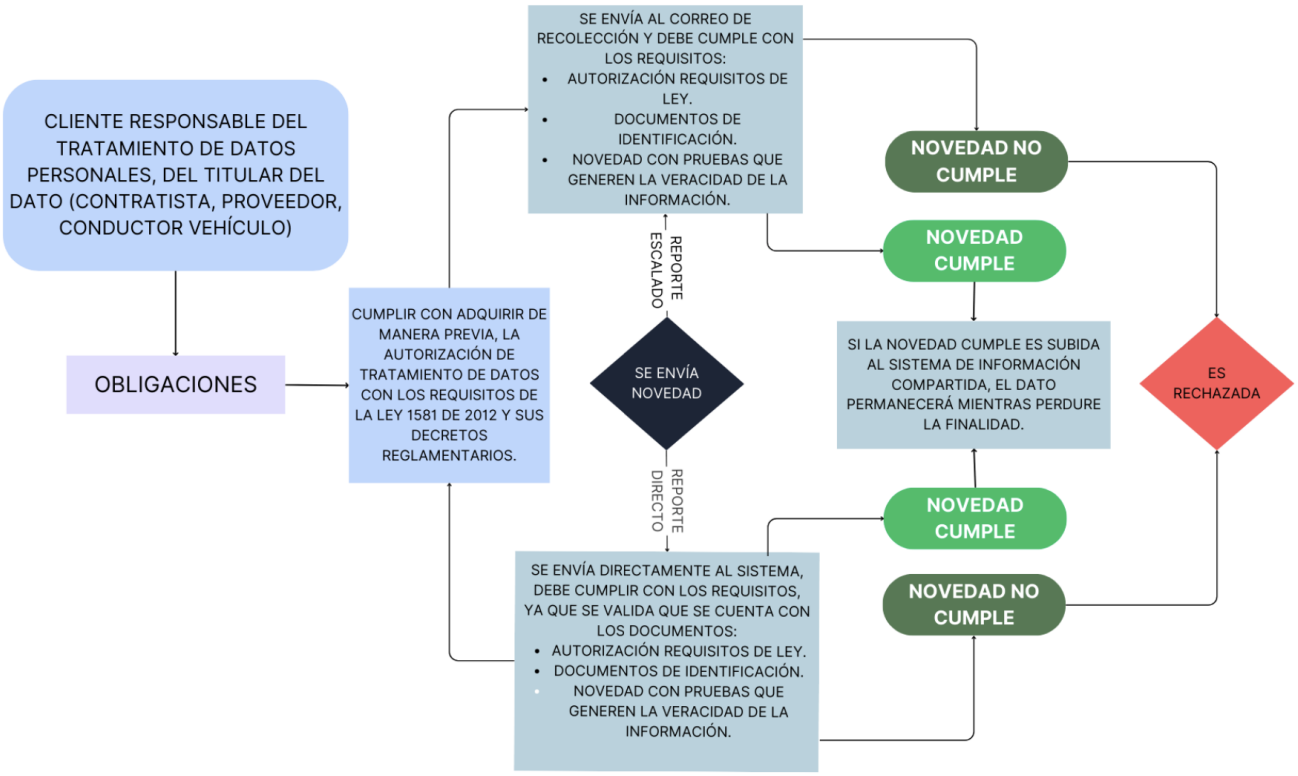
Este se realiza enviando directamente la novedad al correo electrónico del área de recolección previo al haber requerido la autorización del titular de la información por cualquier medida inequívoca que autorice el tratamiento, cumpliendo ésta con las características y finalidades correspondientes indicadas en la norma que versen sobre la profesión u oficio del conductor a luces de la ley 1581 de 2012 como dato de carácter público, adicionada en el decreto 1377 de 2013 artículo 5, 6 y 7. Esto en cumplimiento de las demás disposiciones legales sobre el tratamiento de datos personales con los cuales debe contar el cliente, como su propia política de tratamiento de datos personales, aviso de privacidad donde se pueda indicar de manera resumida su finalidad en la página web con la que cuente el cliente.

Es importante que el cliente, cumpla con el deber de informarle previamente al titular sobre la realización del reporte y guardar soporte de dicho preaviso; el titular es el dueño del dato que va a ser reportado e ineludiblemente se debe cumplir con el aviso con la autorización de tratamiento de datos, en cumplimiento de la ley 1581 de 2012.

Para que el área de recolección reciba el reporte es necesario contar con la siguiente información:

- Copia de la cédula de ciudadanía del titular de la información
- Autorización tratamiento de datos, con fines específicos para el sector transporte y prevención riesgo Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM) y demás conexos.
- Breve descripción de la novedad que se desea subir al SISCOM con información exacta, objetiva y verificable.
- Pruebas que respalden el reporte

Una vez recibida la información el área de recolección hace la subida de la información para que el cliente a través del usuario suscriptor sea quien a través de la herramienta apruebe o rechace el reporte en la plataforma, teniendo en cuenta los criterios de veracidad, claridad y concordancia de la novedad junto con el documento que acredite la autorización del titular de la información para el tratamiento de sus datos personales.



Reporte de cargue directo:

Se puede realizar el reporte directamente en la plataforma, los usuarios suscriptores pueden incluir reportes en el componente del sistema de información compartida SISCOM, a través de la plataforma SIRIEST, garantizando la veracidad, calidad y legalidad de los datos, en cumplimiento de las disposiciones legales vigentes relacionadas con el LA/FT/FP, SIPLAFT y SARLAFT y la protección de datos personales.

Este procedimiento aplica para todos los usuarios suscriptores que tengan acceso autorizado al sistema SIRIEST para la inclusión de novedades o reportes relacionados con conductas consideradas riesgos asociados a el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM).

En este procedimiento intervienen, el usuario suscriptor (persona designada por la empresa suscriptora) y el área de Recolección de RISKS INTERNATIONAL S.A.S.

Área de recolección: su rol es apoyar y gestionar las alertas por no cargue completo de documentación o asociadas al dato reportado solo cuando el sistema detecta inconsistencias o faltantes en los documentos cargados.
Usuario Suscriptor: su rol es incluir directamente los reportes en SIRIEST, garantizando el cumplimiento de los requisitos legales, en su calidad de Responsable de conformidad a la ley 1581 de 2012 y los deberes establecidos en el anexo 4 del presente manual.

El sistema SIRIEST cuenta con un módulo exclusivo para que el usuario suscriptor realice el cargue directo de novedades al sistema de información compartida (SISCOM), en cumplimiento del marco normativo de SARLAFT, la Ley 1581 de 2012 y demás dispuesta en el marco normativo.

El usuario suscriptor debe diligenciar y aportar como soporte de cumplimiento normativo: en el módulo "Subir Novedad", los siguientes documentos:

- Identificación del titular del dato (persona natural y/o vehículo).
- Autorización para el tratamiento de datos personales, con fines específicos para el sector transporte y prevención riesgo Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM) y demás conexos.
- Documento de identidad del titular (copia legible).
- Pruebas objetivas que respalden la novedad (documentos, fotos, contratos, manifiestos, anulación de manifiestos, actas, decisiones, etc.).
- Clasificación de la novedad asociada a los riesgos descritos en el anexo 1 “Glosario” en la definición de Riesgos LAFT, el suscriptor deberá identificar a qué riesgo se asocia el tipo de novedad.

Cargados los documentos, el sistema habilita al usuario suscriptor, quien deberá resumir la novedad en un máximo de 400 caracteres, de forma objetiva, conforme al riesgo asociado y verificable con los soportes en su poder. Al finalizar este proceso, la novedad queda registrada automáticamente en el sistema y se mantiene visible para los demás suscriptores, salvo que exista una alerta o en auditoría posterior, se evidencie alguna situación a subsanar.

Se cuenta con un sistema de alerta que permite bajo el principio de veracidad de la información descartar novedades que no cumplan dichos principios, o que provengan de fuentes anónimas, incompletas o no verificables y además evidencia al área de recolección que no se cargó ningún documento requerido o algún documento no cumple con las características mínimas de legalidad, objetividad o veracidad.

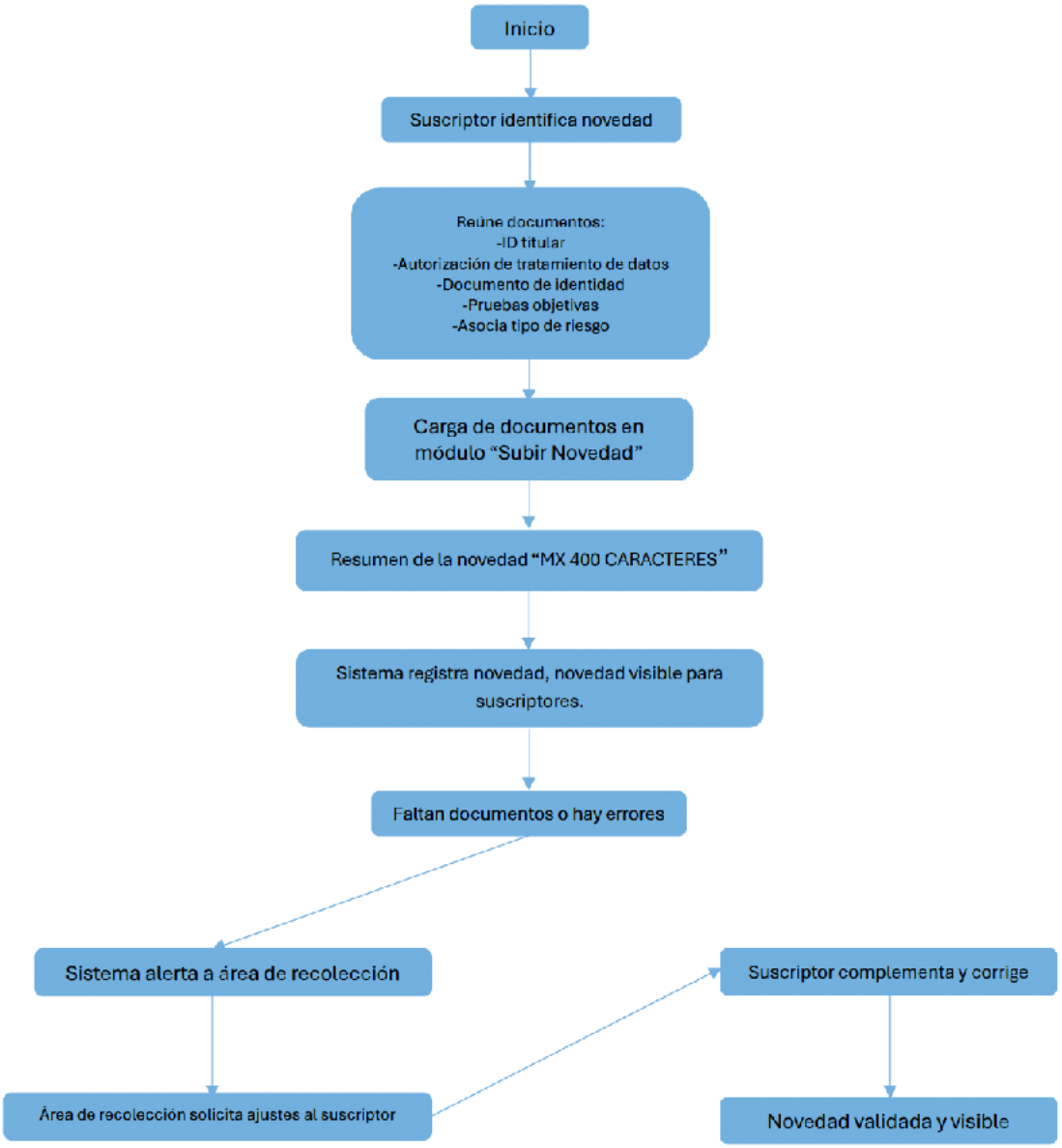
En tales casos, el área de recolección notificará al usuario suscriptor para que subsane los documentos faltantes o inválidos.

El suscriptor tendrá un plazo para complementar la información, en cumplimiento a lo establecido por la Ley 1581 de 2012 sobre la veracidad y finalidad en el tratamiento de datos personales. El dato tendrá anotación de no visible, no será consultable por ningún suscriptor, hasta su subsanación.

El área de recolección apoya la parte técnica del sistema y cuenta con el apoyo del área legal, recibe quejas o consultas del usuario suscriptor, adicionalmente de manera esporádica y aleatoria, realiza auditorías y tramita los casos en que el sistema detecte inconsistencias en los documentos cargados, o cuando falten documentación del paso a paso para el cargue de documentación.

RISKS INTERNATIONAL SAS, podrá usar en cualquier momento la documentación que respalde la autorización y veracidad del dato, que se encuentre en el sistema conforme a las obligaciones contractuales, a efectos de tramitar las consultas y/o solicitudes que eleve el titular o cuando lo requiera autoridad competente.

Flujo del proceso de inclusión de Novedades en SIRIEST



Persona o área responsable de la protección de datos personales

EL OFICIAL DE CUMPLIMIENTO Y OFICIAL DE PROTECCIÓN DE DATOS PERSONALES EN CABEZA DEL DR HERNAN DARIO ACEVEDO es la persona encargada de la función de protección de datos, la cual se puede contactar en la (teléfono 6017941834 y dirección de correo electrónico **habeasdata@risksint.com**) (Bogotá).

MECANISMOS GRATUITOS Y DE FÁCIL ACCESO PARA PRESENTAR LA SOLICITUD DE SUPRESIÓN DE DATOS O LA REVOCATORIA DE LA AUTORIZACIÓN OTORGADA

El Titular del dato puede acudir a los siguientes mecanismos para presentar sus consultas o reclamos y por ende solicitar acceso, actualización, supresión, rectificación de datos personales y revocatoria de la autorización, entre otros:
Correo electrónico: **habeasdata@risksint.com**

VIDEO VIGILANCIA

- RISKS INTERNATIONAL S.A.S utiliza diversos medios de videovigilancia instalados en diferentes sitios internos y externos de nuestras instalaciones u oficinas.
- RISKS INTERNATIONAL S.A.S informa sobre la existencia de estos mecanismos mediante la difusión en sitios visibles de anuncios de video-vigilancia.
- La información recolectada se utilizará para fines de seguridad de las personas, los bienes e instalaciones. Esta información puede ser empleada como prueba en cualquier tipo de proceso ante cualquier tipo de autoridad y organización.

MEDIDAS DE SEGURIDAD APLICADAS AL TRATAMIENTO DE LAS BASES DE DATOS

Proteger la información es una condición crucial del tratamiento de datos personales.
La seguridad es un proceso dinámico en constante evolución y prueba. Garantizamos un nivel de seguridad apropiado en las diferentes etapas del tratamiento de datos personales en donde las medidas de seguridad son objeto de evaluación y revisión.

Dichas medidas están enfocadas para mitigar los siguientes riesgos: acceso no autorizado a los datos personales, pérdida, destrucción (accidental o no autorizada), contaminación (por virus informático) uso fraudulento, consulta, copia, modificación, adulteración, revelación, comunicación, o difusión no autorizados.

Para establecer las medidas se tienen en cuenta, entre otras, las técnicas de seguridad existentes en general y para sectores específicos, los riesgos que presente el tratamiento y la naturaleza de los datos que deban protegerse, la probabilidad y severidad del daño

obtenido, la sensibilidad de la información y el contexto en el que es realizado el tratamiento y las eventuales consecuencias negativas para los titulares de los datos.

Varios factores son cruciales para garantizar la seguridad de la información. Ninguno es suficiente por sí sólo, razón por la cual es necesario que todos confluyan para otorgar seguridad a la información, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Estos pilares sintetizan los elementos fundamentales de la seguridad en nuestra organización:

- **Enfoque preventivo de incidentes de seguridad:** Todos los esfuerzos tendrán como meta evitar que situaciones que comprometan la seguridad de la información. En caso de presentarse incidentes de seguridad se dará respuesta a los mismos y a partir de las vulnerabilidades detectadas se efectuarán mejoras en la seguridad de la información.
- **Medidas humanas:** Se trabajará para generar una cultura de seguridad de la información mediante capacitación y concientización del equipo humano de nuestra empresa con miras a que conozcan la importancia de mantener la información segura

y su responsabilidad personal para que en nuestra organización no ocurran incidentes de seguridad.

- **Pautas técnicas y físicas**: Se utilizarán equipos, muebles, software y procesos razonables y acordes para garantizar la seguridad de la información.
- **Oficial de seguridad y medidas administrativas**: Se asignará a una persona o dependencia la responsabilidad de velar por garantizar la seguridad de la información.
- **Herramientas contractuales**: En los contratos se incluirá cláusulas exigiendo el respeto de las medidas de seguridad, la confidencialidad y uso lícito de la información.
- **Revisión periódica**: Todas las medidas de seguridad serán objeto de evaluación anual con miras a establecer el nivel de utilidad de estas y, en caso de ser necesario, implementar estrategias adicionales para mejorar el nivel de seguridad de la información.

Protegemos la información mediante varios mecanismos como, entre otros, los siguientes:

- Protección de acceso a los datos mediante contraseñas y roles de diferentes niveles de autoridad.
- Protección de las contraseñas.
- Aseguramiento del nivel de complejidad de las contraseñas de los usuarios
- Rastreo de todas las actividades realizadas con las plataformas y sus datos.
- Procedimientos de recuperación y redundancia
- Almacenamiento de las copias de respaldo.
- Cifrado y protección por contraseña de los computadores desde los que se realiza la manipulación de los datos.

Adicionalmente, contamos con una política de seguridad de información y datos personales de obligatorio cumplimiento

GESTIÓN DE INCIDENTES DE SEGURIDAD

El literal n) del artículo 17 de la Ley Estatutaria 1581 de 2012 impone al Responsable del Tratamiento el deber de informar a la Superintendencia de Industria y Comercio (SIC) los incidentes de seguridad que generen riesgos en la administración de los datos. Esa misma obligación la debe cumplir el Encargado del Tratamiento por mandato del literal k) del artículo 18 de la citada ley. Esto ordenan dichos artículos:

> **"ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO.** Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:
> (…)
> 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."
>
> **ARTÍCULO 18. DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO.** Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:
> (…)
> k) Informar a la 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;"

El Capítulo II, Título V de la Circular Única de la Superintendencia de Industria y Comercio establece que las organizaciones que están obligadas a inscribir las Bases de Datos Personales ante el Registro Nacional de Bases de Datos (en adelante "RNBD"), deberán reportar el incidente de seguridad dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o el área encargada de atenderlos[7].

La SIC exige que en el reporte del incidente se señala lo siguiente:

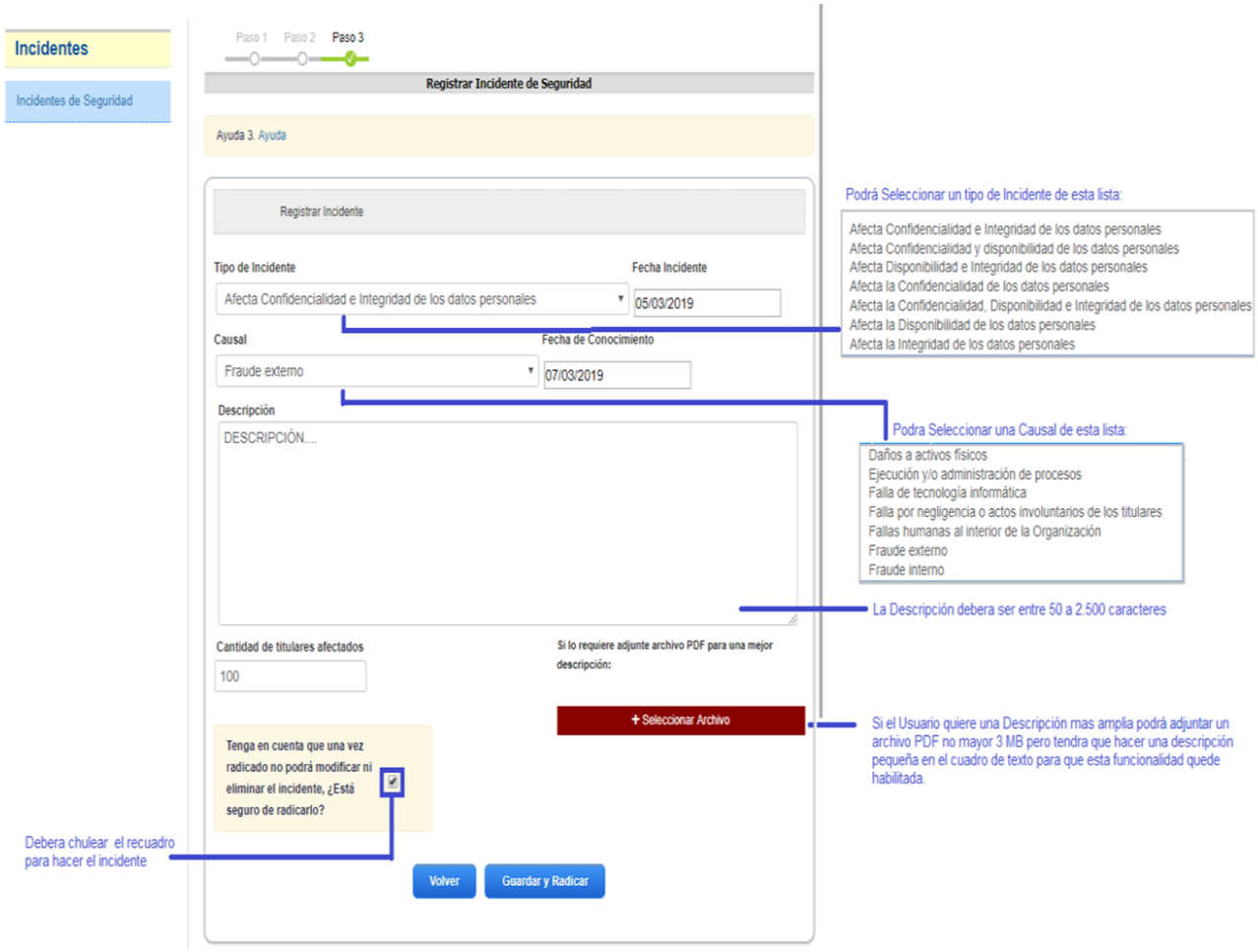
- Nombre de la base de datos afectada e inscrita en el Registro Nacional de Bases de Datos (RNBD)
- Categoría de datos afectados

---

[7] *"CIRCULAR ÚNICA DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO*
TÍTULO V PROTECCIÓN DE DATOS PERSONALES
*CAPÍTULO SEGUNDO: REGISTRO NACIONAL DE BASES DE DATOS –RNBD**
2.1. Información adicional que deberá inscribirse en el Registro Nacional de Bases de Datos RNBD

"(ii) Incidentes de seguridad. Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de ***información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado****, que deberán reportarse al RNBD por parte de los Responsables del Tratamiento que se encuentran obligados a registrar sus bases de datos en el RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos"*

- Diligenciar el siguiente formulario de incidentes[8]:



Lo anterior, se replica en los mismos términos en la Circular externa 2 del 3 de noviembre de 2015 de la SIC.

Estas son algunas de las recomendaciones de la SIC publicadas en la guía de gestión de incidentes de seguridad de 2020:

- Adoptar medidas correctivas e inmediatas para mitigar los daños causados por el incidente.

[8] El formulario del incidente fue tomado de: SIC. Manual de Usuario del Registro Nacional de Bases de Datos – RNBD. Versión 6.7 - Vigente desde 06/07/2023. Página 94. Publicado en: https://www.sic.gov.co/sites/default/files/files/2023/Manual%20de%20UsuarioRNBD%20R-06072023.pdf (Última consulta: noviembre 4 de 2025)

- Realizar actividades preventivas para evitar futuros incidentes de seguridad
- Documentar todos los aspectos de cada incidente de seguridad en los registros internos de las organizaciones. Según dicha entidad, se debe incluir en el registro documental lo siguiente:
    - Una descripción general de las circunstancias del incidente de seguridad (incluidas las Bases de Datos y las clases de datos -sensibles, privados, etc.- comprometidos).
    - Las categorías de Titulares de la información afectados.
    - La fecha y hora del incidente de seguridad y del descubrimiento del mismo.
    - Las indagaciones preliminares e investigaciones realizadas por la organización.
    - Las medidas correctivas.
    - Los responsables del manejo del incidente de seguridad.
    - La prueba del reporte efectuado ante la SIC, así como la comunicación realizada a los Titulares de la información, si fue necesario.
    - La evaluación del nivel de riesgo derivado del incidente de seguridad en los Titulares y los factores tenidos en cuenta.
    - La inclusión de detalles personales, cuando deban establecerse.
- Contar con un protocolo para el manejo de incidentes de seguridad
- Entrenar periódicamente al equipo humano de la organización para actuar frente al incidente de seguridad.
- Crear o contar con un equipo de respuesta ante incidentes de seguridad

En la siguiente gráfica[9] se resumen los pasos para responder a un incidente de seguridad:

[9] Ilustración tomada de la guía de gestión de incidentes de seguridad de 2020 (pág 16).

La labor de gestión de incidentes de seguridad se asigna a: ÁREA DE RECOLECCIÓN - MICHAEL QUINTERO quien debe reportar a la Gerencia de la empresa las actividades realizadas para cumplir oportunamente esta actividad.

OBLIGACIONES FRENTE AL REGISTRO NACIONAL DE BASES DE DATOS (RNBD)

La inscripción en el Registro Nacional de Bases de Datos (RNBD) es obligatoria a las sociedades y entidades sin ánimo de lucro que tengan activos totales superiores a cien mil (100.000) Unidades de Valor Tributario (UVT) y las entidades de naturaleza pública[10].

[10] Cfr. Decreto 90 del 18 de enero de 2018

De conformidad con los numerales 2.1. (literal f) y 2.3. del Capítulo V[11] de la Circular Única de la Superintendencia de Industria y Comercio (SIC), la actualización puede versar sobre los siguientes aspectos y plazos:

TIPO DE ACTUALIZACIÓN	PLAZO
Cambios sustanciales[12] sobre sobre la información registrada en el RNBD	Dentro de los primeros diez (10) días hábiles de cada mes, a partir de la inscripción de la base de datos
Novedades no sustanciales	Anualmente, entre el 2 de enero y el 31 de marzo.
Información sobre reclamos presentados por los Titulares de los Datos[13]	Dentro de los quince (15) primeros días hábiles de los meses de febrero y agosto de cada año, a partir de su inscripción
Reporte de incidentes de seguridad	Dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.
Registro de nuevas bases de datos	La inscripción debe realizarse dentro de los dos (2) meses siguientes a partir de la creación de la nueva base.

Según el Manual del RNBD[14] de la SIC, para poder realizar cualquiera de las anteriores actividades es necesario que la empresa registre cualquiera de estos dos tipos de usuarios ante la plataforma tecnológica del RNBD:

- *"Usuario Administrador: Pueden existir varios usuarios administradores. Este, tiene permisos para registrar bases de datos, registrar novedades y crear usuario (s) Operativo (s) pero no recibe notificaciones del sistema.*

[11] Versión disponible con fecha del 15 de diciembre de 2025 y publicada en: https://www.sic.gov.co/sites/default/files/normatividad/092022/T%C3%ADtulo%20V%20Versi%C3%B3n%2029-09-2022.pdf (Última consulta: 15/XII/2025 a las 11:30 AM)

[12] "Son cambios sustanciales los que se relacionen con la finalidad de la base de datos, el Encargado del Tratamiento, los canales de atención al Titular, la clasificación o tipos de datos personales almacenados en cada base de datos, las medidas de seguridad de la información implementadas, la Política de Tratamiento de la Información y la transferencia y transmisión internacional de datos personales". (Numeral 2.3. del Capítulo V de la Circular Única de la SIC.

[13] "*Corresponde a la información de los reclamos presentados por los Titulares ante el Responsable y/o el Encargado del tratamiento, según sea el caso, dentro de un semestre calendario (enero – junio y julio – diciembre). Esta información se reportará teniendo en cuenta lo manifestado por los Titulares y los tipos de reclamos prestablecidos en el RNBD. El reporte deberá ser el resultado de consolidar los reclamos presentados por los Titulares ante los Responsables del Tratamiento que se encuentran obligados a registrar sus bases de datos en el RNBD y sus respectivos Encargados del Tratamiento*" (Numeral 2.1. -Lit f, num i- del Capítulo V de la Circular Única de la SIC.

[14] https://www.sic.gov.co/registro-nacional-de-bases-de-datos

- *"Usuario Operativo: Su función es incluir la información de las bases de datos en el Registro, no podrá crear otros usuarios, finalizar el registro de las bases de datos, registrar novedades de eliminación de base de datos o incidentes, ni recibirá ningún tipo de notificación."*

La labor de registro y actualización de la información en el RNBD se asigna a: OFICIAL DE CUMPLIMIENTO Y DE PROTECCIÓN DE DATOS PERSONALES DR HERNAN DARIO ACEVEDO , quien debe reportar a la Gerencia de la empresa las actividades realizadas para cumplir oportunamente estas actividades.

MONITOREO, CONTROL Y SUPERVISIÓN DEL CUMPLIMIENTO DEL MANUAL Y LAS MEDIDAS ADOPTADAS EN EL MISMO.

El monitoreo, control o supervisión del cumplimiento del presente manual interno es fundamental para la empresa porque no solo ayuda a que todo el equipo siga los mismos procedimientos y directrices para que el trabajo se realice de manera uniforme y consistente, sino que nos permite cumplir con la regulación, evitando incurrir en riesgos reputacionales, de confianza y legales que pueden generar pérdidas a la sociedad y eventuales sanciones.
Mediante labores de monitoreo, podemos identificar áreas de mejora y ajustar procedimientos para ser más eficientes y competitivos.

La labor de monitoreo y control del cumplimiento de este manual y de las políticas sobre tratamiento de datos se asigna a: OFICIAL DE CUMPLIMIENTO Y DE PROTECCIÓN DE DATOS PERSONALES DR HERNAN DARIO ACEVEDO CON EL APOYO DEL ÁREA DE CALIDAD., quien debe reportar a la Gerencia de la empresa las actividades realizadas para cumplir oportunamente estas actividades.

ENTRENAMIENTO Y SENSIBILIZACIÓN AL EQUIPO SOBRE TRATAMIENTO DE DATOS PERSONALES.

La empresa realizará anualmente actividades de entrenamiento y sensibilización sobre el tratamiento de datos personales para consolidar una cultura de debido tratamiento de datos personales con miras a que todos los miembros del equipo comprendan la importancia de proteger la información y las reglas que se deben observar sobre el particular. Estos entrenamientos ayudarán a aumentar la conciencia sobre las normativas legales y éticas relacionadas con el tratamiento de datos.

La labor de entrenamiento y sensibilización sobre tratamiento de datos se asigna a: AL ÁREA DE FORMACIÓN Y AL OFICIAL DE CUMPLIMIENTO Y DE PROTECCIÓN DE DATOS PERSONALES DR HERNAN DARIO ACEVEDO., quien debe reportar a la Gerencia de la empresa las actividades realizadas para cumplir oportunamente estas actividades.

OTROS DOCUMENTOS QUE HACEN PARTE DE ESTE MANUAL

Los siguientes documentos hacen parte del presente manual:

- Política de tratamiento de datos personales
- Política de seguridad de información y datos personales.
- Formato de autorización del titular de la información

FECHA DE ENTRADA EN VIGENCIA DEL PRESENTE MANUAL

Este manual fue aprobado luego de la expedición de la ley 1581 de 2012 y del decreto 1377 de 2013. Posteriormente fue modificada para incorporar algunos aspectos que establecen los decretos 886 de 2014, 1074 de 2015 y la Circular Externa 002 de 2015 de la Superintendencia de Industria y Comercio.

DATOS DE CONTACTO:

Nombre o razón social: RISKS INTERNATIONAL S.A.S
NIT: 900352786-5
Domicilio o dirección de correspondencia: CALLE 25B 39 A - 30 - Empresa en Trabajo Remoto
Correo electrónico: habeasdata@risksint.com
Teléfono: 6017941834

A N E X O S

ANEXO 1. GLOSARIO

- Autorización: Consentimiento previo, expreso e informado del titular del dato para llevar a cabo el tratamiento.

- Cliente: 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 cliente 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.

- Consulta: solicitud del titular del dato o las personas autorizadas por éste o por la ley, para conocer la información que reposa sobre ella en bases de datos o archivos.

- Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

  Estos datos se clasifican en sensibles, públicos, privados y semiprivados.

  - Dato personal sensible: Información que afecta la intimidad de la persona o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos (huellas dactilares, entre otros)

  - Dato personal público: Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados. Son públicos, entre otros, los datos contenidos en documentos públicos, registros públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva, los relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Son públicos los datos personales existentes en el registro mercantil de las Cámaras de Comercio (Artículo 26 del C.Co).

Estos datos pueden ser obtenidos y ofrecidos sin reserva alguna y sin importar si hacen alusión a información general, privada o personal.

- Dato personal privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para la persona titular del dato. Ejemplos: libros de los comerciantes, documentos privados, información extraída a partir de la inspección del domicilio.

- 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 e incumplimiento de las obligaciones financieras o los datos relativos a las relaciones con las entidades de la seguridad social.

- Encargado del tratamiento: persona que realiza el tratamiento de datos por cuenta del responsable del tratamiento.

- Incidente de seguridad: Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos.

- Proveedor: Organización o persona que proporciona un producto o servicio.

- Reclamo: solicitud del titular del dato o las personas autorizadas por éste o por la ley para corregir, actualizar o suprimir sus datos personales.

- Responsable del tratamiento: persona que decide sobre, entre otras, la recolección y fines del tratamiento. Puede ser, a título de ejemplo, la empresa dueña de la bases de datos o sistema de información que contiene datos personales.

- **Riesgos Lavado de Activos y Financiación del Terrorismo (LAFT):** son las posibles pérdidas que una empresa enfrenta al ser utilizada para fines ilícitos, como multas, sanciones, fraude, corrupción y daño reputacional, siendo los siguientes riesgos**:**
  1. **Riesgo de Contagio:** Es la posibilidad de pérdida que una empresa puede sufrir, directa o indirectamente, por una acción o experiencia de una contraparte con la que mantiene relaciones contractuales, comerciales o reputacionales.
  2. **Riesgo Legal:** Es la posibilidad de pérdida en que incurre una empresa al ser sancionada, multada u obligada a indemnizar por el incumplimiento de normas, contratos o disposiciones legales. Este riesgo puede surgir por negligencia, mala fe o desconocimiento normativo.
  3. **Riesgo Operativo:** Es la posibilidad de incurrir en pérdidas por deficiencias en los procesos, recursos humanos, tecnología, infraestructura o eventos externos. Incluye el riesgo legal y reputacional asociado.

4. **Riesgo Reputacional:** Es la posibilidad de pérdida debido al desprestigio, mala imagen o publicidad negativa (cierta o no), que afecte la percepción pública de la empresa, reduciendo su capacidad de generar ingresos o confianza.
5. **Riesgo Inherente**: Corresponde al nivel de riesgo propio de una actividad sin considerar la existencia de controles. Representa el riesgo bruto antes de aplicar medidas preventivas o mitigantes.
6. **Riesgo Residual:** Es el nivel de riesgo que permanece luego de aplicar controles efectivos. Este riesgo representa la exposición real de la empresa tras haber gestionado el riesgo inherente.

- SIRIEST, es una herramienta tecnológica que funciona en una base de algoritmos automatizados que atraen información de carácter público, de diferentes fuentes públicas para la mitigación del riesgo asociado a LAFT, C/ST entre los cuales encontramos las principales fuentes a nivel nacional, como lo son policía, procuraduría, contraloría, consulta de procesos ante la rama judicial entre otras y a nivel internacional las primeras fuentes de los más buscados de EEUU, Interpol, entre otras que ayudan a realizar una validación en línea o Due Diligence o debida diligencia para cumplir con normas como el SARLAFT - SIPLAFT - SAGRILAFT.

- SISCOM, es un sistema de información compartida, el cual es alimentado por información de las compañías de transporte y sus Oficiales de Cumplimiento que obtienen el servicio, sobre personas y vehículos en el ejercicio de la actividad, en esta base de datos de información compartida se encuentran datos de personas naturales quienes son los titulares de la información, entre los cuales se encuentran datos personales relacionados con la prestación del oficio de transporte como la profesión u oficio de los conductores y aquellos que pertenecen a la cadena logística del sector transporte, también datos sobre novedades o reportes relacionados con conductas consideradas riesgos o señales de alerta asociados al Lavado de Activos, la Financiación del Terrorismo y la financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM)
- LAFT, Lavado de activos y Financiación del Terrorismo.

- Titular del dato: Es la persona natural a que se refieren los datos.

- Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales como, entre otros, la recolección, el almacenamiento, el uso, la circulación o supresión de esa clase de información.

- Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro (transmisión nacional) o fuera de Colombia (transmisión internacional) y que tiene por objeto la realización de un tratamiento por el Encargado por cuenta del Responsable.

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

ANEXO 2. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES.

El tratamiento de datos personales debe realizarse respetando las normas generales y especiales sobre la materia y para actividades permitidas por la ley. En el desarrollo, interpretación y aplicación de la presente política, se aplicarán de manera armónica e integral los siguientes principios:

Principios relacionados con la recolección de datos personales.

- Principio de libertad: Salvo norma legal en contrario, la recolección de los datos sólo puede ejercerse con la autorización previa, expresa e informada del titular. Los datos personales no podrán ser obtenidos o divulgados sin el previo consentimiento del titular, o en ausencia de mandato legal o judicial que releve el consentimiento.

  Se deberá informar al titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y por tanto, no podrá recopilarse datos sin la especificación sobre la finalidad de los mismos.

  El principio de libertad debe observarse tanto para el caso de los datos que se recolectan a través de formatos como los que hacen parte de los anexos o documentos que entregan los titulares de los datos a RISKS INTERNATIONAL S.A.S
  No se podrán utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de datos personales.
- Principio de limitación de la recolección: Sólo deben recolectarse los datos personales que sean estrictamente necesarios para el cumplimiento de las finalidades del tratamiento, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo del tratamiento. En consecuencia, debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario. Es decir, los datos deberán ser: (i) adecuados, (ii) pertinentes y (iii) acordes con las finalidades para las cuales fueron previstos.

Principios relacionados con el uso de datos personales.

- Principio de finalidad: El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al titular. Se deberá comunicar al titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y, por tanto, no podrán recopilarse datos sin una finalidad específica.

Los datos deben ser tratados de acuerdo a los usos autorizados. Si, con el tiempo, el uso de los datos personales cambia a formas que la persona, no espera, es necesario obtener nuevamente el consentimiento previo del titular.

- Principio de temporalidad: Los datos personales se conservarán únicamente por el tiempo razonable y necesario para cumplir la finalidad del tratamiento y las exigencias legales o instrucciones de las autoridades de vigilancia y control u otras autoridades competentes. Los datos serán conservados cuando ello sea necesario para el cumplimiento de una obligación legal o contractual. Para determinar el término del tratamiento se considerarán las normas aplicables a cada finalidad y los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

  Una vez cumplida la (las) finalidad(es) se procederá a la supresión de los datos
- Principio de no discriminación: Queda prohibido realizar cualquier acto de discriminación por las informaciones recaudadas en las bases de datos o archivos.

- Principio de reparación: Es obligación indemnizar los perjuicios causados por las posibles fallas en el tratamiento de datos personales.

Principios relacionados con la calidad de la información.

- 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. Se deberán adoptar medidas razonables para asegurar que los datos sean precisos y suficientes y, cuando así lo solicite el Titular o cuando RISKS INTERNATIONAL S.A.S lo determine, sean actualizados, rectificados o suprimidos cuando sea procedente.

Principios relacionados con la protección, el acceso y circulación de datos personales

- Principio de seguridad: Cada persona vinculada con RISKS INTERNATIONAL S.A.S deberá cumplir las medidas técnicas, humanas y administrativas que establezca la empresa para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Adicionalmente, deberá cumplir la política de seguridad de información y datos personales de RISKS INTERNATIONAL S.A.S.

- Principio de transparencia: en el tratamiento debe garantizarse el derecho del titular a obtener en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

- Principio de acceso restringido: Sólo se permitirá acceso a los datos personales a las siguientes personas:

  - Al titular del dato
  - A las personas debidamente autorizadas por el titular del dato
  - A las personas que por mandato legal u orden judicial sean autorizadas para conocer la información del titular del dato.
  - A las demás personas legitimadas según lo indica el artículo 20 del decreto 1377 de 2013.

  En todos los casos, antes de dar acceso a los datos se debe establecer con certeza y suficiencia la identidad de la persona que solicita conocer los datos personales.

  Los datos personales, salvo la información pública, no podrán estar disponibles en internet u 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 y a la presente política.

- Principio de circulación restringida: Sólo se puede enviar o suministrar los datos personales a las siguientes personas:

  - Al titular del dato
  - A las personas debidamente autorizadas por el titular del dato
  - A las demás personas legitimadas según lo indica el artículo 20 del decreto 1377 de 2013.
  - A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial

  En este último caso, de conformidad con la Corte Constitucional, se procederá de la siguiente manera:

  En primer lugar, la entidad pública o administrativa debe justificar su solicitud indicando el vínculo entre la necesidad de obtener el dato y el cumplimiento de sus funciones constitucionales o legales.

  En segundo lugar, con la entrega de la información se le informará a la entidad pública o administrativa que debe cumplir los deberes y obligaciones que le impone la ley 1581 de 2012 y sus normas reglamentarias como Responsable del tratamiento. La entidad administrativa receptora de los datos personales debe cumplir con las obligaciones de protección y las garantías que se derivan de la citada ley, en especial la observancia de los principios de finalidad, uso legítimo, circulación restringida, confidencialidad y seguridad.

- 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 ello corresponda al desarrollo de las actividades autorizadas en la ley.

ANEXO 3. DERECHOS DE LOS TITULARES DE LOS DATOS.

Las personas obligadas a cumplir estas políticas deben respetar y garantizar los siguientes derechos de los titulares de los datos:

- Conocer, actualizar y rectificar los datos personales. Para el efecto, es necesario establecer previamente la identificación de la persona para evitar que terceros no autorizados accedan a los datos del titular del dato.

- Obtener copia de la autorización.

- Informar sobre el uso que RISKS INTERNATIONAL S.A.S ha dado o está dando a los datos personales del titular.

- Dar trámite a las consultas y reclamos siguiendo las pautas establecidas en la ley y en la presente política.

- Acceder a la solicitud de revocatoria de la autorización y/o supresión del dato personal cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento por parte de RISKS INTERNATIONAL S.A.S se ha incurrido en conductas contrarias a la ley 1581 de 2012 o a la Constitución.

  El Titular también podrá revocar la autorización y solicitar la supresión del dato, cuando no exista un deber legal o contractual que le imponga su permanencia en la base de datos o archivo del Responsable o Encargado.

  La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos del Responsable o Encargado.

- Acceder en forma gratuita a sus datos personales. La información solicitada por el Titular podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos.

Los derechos de los Titulares, de conformidad con el artículo 20 del decreto 1377 de 2013, podrán ejercerse por las siguientes personas:

a. Por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición RISKS INTERNATIONAL S.A.S
b. Por sus causahabientes, quienes deberán acreditar tal calidad.
c. Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.

d. Por estipulación a favor de otro o para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

ANEXO 4. DEBERES DE RISKS INTERNATIONAL S.A.S CUANDO OBRA COMO RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES.

Todos los obligados a cumplir esta política deben tener presente que RISKS INTERNATIONAL S.A.S está obligado a cumplir deberes impuestos por la ley colombiana. Por ende, deben obrar de tal forma que cumplan las siguientes obligaciones:

Deberes de RISKS INTERNATIONAL S.A.S respecto del titular del dato.

- Solicitar y conservar, en las condiciones previstas en esta política, copia de la respectiva autorización otorgada por el titular.
- Informar de manera clara y suficiente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data, es decir, conocer, actualizar o rectificar sus datos personales.
- Informar a solicitud del titular sobre el uso dado a sus datos personales.
- Tramitar las consultas y reclamos formulados en los términos señalados en la presente política.

Deberes de RISKS INTERNATIONAL S.A.S respecto de la calidad, seguridad y confidencialidad de los datos personales

- Observar los principios de veracidad, calidad, seguridad y confidencialidad en los términos establecidos en esta política.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Actualizar la información cuando sea necesario.
- Rectificar los datos personales cuando ello sea procedente.

Deberes de RISKS INTERNATIONAL S.A.S cuando realiza el tratamiento a través de un encargado.

- Suministrar al encargado del tratamiento únicamente los datos personales cuyo tratamiento esté previamente autorizado. Cuando se trate de transmisiones nacionales

e internacionales se deberá suscribir un contrato de transmisión de datos personales o pactar cláusulas contractuales que contengan lo dispuesto en el artículo 25 del decreto 1377 de 2013.

- Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

- Comunicar de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.

- Informar de manera oportuna al encargado del tratamiento, las rectificaciones realizadas sobre los datos personales para que éste proceda a realizar los ajustes pertinentes.

- Exigir al encargado del tratamiento, en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

- Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

Deberes de RISKS INTERNATIONAL S.A.S respecto de la Superintendencia de Industria y Comercio

- Informarle las eventuales violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

ANEXO 5. DEBERES DE RISKS INTERNATIONAL S.A.S CUANDO OBRA COMO ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES.

Si RISKS INTERNATIONAL S.A.S realiza el tratamiento de datos en nombre de otra entidad u organización (Responsable del Tratamiento) deberá cumplir los siguientes deberes:

- Establecer que el Responsable del tratamiento está autorizado para tratar los datos que suministra a RISKS INTERNATIONAL S.A.S .
- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Realizar oportunamente la actualización, rectificación o supresión de los datos.
- Actualizar la información reportada por los responsables del tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
- Tramitar las consultas y los reclamos formulados por los titulares en los términos señalados en la presente política.
- Registrar en la base de datos la leyenda “reclamo en trámite” en la forma en que se establece en la presente política.
- Insertar en la base de datos la leyenda “información en discusión judicial”, una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
- Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- Permitir el acceso a la información únicamente a las personas autorizadas por el titular o facultadas por la ley para dicho efecto.
- Informar a la 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. De conformidad con la Circular Externa 002 de 2015 de la Superintendencia de Industria y Comercio, los incidentes de seguridad deberán reportarse al RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

ANEXO 6. SOBRE LA CONSULTA Y DIRECCIONAMIENTO DE INFORMACIÓN PÚBLICA.

RISKS INTERNATIONAL SAS, atendiendo lo dispuesto en la ley 1581 de 2012, comprende que la información que redirecciona como intermediario facilitador, puede ser consultable en las fuentes de información pública y permite su acceso consulta y direccionamiento conforme a los parámetros de cada entidad pública quien a su vez cumple los principios de transparencia y acceso a la información en los términos de la Ley 1712 de 2014.

Información pública, conforme lo dispuesto en el artículo 6 de Ley 1712 de 2014, se define:

Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

El numeral 2 del artículo 3 del Decreto 1377 de 2013, dispone:

"(…) 2. Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.(…)"

Los datos públicos pueden encontrarse en páginas de acceso público, y es responsabilidad de las entidades estatales realizar las correcciones, actualizaciones o eliminaciones correspondientes, de acuerdo con los principios de la Constitución y la Ley. La Ley 1712 de 2014 establece que toda información de interés público producida por entidades estatales debe ser oportuna, objetiva, veraz, completa y accesible.

El artículo 2 literal b de la ley 1581 de 2012, dispone:

"El régimen de protección de datos personales que se establece en la presente ley no será de aplicación: (…)

b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo; (…)"

Los datos personales de naturaleza pública no requieren autorización para su tratamiento, de conformidad a lo establecido en el artículo 10 de la Ley 1581 de 2012:

(…) Artículo 10. Casos en que no es necesaria la autorización. *La autorización del Titular no será necesaria cuando se trate de: (…)*

b) Datos de naturaleza pública (…)

RISKS ITERNATIONAL SAS y todo aquel que consulta información en fuentes públicas nacionales o internacionales, lo hace bajo calidad de usuario de la informacion pública, de tal forma, que atendiendo los parámetros de consulta de cada entidad, se consulta la misma y direcciona a efectos de que los clientes puedan efectuar la *consulta en listas* como parte de la aplicación de medidas de prevención de riesgos de ***Lavado de Activos***, la Financiación del ***Terrorismo*** y la Financiación de la ***Proliferación*** de Armas de Destrucción Masiva (LA/FT/FPADM) y demás conexos.

RISKS INTERNATIONAL SAS, atendiendo el principio de responsabilidad demostrada, requiere a sus clientes la consecución previa de la autorización por parte del titular, aunque no sea obligatorio para este tipo de información, en cumplimiento del principio accountability y de conformidad a los procedimientos ya explicados en el presente manual.