



POLITICA

TRATAMIENTO DE DATOS PERSONALES

PO-04

Ultima revisión:

2023-03-31

Versión: 02

Pág. 1 de 33

Política de Tratamiento de Datos Personales – Derecho Habeas Data

REDES Y SISTEMAS INTEGRADOS SAS, REDSIS.A.S.



Capítulo I

Políticas y Seguridad de Procedimientos

1. Base legal y ámbito de aplicación.

El derecho a la Protección de los Datos tiene como finalidad permitir a todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en archivos o bases de datos. Este derecho constitucional se recoge en los artículos 15 y 20 de la Constitución Política; en la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la ley de Protección de Datos Personales (LEPD); en el decreto 1074 de 2015, y capítulo 25 sección 3 Artículo 2.2.2.25.3.2 del decreto 1074 de 2015, por el cual se reglamenta parcialmente la 1581 de 2012.

Cuando el Titular de los datos presta su consentimiento para que estos formen parte de una base de datos de una institución, pública o privada, jurídica o natural, ésta se hace mediante el responsable del tratamiento de estos datos y adquiere una serie de obligaciones como son: la de tratar dichos datos con seguridad y cautela, velar por su integridad y aparecer como órgano a quien el Titular puede dirigirse para el seguimiento de la información y el control de la misma, pudiendo ejercitar los derechos de consultas y reclamos.

Si bien, la responsabilidad del tratamiento de los datos recae en el responsable del tratamiento, sus competencias se materializan en las funciones que corresponden a su personal de servicio. El personal de la institución responsable del tratamiento con acceso, directo o indirecto a las bases de datos que contienen los datos personales debe conocer la normativa de protección de datos, la política de protección de datos de la organización; y deben cumplir con las obligaciones en materia de seguridad de los datos correspondientes a sus funciones y cargo.



Para velar con el cumplimiento de sus obligaciones de seguridad, la sociedad **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, nombra como Oficial de Cumplimiento a la Oficina de Asuntos Legales y como responsables de seguridad a la Oficina de IT, quienes serán los encargados de desarrollar, coordinar, controlar y verificar el cumplimiento de las medidas de seguridad recogidas en este manual.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento y se encuentra dirigida a todos los usuarios de datos, que son tanto el personal propio como al personal externo de la sociedad **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**

Todos los usuarios identificados en el presente Manual, están obligados a cumplir con las medidas de seguridad establecidas para el tratamiento de los datos y están sujetos al deber de confidencialidad, incluso después de acabada su relación laboral o profesional con la organización responsable del tratamiento. El deber de confidencialidad, recogido en el artículo 4 literal h) de la ley de Protección de Datos (LEPD), se formaliza a través de la firma de un acuerdo de confidencialidad suscrito entre el usuario y el responsable del tratamiento.

Tipo de Norma	Número y fecha de expedición	Título	Expedida por	Aplicación específica
Ley Estatutaria	1581 de 2012	<i>“Por la cual se dictan disposiciones generales para la protección de datos personales”.</i>	Congreso de la Republica.	Por medio de la cual desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.
Ley	1273 de 2009	<i>Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la</i>	Congreso de la Republica.	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan



		<i>protección de la información de los datos"</i>		integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Decreto	1377 de 2013	<i>"Por medio del cual se reglamenta parcialmente la ley 1581 de 2012"</i>	Presidente de la República de Colombia.	Mediante la cual se reglamenta parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto	1074 de 2015	<i>"Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo."</i>	Presidente de la República de Colombia.	El Ministerio de Comercio, Industria y Turismo tiene como objetivo primordial dentro del marco de su competencia: formular, adoptar, dirigir y coordinar las políticas generales en materia de desarrollo económico y social del país, relacionadas con la competitividad, integración y desarrollo de los sectores productivos de la industria

2. Definiciones establecidas en el artículo 3 de la LEPD y el capítulo 25 sección 1 artículo 2.2.2.25.1.3 del Decreto 1074 de 2015.

- ✓ **Acceso autorizado:** Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autenticación correcta, generalmente mediante el ingreso de usuario y contraseña.
- ✓ **Autenticación:** Procedimiento de verificación de la identidad de un usuario.
- ✓ **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
- ✓ **Aviso de privacidad:** Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.
- ✓ **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.



- ✓ **Bases de Datos Automatizada:** Se entenderá como aquella cuyo tratamiento se realiza mediante dispositivos de cómputo o digitales, para todos los efectos del presente documento.
- ✓ **Bases de Datos no Automatizada:** Se entiende como aquella cuyo tratamiento se realiza en físico por medio de cualquier sistema, para todos los efectos de este manual.
- ✓ **Contraseña:** Señal secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autenticación de usuarios que permite el acceso autorizado.
- ✓ **Control de acceso:** Mecanismo que permite acceder a dispositivos, información o bases de datos mediante la autenticación.
- ✓ **Copia de respaldo:** Copia de los datos de una base de datos en un soporte que permita su recuperación.
- ✓ **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- ✓ **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.
- ✓ **Datos sensibles:** Se entiende por datos sensible aquellos que afectan la intimidad del Titular 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.



- ✓ **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.
- ✓ **Identificación:** Proceso de reconocimiento de la identidad de los usuarios.
- ✓ **Incidencia:** Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos o de los datos personales que contienen.
- ✓ **Niveles de Seguridad:** Se definen para todos los efectos de este manual como los niveles de protección que tienen implementada el responsable del tratamiento sobre los datos personales que administra y trata, y que se clasifican en básico, medio y alto, dependiendo del sistema de tratamiento y de la clase de datos personales que involucre en ese procedimiento.
- ✓ **Perfil de usuario:** Grupo de usuarios a los que se da acceso.
- ✓ **Recurso protegido:** Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.
- ✓ **Responsable de seguridad:** Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad.
- ✓ **Sistema de Etiquetado:** Sistema empleado por la Superintendencia de Industria y Comercio, con el fin de identificar las bases de datos sobre las cuales tengan conocimiento de algún tipo de irregularidad o se detecte algún tipo de inconsistencia con las medidas implementadas para la seguridad de los datos personales que almacenan.
- ✓ **Sistema de información:** Conjunto de bases de datos, programas, soportes y/o equipos empleados para el tratamiento de datos personales.
- ✓ **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.



- ✓ **Soporte:** Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, etc.
- ✓ **Usuario:** Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.
- ✓ **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.
- ✓ **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- ✓ **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.
- ✓ **Transmisión:** Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

3. Principios de la protección de datos.

El artículo 4 de la Ley de Protección de Datos (LEPD), establece unos principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

- ✓ **Principio de legalidad:** El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la Ley de Protección de Datos (LEPD), el Decreto 1074 de 2015 y en las demás disposiciones que la desarrollen.
- ✓ **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.



✓ **Principio de libertad:** El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento. El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad, salvo en los siguientes casos que exceptúa el artículo 10 de la Ley de Protección de Datos (LEPD):

- 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.

✓ **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.

✓ **Principio de transparencia:** En el tratamiento debe garantizarse el derecho del Titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

- El tratamiento al cual será sometidos sus datos y la finalidad del mismo.



- El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.
 - Los derechos que le asisten como Titular.
 - La identificación, dirección física, el correo electrónico y el teléfono del responsable del tratamiento.
- ✓ **Principio de acceso y circulación restringida:** El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la Ley de Protección de Datos (LEPD) y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.
- ✓ **Principio de seguridad:** La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento todo personal que tenga acceso, directo o indirecto, a los datos. Los usuarios que accedan a los sistemas de información del responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Estas normas y medidas de seguridad se recogen en el presente documento, de obligado cumplimiento para todo usuario y personal de la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.** Cualquier modificación de las normas y medidas en materia de seguridad de datos personales por parte del responsable del tratamiento ha de ser puesta en conocimiento de los usuarios.



- ✓ **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 solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPD y en los términos de esta.

4. Categorías especiales de datos.

4.1. Datos sensibles.

Los datos sensibles son aquellos que afectan la intimidad del Titular 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 partidopolítico 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.

Según el artículo 6 de la Ley Estatutaria de Protección de datos Personales (LEPD), se prohíbe el tratamiento de datos sensibles, excepto cuando:

- ✓ El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- ✓ El tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- ✓ El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos



no se podrán suministrar a terceros sin la autorización del Titular.

- ✓ El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- ✓ El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

4.2. Derechos de los niños, niñas y adolescentes

El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes requisitos:

- ✓ Que responda y respete el interés superior de los niños, niñas y adolescentes.
- ✓ Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor a su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, cumpliendo en todo

	POLITICA	PO-04 Última revisión: 2023-03-31 Versión: 02 Pág. 12 de 33
	TRATAMIENTO DE DATOS PERSONALES	

momento con los principios y obligaciones recogidos en la LEPD y el Decreto 1074 de 2015. En todo caso, el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre los datos de los niños, niñas adolescentes se ejercerán por las personas que estén facultadas para representarlos.

4.3 Derechos de los Titulares.

De acuerdo con el artículo 8 de la LEPD y al capítulo 25 sección 4 del decreto 1074 de 2015, los Titulares de los datos pueden ejercer una serie de derechos en relación con el tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas.

- ✓ Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- ✓ Por sus causahabientes, quienes deberán acreditar tal calidad.
- ✓ Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
- ✓ Por estipulación a favor de otro y para otro.

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

Los derechos del Titular son los siguientes:

- **Derecho de acceso o consulta:** Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que les han dado a sus datos personales.
- **Derechos de quejas y reclamos.** La Ley distingue cuatro tipos de reclamos:



- **Reclamo de corrección:** el derecho del Titular a que se actualicen, rectifique o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- **Reclamo de supresión:** el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
- **Reclamo de revocación:** el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
- **Reclamo de infracción:** el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.
- **Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento:** salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la LEPD.
- **Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones:** el Titular o causahabiente solo podrá elevar esta queja una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

5. Autorización de la política de tratamiento.

De acuerdo con el artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte de la sociedad **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, en los términos y condiciones recogidos en la misma.

	POLITICA	PO-04 Ultima revisión: 2023-03-31 Versión: 02 Pág. 14 de 33
	TRATAMIENTO DE DATOS PERSONALES	

No será necesaria la autorización del Titular 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.

6. Responsable del tratamiento.

El responsable del tratamiento de las bases de datos objeto de esta política es la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, cuyos datos de contacto son:

Dirección: Calle 1b #30-61

Correo electrónico: protecciondedatospersonales@redsis.com

Teléfono: 605 3133630

6.1. Las obligaciones del responsable del tratamiento.

Las obligaciones en materia de seguridad de los datos de la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.** son las siguientes:

- ✓ Coordinar e implantar las medidas de seguridad recogidas en el presente documento.
- ✓ Difundir el referido documento entre el personal afectado.
- ✓ Mantener este Manual actualizado y revisado siempre que se produzcan cambios relevantes en el sistema de información, el sistema de tratamiento, la organización de la institución, el contenido de la información de las bases de datos, o como

	POLITICA	PO-04 Última revisión: 2023-03-31 Versión: 02 Pág. 15 de 33
	TRATAMIENTO DE DATOS PERSONALES	

consecuencia de los controles periódicos realizados. De igual modo, se revisará su contenido cuando se produzca algún cambio que pueda afectar al cumplimiento de las medidas de seguridad.

- ✓ Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos.
- ✓ Cuidar que el acceso mediante sistemas y aplicaciones informáticas se lleve a cabo mediante acceso identificado y contraseña.
- ✓ Autorizar, salvo delegación expresa a usuarios autorizados e identificados en este Manual, la salida de soportes fuera de los establecimientos donde se encuentran las bases de datos; las entradas y salidas de información por red, mediante dispositivos de almacenamiento electrónico o en papel y el uso de módems y las descargas de datos.
- ✓ Verificar por lo menos semestralmente la correcta aplicación del procedimiento de copias de respaldo y recuperación de datos.
- ✓ Garantizar la existencia de una lista de usuarios autorizados y perfiles de usuario.
- ✓ Analizar, junto con el responsable de seguridad correspondiente, las incidencias registradas para establecer las medidas correctoras oportunas cada que se presenten las mismas, y determinar la necesidad de proponer la implementación de nuevas medidas preventivas dentro de la auditoría anual.
- ✓ Realizar una auditoría, interna o externa, para verificar el cumplimiento de las medidas de seguridad en materia de protección de datos, al menos cada año.

7. Tratamiento y finalidades de las bases de datos

La empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, en el desarrollo de sus actividades, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.



De acuerdo con lo establecido en la Ley 1581 de 2012 y de conformidad con las autorizaciones impartidas por los titulares de la información, la sociedad **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.** realizará operaciones o conjunto de operaciones que incluyen recolección de datos, su almacenamiento, uso, circulación y/o supresión, entrega de los datos a terceras entidades a título de encargados o de responsables; esto de acuerdo con el acuerdo al que entre las partes se llegue. Este Tratamiento de datos se realizará exclusivamente para las finalidades autorizadas y previstas en la presente Política y en las autorizaciones específicas otorgadas por parte del titular. De la misma forma se realizará Tratamiento de Datos Personales cuando exista una obligación legal o contractual para ello, siempre bajo los lineamientos de las políticas de Seguridad de la Información de la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, en todos los casos los datos personales podrán ser tratados con la finalidad de adelantar los procesos de control y auditorías internas y externas y evaluaciones que realicen los organismos de control. Asimismo y en ejecución del objeto social de la sociedad **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, los datos personales serán tratados de acuerdo con el grupo de interés y en proporción a la finalidad o finalidades que tenga cada tratamiento, como se describe a continuación:

La siguiente tabla presenta las distintas bases de datos y las finalidades asignadas a cada una de ellas:

Tabla I. Bases de datos y finalidades

Nombre	Finalidad
Empleados	Los datos serán utilizados con las siguientes finalidades: Solicitud de datos concernientes a identificación personal, información de contacto, datos de carácter académico, datos del historial laboral, profesional y financiero; desarrollar adecuadamente el proceso de registro y vinculación laboral; implementar acciones de bienestar laboral; difundir ofertas laborales para participar en procesos internos de selección de personal en la Institución; comunicar información institucional; realizar los procesos de debida diligencia, consulta en listas restrictivas nacionales e internacionales, validaciones, reportes y demás análisis en



POLITICA

TRATAMIENTO DE DATOS PERSONALES

PO-04

Ultima revisión:

2023-03-31

Versión: 02

Pág. 17 de 33

	<p>cumplimiento del SAGRILAF y Programa de Transparencia y Ética Empresarial – PTEE de Redsis para prevenir los riesgos de LA/FT/FPADM y C/ST; ejecutar actividades con fines estadísticos; desarrollar adecuadamente el proceso de actualización de los datos; desarrollar los procesos de inscripción en congresos; eventos o seminarios organizados por la Institución; adelantar la actualización de datos y verificación de identidad de los trabajadores y sus familiares (pareja, padres hijos); Suministro de información a las empresas con la cuales se tiene convenio, al fondo de empleados, confección de artículos de dotación, envío de información a través de mensajes de texto y correos electrónicos, entrega y asignación de equipos a los colaboradores; redacción de informes de gestión humana; proceso de afiliación sistema de seguridad social y cajas de compensación del colaborador y sus beneficiarios; entrega de referencias laborales, uso de imágenes fotográficas y videos con fines corporativos, obtención y suministro de datos de los hijos de los colaboradores en el desarrollo de actividades recreativas y de bienestar a través de la Instituciones o entidades aliadas, evaluaciones de desempeño; generación de certificaciones laborales, de ascenso, traslado, entrevista de retiro, en procesos de auditoría y control interno y externo, en la entrega de reportes obligatorios institucionales en entrevistas de retiro, desactivación de sistemas de información, uso de huellas digitales y demás datos de salud y/o datos sensibles para los fines misionales; las anteriores finalidades son enunciativas y no taxativas.</p>
Proveedores	<p>Los datos serán utilizados con las siguientes finalidades: Solicitud de ofertas y propuestas económicas para la adquisición de productos y servicios; para el análisis y viabilidad de cada producto y/o servicio; envío de comunicaciones a través de mensajes de texto y correos electrónico; presentación de informes pertinentes a los diferentes entes de control; revisión y verificación de referencias comerciales; gestiones pre contractuales y contractuales; suministro de información en procesos de auditoría interna y externa que se realicen al interior de la institución; envío de información de los productos, servicios o novedades de la fundación; realizar los procesos de debida diligencia, de consulta en listas restrictivas nacionales e internacionales, validaciones, reportes y demás análisis en cumplimiento del SAGRILAF – Sistema de Autocontrol y Gestión Integral del Riesgo de Lavado de Activos y Financiación del Terrorismo y el programa de transparencia y ética empresarial - PTEE de Redsis para prevenir los riesgos de LA/FT/FPADM y C/ST; las anteriores finalidades son enunciativas y no taxativas.</p>
Clientes	<p>Los datos serán utilizados con las siguientes finalidades: Realizar los procesos de debida diligencia, de consulta en listas restrictivas nacionales e internacionales, validaciones, reportes y demás análisis en cumplimiento del SAGRILAF – Sistema de Autocontrol y Gestión Integral del Riesgo de Lavado de Activos y Financiación del Terrorismo y el programa de transparencia y ética empresarial - PTEE de Redsis para prevenir los riesgos de LA/FT/FPADM y C/ST; en la transmisión de los datos a las entidades que regulan el negocio en temas tributarios y aduaneros; gestionar trámites como solicitudes, quejas y/o reclamos, reportes a centrales de riesgo por incumplimiento de las obligaciones financieras derivadas</p>



POLITICA

TRATAMIENTO DE DATOS PERSONALES

PO-04

Ultima revisión:

2023-03-31

Versión: 02

Pág. 18 de 33


	<p>de la relación comercial, envío de comunicaciones a través de mensajes de texto y correos electrónico; para llevar un historial de consumo, efectuar las gestiones pertinentes para el desarrollo de la etapa de preventa, venta y posventa, respecto de los productos ofrecidos por la empresa REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S., que haya o no adquirido respecto de cualquier relación de negocios subyacente que tenga con ella, uso de imágenes fotográficas y videos con fines corporativos, Gestión comercial, Conocer la información del comportamiento de los clientes institucionales y de e-commerce y sus canales de contacto para realizar ofrecimientos ajustados a sus necesidades; envío de información de los productos, servicios o novedades de la compañía, Conservar registros históricos de la compañía y mantener contacto comercial; Se realizará el envío de la información otorgada y autorizada por el titular las entidades con las cuales se tienen convenios, estas transferencias estarán siempre mediadas por un documento que garantice que el tratamiento que se le dará a sus datos será el mandado por la normatividad vigente. Las anteriores finalidades son enunciativas y no taxativas.</p>
Visitantes	<p>Los datos serán utilizados con las siguientes finalidades: Identificar los datos personales del visitante que ingresa a las instalaciones de la empresa, Autorizar la entrada a las diferentes áreas o dependencias, envío de información en mensajes de texto y correos electrónico con motivos promocionales y/o informativos; Se realizará el envío de la información otorgada y autorizada por el titular las entidades con las cuales se tienen convenios, estas transferencias estarán siempre mediadas por un documento que garantice que el tratamiento que se le dará a sus datos será el mandado por la normatividad vigente. Las anteriores finalidades son enunciativas y no taxativas.</p>
Eventos	<p>Los datos serán utilizados con las siguientes finalidades: Para hacer seguimiento a las actividades y realizar acciones de mercadeo, llevar registros de asistencia, efectuar las inscripciones a los capacitaciones virtuales que realicen, enviar información promocional sobre los eventos programados, vía correo electrónico, mensaje de texto, entre otros, efectuar encuestas de satisfacción, realizar videos e imágenes fotográficas con fines corporativos; ejecutar actividades con fines estadísticos; desarrollar adecuadamente el proceso de actualización de los datos, enviar invitaciones y constancias de asistencia a los mismos, en caso de que sean solicitados; las anteriores finalidades son enunciativas y no taxativas.</p>
Visitantes Página Web	<p>Los datos serán utilizados con las siguientes finalidades: Identificar los datos personales de los visitantes de la página web, el envío de información por correo electrónico con motivos promocionales y/o informativos, así como el envío de las cotizaciones sobre nuestros productos y servicios; y de la información requerida por los visitantes. Las anteriores finalidades son enunciativas y no taxativas.</p>
Video y Vigilancia	<p>Los datos serán utilizados con las siguientes finalidades: monitoreo y control para la vigilancia de entrada, salida y tráfico de personas dentro de la compañía, así como para el control de ingreso y salida de vehículos de los parqueaderos; monitoreo de incidentes, medida</p>



	de disuasión de conductas irregulares de terceros, monitoreo y control de la prestación de los servicios institucionales; Se realizará el envío de la información otorgada y autorizada por el titular las entidades con las cuales se tienen convenios, estas transferencias estarán siempre mediadas por un documento que garantice que el tratamiento que se le dará a sus datos será el mandado por la normatividad vigente. Las anteriores finalidades son enunciativas y no taxativas.
Aspirantes	Los datos serán utilizados para las siguientes finalidades: Almacenar la información general de los candidatos que repose en sus hojas de vida, los soportes laborales y académicos que la acrediten, citar a los aspirantes en proceso de selección a las entrevistas programadas, realización de visitas domiciliarias, verificación de referencias laborales, personales, experiencia laboral y trayectoria profesional con el fin de participar en los procesos de selección que se inicien para llenar un vacante, enviarles comunicaciones físicas o por medio de mensajes de datos para notificarles la apertura de esas convocatorias, citarlos para que presenten las pruebas técnicas de actitud o de conocimiento, enviarles los resultados de las mismas, cuando las características del proceso de selección así lo requieran y realizar los futuros procesos de contratación laboral; realizar consultas ante los operadores de la información crediticia como data crédito o cualquier otra entidad que administre esta clase de información según los procedimientos de contratación establecidos por Redsis; realizar los procesos de debida diligencia, de consulta en listas restrictivas nacionales e internacionales, validaciones, reportes y demás análisis en cumplimiento del SAGRILAFT – Sistema de Autocontrol y Gestión Integral del Riesgo de Lavado de Activos y Financiación del Terrorismo y el programa de transparencia y ética empresarial PTEE de Redsis para prevenirlos riesgos de LA/FT/FPADM y C/ST Las anteriores finalidades no son taxativas, sólo enunciativas.
Empleados Retirados	Los datos serán utilizados para las siguientes finalidades: 1. Servir de base para la expedición de los certificados laborales, previstos en el Artículo 57 numeral 7 del Código Sustantivo del Trabajo, a solicitud de los empleados retirados o sus causahabientes; 2. Con el fin de tener respaldo para absolver las solicitudes o requerimientos que se formulen en materia de pensiones; y 3. Para otorgar las referencias laborales a los potenciales empleadores del ex empleado cuando éste así lo autorice. Las anteriores finalidades son enunciativas y no taxativas.

7.1 Atención a los Titulares de datos

El Oficial de Cumplimiento será el encargado de la atención de peticiones, consultas y reclamos ante la cual el titular de los datos puede ejercer sus derechos, en el siguiente Correo electrónico: protecciondedatospersonales@redsis.com.

	POLITICA	PO-04 Última revisión: 2023-03-31 Versión: 02 Pág. 20 de 33
	TRATAMIENTO DE DATOS PERSONALES	

8. Procedimientos para ejercer los derechos del Titular.

8.1. Derecho de acceso o consulta.

Según el capítulo 25 sección 4 del decreto 1074 de 2015, el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

1. Al menos una vez cada mes calendario.
2. Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, solamente podrá cobrar al Titular gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, enviado al correo electrónico protecciondedatospersonales@redsis.com, indicando en el asunto “ejercicio del derecho de acceso o consulta” la solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Petición en que se concreta la solicitud de acceso o consulta.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada, cuando corresponda.

	POLITICA	PO-04 Última revisión: 2023-03-31 Versión: 02 Pág. 21 de 33
	TRATAMIENTO DE DATOS PERSONALES	

El Titular podrá elegir una de las siguientes formas de consulta de la base de datos para recibirla información solicitada:

- Visualización en pantalla.
- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Correo u otros medios electrónicos.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**


Una vez recibida la solicitud, la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atenderla consulta dentro de dicho término, se informará al interesado, expresando los motivos de lademora 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. Estos plazos están fijados en el artículo 14 de la LEPD.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

8.2. Derechos de quejas y reclamos.

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.** enviado, mediante un correo electrónico a la dirección electrónica protecciondedatospersonales@redsis.com indicando en el asunto “ejercicio del derecho queja o reclamo”, la solicitud deberá contener los siguientes datos:

- ✚ Nombre y apellidos del Titular.

	POLITICA	PO-04 Última revisión: 2023-03-31 Versión: 02 Pág. 22 de 33
	TRATAMIENTO DE DATOS PERSONALES	

- + Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- + Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o inflación.
- + Dirección para notificaciones, fecha y firma del solicitante.
- + Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

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

La empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, resolverá la petición de consulta en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender al reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá el reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Una vez agotado el trámite de reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

9. Medidas de seguridad

La empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha



implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso noautorizado o fraudulento.

Por otra parte, la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

A continuación, se exponen las medidas de seguridad implantadas por la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, que están recogidas y desarrolladas en este documento (Tablas II, III, IV y V).

Tabla II. Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) y bases de datos (automatizadas, no automatizadas)

Auditoria	Auditoría ordinaria (interna o externa) cada año. Eventuales Auditorías extraordinaria por modificaciones sustanciales en los sistemas de información. Informe de detección de deficiencias y propuesta de correcciones. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento. Conservación del Informe a disposición de la autoridad.
Gestión de documentos y soportes	Medidas tales como, destructora de papel que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos. Acceso restringido al lugar donde se almacenan los datos. Sistema de etiquetado o identificación del tipo de información. Inventario de los soportes en los que se almacenan bases de datos. Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico.
Control de acceso	Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones, de acuerdo con el rol que desempeña. Lista actualizada de usuarios y accesos autorizados. Autorización escrita del titular de la información para la entrega de sus datos a terceras personas, para evitar el acceso a datos con derechos distintos de los autorizados. Concesión, alteración o anulación de permisos por el personal autorizado.



Incidencias	Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras. Procedimiento de notificación y gestión de incidencias.
Personal	Definición de las funciones y obligaciones de los usuarios con acceso a los datos. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de estas.
Políticas y Procedimientos	Elaboración e implementación del Manual de obligatorio cumplimiento para el personal. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, procedimiento de copias y recuperación de datos, medidas de seguridad para el transporte, destrucción y reutilización de documentos, identificación de los encargados del tratamiento.

Tabla III. Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) según el tipo de bases de datos

Bases de datos no automatizadas			Bases de datos automatizadas	
Archivo	Almacenamiento de documentos	Custodia de documentos	Identificación y autenticación	Telecomunicaciones
1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y ejercicio de los derechos de los Titulares.	1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.	1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de estos.	1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización. 2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.	1. Acceso a datos mediante redes seguras.



Tabla IV. Medidas de seguridad para datos privados según el tipo de bases de datos

Bases de datos automatizadas y no automatizadas		
Auditoría	Responsable de seguridad	Políticas y Procedimientos Habeas Data
<p>Auditoría ordinaria (interna o externa) cada año.</p> <p>eventuales Auditorías extraordinaria por modificaciones sustanciales en los sistemas de información.</p> <p>Informe de detección de deficiencias y propuesta de correcciones.</p> <p>Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.</p> <p>Conservación del Informe a disposición de la autoridad.</p>	<p>Designación de uno o varios responsables de seguridad.</p> <p>Designación de uno o varios encargados del control y la coordinación de las medidas del Manual políticas y procedimientos.</p> <p>Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.</p>	<p>Controles al menos una vez al año de cumplimiento, consistente en la auditoria anual, así como la capacitación al personal mínimo una vez al año.</p>

Bases de datos automatizadas			
Gestión de documentos y soportes	Control de acceso	Identificación y autenticación	Incidencias
<p>Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, formade envío, responsable de la recepción o entrega.</p>	<p>Control de acceso al lugar o lugares donde se ubican los sistemas de información.</p>	<p>Mecanismo que limite el número de intentos reiterados de acceso no autorizados.</p>	<p>Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente.</p> <p>Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.</p>

Tabla V. Medidas de seguridad para datos sensibles según el tipo de bases de datos

Bases de datos no automatizadas			
Control de acceso	Almacenamiento de documentos	Copia o reproducción	Traslado de documentación
<p>Acceso solo para personal autorizado.</p>	<p>Archivadores, armarios u otros ubicados en áreas de acceso protegidas con</p>	<p>Solo por usuarios autorizados.</p> <p>Dstrucción que impida el acceso o recuperación de los datos.</p>	<p>Medidas que impidan el acceso o manipulación de documentos.</p>



POLITICA

TRATAMIENTO DE DATOS PERSONALES

PO-04

Ultima revisión:

2023-03-31

Versión: 02

Pág. 26 de 33

Mecanismo de identificación de acceso. Registro de accesos de usuarios no autorizados.	de llaves u otras medidas.		
-------------------------------------------------------------------------------------------	----------------------------	--	--

Bases de datos automatizadas		
Gestión de documentos y soportes	Control de acceso	Telecomunicaciones
Sistema de etiquetado confidencial. Cifrado de datos. Cifrado de dispositivos portátiles cuando sean retirados.	Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede. Control del registro de accesos por el responsable de seguridad. Informe mensual. Conservación de los datos: por el periodo que las leyes impongan.	Transmisión de datos mediante redes electrónicas cifradas.

9.1. Responsables de seguridad

Los encargados de seguridad tienen las siguientes funciones:

- Coordinar y controlar la implantación de las medidas de seguridad, y colaborar con el responsable del tratamiento en la difusión del manual de Políticas y Procedimientos Habeas Data.
- Coordinar y controlar los mecanismos que permiten acceder a la información contenida en las bases de datos y elaborar un informe periódico sobre dicho control.
- Gestionar los permisos de acceso a los datos por parte de los usuarios autorizados identificados en este manual.
- Habilitar el registro de incidencias a todos los usuarios para que comuniquen y registren las incidencias relacionadas con la seguridad de los datos; así como acordar con el responsable del tratamiento las medidas correctoras y registrarlas.



- Comprobar periódicamente, la validez y vigencia de la lista de usuarios autorizados, la existencia y validez de las copias de seguridad para la recuperación de los datos, la actualización en este manual y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.
- Definir los tiempos dentro de los cuales se realizarán las auditorias, los cuales NO podrán ser superiores a un año.
- Recibir y analizar el informe de auditoría para elevar sus conclusiones y proponer medidas correctoras al responsable del tratamiento.
- Gestionar y controlar los registros de entradas y salidas de documentos o soportes que contengan datos personales.

9.2. Usuarios

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

La sociedad **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, cumple con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación sobre bases de datos y sistemas de información, y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.** se definen, con carácter general, según el tipo de actividad que desarrollan de acuerdo con sus funciones dentro de la institución y, específicamente, por el contenido de este Manual. La lista de usuarios y perfiles con acceso a los recursos protegidos están recogidos en este documento.

	POLITICA	PO-04 Última revisión: 2023-03-31 Versión: 02 Pág. 28 de 33
	TRATAMIENTO DE DATOS PERSONALES	

Con carácter general, cuando un usuario trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en este manual de Políticas y Procedimientos Habeas Data por parte del personal al servicio de la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, es sancionable de acuerdo con la normativa aplicable a la relación jurídica existente entre el usuario y la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.** son las siguientes:

- **Deber de secreto:** Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios de la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.** no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de los mismos.
- **Funciones de control y autorizaciones delegadas:** El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos.
- **Obligaciones relacionadas con las medidas de seguridad implantadas:**
 - ✓ Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.



- ✓ No revelar información a terceras personas ni a usuarios no autorizados.
 - ✓ Observar las normas de seguridad y trabajar para mejorarlas.
 - ✓ No realizar acciones que supongan un peligro para la seguridad de la información.
 - ✓ No sacar información de las instalaciones de la organización sin la debida autorización.
-
- **Uso de recursos y materiales de trabajo:** Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, personas que no hagan parte de la planta de personal de la empresa, requieran la salida de dispositivos periféricos o extraíbles, se deberán comunicarse al responsable de seguridad correspondiente que podrá autorizarla y, en su caso, registrarla.
 - **Uso de impresoras, escáneres y otros dispositivos de copia:** Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos.
 - **Obligación de notificar incidencias:** Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento al responsable de seguridad que corresponda, quien se encargará de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.



- **Deber de custodia de los soportes utilizados:** Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.
- **Responsabilidad sobre los terminales de trabajo y portátiles:** Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción
- **Uso limitado de Internet y del correo electrónico:** El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades.
- **Salv guarda y protección de contraseñas:** Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.
- **Copias de respaldo y recuperación de datos:** Debe realizarse copia de seguridad de toda la información de bases de datos personales de la institución.



- **Deber de archivo y gestión de documentos y soportes:** Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad recogidas en este manual.

10. Transferencia de datos a terceros países.

De acuerdo con el Título VIII de la LEPD, se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia en la de acuerdo con la circular 005 de 10 de agosto de 2017, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:

- ✓ Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- ✓ Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.
- ✓ Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- ✓ Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- ✓ Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.

	POLITICA	PO-04 Última revisión: 2023-03-31 Versión: 02 Pág. 32 de 33
	TRATAMIENTO DE DATOS PERSONALES	

- ✓ Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. El Superintendente está facultado para requerir información y adelantar las diligencias tendentes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Las transmisiones internacionales de datos personales que se efectúen entre un responsable y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales.

11. Vigencia

Las bases de datos responsabilidad de la empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad para la cual son recabados los datos. Una vez cumplida la finalidad o finalidades del tratamiento, y sin perjuicio de normas legales que dispongan lo contrario. La empresa **REDES Y SISTEMAS INTEGRADOS SAS, REDSIS S.A.S.**, procederá a la supresión de los datos personales en su posesión salvo que exista una obligación legal o contractual que requiera su conservación. Por todo ello, el presente documento entra en vigencia el día 31/03/2023.



POLITICA

TRATAMIENTO DE DATOS PERSONALES

PO-04

Ultima revisión:

2023-03-31

Versión: 02

Pág. 33 de 33

TABLA DE CONTROL DE CAMBIOS

VER	DESCRIPCION DE LA ACTUALIZACION	FECHA DE VIGENCIA	REVISADO POR	APROBADO POR
1	✓ Documento inicial	2020-10-15	Jefe de Asuntos Legales	Gerente General
2	✓ Cambio total del documento	2023-03-31	Director de Asuntos Legales	Presidente