

Resolución N°

"Por la cual se actualiza la Política de Protección de Datos Personales de la Superintendencia de Vigilancia y Seguridad Privada"

EL SUPERINTENDENTE DE VIGILANCIA Y SEGURIDAD PRIVADA

En ejercicio de sus facultades constitucionales y legales, especialmente las conferidas por el Decreto Ley 356 de 1994, la Ley 1437 de 2011, la Ley 1581 de 2012, y demás normas concordantes,

CONSIDERANDO:

Que la **Ley 1266 de 2008** por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y proveniente de terceros países y se dictan otras disposiciones.

Que la **Ley 1581 de 2012** desarrolla las disposiciones generales para la protección de datos personales, estableciendo los principios y obligaciones que deben seguirse en el tratamiento de datos personales para garantizar su confidencialidad, integridad y disponibilidad.

Que la **Ley 1273 de 2009** tipifica penalmente las conductas contra la confidencialidad, integridad y disponibilidad de la información, estableciendo la protección de los datos como un bien jurídico tutelado.

Que la **Ley 1712 de 2014**, conocida como la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, regula el acceso a la información pública y establece los procedimientos y garantías para asegurar la transparencia en la administración pública, incluyendo la protección de la información y los datos personales.

Que el **Decreto 1078 de 2015** expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, que incorpora normativas sobre la gestión de la seguridad de la información

Página 1 de 3

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURÍDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

Resolución N°

y establece los derechos generales para los titulares de datos personales como el derecho de conocer, actualizar y rectificar sus datos.

Que la Superintendencia de Vigilancia y Seguridad Privada adopto la Política de Protección de Datos personales a través de la Resolución 201737000588837 del 10 de agosto de 2017, y la actualizó mediante la Resolución 20191400084337 08 de septiembre de 2019.

Que la Superintendencia se alinea a la Resolución 7870 de 2022 del Ministerio de Defensa Nacional, Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos de las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa.

Que la Superintendencia de Vigilancia y Seguridad Privada ha adoptado la Norma Técnica Colombiana NTC-ISO/IEC 27001 como base para la implementación, mantenimiento y mejora continua de su Sistema de Gestión de Seguridad de la Información (SGSI), alineándose con los estándares internacionales y con el Modelo de Seguridad y Privacidad de la Información del Gobierno Digital (MinTIC).

En mérito de lo expuesto,

RESUELVE

ARTÍCULO PRIMERO: Actualizar la Política Institucional de Protección de Datos Personales, para los directivos, funcionarios, contratistas y terceros que tengan relación con la SuperVigilancia, de conformidad a lo enunciado en la parte considerativa del presente acto administrativo.

ARTÍCULO SEGUNDO: La presente Resolución rige a partir de la fecha de su publicación y complementa lo establecido en las Resoluciones No. 201737000588837 del 10 de agosto de 2017 por la cual se adoptó La “Política de Protección de Datos Personales” y la Resolución No.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURÍDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

Resolución N°

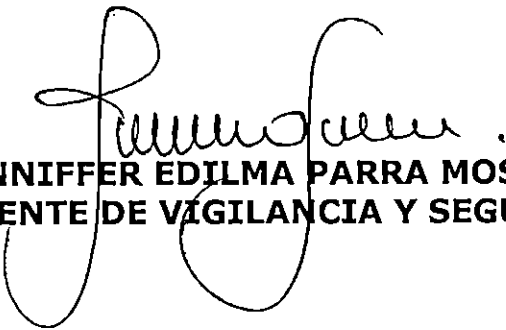
20191400084337 08 de septiembre de 2019 por medio de la cual se actualizó la “Política de Protección de Datos Personales de la Superintendencia de Vigilancia y Seguridad Privada”.

ARTÍCULO TERCERO: Designar a la Oficina de Sistemas de la Superintendencia de Vigilancia y Seguridad Privada como la encargada de liderar la implementación, monitoreo, actualización continua, difusión y socialización de la Política de Protección de Datos Personales.

ARTÍCULO CUARTO: Derogar cualquier resolución, acto administrativo o disposición que sea incompatible con lo dispuesto en la presente Resolución. Política de Protección de Datos Personales

ARTÍCULO QUINTO: La presente Resolución entrará en vigor a partir de la fecha de su publicación. La Oficina de Comunicaciones será responsable de su divulgación y de garantizar que sea incluida en el plan institucional de capacitación e inducción.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE



YENNIFFER EDILMA PARRA MOSCOSO
SUPERINTENDENTE DE VIGILANCIA Y SEGURIDAD PRIVADA

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACION
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		



Supervigilancia

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

POLITICA DE PROTECCIÓN
DE DATOS PERSONALES

2025

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

TABLA DE CONTENIDO

1.

INTRODUCCIÓN

4

2.

OBJETIVOS GENERALES

4

3.

ALCANCE

4

4.

DESTINATARIOS

4

5.

MARCO NORMATIVO

4

5.1.

Constitución Política de Colombia

4

5.2.

Leyes

4

5.3.

Decretos

5

5.4.

Resoluciones

6

6.

PRINCIPIOS RECTORES

6

7.

CLASIFICACION DE DATOS PERSONALES

8

8.

DEFINICIONES

9

9.

RESPONSABLE Y RESPONSABILIDAD DEL TRATAMIENTO

12

9.1.

Responsable del Tratamiento de Datos Personales

12

9.2.

Control de Acceso y Protección de la Información

12

9.3.

Responsabilidad del tratamiento de Datos Personales

12

10.

FINALIDAD Y TRATAMIENTO DEL DATO PERSONAL - DERECHOS Y DEBERES

13

10.1.

Finalidad y Tratamiento de los datos Personales

13

10.2.

Derechos de los Titulares

15

10.3.

Deberes de la SVSP como Responsable del Tratamiento de Datos

16

10.4.

Datos personales de los Niños, Niñas y Adolescentes

18

11.

PROCEDIMIENTOS

18

11.1.

Autorización del Titular

18

11.1.1.

Como Obtener la Autorización

18

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

11.2. Casos en que NO se Requiere la Autorización 19

11.3. El Ejercicio del Derecho de Habeas Data 19

11.3.1. Derecho de Acceso a los Datos..... 19

11.3.2. Procedimiento para Peticiones, Consultas, Quejas y Reclamos de los Titulares de Datos Personales. 20

11.3.3. Reclamos..... 20

11.4. Grupo Responsable de la Atención de las Peticiones, Quejas, Reclamos, Denuncias y Sugerencias 21

11.5. Mecanismos Para Conocer la Política de Tratamiento 21

11.6. Contenidos de las Bases de Datos de la SVSP 21

12. VIGENCIA DE LAS BASES DE DATOS 22

13. VIGENCIA DOCUMENTO 22

14. ANEXOS..... 23

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

1. INTRODUCCIÓN

La Superintendencia de Vigilancia y Seguridad Privada, como entidad responsable de la inspección, vigilancia y control del sector de la seguridad privada en Colombia, desarrolla la Política de Tratamiento y Protección de Datos Personales, alineada con su misión, visión y objetivos estratégicos, así como con lo establecido en la Constitución Política en su artículo 15 y el marco normativo y técnico definido por las autoridades competentes en la materia.

Así mismo, en cumplimiento de lo dispuesto en la Constitución Política de Colombia, la Ley 1266 de 2008, la Ley 1581 de 2012, la Ley 1712 de 2014, y sus decretos reglamentarios, incluyendo el Decreto 1377 de 2013 y el Decreto 886 de 2014, compilados en el Decreto 1074 de 2015, se establece el presente marco normativo para garantizar un adecuado tratamiento de los datos personales.

2. OBJETIVOS GENERALES

Establecer los lineamientos para el tratamiento, manejo, protección y actualización de la información sensible y los datos personales de los ciudadanos, vigilados, servidores públicos y demás que son registrados en las bases de datos de la Superintendencia de Vigilancia y Seguridad Privada, obtenidos en cumplimiento a la misionalidad y de conformidad a lo establecido por la normatividad legal vigente.

3. ALCANCE

La política de tratamiento y protección de datos personales contenida en este documento aplica a todas las bases de datos que contengan datos personales; y que sean objeto de tratamiento por parte de la Superintendencia de Vigilancia y Seguridad Privada, considerado como responsable del tratamiento de esta información al secretario general o a quien este designe.

4. DESTINATARIOS

La presente política está dirigida a la ciudadanía en general, terceros que acceden a la información en virtud de una relación contractual o legal con la Superintendencia de Vigilancia y Seguridad Privada, así como cualquier otro actor que realice tratamiento de datos personales bajo su responsabilidad. Esta política es de obligatorio cumplimiento para los funcionarios y contratistas de la Superintendencia de Vigilancia y Seguridad Privada.

5. MARCO NORMATIVO

5.1. Constitución Política de Colombia

5.2. Leyes

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango - Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano - Oficina Jurídica	GESTIÓN JURÍDICA
Revisó y Aprobó	Sol Marina Cure Flórez - jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

Ley Estatutaria 1266 de 2008, "Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

Ley 1273 de 2009, "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 integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Ley 1437 de 2011 "Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo".

Ley 1448 de 2011, "Por la cual se dictan medidas de atención, asistencia y reparación integral a las víctimas del conflicto armado interno y se dictan otras disposiciones".

Ley Estatutaria 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales".

Ley 1712 de 2014, "Por medio de la cual se crea la Ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones".

Ley 1755 de 2015, "Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo".

5.3. Decretos

Decreto 356 de 1994, "Por el cual se expide el Estatuto de Vigilancia y Seguridad Privada".

Decreto 2187 de 2001, "por el cual se reglamenta el Estatuto de Vigilancia y Seguridad Privada contenido en el Decreto -ley 356 del 11 de febrero de 1994".

Decreto 1727 de 2009, Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información".

Decreto 1377 de 2013, "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".

Decreto 857 de 2014, "Por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013", Por medio de la cual se expiden normas para fortalecer el marco

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones.

Decreto 886 de 2014, "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos".

Decreto 103 de 2015, "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".

Decreto Único Reglamentario 1074 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo" (Capítulo 25: reglamenta parcialmente la Ley 1581 de 2012 y, Capítulo 26: reglamenta la información mínima que debe contener el Registro Nacional de Bases de Datos).

Decreto 1083 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública".

Decreto 1759 de 2016, "Por el cual se modifica el Artículo 2.2.2.26.3.1 del Decreto 1074 de 2015".

Decreto único Reglamentario del Sector Comercio, Industria y Turismo (Modifica el Plazo de Inscripción de las bases de datos en el Registro Nacional de Bases de Datos).

Decreto 1499 de 2017, "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015".

Decreto 090 de 2018, "Por el cual se modifican los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo (Modifica el ámbito de aplicación y el plazo de inscripción en el Registro Nacional de Bases de Datos)".

5.4. Resoluciones

Resolución 0644 de 2025 "Por la cual se adopta la Política Sectorial de Interoperabilidad para el Sector Defensa".

6. PRINCIPIOS RECTORES

Para el desarrollo y aplicación del tratamiento de datos personales registrados en las bases de datos y archivos se observarán los principios rectores establecidos en el artículo 4º de la Ley 1581 de 2012 y la Ley 1712 de 2014, los cuales serán objeto de aplicación de criterios de armonización.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información 	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica 	GESTIÓN JURÍDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas 	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		



Supervigilancia

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

Principio de legalidad. El tratamiento debe sujetarse a lo establecido en la ley 1581 de 2012 y demás disposiciones normativas que se 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 sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular en los casos que establezca la Ley. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Principio de veracidad o calidad. La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. No se debe dar tratamiento de datos parciales, incompletos, fraccionados o que induzcan al 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. Los sujetos obligados están en el deber de proporcionar y facilitar el acceso a la información en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales o legales.

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 y la Constitución. En este sentido, el tratamiento sólo 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 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.

Principio de seguridad. La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento 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.

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 y en los términos de la misma.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		



Supervigilancia

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

Principio de Interpretación Integral de los Derechos Constitucionales. La protección de datos personales debe interpretarse en armonía con el derecho a la información (artículo 20 de la Constitución), garantizando un equilibrio entre la privacidad y el acceso a la información pública. Este principio asegura que el tratamiento de datos personales no implica restricciones injustificadas a otros derechos fundamentales y que su aplicación se realiza de manera proporcional y garantizada.

Principio de Necesidad. La recolección y tratamiento de datos personales deben limitarse únicamente a la información estrictamente indispensable para cumplir con las finalidades establecidas. Este principio previene la recopilación excesiva o desproporcionada de datos, asegurando que la Superintendencia solo almacena información que sea realmente útil y relevante.

7. CLASIFICACION DE DATOS PERSONALES

Dato personal: O información personal, corresponde a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Art. 3. Ley 1581 de 2012). Para efectos de la presente Política se entiende como la información suministrada por el usuario para su registro, lo cual incluye nombre, identificación, edad, género, dirección, correo electrónico y teléfono, entre otros.

Dato privado: Es el dato que, por su naturaleza íntima o reservada, sólo es relevante para el titular. (Art 3. Ley 1266 de 2008)

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. (Art 3. Decreto 1377 de 2013 compilado por el Decreto 1074 de 2015).

Dato semiprivado: Es 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 dato financiero, y crediticio de actividad comercial o de servicios a que se refiere el título IV de la Ley 1266. (Art 3. Ley 1266 de 2008).

Datos sensibles: Se entiende por datos sensibles 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

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información <i>MAA</i>	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica <i>JS</i>	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas <i>SMCF</i>	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		



Supervigilancia

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Art 3. Decreto 1377 de 2013, compilado por el Decreto 1074 de 2015). Los datos sensibles solo pueden ser tratados con autorización previa, expresa e informada del titular, salvo en los casos en los que la ley lo exima, como en situaciones de interés vital o procesos judiciales. La Supervigilancia, de acuerdo con su política de seguridad de la información, garantiza protocolos de protección de la información para evitar accesos indebidos o usos no autorizados.

8. DEFINICIONES

Para la correcta interpretación y aplicación de la presente Política, para todos los efectos, se adoptarán las siguientes definiciones:

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales. (Art 3. Ley 1581 de 2012)

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. (Art 3. Decreto 1377 de 2013, compilado por el Decreto 1074 de 2015)

Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento (Art 3. Ley 1581 de 2012). Para la aplicación de la presente Política, debe distinguirse dos clases de bases de datos; las automatizadas, es decir, aquellas que se almacenan y administran a través de herramientas informáticas y las bases de datos manuales o archivos, donde la información se encuentra organizada o almacenada en medio físico y contienen información personal, tal como nombre, identificación, números de teléfono, correo electrónico, etc.

Custodio de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. (Aspecto que fuera adaptado de la norma ISO/IEC 27001:2022). Numeral 5 de la Guía para la Gestión y Clasificación de Activos de Información emitida por el Ministerio de las Tecnologías de la Información y las Comunicaciones, "Seguridad y Privacidad de la Información".

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. (Art 3. Ley 1581 de 2012)

Foro: Servicio automatizado de mensajes, a menudo moderado por un propietario, a través del cual los suscriptores reciben mensajes dejados por otros suscriptores

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

por un tema dado. Los mensajes pueden ser enviados, entre otros, por correo electrónico.

Funciones legales: Este aparte hace referencia a las actuaciones administrativas, procesos sancionatorios, relaciones contractuales, laborales, y respuesta a peticiones en general, que se llevan a cabo al interior de la entidad; teniendo en cuenta que, para cumplir la misionalidad de la SVSP se requiere identificar plenamente a los actores involucrados en cada uno de los anteriores. (las normas que los complementen adicionen, modifique o deroguen).

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. (Art 6. Ley 1712 de 2014)

Información Pública: Es toda información que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal. (Art 6. Ley 1712 de 2014)

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en los artículos 6º y 18 de la Ley 1712 de 2014.

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en los artículos 6º y 19 de la Ley 1712 de 2014.

Mandato legal: Cuando la ley indique que se tiene el deber legal de poner en conocimiento de autoridad o funcionario competente un hecho, objeto de sus competencias.

Orden Judicial: Cuando en el marco de un proceso judicial o administrativo, medie orden que indique la obligación de suministrar información, cuyo fin sea la indicada por la constitución y la ley.

PIGDP: Programa Integral de Gestión de Datos Personales. Resultado de un proceso de debida diligencia al interior de la organización que incorpora políticas que respondan a los ciclos internos de gestión de datos y que generen resultados medibles, mediante la aplicación de buenas prácticas de gestión de datos personales. (Guía para la Implementación del Principio de Responsabilidad Demostrada - Accountability, Superintendencia de Industria y Comercio).

Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		



Supervigilancia

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

Información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso, (Aspecto que fuera adaptado de la norma ISO/IEC 27002:2013). Numeral 5 de la Guía para la Gestión y Clasificación de Activos de Información emitida por el Ministerio de las Tecnologías de la Información y las Comunicaciones, "Seguridad y Privacidad de la Información"

Publicar: Hacer que un documento, o una información, determinados sea visible a través del sitio web institucional. (Estrategia de Gobierno en Línea, MinTIC)

Registro Nacional de Bases de Datos (RNB): El RNBD es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país. El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos (Art 25. Ley 1581 de 2012)

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. (Art 3. Ley 1581 de 2012)

Servicios: Son las ayudas en línea que la SVSP provee actualmente, o que piensa proveer en el futuro a los usuarios, por medio de su respectivo sitio web o cualquier otro medio digital, como publicación de noticias o actividades propias de la gestión institucional, trámites en línea, consultas, foros y buzón de quejas y reclamos, entre otros. (Estrategia de Gobierno en Línea, MinTIC)

Sujetos Obligados: Se refiere a cualquier persona natural o jurídica, pública o privada incluida en el artículo 5 de la Ley 1712 de 2014, corregido por el artículo 1 del Decreto Nacional 1494 de 2015.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento. (Art 3. Ley 1581 de 2012)

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. (Art 3. Decreto 1377 de 2013, compilado por el Decreto 1074 de 2015)

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos 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. (Art 3. Decreto 1377 de 2013, compilado por el Decreto 1074 de 2015)

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURÍDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales. Tales como la recolección, almacenamiento, uso, circulación o supresión. (Art 3. Ley 1581 de 2012)

Usuario: El usuario es la persona natural o jurídica que, en los términos y circunstancias previstos en la ley 1266 de 2008, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos. (Art 3. Ley 1266 de 2008).

9. RESPONSABLE Y RESPONSABILIDAD DEL TRATAMIENTO

9.1. Responsable del Tratamiento de Datos Personales

La SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA DE COLOMBIA, en adelante SVSP: Organismo del orden nacional, de carácter técnico, naturaleza pública, adscrito al Ministerio de Defensa Nacional, con personería jurídica, autonomía administrativa y financiera, delega como responsable del tratamiento de esta información al Secretario General de la entidad y/o a quien este designe. Aunque la delegación sea posible, la SVSP seguirá siendo la responsable final ante los titulares y las autoridades.

9.2. Control de Acceso y Protección de la Información

En cumplimiento de la Ley 1581 de 2012 y el Decreto 2355 de 2006, la Superintendencia de Vigilancia y Seguridad Privada (SVSP) adoptará medidas para garantizar la seguridad, confidencialidad y acceso controlado a la información que maneja. Por ello Solo se permitirá el acceso a información relacionada con trámites y registros a aquellas personas que acrediten debidamente su representación mediante los mecanismos establecidos.

Para garantizar el cumplimiento de la normativa en protección de datos y acceso a la información pública, la SVSP implementará medidas que permitan asegurar la correcta clasificación y reserva de la información, protegiendo así los derechos de los titulares.

9.3. Responsabilidad del tratamiento de Datos Personales

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURÍDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

La SVSP es la responsable del tratamiento de los datos personales, datos sensibles suministrados por los ciudadanos, vigilados, usuarios, servidores públicos y demás; hará uso de estos únicamente para las finalidades que se encuentra facultada de acuerdo con los lineamientos definidos para su operación. Para ello la Supervigilancia implementa diferentes controles de seguridad como: Otorgar acceso a los datos sensibles únicamente a personal autorizado, implementación de controles de seguridad como firewall para monitorear y controlar el tráfico de red para bloquear intentos de acceso no autorizado, capacitación y sensibilización en seguridad de la información a los funcionarios y contratistas de la Supervigilancia en temas como identificación de correos sospechosos phishing y gestión segura de contraseñas para reducir significativamente los riesgos.

Los datos de identificación del responsable del tratamiento de datos son:

Administrativo y Centro de Información al Ciudadano:	Calle 24A No. 59-42 Torre 4 Piso 3 Centro Empresarial Sarmiento Angulo
Horario de Atención al Público:	Lunes a viernes de 8:00 a.m. a 5:00 p.m.
Teléfonos:	PBX: 57 1 - 3078038 - FAX: 57 1 - 3274017
Linea Gratuita Nacional:	018000 119703
Correo electrónico:	contactenos@supervigilancia.gov.co
Sitio web	www.supervigilancia.gov.co

10. FINALIDAD Y TRATAMIENTO DEL DATO PERSONAL - DERECHOS Y DEBERES

10.1. Finalidad y Tratamiento de los datos Personales

Los datos personales que la SVSP recolecte, almacene, use, circule y suprima, serán utilizados para alguna de las siguientes finalidades;

En relación con la naturaleza y las funciones propias de SPVS

Registrar, administrar y actualizar la información de empresas y personas naturales sujetas a inspección, vigilancia y control

Llevar a cabo los procesos de selección, contratación y vinculación de servidores públicos y contratistas de la entidad.

Para los fines administrativos propios de La Superintendencia de Vigilancia y Seguridad Privada.

Caracterizar ciudadanos y grupos de interés para adelantar estrategias de mejoramiento en la prestación del servicio.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

- Dar tratamiento y respuesta a las peticiones, quejas, reclamos, denuncias, sugerencias y/o felicitaciones presentadas.
- Conocer y consultar la información del titular del dato que reposen en bases de datos de entidades públicas o privadas.
- Adelantar encuestas de satisfacción de usuarios.
- Envío de información de interés general.
- Recopilar información de ciudadanos asistentes a capacitaciones desarrolladas por la entidad.
- Autorizar y controlar el acceso a las instalaciones de la Superintendencia, garantizando la seguridad de la información y los recursos físicos.
- Realizar encuestas de satisfacción para evaluar la percepción de los usuarios sobre los servicios prestados por la entidad.
- Alimentar y actualizar los sistemas de información internos de la Supervigilancia para garantizar la trazabilidad de sus procesos.
- Implementar y evaluar programas de bienestar laboral, salud ocupacional y planes de emergencia
- Caracterizar a los ciudadanos y grupos de interés con el fin de mejorar la prestación del servicio.
- Recibir, gestionar y dar respuesta a peticiones, quejas, reclamos, denuncias y sugerencias presentadas por la ciudadanía.

En relación con el funcionamiento de la SVSP

• Recurso Humano.

El Tratamiento de los datos se realizará para la vinculación, desempeño de funciones o prestación de servicios, retiro o terminación, dependiendo del tipo de relación jurídica entablada con la SVSP (incluye, entre otros, funcionarios, exfuncionarios, judicantes, practicantes y aspirantes a cargos).

• Proveedores y Contratistas de la SVSP

El Tratamiento de los datos se realizará para los fines relacionados con el desarrollo el proceso de gestión contractual de bienes y/o servicios que la SVSP requiera para su funcionamiento.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

• Seguridad en instalaciones de la SVSP

El registro y tratamiento de datos que realizará el Responsables o Encargados del Tratamiento de datos personales, por medio de cámaras, videocámaras, análogas o digitales, cámaras IP o mini-cámaras, circuitos cerrados de televisión (CCTV) y, en general, cualquier medio por el cual se realice el Tratamiento de imágenes de Titulares de datos personales, en especial con fines de vigilancia, para orientarlos en el cumplimiento de sus deberes en materia de protección de datos personales, y (ii) a los Titulares de la información, para que tengan conocimiento de cómo ejercer sus derechos frente a los primeros.

El fin que cumplen estos sistemas es garantizar la integridad de personas, bienes y espacios objeto de toma de imágenes; la entrega de estas a terceros se hará de conformidad a lo regulado por la Ley; en todo caso se conservarán las imágenes sólo por el tiempo estrictamente necesario para cumplir con la finalidad del sistema y sus capacidades.

10.2. Derechos de los Titulares

- Conocer, actualizar y rectificar sus datos personales frente a la SVSP como responsable y Encargado del Tratamiento. Este derecho se podrá ejercer entre otros ante 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 a la SVSP como responsable y Encargado del Tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012.
- Ser informado por la SVSP como responsable del Tratamiento y Encargado del Tratamiento, previa solicitud, respecto del uso que la ha dado a sus datos personales;
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato personal 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 la Ley 1581 de 2012 y a la Constitución.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURÍDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

Revocar la autorización y/o solicitar la supresión del dato, siempre que no exista un deber legal o contractual que impida eliminarlos.

Abstenerse de responder las preguntas sobre datos sensibles. Tendrá carácter facultativo las respuestas que versen sobre datos sensibles o sobre datos de las niñas y niños y adolescentes.

Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

10.3. Deberes de la SVSP como Responsable del Tratamiento de Datos

Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.

Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

Actualizar la información, comunicando 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 este se mantenga actualizada.

Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente Ley.

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

Tramitar las consultas y reclamos formulados en los términos señalados en la presente Ley.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango - Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano - Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez - Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		



Supervigilancia

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

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.

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.

Informar a solicitud del Titular sobre el uso dado a sus datos.

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.

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

Garantizar que el intercambio de información con otras entidades del sector defensa cumpla con todos los principios aplicables al tratamiento de datos personales.

Implementar protocolos de seguridad digital que prevengan accesos no autorizados a la información personal y reduzcan riesgos de vulneración de datos.

Asegurar que las bases de datos utilizadas en interoperabilidad cumplan con los estándares definidos en la normativa vigente, garantizando la protección de los derechos de los titulares de la información.

Implementar y garantizar mecanismos de control de acceso a la información, permitiendo su consulta únicamente a personas que acrediten debidamente su representación y cumplan con los requisitos establecidos.

Adoptar medidas de seguridad para prevenir accesos no autorizados, uso indebido o filtración de información, asegurando la confidencialidad e integridad de los datos personales.

Reportar de manera inmediata a las autoridades competentes cualquier incidente que afecte la seguridad de la información y adoptar las acciones correctivas necesarias.

Asegurar el cumplimiento de la normativa en protección de datos y acceso a la información pública, aplicando criterios claros para la clasificación y reserva de la información.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango - Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano - Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez - jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

La Supervigilancia debe registrar las bases de datos en el Registro Nacional de Bases de Datos (RNBD), administrado por la Superintendencia de Industria y Comercio (SIC), conforme a lo establecido en el artículo 25 de la Ley 1581 de 2012 Reglamentado por el Decreto 886 del 2014, compilado por el Decreto 1074 del 2015. Registro fundamental para asegurar la supervisión y transparencia en el tratamiento de los datos personales administrados por la Supervigilancia.

10.4. Datos personales de los Niños, Niñas y Adolescentes

Los datos personales de los menores de edad tienen una especial protección y por lo tanto su tratamiento está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7º de la Ley 1581 de 2012 y cuando dicho tratamiento cumpla con los siguientes parámetros y 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 de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. 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.

11. PROCEDIMIENTOS

11.1. Autorización del Titular

Sin perjuicio de las excepciones previstas en la Ley, para el tratamiento de datos se requiere previa autorización expresa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior. (ver anexo 1).

11.1.1. Como Obtener la Autorización

Existen diferentes medios por los cuales los titulares manifiestan la autorización para el tratamiento de sus datos:

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

Por escrito: escrito que debe ser radicado en la sede de la SVSP, en los horarios de atención o por medio del correo electrónico: contactenos@supervigilancia.gov.co

De forma verbal; por medio de una solicitud verbal en las líneas telefónicas, atención personalizada, en los horarios de atención de la SVSP, donde se obtiene una respuesta por el mismo medio.

Mediante conductas inequívocas del titular de la información, las cuales permiten concluir a los responsables que se otorgó la autorización. Lo cual puede ser cuando se tratan imágenes captadas por sistemas de videovigilancia, en los que se debe comunicar previamente a las personas que van a ingresar a un establecimiento que sus imágenes van a ser tomadas, conservadas o usadas de cierta manera y, conociendo tal situación, los titulares ingresan al establecimiento.

Mediante firma: la suscripción de formatos oficiales establecidos para dicho propósito, los cuales evidencien de manera clara e inequívoca el consentimiento del titular.

11.2. Casos en que NO se Requiere la Autorización

- La autorización del Titular no será necesaria cuando se trate de:
 - Información requerida por la SVSP en ejercicio de sus funciones legales, por mandato legal 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.

11.3. El Ejercicio del Derecho de Habeas Data

11.3.1. Derecho de Acceso a los Datos

La SVSP garantiza el derecho de acceso a los datos personales, una vez se haya verificado la identidad del titular y/o representante, poniendo a disposición de éste, los respectivos datos personales; por medio de los canales de comunicación autorizados por la entidad entre ellos; presenciales y/o

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango - Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano - Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez - jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

electrónicos sencillos y con disponibilidad permanente, los cuales permitan el acceso directo del titular a los datos personales.

Las peticiones radicadas por cualquiera de estos medios después de las 5:00 PM, se entenderá radicada del siguiente día hábil, para efectos de contar términos, en atención al horario en que presta servicio la entidad.

11.3.2. Procedimiento para Peticiones, Consultas, Quejas y Reclamos de los Titulares de Datos Personales.

Las solicitudes relacionadas con el tratamiento de datos personales serán atendidas en un plazo máximo de diez (10) días hábiles, contados a partir de la fecha de recepción.

Si no es posible responder dentro de este término, se informará al interesado antes de su vencimiento, indicando los motivos de la demora y la fecha en que se atenderá su solicitud. En todo caso, la respuesta no podrá superar los plazos establecidos en la normatividad vigente.

Cuando la consulta o petición esté relacionada con información de entidades o personas sujetas a inspección, vigilancia y control por parte de la Superintendencia de Vigilancia y Seguridad Privada, y esta no sea la responsable del tratamiento de los datos, se informará de dicha situación al interesado y se remitirá la solicitud a la entidad correspondiente para su trámite.

11.3.3. Reclamos

Los titulares de los datos personales o sus causahabientes que consideren que la información contenida en una base de datos debe ser corregida, actualizada o suprimida, o que adviertan un posible incumplimiento de las normas de protección de datos, podrán presentar un reclamo a través de los canales de comunicación establecidos.

El reclamo deberá contener, al menos, la siguiente información:

- Nombre e identificación del titular.
- Descripción clara y completa de los hechos que motivan el reclamo.
- Dirección física o electrónica para recibir la respuesta y conocer el estado del trámite.
- Documentos y pruebas que el solicitante desee hacer valer.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURÍDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		



POLITICA DE PROTECCIÓN DE DATOS PERSONALES

Si la entidad que recibe el reclamo no es competente para resolverlo, deberá trasladarlo a la autoridad o entidad correspondiente e informar de esta situación al interesado.

Cuando el reclamo se presente de manera incompleta, se requerirá al interesado para que subsane la omisión dentro del plazo establecido. Si el solicitante no proporciona la información solicitada dentro del tiempo estipulado, se entenderá que ha desistido del trámite.

Una vez recibido el reclamo en debida forma, se registrará en la base de datos con una anotación que indique que se encuentra en trámite, la cual se mantendrá hasta su resolución definitiva.

Si no es posible atender el reclamo dentro del término inicialmente previsto, se informará al interesado sobre los motivos de la demora y la fecha estimada de respuesta, asegurando que el plazo adicional no exceda el tiempo razonable establecido en la normativa aplicable.

Para acudir ante la autoridad competente en materia de protección de datos, el titular deberá haber agotado previamente el trámite de consulta o reclamo ante el responsable o encargado del tratamiento.

11.4. Grupo Responsable de la Atención de las Peticiones, Quejas, Reclamos, Denuncias y Sugerencias

La atención y respuesta a las peticiones, quejas, reclamos, denuncias y sugerencias será responsabilidad de las áreas designadas por la entidad, garantizando una gestión eficiente y oportuna. Cada solicitud será tramitada por el equipo competente según la naturaleza del requerimiento, asegurando el cumplimiento de los principios de legalidad, transparencia y protección de datos personales.

11.5. Mecanismos Para Conocer la Política de Tratamiento

El Titular puede acceder a nuestra política de protección de datos personales, la cual se encuentra publicada en el siguiente link:

<https://supervigilancia.gov.co/publicaciones/492/politica-de-privacidad-y-condiciones-de-uso/>

11.6. Contenidos de las Bases de Datos de la SVSP

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano - Oficina Jurídica	GESTIÓN JURÍDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

En las bases de datos de la SVSP se almacena información general como nombre completo número y tipo de identificación, género y datos de contacto (correo electrónico, dirección física, teléfono fijo y móvil). En adición a estos, y dependiendo de la naturaleza de la base de datos, la ENTIDAD puede tener datos específicos requeridos para el tratamiento al que serán sometidos los datos. En las bases de datos se podrá almacenar información sensible con previa autorización de su titular, en cumplimiento de lo establecido en los artículos 5 y 7 de la ley 1581 de 2012.

12. VIGENCIA DE LAS BASES DE DATOS

Las Políticas de Tratamiento de Datos Personales de la ENTIDAD estarán vigentes a partir de la aprobación del presente documento. La ENTIDAD se reserva el derecho a modificarlas, en los términos y con las limitaciones previstas en la ley. Las bases de datos administradas por la ENTIDAD se mantendrán indefinidamente, mientras desarrolle su objeto, y mientras sea necesario para asegurar el cumplimiento de obligaciones de carácter legal, particularmente laboral y contable, pero los datos podrán ser eliminados en cualquier momento a solicitud de su titular, en tanto esta solicitud no contraría una obligación legal de la ENTIDAD o una obligación contenida en un contrato entre la ENTIDAD y Titular.

Las bases de datos en las que se registrarán los datos personales tendrán una vigencia igual al tiempo en que se mantenga y utilice la información para las finalidades descritas en esta política. Una vez se cumpla(n) esa(s) finalidad(es) y siempre que no exista un deber legal o contractual de conservar su información, sus datos serán eliminados de nuestras bases de datos.

13. VIGENCIA DOCUMENTO

La Política de Tratamiento y Protección de Datos Personales entrará en vigor una vez sea aprobada y publicada. Su contenido será revisado, modificado y actualizado conforme a nuevos lineamientos, requerimientos legales o directrices internas o externas que así lo exijan. Este documento constituye una actualización normativa y procedimental de la política previamente publicada.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango - Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano - Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez - jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		



Supervigilancia

POLITICA DE PROTECCIÓN DE DATOS PERSONALES

14. ANEXOS



Supervigilancia

FORMATO AUTORIZACIÓN DE TRATAMIENTO DE DATOS PERSONALES

a. Con el diligenciamiento del presente documento, autorizo de manera expresa, consciente, informada y previa a La Superintendencia de vigilancia y Seguridad Privada a capturar mis datos y a conservarlos bajo su operación, control o supervisión con el fin de utilizarlos para difundir información relativa al objeto social de la misma, promoción comercial de eventos y actividades conexas y para los fines establecidos en la Política de Tratamiento y Privacidad publicada en la página web de dicha compañía. Autorizo a La Superintendencia de vigilancia y Seguridad Privada a transferir y transmitir mis datos a terceros receptores de los mismos.

b. Dedaro que La Superintendencia de vigilancia y Seguridad Privada., me ha informado de los derechos que me asisten como titular de los datos suministrados, de acuerdo con el artículo 8 de la Ley 1581 de 2012, los cuales corresponden a: I. Conocer, actualizar y rectificar los datos personales frente a La Superintendencia de vigilancia y Seguridad Privada II. Solicitar prueba de la autorización otorgada; III. Ser informado por La Superintendencia de vigilancia y Seguridad Privada, previa solicitud, el uso que se le ha dado a los datos; IV. Presentar quejas ante la Superintendencia de Industria y Comercio por infracciones frente a la presente Ley; V. Revocar la autorización y/o solicitar la supresión del dato cuando no se hayan respetado los principios, derechos y garantías constitucionales y legales. Responsable del tratamiento: La Superintendencia de vigilancia y Seguridad Privada., NIT 800217123-2, dirección: Calle 24A No. 59-42 Torre 4 Piso 3 Centro Empresarial Sarmiento Angulo.

c. Autorizó (amos) en forma expresa, permanente e irrevocable a La Superintendencia de vigilancia y Seguridad Privada., o la persona o entidad que éste designe, para obtener de cualquier fuente lícita, o base de datos las informaciones y referencias respectivas a la persona o personas por quien actúo (actuamos) y que represento (representamos) su comportamiento y crédito comercial, hábitos de pago y en general el cumplimiento de sus obligaciones.

Dedaro que la información contenida en el presente formulario ha sido expresada de manera voluntaria y consciente de las regulaciones en cada una de los literales (a, b, c,) de tal manera que me hago responsables de la información allí contenida.

Nombre Legible del solicitante o Representante Legal

Firma del solicitante o Representante Legal No.

Cédula o NIT

Ciudad

Fecha

Superintendencia de Vigilancia y Seguridad Privada
Calle 24A No. 59-42 Torre 4
Piso 3 Centro Empresarial Sarmiento Angulo
Sarmiento Angulo (+601) 307 8038
Línea gratuita 01 8000 119703

Código: FOR-GDO-330-013
Fecha aprobación: 05/06/2024
Versión: 20

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango - Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano - Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez - jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		