POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES EN LA UNIDAD DE INFORMACIÓN Y ANÁLISIS FINANCIERO - UIAF

La Unidad de Información y Análisis Financiero –UIAF-, es una unidad administrativa especial, adscrita al Ministerio de Hacienda y Crédito Público, creada mediante la Ley 526 de 1999, modificada por las leyes 1121 de 2006, 1762 de 2015 y enmarcada en la Ley Estatutaria de Inteligencia 1621 de 2013, cuyas funciones son las de intervenir en la economía del Estado mediante actividades de inteligencia financiera, a fin de detectar y prevenir el lavado de activos, la financiación del terrorismo, el contrabando y el fraude aduanero; y también hace parte de la comunidad de inteligencia del Estado colombiano, mediante actividades de inteligencia y contrainteligencia, según lo estipulado en el artículo 3º de la Ley 1621 de 2013.

1.- Fundamentos Constitucionales del Habeas Data.-

El artículo 15 de la Constitución Política consagra el Habeas Data, el cual se concibe como derecho fundamental y garantía para hacer efectivo el respeto de derechos fundamentales, como el de la intimidad, el buen nombre, el debido proceso, entre otros.

La norma constitucional señala:

> "Artículo 15.- Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y archivos de entidades públicas y privadas.
>
> "En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y las formalidades que establezca la ley.

> "Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad, y demás documentos privados, en los términos que señale la ley".

Por su parte, el artículo 20 de la Constitución dispone:

> "Artículo 20.- Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.
>
> Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura"

El Habeas Data fue desarrollado en las leyes 1266 de 2008, relacionada específicamente con bases de datos de naturaleza financiera, crediticia, comercial y de servicios; y posteriormente mediante Ley 1581 de 2012, se desarrolló una Ley de Habeas Data General, cuyo objeto es desarrollar el derecho constitucional de 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 Carta.

2.- Régimen especial de los organismos de inteligencia del Estado Colombiano. La reserva como excepción.-

Es importante destacar que, teniendo en cuenta la naturaleza de organismo de inteligencia y contrainteligencia del Estado Colombiano que las leyes especiales, y de manera expresa la Ley Estatutaria de los organismos y actividades de Inteligencia 1621 de 2013 le otorgan a la UIAF, ésta, como los demás organismos de inteligencia, tienen unos privilegios en relación con el derecho y garantía constitucional de Habeas Data, consagrado en el artículo 15 de la Constitución. Este puede resumirse bajo el concepto de reserva, garantía esta que cobija no solamente al tratamiento de datos propio de estos organismos, el cual en sentido técnico se refiere al llamado ciclo de inteligencia que consiste en la recolección, tratamiento y difusión de datos, como se analizará en la presente política, como en otros aspectos: reserva de fuentes, agentes, medios y capacidades que tiene o de las cuales hace uso la entidad de inteligencia y contrainteligencia para el desarrollo de su actividad.

3.- Régimen estatutario de Habeas Data.-

El artículo 2º de la Ley 1581 de 2012 establece:

Artículo 2°. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

No obstante, la propia norma señala en el inciso siguiente que el régimen de protección de datos no será de aplicación:

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

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley;

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

c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;

d) A las bases de datos y archivos de información periodística y otros contenidos editoriales;

e) A las bases de datos y archivos regulados por la Ley 1266 de 2008;

f) A las bases de datos y archivos regulados por la Ley 79 de 1993."

Sin embargo, no se trata de una exclusión absoluta, pues como acto seguido dice la norma, los principios de Habeas data contenidos en el artículo 4º de esa norma serán aplicables, siempre y cuando no riñan con los datos reservados.

Señala el parágrafo:

> **"Parágrafo.** Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley **y sin reñir con los datos que tienen características de estar amparados por la reserva legal.** En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley."

También señala el parágrafo el principio de concurrencia, según el cual la normatividad especial que regule bases de datos exceptuadas que contengan principios sobre el tema, se aplicarán de manera concurrente a los de la Ley 1581 de 2012.

4.- Principios Rectores de Habeas Data. Excepción y no exclusión. Aplicación de la norma general y las normas especiales bajo el criterio de ponderación.

TÍTULO II

PRINCIPIOS RECTORES

Artículo 4°. Principios para el Tratamiento de datos personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

a) **Principio de legalidad en materia de Tratamiento de datos:** El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;

b) **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;

c) **Principio de libertad:** El Tratamiento sólo 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 releve el consentimiento;

d) **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;

e) **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;

f) **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 presente 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 presente 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 presente ley;

g) **Principio de seguridad:** La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, 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;

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 presente ley y en los términos de la misma

La determinación normativa legal fue interpretada por la Corte Constitucional, quien señala unos criterios interpretativos de los preceptos transcritos. Señala que la norma crea una excepción a ciertos principios, una modulación con otros y una concurrencia con normas especiales, pero no una exclusión. Ello supondrá, en la práctica, un análisis concreto de ponderación constitucional entre preceptos de derecho iusfundamental.

"**2.4.5.1. *Interpretación de los preceptos***

El inciso tercero señala que el régimen de protección del proyecto de ley "*no será de aplicación*" a los siguientes ámbitos: **a)** bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico; **b)** bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control de lavado de activos y financiamiento del terrorismo; **c)** bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia; **d)** bases de datos y archivos de información periodística y otros contenidos editoriales; **e)** bases de datos y archivos regulados por la Ley 1266 de 2008 –datos financieros y comerciales para calcular riesgo crediticio; y **f)** bases de datos y archivos regulados por la Ley 79 de 1993 –información estadística.

Además, el parágrafo precisa que los principios de protección contenidos en el proyecto *"(…) serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal."* También dispone que los principios que se establezcan en la normativa que regule los datos exceptuados, se deberán aplicar de manera concurrente con los estipulados en el proyecto.

Una lectura conjunta del inciso tercero y del parágrafo permite concluir que el primero **prevé una serie de casos exceptuados de las reglas del proyecto de ley, debido a que requieren reglas especiales**, como las que se introdujeron en la Ley 1266 para datos personales financieros y comerciales destinados a calcular el riesgo crediticio. Estas hipótesis requieren una regulación especial, por cuanto son ámbitos en los que existe una fuerte tensión entre el derecho al habeas data y otros principios constitucionales (como el derecho a la información, la seguridad nacional y el orden público), tensión que para ser resuelta requiere reglas especiales y complementarias. Sin embargo, de conformidad con la primera parte del parágrafo, **estas hipótesis no están exceptuadas de los principios**, como garantías mínimas de protección del habeas data. En otras palabras, **las hipótesis enunciadas en el inciso tercero son casos exceptuados –no excluidos- de la aplicación de las disposiciones de la ley, en virtud del tipo de intereses involucrados en cada uno y que ameritan una**

regulación especial y complementaria, salvo respecto de las disposiciones que tienen que ver con los principios. Varias razones soportan esta interpretación:

En primer lugar, como se indicó en el informe de ponencia para segundo debate en Senado, este parágrafo se introdujo con el fin de precisar que el artículo 2 no introduce un régimen de exclusión sino de excepción para ámbitos que requieren regulaciones especiales, pero a los que le son aplicables los principios generales contenidos en el proyecto de ley. Al respecto, se indicó:

> *"La inclusión del parágrafo obedece a que sin importar la finalidad que tenga la base de datos, mientras esta contenga información y datos personales se deberá respetar los principios generales que regulan el tratamiento y protección de datos; así lo ha sostenido en reiteradas ocasiones la Corte Constitucional al enunciar el desarrollo y alcance que deben tener los principios que regulan el tema de la protección de la información. Una legislación unificada y clara sobre el tema en desarrollo se hace completamente necesaria respondiendo siempre a los principios de necesidad y proporcionalidad, motivo por el cual pretender dejar bases de datos sin que les sea aplicable los principios de la administración de datos, solo debería hacerse en respuesta a un estudio particular de cada caso que sobre fundamentos verídicos y con argumentación suficiente que permita, a través del test de razonabilidad, decidir y motivar por qué no se aplicarán los principios básicos que desarrolla un derecho fundamental, basta con analizar desde la óptica de la Corte los principios de libertad, necesidad, veracidad, integridad, finalidad. Y su importancia en el desarrollo del derecho fundamental al Hábeas Data, la protección de datos personales y la autodeterminación informática."*

En segundo lugar, desde el punto de vista teleológico, estos preceptos deben interpretarse dentro del propósito del proyecto de ley: introducir en el ordenamiento una serie de principios básicos aplicables al tratamiento de todos los datos personales, independientemente de su clasificación, lo que es incompatible con la existencia de regímenes excluidos.

En tercer lugar, y como se analizará más adelante, las garantías previstas en el artículo 4 son principios que ya habían sido recogidos por la jurisprudencia constitucional como garantías derivadas del derecho fundamental al habeas data y, por tanto, incluso en

ausencia de una ley que lo disponga, son de aplicación obligatoria al tratamiento de todo tipo de dato personal.

En consecuencia, una interpretación del inciso tercero del artículo 2 consonante con la Constitución y el contenido y finalidad del proyecto de ley es que aquél no prevé regímenes excluidos de la aplicación de la ley sino exceptuados de algunas de sus disposiciones en virtud de los intereses que se hallan en tensión. Esos casos exceptuados deben ser regulados por leyes estatutarias especiales y complementarias, las cuales deberán sujetarse a las exigencias del principio de proporcionalidad.

En este orden de ideas, las leyes especiales que se ocupen de los ámbitos exceptuados deberán **(i)** perseguir una finalidad constitucional, **(ii)** prever medios idóneos para lograr tal objetivo, y **(iii)** establecer una regulación que en aras de la finalidad perseguida, no sacrifique de manera irrazonable otros derechos constitucionales, particularmente el derecho al habeas data. Además, de conformidad con los principios que se examinarán más adelante, el cumplimiento de las garantías y la limitación del habeas data dentro de los límites de la proporcionalidad debe ser vigilada y controlada por un órgano independiente, bien sea común o sectorial.

Antes de terminar, tal como se hizo en la sentencia C-1011 de 2008, la Sala se permite recordar que aunque en principio es constitucional la consagración de algunas excepciones a la aplicación de algunas disposiciones de la ley, ello no significa que aquellos ámbitos, así como todos los demás en los que se lleva a cabo tratamiento de datos personales, estén excluidos de las garantías básicas del derecho al habeas data, así como de las garantías de otros derechos fundamentales que en cada caso puedan resultar lesionados con el tratamiento de datos personales"

Es importante destacar que la ley 1621 de 2013 establece la obligación de crear unos Manuales de Doctrina que han de trazar criterios sobre el tratamiento de datos de inteligencia, por lo menos en el tema sensible de reserva de información, fuentes, agentes, medios y capacidades (artículo 16). Adicionalmente, los artículos 28 a 32 establecen la creación y objetivos de los Centros de Protección de Datos de Inteligencia y Contrainteligencia, la depuración de datos de inteligencia y contrainteligencia, los Centros de Protección de Datos y la supervisión de esta actividad. Se transcriben:

"Bases de Datos y Archivos de Inteligencia y Contrainteligencia

Artículo 28. *Centros de Protección de Datos de Inteligencia y Contrainteligencia*. Cada uno de los organismos que desarrolla actividades de inteligencia y contrainteligencia tendrá un Centro de Protección de datos y archivos de inteligencia y Contrainteligencia (CPD). Cada Centro tendrá un responsable que garantizará que los procesos de recolección, almacenamiento, producción y difusión de la información de inteligencia y contrainteligencia estén enmarcados en la Constitución y la Ley. Para ello se llevarán a cabo los talleres de capacitación necesarios dentro de cada organismo.

Artículo 29. *Objetivos de los Centros de Protección de Datos de Inteligencia y Contrainteligencia (CPD).* Cada CPD tendrá los siguientes objetivos:

a. Controlar el ingreso y la salida de información a las bases de datos y archivos de inteligencia y contrainteligencia, garantizando de manera prioritaria su reserva constitucional y legal;

b. Asegurar que aquellos datos de inteligencia y contrainteligencia que una vez almacenados no sirvan para los fines establecidos en el artículo 5 de la presente ley, sean retirados;

c. Garantizar que la información no será almacenada en las bases de datos de inteligencia y contrainteligencia por razones de género, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica, pertenencia a una organización sindical, social o de derechos humanos, o para promover los intereses de cualquier partido o movimiento político o afectar los derechos y garantías de los partidos políticos de oposición.

Artículo 31. *Comités de Actualización, Corrección y Retiro de Datos y Archivos de Inteligencia*. Cada organismo de inteligencia creará un comité para la corrección, actualización y retiro de datos e información de inteligencia de conformidad con los principios, límites y fines establecidos en la presente ley. La información que haya sido recaudada para fines distintos de los establecidos en el artículo 4° de la presente ley, o por las razones establecidas en el último inciso del mismo artículo, será retirada de las bases de datos y archivos de inteligencia, y almacenada en un archivo histórico hasta tanto la Comisión para la depuración rinda su informe de recomendaciones.

Artículo 32. *Supervisión y Control*. El informe anual de los Inspectores de Fuerza y las Oficinas de control interno, o quienes hagan sus veces, contemplado en el artículo 18

de la presente ley deberá incluir la verificación del cumplimiento de los procesos de actualización, corrección y retiro de datos y archivos de inteligencia y contrainteligencia.

5.- Reserva de la información de los organismos de inteligencia del Estado Colombiano.-

En este punto, y como se adelantó arriba, es importante tener en cuenta las normas de reserva legal que se establecen tanto en la ley 1621 de 2013 como en su norma reglamentaria, Decreto único 1070 de 2015.

De acuerdo a estas disposiciones, la reserva opera respecto de la información, los medios, los métodos, agentes, capacidades del organismo de inteligencia y contrainteligencia:

Ley 1621 de 2013:

Artículo 33. *Reserva*. Por la naturaleza de las funciones que cumplen los organismos de inteligencia y contrainteligencia sus **documentos, información y elementos técnicos estarán amparados por la reserva legal** por un término máximo de treinta (30) años contados a partir de la recolección de la información y tendrán carácter de información reservada.

Excepcionalmente y en casos específicos, por recomendación de cualquier organismo que lleve a cabo actividades de inteligencia y contrainteligencia, el Presidente de la República podrá acoger la recomendación de extender la reserva por quince (15) años más, cuando su difusión suponga una amenaza grave interna o externa contra la seguridad o la defensa nacional, se trate de información que ponga en riesgo las relaciones internacionales, esté relacionada con grupos armados al margen de la ley, o atente contra la integridad personal de los **agentes o las fuentes**.

Parágrafo 1°. El Presidente de la República podrá autorizar en cualquier momento, antes del cumplimiento del término de la reserva, la desclasificación total o parcial de los documentos cuando considere que el levantamiento de la reserva contribuirá al interés general y no constituirá una amenaza contra la vigencia del régimen democrático, la seguridad, o defensa nacional, **ni la integridad de los medios, métodos y fuentes.**

Artículo 34. *Inoponibilidad de la Reserva*. El carácter reservado de los documentos de inteligencia y contrainteligencia no será oponible a las autoridades judiciales, disciplinarias y fiscales que lo soliciten para el debido ejercicio de sus funciones, siempre que su difusión **no ponga en riesgo la seguridad o la defensa nacional, ni la integridad personal de los ciudadanos, los agentes, o las fuentes.** Corresponderá a dichas autoridades asegurar la

reserva de los documentos que lleguen a conocer en desarrollo de lo establecido en el presente artículo.

Decreto 1070 de 2015.-

RESERVA LEGAL, NIVELES DE CLASIFICACIÓN, SISTEMA PARA LA DESIGNACIÓN DE LOS NIVELES DE ACCESO A LA INFORMACIÓN Y DESCLASIFICACIÓN DE DOCUMENTOS

ARTÍCULO 2.2.3.6.1. RESERVA LEGAL. En los términos del artículo 33 de la Ley 1621 de 2013, los documentos, información y elementos técnicos de los organismos de inteligencia y contrainteligencia estarán amparados por la reserva legal y se les asignará un nivel de clasificación de acuerdo con lo establecido en el siguiente artículo. ***(Decreto 857 de 2014 artículo 10)***

ARTÍCULO 2.2.3.6.2. NIVELES DE CLASIFICACIÓN DE LA INFORMACIÓN. Los niveles de clasificación de seguridad de la información que goza de reserva legal serán los siguientes:

a) Ultrasecreto. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al exterior del país los intereses del Estado o las relaciones internacionales.

b) Secreto. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al interior del país los intereses del Estado.

c) Confidencial. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar directamente las instituciones democráticas.

d) Restringido. Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información de las instituciones militares, de la Policía Nacional o de los organismos y dependencias de inteligencia y contrainteligencia, sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar en las citadas instituciones y organismos, su seguridad, operaciones, medios, métodos, procedimientos, integrantes y fuentes.

PARÁGRAFO. Los documentos de inteligencia y contrainteligencia que contengan información relacionada con diferentes niveles de clasificación de seguridad asumirán la del nivel más alto que tenga la información contenida en ellos.

Sin perjuicio de lo establecido en el artículo 34 de la Ley 1621 de 2013, a mayor nivel de clasificación de seguridad de la información, mayores serán las restricciones y controles para el acceso a la misma por parte de los receptores, las autoridades, los servidores públicos y asesores que deban conocer de ella. Estas restricciones deberán quedar establecidas en actos administrativos, manuales, protocolos, tarjetas de autorización para manejo y acceso a la información y contratos respectivos en cada uno de los organismos de inteligencia y contrainteligencia. ***(Decreto 857 de 2014 artículo 11)***

ARTÍCULO 2.2.3.6.3. CRITERIOS PARA DAR ACCESO A LA INFORMACIÓN. Los organismos de inteligencia y contrainteligencia para dar acceso interno y externo a la información que goza de reserva legal y tenga nivel de clasificación, cumplirán con los siguientes criterios:

a) Mantener el principio de compartimentación a partir de la necesidad de saber y conocer estrictamente lo necesario para el desempeño de la función que le es propia. Así mismo, establecerán un mecanismo interno que determine los niveles de acceso para cada funcionario o asesor del organismo de inteligencia y contrainteligencia.

b) Entre mayor sea el nivel de clasificación de la información, mayores serán las restricciones como los controles que se deben aplicar para tener acceso a ella.

c) Identificar a los receptores de productos de inteligencia y contrainteligencia, estableciendo su nivel de acceso.

d) Desarrollar guías y/o protocolos, cuando sea el caso, para recibir, compartir e intercambiar información de inteligencia y contrainteligencia.

e) Implementar de forma física y/o mediante la utilización de herramientas tecnológicas, el sistema de acceso a los diferentes niveles de clasificación, con capacidades de administración, monitoreo y control, con base en los cargos, perfiles y funciones determinadas en la estructura de cada organismo de inteligencia y contrainteligencia.

f) Suscribir acuerdos, protocolos o convenios, en los términos de la Constitución y la Ley, para recibir, compartir o intercambiar información que goce de reserva legal con agencias de inteligencia y contrainteligencia extranjeras.

Cada organismo documentará sus procedimientos, en sus manuales o protocolos, para asegurar la reserva legal, los niveles de clasificación y dar acceso a la información a las autoridades o receptores competentes. ***(Decreto 857 de 2014 artículo 12)***

CAPÍTULO 7
SEGURIDAD Y RESTRICCIONES EN LA DIFUSIÓN DE PRODUCTOS E INFORMACIÓN DE INTELIGENCIA Y CONTRAINTELIGENCIA

ARTÍCULO 2.2.3.7.1. SEGURIDAD Y RESTRICCIONES EN LA DIFUSIÓN DE PRODUCTOS DE INTELIGENCIA Y CONTRAINTELIGENCIA. Los organismos y dependencias de inteligencia y contrainteligencia deberán para los casos de difusión de productos de inteligencia y contrainteligencia a los receptores autorizados por la ley, indicar la reserva legal a la que está sometida la información y expresar, al receptor autorizado de la misma, si se trata de un producto de inteligencia o contrainteligencia "de solo conocimiento" o "de uso exclusivo", teniendo como referencia las siguientes restricciones para cada caso, así:

a) De solo conocimiento. Es aquel producto de inteligencia y contrainteligencia que tiene un receptor autorizado por ley, solo para conocimiento directo y, únicamente, como referencia o criterio orientador para tomar decisiones dentro de su órbita funcional. El receptor autorizado recibe el producto bajo las más estrictas medidas de seguridad, reserva legal y protocolos adecuados. El receptor autorizado no podrá difundir la información contenida en el producto de inteligencia y contrainteligencia.

b) De uso exclusivo. Es aquel producto de inteligencia y contrainteligencia que tiene un receptor autorizado por ley, solo para su conocimiento directo y uso exclusivo. Este producto solo podrá ser empleado como referencia para tomar decisiones dentro de su órbita funcional. El receptor autorizado recibe el producto, bajo las más estrictas medidas de seguridad, reserva legal y protocolos adecuados. El receptor autorizado podrá difundir esta clase de información bajo su responsabilidad, únicamente, para establecer cursos de acción que permitan la toma de decisiones para el cumplimiento de los fines establecidos en la Constitución y la ley.

En ninguno de los anteriores casos, se podrá revelar fuentes, métodos, procedimientos, identidad de quienes desarrollan o desarrollaron actividades de inteligencia y contrainteligencia o poner en peligro la seguridad y defensa nacional.

Las autoridades competentes y los receptores de productos de inteligencia o contrainteligencia deberán garantizar, en todo momento, la reserva legal de la misma.

No se entregarán productos de inteligencia y contrainteligencia a aquellas autoridades competentes o receptores autorizados que no garanticen, por escrito, la reserva legal, la seguridad y la protección de la información contenida en los documentos o informes que les vayan a ser suministrados.

El documento con el cual se traslade la reserva legal de la información, a las autoridades competentes o receptores autorizados, deberá especificar la prohibición de emitir copias o duplicados de la misma, alertando sobre las acciones penales y disciplinarias que acarrea la no observancia de lo consagrado en la ley. ***(Decreto 857 de 2014 artículo 13)***

ARTÍCULO 2.2.3.7.2. SUMINISTRO DE INFORMACIÓN. Cuando proceda, el organismo de inteligencia y contrainteligencia, responsable de dar respuesta legal a un requerimiento de información de inteligencia, deberá verificar previamente que:

a) La solicitud se ajuste a lo preceptuado en el artículo 34 de la Ley 1621 de 2013.

b) La respuesta identifique el nivel de clasificación, correspondiente a la naturaleza del documento o la información que se ponga en conocimiento de la autoridad competente.

c) La respuesta debe reflejar adecuadamente la valoración de la información, el uso de términos condicionales y dubitativos, que garantice entre otros la reserva, el debido proceso, el buen nombre y el derecho a la intimidad.

d) La respuesta cumpla los protocolos de seguridad, acceso y reserva.

e) La respuesta con la información suministrada no debe poner en peligro o riesgo la seguridad y defensa nacional, y, en los organismos que integran la comunidad de inteligencia, sus métodos, sus procedimientos, sus medios, sus fuentes, sus agentes, sus servidores públicos o sus asesores. Los criterios de valoración y ponderación del presente literal los fijará el Jefe o Director de cada organismo, según corresponda.

f) La respuesta no debe dar a conocer capacidades, procedimientos, métodos, medios, elementos técnicos, fuentes, operaciones o actividades de inteligencia o contrainteligencia.

g) La respuesta debe quedar debidamente registrada para tener la trazabilidad de la misma. En el documento de respuesta se debe trasladar a las autoridades competentes o receptores autorizados la reserva legal de la información y especificar las prohibiciones o restricciones de su

difusión, alertando sobre las acciones penales y disciplinarias que acarrea la no observancia de lo consagrado en la ley. ***(Decreto 857 de 2014 artículo 14)***

CAPÍTULO 8
CENTROS DE PROTECCIÓN DE DATOS DE INTELIGENCIA Y CONTRAINTELIGENCIA

ARTÍCULO 2.2.3.8.1. CENTROS DE PROTECCIÓN DE DATOS DE INTELIGENCIA Y CONTRAINTELIGENCIA (CPD). Los Jefes o Directores de cada uno de los organismos de inteligencia y contrainteligencia implementarán y/o adecuarán los CPD y archivos de inteligencia y contrainteligencia, designando un responsable por cada CPD en cada una de las dependencias, según su órbita funcional, nivel de clasificación de la información, desarrollo de la función en sus actividades estratégicas, operacionales o tácticas, o sus equivalentes, en cada uno de los organismos que hacen parte de la comunidad de inteligencia.

Los Jefes o Directores de inteligencia y contrainteligencia implementarán un plan anual de capacitación, para el personal responsable y comprometido en el ingreso, permanencia, difusión y protección de la información de inteligencia y contrainteligencia, en los CPD y en los archivos respectivos, que permita dar cumplimiento a los fines, límites y principios de la Ley 1621 de 2013. ***(Decreto 857 de 2014 artículo 15)***

ARTÍCULO 2.2.3.8.2. ACTUALIZACIÓN, CORRECCIÓN Y RETIRO DE DATOS Y ARCHIVOS DE INTELIGENCIA. Para atender lo establecido en el artículo 31 de la Ley 1621 de 2013, los Jefes o Directores de los organismos de inteligencia y contrainteligencia crearán un comité para la actualización, corrección y retiro de datos y archivos de inteligencia.

El comité de actualización, corrección y retiro de datos y archivos de inteligencia en cada uno de los organismos que integran la comunidad de inteligencia, para efectos de fijar los criterios de actualización, corrección y retiro de datos y archivos de inteligencia y contrainteligencia, deberá observar los límites, fines y principios de los artículos 4 y 5 de la Ley 1621 de 2013.

Una vez conformado el comité de actualización, corrección y retiro de datos y archivos de inteligencia en cada uno de los organismos que integran la comunidad de inteligencia, este comité deberá presentar al Jefe o Director del organismo de inteligencia y contrainteligencia, un primer informe de avance e implementación dentro de los seis meses siguientes a su conformación y, posteriormente, el comité presentará un informe periódico, cada cuatro meses, o, en forma extraordinaria, cuando lo requiera el Jefe o Director del organismo. ***(Decreto 857 de 2014 artículo 16)***

CAPÍTULO 9
MECANISMOS DE PROTECCIÓN DE LA INTEGRIDAD E IDENTIDAD DE LOS SERVIDORES PÚBLICOS DE LOS ORGANISMOS DE INTELIGENCIA Y CONTRAINTELIGENCIA

ARTÍCULO 2.2.3.9.1. PROTECCIÓN DE LA IDENTIDAD. Para garantizar la protección de la identidad de los servidores públicos que desarrollan actividades de inteligencia y contrainteligencia, la Registraduria Nacional del Estado Civil, en coordinación con las Direcciones y Jefaturas de Inteligencia de las Fuerzas Militares, la Policía Nacional, la Dirección Nacional de Inteligencia y la Unidad de Información y Análisis Financiero, establecerán mecanismos, manuales de procedimiento, formas de llevar los registros, trámites ágiles para la expedición del documento de nueva identidad, control de archivos y bases de datos, entre otros aspectos, que permitan mantener sistemas adecuados, seguros, confiables y reservados, a la hora de asignar nueva identidad con cupo numérico a quienes deban realizar misiones y operaciones de inteligencia y contrainteligencia previamente autorizadas.

El suministro de nueva identidad solo se realizará previa solicitud escrita del respectivo Director o Jefe de Inteligencia y contrainteligencia, únicamente para las personas que él determine y que desarrollen misiones de trabajo en el marco de los artículos 4 y 5 de la Ley 1621 de 2013.

La nueva identidad solo se suministrará por el tiempo necesario, prorrogable y controlable por quien autoriza, para cumplir con la misión y garantizar la protección e integridad del servidor público que en ella participe.

Los Comandantes de Fuerza, las Jefaturas y las Direcciones de los organismos de inteligencia y contrainteligencia adoptarán los procedimientos administrativos, académicos y demás que sean necesarios para facilitar la protección de la identidad funcional e instruir a los servidores públicos que harán uso de ella.

PARÁGRAFO. El Director o Jefe de Inteligencia y contrainteligencia será quien determine el tiempo necesario y tendrá la potestad de requerir, en el momento que lo estime pertinente, la cancelación de la nueva identidad, mediante documento escrito clasificado dirigido al Registrador Nacional del Estado Civil. ***(Decreto 857 de 2014 artículo 17)***

ARTÍCULO 2.2.3.9.2. MEDIDAS DE SEGURIDAD. La Registraduria Nacional del Estado Civil, en coordinación con los organismos de inteligencia y contrainteligencia, establecerá los protocolos, medidas de seguridad y mecanismos necesarios, incluyendo estudios de seguridad y pruebas de confiabilidad de los funcionarios responsables de la administración del sistema de

nueva identidad, garantizando en todo momento y lugar la reserva legal. ***(Decreto 857 de 2014 artículo 18)***

ARTÍCULO 2.2.3.9.3. MECANISMOS DE PROTECCIÓN PARA LOS SERVIDORES PÚBLICOS QUE DESARROLLAN ACTIVIDADES DE INTELIGENCIA Y CONTRAINTELIGENCIA Y SU NÚCLEO FAMILIAR. Para garantizar la debida protección de los servidores públicos pertenecientes a los organismos que desarrollan actividades de inteligencia y contrainteligencia, que con ocasión del cumplimiento de sus funciones y actividades se vean compelidos a riesgo o amenaza, actual e inminente, contra su integridad personal o la de su núcleo familiar, las Direcciones y Jefaturas de Inteligencia de las Fuerzas Militares, la Policía Nacional, la Dirección Nacional de Inteligencia, la UIAF y de los demás organismos de inteligencia y contrainteligencia que se creen por ley, coordinarán la realización del estudio técnico de nivel de amenaza o riesgo, para la toma de las decisiones a que haya lugar, con la dependencia de contrainteligencia, su equivalente o se apoyarán con otro organismo de la comunidad de inteligencia para tal fin.

El estudio técnico de nivel de amenaza o riesgo, para la toma de decisiones en materia de protección, se realizará al servidor público perteneciente a un organismo de inteligencia y contrainteligencia que se encuentre por sus funciones en situación de amenaza o riesgo, y, cuando sea el caso, se efectuará al núcleo familiar de dicho servidor, siempre que estén dentro del primer grado de consanguinidad, primero de afinidad, primero civil, cónyuge, compañero o compañera permanente.

Los Comandantes de Fuerza, las Jefaturas y las Direcciones de los organismos de inteligencia y contrainteligencia adoptarán los procedimientos que sean necesarios para implementar los mecanismos de protección para los servidores públicos que desarrollan actividades de inteligencia y contrainteligencia y su núcleo familiar.

Los Comandantes de Fuerza, los Jefes y los Directores de los organismos de inteligencia y contrainteligencia adelantarán los trámites legales y las coordinaciones directas para garantizar las medidas de protección que se estimen necesarias y pertinentes.

PARÁGRAFO 1. Las hojas de vida, los perfiles o los datos de los servidores públicos de inteligencia y contrainteligencia y de los contratistas que lleven a cabo estas actividades, no deberán ser revelados, incorporados, ni publicados en páginas y/o portales electrónicos o web u otros medios similares.

PARÁGRAFO 2. Las autoridades competentes que por razón de sus funciones conozcan acerca de la identidad y actividades propias de los servidores públicos de los organismos de inteligencia

y contrainteligencia, deberán garantizar la reserva legal de dicha información como mecanismo de protección. ***(Decreto 857 de 2014 artículo 19).***

6.- Política de Habeas Data en relación con bases de datos que puedan tener parcial o totalmente el carácter de públicas y no estén cobijadas por el régimen especial de reserva.

La Policía de Tratamiento de Información Personal de la UIAF, la cual se manejará y gestionará de conformidad con la Ley 1621 de 2013, 1581 de 2012 y demás normas que regulan la materia. Los lineamientos que se presentan a continuación, se aplican para las bases de datos o archivos de la UIAF, que contengan datos personales de sus funcionarios y familiares, usuarios, visitantes y contratistas, cuya finalidad será la de salvaguardar su información y dar un tratamiento adecuado, en los términos exigidos en la ley.

El titular del dato personal, acepta que a través del registro de información por los diferentes canales de atención al ciudadano dispuestos por la UIAF, está recoge datos personales, los cuales no se cederán a terceros sin su conocimiento y autorización.

Información básica del responsable y encargado del tratamiento de la información personal suministrada a la UIAF:

- Responsable y encargado del tratamiento de datos personales: Unidad de Información y Análisis Financiero – UIAF.
- NIT: 830068074-9
- Ubicación: Carrera 7 No. 31-10, Piso 6, Bogotá D.C.
- Horario de atención: lunes a viernes de 8:00 a.m. a 5:00 p.m.
- PBX: (571) 288 5222
- Línea Gratuita Nacional: 01 8000 11 11 83
- Correo Electrónico: oficinajuridica@uiaf.gov.co

6.1.- GENERALIDADES

De acuerdo con la definicion establecida en la ley 1581 de 2012, el dato personal es cualquier informacion vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables, como el nombre, la edad, el sexo, el estado civil, el domicilio, entre otros.

Estos datos pueden almacenarse en cualquier soporte fisico o electronico y ser tratados de forma manual o automatizada.

La siguiente política de tratamiento de datos personales de la UIAF, regula la recolección, almacenamiento, tratamiento, administración, transferencia, transmisión y protección de la información de datos personas que se reciban de empleados y terceros, en concordancia con lo estipulado en la Constitución Política de Colombia, la Ley 1581 de 2012, sus decretos reglamentarios y demás normas complementarias, y que no sea de aquellos cobijados por el régimen de reserva obligatorio para los organismos de inteligencia del Estado Colombiano.

Para la interpretación y armonización de la política de tratamiento de datos personales, se definen los siguientes términos, según lo estipulado en la Ley 1581 de 2012:

- **Autorización:** consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personas.
- **Base de datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Titular:** persona natural cuyos datos personales sean objeto de tratamiento.
- **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 (Decreto 1377 de 2013).
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la Republica de Colombia, cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

La Ley 1266 de 2008 define los siguientes tipos de datos de carácter personal:

a) Dato privado: “Es el dato que por su naturaleza íntima o reservada sólo es relevante para el Titular”.

b) Dato semiprivado: "Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV" de la Ley 1266.

c) Dato público: "Es el dato calificado como tal según los mandatos de la Ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados", de conformidad con la Ley 1266 de 2008. "Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas".

Adicionalmente, la Ley 1581 de 2012 establece las siguientes categorías especiales de datos personales:

d) 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 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".

La Ley 1581 de 2012 prohíbe el tratamiento de datos sensibles con excepción de los siguientes casos:

1. Cuando el Titular otorga su consentimiento,
2. Es necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado,
3. Es 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,
4. Se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y
5. Tenga una finalidad histórica, estadística o científica, en este último caso deben adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

e) Datos personales de los niños, niñas y adolescentes: Se debe tener en cuenta que aunque la Ley 1581 de 2012 prohíbe el tratamiento de los datos personales de los niños, niñas y adolescentes, salvo aquellos que por su naturaleza son públicos, la Corte Constitucional precisó que independientemente de la naturaleza del dato, se puede realizar el tratamiento de éstos *"siempre y cuando el fin que se persiga con dicho tratamiento responda al interés superior de los niños, niñas y adolescentes y se asegure sin excepción alguna el respeto a sus derechos prevalentes".*

También la ley define los siguientes roles:

a) Responsable de 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"*. La Superintendencia de Industria y Comercio, de acuerdo con la ley es Responsable de Tratamiento de datos personales contenidos en sus bases de datos,

b) 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". La SIC podrá realizar el tratamiento de sus datos personales a través de Encargados.*

6.2.- DISPOSICIONES GENERALES ESTABLECIDAS EN LA LEY 1581 DE 2012 PARA LA PROTECCIÓN DE DATOS PERSONALES

La Ley 1581 de 2012 desarrolla el derecho constitucional a conocer, actualizar y rectificar la información recogida en bases de datos y los demás derechos, libertades y garantías a que se refieren los artículos 15 y 20 de la Constitución (derecho a la intimidad y derecho a la información, respectivamente).

La citada ley se aplica a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por parte de entidades públicas o privadas.

Considerando el modo de conservación de una base de datos, se puede distinguir entre bases de datos automatizadas y bases de datos manuales o archivos.

Las bases de datos automatizadas son aquellas que se almacenan y administran con la ayuda de herramientas informáticas.

Las bases de datos manuales o archivos son aquellas cuya información se encuentra organizada y almacenada de manera física, como las fichas de pedidos a proveedores que contengan información personal relativa al proveedor, como nombre, identificación, números de teléfono, correo electrónico, etc.

La ley, como se señaló en el acápite de régimen de reserva de los organismos de inteligencia del Estado Colombiano, exceptúa del régimen de protección:

- Los archivos y las bases de datos pertenecientes al ámbito personal o doméstico;
- Los que tienen por finalidad la seguridad y la defensa nacionales, la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo,
- Los que tengan como fin y contengan información de inteligencia y contrainteligencia,
- Los de información periodística y otros contenidos editoriales,
- Los regulados por la Ley 1266 de 2008 (información financiera y crediticia, comercial, de servicios y proveniente de terceros países) y
- Los regulados por la Ley 79 de 1993 (sobre censos de población y vivienda).

6.3.- DEBERES DEL RESPONSABLE DEL TRATAMIENTO

El Responsable del Tratamiento ha sido definido por la Ley 1581 de 2012 como la 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.

Son deberes de los Responsables del Tratamiento y, por consiguiente, de la UIAF los establecidos en el artículo 17 de la Ley 1581 de 2012:

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

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

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

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

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

f) 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 éste se mantenga actualizada.

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

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la citada ley.

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

j) Tramitar las consultas y reclamos formulados en los términos señalados en la citada ley.

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la citada ley y en especial, para la atención de consultas y reclamos.

l) 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.

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

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

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

6.4.- RESPONSABLE DEL TRATAMIENTO DE LAS PQRS DEL TITULAR

La UIAF dispone del módulo web de peticiones, quejas, reclamos y denuncias (PQRSD) relacionadas con la UIAF; en todo caso la UIAF es quien determina las finalidades y las formas como se trataran los datos, previa comunicación a los titulares.

Se debe cumplir con los deberes establecidos en la Ley 1581 de 2012, y demás normas complementarias, y mencionados en el numeral 1.2 de esta política.

6.5.- DERECHOS DE LOS TITULARES

La Ley 1581 de 2012 establece que los Titulares de los datos personales tendrán los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.

b) 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 citada ley.

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la citada ley y las demás normas que la modifiquen, adicionen o complementen.

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a la ley y a la Constitución.

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

Adicionalmente, el Decreto reglamentario 1377 de 2013 define que los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos.

6.6.- AUTORIZACIÓN

La UIAF debe solicitar autorización previa, expresa e informada a los titulares de los datos personales sobre los que requiera realizar el tratamiento, cuando se trate de bases públicas no sometidas al régimen especial de reserva.

No se requiere de la autorización en los siguientes casos:

1. Cuando la información sea capturada en ejercicio de sus funciones legales.
2. Cuando el tratamiento recaiga sobre datos de naturaleza pública.
3. Cuando el tratamiento recaiga sobre datos relacionados con el Registro Civil de las personas.
4. Los que tienen por finalidad la seguridad y defensa nacional, la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.
5. Los que tienen como fin y contengan información de inteligencia y contrainteligencia.

Autorización previa: El consentimiento debe ser otorgado por el titular, a más tardar en el momento de la recolección de los datos personales.

Autorización expresa: El consentimiento del titular debe ser explícito y concreto, no son válidas las autorizaciones abiertas y no específicas. Se requiere que el titular manifieste su voluntad de autorizar que la UIAF realice el tratamiento de sus datos personales.

Esta manifestación de voluntad del titular puede darse a través de diferentes mecanismos puestos a disposición por la UIAF, tales como:

- Por escrito, diligenciando un documento de autorización de tratamiento de datos personales.
- De forma verbal; conversaciones telefónicas o en videoconferencias.
- Mediante conductas inequívocas que permitan concluir que otorgó su autorización, a través de su aceptación expresa a los términos y condiciones de una actividad dentro de los cuales se requiera la autorización de los participantes para el tratamiento de sus datos personales.

En ningún caso la UIAF o sus funcionarios, asimilará el silencio del titular a una conducta inequívoca.
Cualquiera que sea el mecanismo utilizado por la UIAF o el funcionario, es necesario que la autorización se conserve para poder ser consultada con posterioridad.

Autorización informada significa que al momento de solicitar el consentimiento al titular, debe informársele claramente:

- Los datos personales que serán recolectados.
- La identificación y datos de contacto del responsable y del encargado del tratamiento.
- Las finalidades específicas del tratamiento que se pretende realizar, es decir: cómo y para qué se va a hacer la recolección, el uso, la circulación de los datos personales.
- Cuáles son los derechos que tiene como titular de los datos personales; para el efecto ver el numeral 1.3 de ésta política.
- El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando éstas versen sobre datos sensibles o sobre los datos de niñas, niños y adolescentes.

6.7.- POLÍTICAS Y PROCEDIMIENTOS

Se establecen las siguientes directrices generales, en el marco de los límites ya señalados en el régimen especial de reserva.

Primero: Cumplir con toda la normatividad legal vigente colombiana que dicte disposiciones para la protección de datos personales.

Segundo: Cumplir con la ley de protección de datos personales de acuerdo con lo contemplado en el Código de Ética.

Tercero: Los funcionarios deben acogerse a las inhabilidades, impedimentos, incompatibilidades y conflicto de intereses contemplados en la Ley 734 de 2002 (Código Disciplinario Único, capitulo cuarto) para el tratamiento de Datos Personales.

Políticas y procedimientos específicos relacionados con el tratamiento de Datos Personales:

a) La UIAF realiza el tratamiento de Datos Personales en ejercicio propio de sus funciones legales y para el efecto no requiere la autorización previa, expresa e informada del Titular. Sin embargo, cuando no corresponda a sus funciones deberá obtener la autorización por medio de

un documento físico, electrónico, mensaje de datos, Internet, sitio web, o también de manera verbal o telefónica o en cualquier otro formato que permita su posterior consulta a fin de constatar de forma inequívoca que sin el consentimiento del titular los datos nunca hubieran sido capturados y almacenados en medios electrónicos o físicos. Así mismo se podrá obtener por medio de conductas claras e inequívocas del Titular que permitan concluir de una manera razonable que este otorgó su consentimiento para el manejo de sus Datos Personales.

b) La UIAF solicitará la autorización a los Titulares de los datos personales y mantendrá las pruebas de ésta, cuando en virtud de las funciones de promoción, divulgación y capacitación, realice invitaciones a charlas, conferencias o eventos que impliquen el Tratamiento de Datos Personales con una finalidad diferente para la cual fueron recolectados inicialmente.

c) En consecuencia, toda labor de tratamiento de Datos Personales realizada en la UIAF deberá corresponder al ejercicio de sus funciones legales o a las finalidades mencionadas en la autorización otorgada por el Titular, cuando la situación así lo amerite.

d) El Dato Personal sometido a Tratamiento deberá ser veraz, completo, exacto, actualizado, comprobable y comprensible. La UIAF mantendrá la información bajo estas características siempre y cuando el titular informe oportunamente sus novedades.

e) Los Datos Personales solo serán Tratados por aquellos Funcionarios de la UIAF que cuenten con el permiso para ello, o quienes dentro de sus funciones tengan a cargo la realización de tales actividades o por los Encargados.

f) La UIAF autorizará expresamente al Administrador de las bases de datos para realizar el tratamiento solicitado por el Titular de la información.

g) La UIAF no hará disponibles Datos Personales para su acceso a través de Internet u otros medios masivos de comunicación, a menos que se trate de información pública o que se establezcan medidas técnicas que permitan controlar el acceso y restringirlo solo a las personas autorizadas por ley o por el titular.

h) Todo Dato Personal que no sea Dato Público se tratará por la UIAF como reservado y/o confidencial, aun cuando la relación contractual o el vínculo entre el Titular del Dato Personal y la UIAF haya finalizado. A la terminación de dicho vínculo, tales Datos Personales deben continuar siendo Tratados de acuerdo con lo dispuesto por el Manual de Archivo y Retención Documental.

i) Cada área de la UIAF debe evaluar la pertinencia de anonimizar los actos administrativos y/o documentos de carácter público que contengan datos personales, para su publicación.

j) El Titular, directamente o a través de las personas debidamente autorizadas, podrá consultar sus Datos Personales en todo momento y especialmente cada vez que existan modificaciones en las Políticas de Tratamiento de la información.

k) La UIAF suministrará, actualizará, ratificará o suprimirá los Datos Personales a solicitud del Titular para corregir información parcial, inexacta, incompleta, fraccionada que induzca al error o aquella que haya sido tratada previa a la vigencia de la ley y que no tenga autorización o sea prohibida.

l) Cuando le sea solicitada información, ya sea mediante una petición, consulta o reclamo por parte del Titular, sobre la manera como son utilizados sus Datos Personales, la UIAF deberá entregar dicha información.

m) A solicitud del Titular y cuando no tenga ningún deber legal o contractual de permanecer en las bases de datos de la UIAF, los Datos Personales deberán ser eliminados. En caso de proceder una revocatoria de tipo parcial de la autorización para el Tratamiento de Datos Personales para algunas de las finalidades la UIAF podrá seguir utilizando los datos para las demás finalidades respecto de las cuales no proceda dicha revocatoria.

n) Las políticas establecidas por la UIAF respecto al tratamiento de Datos Personales podrán ser modificadas en cualquier momento. Toda modificación se realizará con apego a la normatividad legal vigente, y las mismas entrarán en vigencia y tendrán efectos desde su publicación a través de los mecanismos dispuestos por la UIAF para que los titulares conozcan la política de tratamiento de la información y los cambios que se produzcan en ella.

o) Los Datos Personales solo podrán ser tratados durante el tiempo y en la medida que la finalidad de su tratamiento lo justifique.

p) La UIAF será más rigurosa en la aplicación de las políticas de tratamiento de la información cuando se trate del uso de datos personales de los niños, niñas y adolescentes asegurando la protección de sus derechos fundamentales.

q) La UIAF podrá intercambiar información de Datos Personales con autoridades gubernamentales o publicas tales como autoridades administrativas, de impuestos, organismos de investigación y autoridades judiciales, cuando la soliciten en ejercicio de sus funciones.

r) Los Datos Personales sujetos a tratamiento deberán ser manejados proveyendo para ello todas las medidas tanto humanas como técnicas para su protección, brindando la seguridad de que ésta no pueda ser copiada, adulterada, eliminada, consultada o de alguna manera utilizada sin autorización o para uso fraudulento.

s) Cuando finalice alguna de la labores de tratamiento de Datos Personales por los Servidores, contratistas o Encargados del tratamiento, y aun después de finalizado su vínculo o relación contractual con la UIAF, éstos están obligados a mantener la reserva de la información de acuerdo con la normatividad vigente en la materia.

t) La UIAF divulgará en sus servidores, contratistas y terceros encargados del tratamiento las obligaciones que tienen en relación con el tratamiento de Datos Personales mediante campañas y actividades de orden pedagógico.

u) La UIAF no realizará transferencia de información relacionada con Datos Personales a países que no cuenten con los niveles adecuados de protección de datos, de acuerdo con los estándares que estén fijados en la misma Superintendencia.

v) El Titular de los datos personales puede ejercer, principalmente, sus derechos mediante la presentación de consultas y reclamos ante la UIAF, en su sede cuyo domicilio es la carrera 7ª No. 31-10 piso 6, de la ciudad de Bogotá D.C., al correo electrónico oficinajuridica@uiaf.gov.co, en el módulo web de Peticiones, Quejas, Reclamos y Denuncias (PQRSD) de la página web: www.uiaf.gov.co, y a la línea telefónica: 288 5222.

w) Cuando exista un Encargado del Tratamiento de Información de Datos Personales, la UIAF deberá garantizar que la información que le suministra sea veraz, completa, exacta, actualizada, comprobable y comprensible.

Adicionalmente le comunicará de manera oportuna todas las novedades a que haya lugar para que la información siempre se mantenga actualizada.

x) En el caso de existir un Encargado del Tratamiento de información de Datos Personales, la UIAF suministrará según el caso, información de Datos Personales únicamente cuyo Tratamiento realice en virtud de sus funciones legales y cuando excepcionalmente éstas no apliquen, con la autorización del Titular.

y) La UIAF Informará al Encargado del Tratamiento de información de Datos Personales, de existir uno, 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.

z) Cuando exista un Encargado del Tratamiento de información de Datos Personales, se exigirá que en todo momento, se respeten las condiciones de seguridad y confidencialidad de la información del Titular establecidas por la UIAF.

6.8.- FINALIDAD DE LA POLITICA

Los datos personales son objeto de tratamiento por parte de la UIAF con las siguientes finalidades:

- Para el envió de información a los funcionarios o familiares, con el correcto manejo para la protección de la identidad. (Ley Estatutaria 1621 de 2013).
- Para la prestación de los servicios de salud a los familiares del funcionario de la UIAF, beneficiario del servicio de salud y bienestar entre otros afines a las actividades realizadas por talento humano para funcionarios y familiares.
- Para el reconocimiento de las relaciones con sus proveedores, acreedores, ciudadanos, mediante el envió de información relevante, la atención de peticiones, quejas, reclamos y denuncias (PQRSD), por parte del área encargada, y la invitación a eventos organizados o patrocinados por la UIAF.
- Para consolidar un suministro oportuno y de calidad con sus proveedores, para la verificación del cumplimiento de sus obligaciones legales con sus trabajadores, a través de la invitación a participar en procesos de selección, la evaluación del cumplimiento de sus obligaciones y la invitación a eventos organizados o patrocinados por la UIAF.
- Para las verificaciones de seguridad ocupacional.
- Para la determinación de obligaciones pendientes, la consulta de información financiera e historia crediticia y el reporte a centrales de información de obligaciones incumplidas, respecto de sus funcionarios o proveedores.
- Para la atención de requerimientos judiciales o administrativos y el cumplimiento de mandatos judiciales o legales.
- Para el manejo de información de carácter operacional.

6.9.- LEGISLACIÓN APLICABLE

Esta politica de proteccion y tratamiento de datos personales, el aviso de privacidad, se rigen por lo dispuesto en la legislacion vigente sobre proteccion de los datos personales a los que se

refieren el Articulo 15 de la Constitucion Politica de Colombia, titulo VII, capitulo primero del regimen penal, la Ley 1266 de 2008, la Ley 1273 de 2009, la Ley Estatutaria 1621 de 2013, la Ley 1581 de 2012, la Ley 1755 de 2015, el Decreto 1377 de 2013, el Decreto 1727 de 2009, Decreto 886 de 2014, el Decreto 1166 de 2016 y demás normas que las modifiquen, deroguen o sustituyan.

6.10.- VIGENCIA

La Politica de Tratamiento de Datos Personales, de la Unidad de Información y Análisis Financiero – UIAF, entrará en vigencia desde el momento de su publicacion en la pagina web: www.uiaf.gov.co.