Tabla de Contenido

1. Consideraciones Generales

El artículo 15 de la Constitución de la República de Colombia consagra el derecho de cualquier persona de conocer, actualizar y rectificar los datos personales que existan sobre ella en bancos de datos o archivos de entidades públicas o privadas. Igualmente, ordena a quienes tienen datos personales de terceros respetar los derechos y garantía previstos en la Constitución cuando se recolecta, trata y circula esa clase de información.

En concordancia con lo anterior, el artículo 20 de la Constitución de la República de Colombia consagra el derecho de cualquier persona, Responsable y/o Encargado del Tratamiento, de recibir información veraz e imparcial.

La presente política está sujeta a la Ley Estatutaria 1581 de 2012 "*Por la cual se dictan disposiciones generales para la protección de datos personales"*, mediante la cual se regula la recolección y el tratamiento de datos personales efectuado por entidades públicas o privadas; la Ley 1266 de 2008 "Por la cual se dictan las disposiciones generales del hábeas 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"; el Decreto Reglamentario 1377 de 2013 "*Por el cual se reglamenta parcialmente la Ley 1581 de 2012"* y las demás disposiciones normativas vigentes en la materia.

La **Contraloría General de la República -CGR-** está comprometida con el cumplimiento de la regulación en materia de protección de datos personales y con el respeto de los derechos de los Titulares de la información. Por eso, adopta la siguiente **Política de Tratamiento de Datos Personales** de imperativa aplicación en todas las actividades que involucren el tratamiento de datos personales.

2. Campo de Aplicación

La política[1] establecida en este documento es de obligatoria aplicación por parte de los empleados públicos de planta (carrera administrativa, provisionales, funcionarios de libre nombramiento y remoción), trabajadores oficiales, contratistas y demás personal, proveedores de servicios y terceros relacionados, que en ejercicio de sus funciones y obligaciones contractuales, según corresponda, realicen tratamiento de datos personales.

3. Definiciones

Las siguientes definiciones están señaladas en la Ley Estatutaria 1581 de 2012; Decreto 1074 de 2015 y en el Decreto Reglamentario 1377de 2013:

- **Anonimización**: Mecanismo técnico o tecnológico por medio del cual se oculta, pixela, difumina o encubre un dato de naturaleza privada, semiprivada o sensible. Un *"dato anónimo"* no permite, razonablemente, establecer a qué persona natural se refiere, vincula o asocia; entonces, dicha información no es un dato personal. Los datos personales que hayan sido objeto de procesos de anonimización, cifrado, presentados con un seudónimo

[1] Inciso tercero del artículo 25 de la Ley Estatutaria 1581 de 2012 y artículo 2.2.2.25.3.1. del Decreto Único Reglamentario 1074 de 2015.

o que, por cualquier medio, tecnología o proceso, se desvinculan o desasocian de una persona natural, pero que puedan utilizarse para volver a identificar a esa persona, siguen siendo datos personales.

- **Aplicación o App:** Cualquier tipo de programa, o desarrollo de software diseñado para que corra en cualquier elemento informático de hardware, tal como un computador de escritorio, portátil o dispositivo móvil.

- **Autoridad Nacional de Protección de Datos Personales:** Es la Superintendencia de Industria y Comercio – Delegatura para la Protección de Datos Personales. Sin embargo, para efectos de sanciones contra autoridad pública, como el caso de la CGR, la competencia corresponderá a la Procuraduría General de la Nación[2].

- **Autorización:** Consentimiento previo, expreso e informado del Titular del dato para llevar a cabo el tratamiento. Esta puede ser escrita, verbal o mediante conductas inequívocas que permitan concluir, de forma razonable, que el Titular otorgó autorización

- **Aviso de Privacidad:** Comunicación, verbal o escrita, generada por el Responsable y/o Encargado del Tratamiento, 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 datos personales que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

- **Bases de datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.

- **Canal de acceso electrónico:** Son aquellas formas mediante las cuales se recolecta o almacena información personal tales como, páginas web, dispositivos móviles y atención telefónica, entre otros.

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

- **Causahabientes:** Aquella persona, física o jurídica, que sustituye o sucede a otra en el derecho de esta última. La persona de la que procede el derecho se denomina causante.

- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Estos datos se clasifican en sensibles, públicos, privados y semiprivados.

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

  Dato personal público: Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados. Son públicos, entre otros, los datos contenidos en documentos públicos, registros públicos, gacetas y boletines oficiales, sentencias judiciales debidamente

[2] Parágrafo del artículo 23 de la Ley 1581 de 2012.

ejecutoriadas que no estén sometidos a reserva, los relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. También son públicos los datos personales existentes en el registro mercantil de las Cámaras de Comercio (Artículo 26 del Código de Comercio). Asimismo, son datos públicos, los que, en virtud de una decisión del Titular o de un mandato legal, se encuentren en archivos de libre acceso y consulta.

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

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

- **Dato personal semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar, no sólo a su Titular, sino a cierto sector o grupo de personas o a la sociedad en general, como, entre otros, el dato referente al cumplimiento e incumplimiento de las obligaciones financieras o los datos relativos a las relaciones con las entidades de la seguridad social.

- **Dato biométrico:** Todos aquellos datos relativos a las características físicas, fisiológicas o comportamentales de una persona que faciliten su identificación

- **Encargado del tratamiento:** persona, natural o jurídica, que realiza el tratamiento de datos por cuenta del responsable del tratamiento.

- **Partes Interesadas**[3]**:** Son las personas, grupos o entidades sobre las cuales la CGR tiene incidencia, así como aquellas que influyen a la entidad. También se conocen como "Públicos internos y externos" de la CGR.

- **Grupos de Valor**[4]**:** Son los ciudadanos, grupos de ciudadanos y entidades a quienes la CGR debe dirigir sus productos y servicios.

- **Reclamo:** solicitud del Titular del dato o las personas autorizadas por éste o por la ley para corregir, actualizar o suprimir sus datos personales o cuando adviertan que existe un presunto incumplimiento del régimen de protección de datos, según el artículo 15 de la ley 1581 de 2012.

- **Responsable del tratamiento:** Persona, natural o jurídica, que decide sobre el tratamiento de los datos personales.

- **Titular del dato:** Es la persona natural a quién se refiere la información.

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

[3] Artículo 30 de la Resolución Organizacional OGZ - 727 DE 2019
[4] Artículo 40 de la Resolución Organizacional OGZ - 727 DE 2019

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

- **Transferencia:** La transferencia de datos tiene lugar cuando el Responsable 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, pudiendo localizarse dentro o fuera del país.

- **Requisito de procedibilidad:** El Titular o causahabiente sólo podrá elevar queja o denuncia ante la Autoridad delegada para la vigilancia del cumplimiento de la Ley una vez haya agotado el trámite de consulta o reclamo ante el Responsable o Encargado del Tratamiento, lo anterior según el artículo 16 de la Ley 1581 de 2012.

4. Principios para el Tratamiento de Datos Personales

El tratamiento de datos personales debe realizarse respetando las normas generales y especiales sobre la materia y para actividades permitidas por la ley.

En el desarrollo, interpretación y aplicación de la presente política, se aplicarán de manera armónica e integral los siguientes principios:

4.1 Principios relacionados con la recolección de datos personales

- **Principio de libertad**[5]**:** Salvo norma legal en contrario, la recolección de los datos sólo puede ejercerse con la autorización previa, expresa e informada del Titular. Los datos personales no podrán ser obtenidos o divulgados sin el previo consentimiento del Titular, o en ausencia de mandato legal o judicial que releve el consentimiento.

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

  El principio de libertad debe observarse tanto para el caso de los datos que se recolectan a través de formatos como los que hacen parte de los anexos o documentos que entregan los Titulares de los datos a la CGR.

- **Principio de limitación de la recolección**[6]**:** Sólo deben recolectarse los datos personales que sean estrictamente necesarios para el cumplimiento de las finalidades del tratamiento, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo del tratamiento. En consecuencia, debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario. Es decir, los datos deberán ser: (i) adecuados, (ii) pertinentes y (iii) acordes con las finalidades para las cuales fueron previstos.

[5] Literal c) del artículo 4 de la Ley Estatutaria 1581 de 2012.
[6] Artículo 2.2.2.25.2.1. del Decreto Único Reglamentario 1074 de 2015.

4.2 Principios Relacionados con el Uso de Datos Personales

- **Principio de finalidad**[7]**:** El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular. Se deberá informar al Titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y, por tanto, no podrán recopilarse datos sin una finalidad específica.

- **Principio de temporalidad**[8]**:** Los datos personales se conservarán únicamente por el tiempo razonable y necesario para cumplir la finalidad del tratamiento y las exigencias legales o instrucciones de las autoridades de vigilancia y control u otras autoridades competentes. Los datos serán conservados cuando ello sea necesario para el cumplimiento de una obligación legal o contractual. Para determinar el término del tratamiento se considerarán las normas aplicables a cada finalidad y los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

4.3 Principios relacionados con la calidad de los datos personales

Principio de veracidad o calidad[9]**:** 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. La CGR deberá adoptar medidas para asegurar que los datos recolectados sean precisos y suficientes, para que de esta manera se pueda garantizar la actualización, supresión o rectificación de los mismo.

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

- **Principio de seguridad**[10]**:** Cada persona vinculada con la CGR deberá cumplir las medidas técnicas, humanas y administrativas que establezca la Entidad para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- **Principio de transparencia**[11]**:** En el tratamiento debe garantizarse el derecho del Titular a obtener, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

- **Principio de acceso restringido**[12]**:** Sólo se permitirá acceso a los datos personales a las siguientes personas:

    - Al Titular del dato.

[7] Literal b) del artículo 4 de la Ley Estatutaria 1581 de 2012.
[8] Artículo 2.2.2.25.2.8. del Decreto Único Reglamentario 1074 de 2015.
[9] Literal d) del artículo 4 de la Ley Estatutaria 1581 de 2012.
[10] Literal g) del artículo 4 de la Ley Estatutaria 1581 de 2012.
[11] Literal e) del artículo 4 de la Ley Estatutaria 1581 de 2012.
[12] Literal f) del artículo 4 de la Ley Estatutaria 1581 de 2012.

- A las personas autorizadas por el Titular del dato.
- A las personas que, por mandato legal u orden judicial, sean autorizadas para conocer la información del Titular del dato.

- **Principio de circulación restringida**[13]**:** Sólo se puede enviar o suministrar datos personales a las siguientes personas:
  - Al Titular del dato.
  - A las personas autorizadas por el Titular del dato.
  - A las autoridades públicas en ejercicio de sus funciones legales o por orden judicial.
- **Principio de confidencialidad**[14]**:** Todas las personas que intervengan en el tratamiento de datos personales están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento o culminada su relación contractual o vínculo jurídico con la CGR, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley.
- **Principio de legalidad en materia de Tratamiento de Datos Personales**[15]**:** El Tratamiento de Datos Personales es una actividad reglada que debe sujetarse a lo establecido en la ley aplicable, en las demás disposiciones que la desarrollen y en la presente Política.

5. Tratamiento al cual serán sometidos los Datos Personales y la Finalidad del mismo

La CGR realizará el tratamiento (recolección, almacenamiento y uso, entre otros) de los datos personales de acuerdo con las condiciones establecidas por el Titular, la ley o las entidades públicas para cumplir, en especial, las actividades propias de su misión y visión como el máximo órgano de control fiscal del Estado, como pueden ser los derivados del acceso a los sistemas de información o bases de datos de entidades públicas y de entidades privadas que dispongan o administren recursos o ejerzan funciones públicas, los datos captados sólo podrán ser tratados para los fines y propósitos de la vigilancia y control fiscal. Adicionalmente se podrán tratar los datos con finalidades relacionadas, entre otras, para la analítica de datos sobre hechos constitutivos de presunto daño fiscal, de búsqueda selectiva de en bases de datos, de analítica predictiva y prospectiva.

El tratamiento de los datos personales se podrá realizar a través de medios físicos, automatizados o digitales, de acuerdo con el tipo y la forma de recolección de la información personal.

La CGR también podrá tratar los datos personales, entre otros, para los siguientes fines:

- Ejercer su derecho de conocer de manera suficiente al titular que pretende contar con algún servicio ofrecido por la Entidad o realizar algún trámite a través de ésta, prestar servicios, y valorar sus gestiones. Efectuar las

[13] Literal f) del artículo 4 de la Ley Estatutaria 1581 de 2012.
[14] Literal h) del artículo 4 de la Ley Estatutaria 1581 de 2012.
[15] Literal a) del artículo 4 de la Ley Estatutaria 1581 de 2012.

actividades pertinentes para el desarrollo de la etapa precontractual, contractual y poscontractual con la CGR, así como dar cumplimiento a la ley colombiana o extranjera y a las órdenes de autoridades judiciales o administrativas.

- Realizar actividades estadísticas, de atención al usuario, actividades de publicidad y convocatorias, directamente o a través de terceros, derivados de cualquier vínculo jurídico o contractual cuyo objeto sea ejercer funciones delegadas por la CGR conducentes al cumplimiento de su misión y visión institucional.

- Implementar estrategias de relacionamiento con los grupos de valor y demás partes interesadas con los cuales la Entidad tenga relaciones contractuales o legales.

- Realizar invitaciones a eventos, mejorar servicios u ofertar nuevos trámites y servicios, y todas aquellas actividades asociadas a la misión y visión de la CGR.

- Gestionar trámites (peticiones, solicitudes, quejas, reclamos) y efectuar encuestas de satisfacción respecto de los trámites y servicios ofrecidos por la CGR.

- Dar a conocer, transferir o trasmitir datos personales, dentro y fuera del país, a las filiales o subsidiarias de la CGR o a terceros a consecuencia de un contrato, ley o vínculo lícito que así lo requiera o para implementar servicios de computación en la nube u otros servicios específicos.

- Conocer, almacenar y procesar toda la información suministrada por los Titulares de datos en una o varias bases de datos, en el formato que estime más conveniente de acuerdo a la naturaleza del negocio, la finalidad de la recolección y el responsable del tratamiento.

- Realizar todas las gestiones de orden tributario, contable, fiscal y de facturación, donde sea aplicable.

Los datos que se recolecten o almacenen sobre los contratistas de la CGR mediante el diligenciamiento de formatos, vía telefónica, o con la entrega de documentos (hojas de vida, anexos) serán tratados para todo lo relacionado con cuestiones laborales de orden legal o contractual. En virtud de lo anterior, la CGR utilizará los datos personales para los siguientes fines:

- Dar cumplimiento en lo que le aplique, a las leyes como, entre otras, de derecho laboral, seguridad social, pensiones, riesgos profesionales, cajas de compensación familiar (Sistema Integral de Seguridad Social) e impuestos;

- Cumplir las instrucciones de las autoridades judiciales y administrativas competentes;

- Implementar las políticas y estrategias necesarias para el tratamiento de la información.

Además de lo anterior, los datos también podrán tratarse para las siguientes finalidades:

- Ordenar, catalogar, clasificar, dividir o separar la información suministrada por los Titulares de datos.

- Verificar, corroborar, comprobar, validar, investigar o comparar la información suministrada por los Titulares de datos, con cualquier información de que disponga legítimamente.

- Acceder, consultar, comparar y evaluar toda la información que sobre el Titular se encuentre almacenada en las bases de datos de antecedentes judiciales, fiscales, disciplinarios o de seguridad, de naturaleza estatal o privada, nacional o extranjera, o cualquier base de datos pública o privada cuando la constitución o la ley así lo requiera.

- Para fines de seguridad de las personas, los bienes e instalaciones de la CGR, podrán ser utilizados como prueba en cualquier tipo de proceso, los datos personales que sean: (i) recolectados directamente en los puntos de seguridad, (ii) tomados de los documentos que suministran los Titulares al personal de seguridad y, (iii) obtenidos de las videograbaciones que se realizan dentro o fuera de las instalaciones de la CGR.

Los datos personales relacionados con la salud son considerados datos sensibles, razón por la cual es facultativo por parte del Titular gestionar y proporcionar esta información, recordando que ostenta el control sobre el tratamiento de dichos datos y, en cualquier momento, podrá solicitar su corrección, actualización o supresión mediante las diferentes herramientas y canales de la CGR, quien solo tratará estos datos sensibles con el fin de:

- Ejercer control sobre el estado de salud del personal a su cargo, contratistas, subcontratistas o usuarios con ocasión de eventos o situaciones específicas que así lo ameriten.

- Para llevar a cabo un trámite específico que así lo requiera, previa autorización expresa del Titular de la Información.

- Suministrarlos cuando lo requiera una autoridad competente en ejercicio de sus funciones.

- Tratamiento de datos biométricos: La CGR podrá recolectar información personal biométrica como huellas, fotografías del rostro (*selfi*), iris, voz, firma, reconocimiento facial o rasgos morfológicos, entre otros, (en adelante los "datos biométricos") con el fin de permitir la identificación de los usuarios o Titulares, conforme a los parámetros de seguridad establecidos en la regulación, las buenas prácticas y las señaladas por las autoridades. Estos datos biométricos son considerados por la regulación colombiana como datos sensibles.

La recolección de esta información se hace en cumplimiento de obligaciones legales como la señalada en el artículo 2.2.17.6.6. del Decreto 1413 de 2017:

> *"**Artículo 2.2.17.6.6. Seguridad de la Información.** Los actores que traten información, en el marco del presente título, deberán adoptar las medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información."*

Unido a lo anterior, el Ministerio de Tecnologías de la Información y las Comunicaciones ha recomendado la implementación de la identificación biométrica como un mecanismo de seguridad de la información, así :

a. *"Las empresas deben identificar sus vulnerabilidades e implementar medidas de protección. Desarrollar una cultura de seguridad y una política de seguridad corporativa.*

b. *Establecer la mentalidad de que la seguridad debe ser prioridad*

c. Implementar análisis de datos para proteger información confidencial (establecer maneras automatizadas para analizar y monitorear grandes volúmenes de datos)

d. Gestionar identidades y autorizaciones

e. Aprovechar las capacidades integradas de los dispositivos móviles (autenticación avanzada por medio de técnicas biométricas de reconocimiento de voz, firma y reconocimiento facial)

f. Monitoreo y evaluación continua

g. Aislar y ocultar dispositivos terminales[16]"

En cumplimiento del artículo 6 del Decreto 1377 de 2013, los usuarios o Titulares no estarán obligados, de ninguna manera, a suministrar sus datos biométricos conforme a lo acá dispuesto. En aquellos casos en que los Titulares opten por no autorizar el uso y Tratamiento de sus datos biométricos a la CGR, conforme la presente política, es claro que la Entidad no podrá permitir el acceso y uso de ciertos servicios a las personas que se nieguen a proveer sus datos biométricos.

Asimismo, en la **CGR,** se informa que no toda fotografía o huella es considerada como un dato biométrico y sensible. En coherencia con el Concepto con número de radicación 17-299565-2 de La Superintendencia de Industria y Comercio precisó lo anterior:

> *"Los datos personales como la huella dactilar y las imágenes de los Titulares se consideran datos biométricos y de carácter sensible cuando son tratados por medios técnicos específicos que permitan la identificación o la autenticación unívoca de una persona física. De lo contrario, se tratará de datos personales de carácter privado."*

Por lo tanto, la recolección y tratamiento de imágenes que no sean consideradas como datos biométricos, serán tratados conforme a las finalidades generales señaladas en esta Política y no les serán aplicables las disposiciones específicas sobre datos sensibles.

6. Derechos de los Titulares de los Datos

Los Titulares de la información tienen derecho a:

- Acceder, rectificar, cancelar, u oponerse a la autorización para que se efectúe el tratamiento de sus datos personales.
- Conocer, actualizar y rectificar los datos personales. Para el efecto, es necesario establecer previamente la identificación de la persona para evitar que terceros no autorizados accedan a los datos del Titular.
- Obtener copia de la autorización.
- Informarse sobre el uso que la CGR ha dado a los datos personales del Titular.

[16] Tomado de: https://www.mintic.gov.co/portal/604/w3-article-15301.html

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

- Acceder a la solicitud de revocatoria de la autorización o supresión del dato personal cuando la autoridad delegada para la verificación del cumplimiento de la ley haya determinado que en el tratamiento por parte de la CGR se ha incurrido en conductas contrarias a la ley 1581 de 2012 o a la Constitución.

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

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

- Acceder en forma gratuita a sus datos personales. La información solicitada por el Titular podrá ser suministrada por cualquier medio, incluyendo los electrónicos.

7. Deberes de la Contraloría General de la República cuando Obra como Responsable del Tratamiento de Datos Personales

La presente política tiene además como propósito informar y dar a conocer a los titulares de la información los deberes que están a cargo de la CGR**,** razón por la cual se encuentra disponible en el sitio web de la Entidad, https://www.contraloria.gov.co.

Quienes estén sujetos a cumplir esta política deben tener presente que la CGR está obligada a cumplir los siguientes deberes impuestos por la ley:

7.1 Deberes de la Contraloría General de la República respecto del Titular del dato personal

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data, es decir, a conocer, actualizar o rectificar sus datos personales.

- Solicitar y conservar, en las condiciones previstas en el numeral 9 de esta política, copia de la respectiva autorización otorgada por el Titular.

- Informar al Titular, de manera clara y suficiente, sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

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

- Tramitar las consultas y reclamos formulados en los términos señalados en el numeral 14 de la presente política.

7.2 Deberes de la Contraloría General de la República respecto de la calidad, seguridad y confidencialidad de los datos personales

- Observar los principios de veracidad, calidad, seguridad y confidencialidad en los términos establecidos en el numeral 4 de esta política.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Actualizar la información cuando sea necesario.
- Rectificar los datos personales cuando ello sea procedente.
- Anonimizar los datos personales de los Titulares siempre que estos sean de carácter semiprivados, privados o sensibles, así como los datos de cualquier categoría de los niños, niñas y adolescentes.

7.3 Deberes de la Contraloría General de la República cuando realiza el tratamiento a través de un Encargado

- Suministrar al Encargado del tratamiento únicamente los datos personales cuyo tratamiento esté previamente autorizado.
- Garantizar que la información que se suministre al Encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Comunicar al Encargado del tratamiento, de forma oportuna, 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.
- Comunicar al Encargado del tratamiento, de manera oportuna, las rectificaciones realizadas sobre los datos personales para que éste proceda a realizar los ajustes pertinentes.
- Exigir al Encargado del tratamiento, en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- Informar al Encargado del tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

7.4 Deberes de la Contraloría General de la República respecto de la autoridad delegada para la verificación del cumplimiento de la ley

- Informar a la Superintendencia de Industria y Comercio y a la Procuraduría General de la Nación 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 y la Procuraduría General de la Nación.

8. Deberes de la Contraloría General de la República cuando Obra como Encargado del Tratamiento de Datos Personales

Si la CGR realiza el tratamiento de datos en nombre de otra entidad u organización (Responsable del Tratamiento) deberá cumplir los siguientes deberes:

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Realizar oportunamente la actualización, rectificación o supresión de los datos.
- Actualizar la información reportada por los Responsables del tratamiento dentro de los cinco (05) días hábiles contados a partir de su recibo.
- Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente política.
- Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se establece en el numeral 14.2 de la presente política.
- Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
- Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Procuraduría General de la Nación, o por autoridad judicial.
- Permitir el acceso a la información únicamente a las personas autorizadas por el Titular o facultadas por la ley para dicho efecto.
- Informar a la Superintendencia de Industria y Comercio y a la Procuraduría General de la Nación 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, la Procuraduría General de la Nación, o autoridad judicial.

9. De la Autorización

9.1 Autorización para tratamiento de datos

Los obligados a cumplir esta política deberán obtener de parte del Titular su autorización previa, expresa e informada para recolectar y tratar sus datos personales. Esta obligación no es necesaria cuando se trate de datos de naturaleza pública.

Para obtener la autorización se deberá seguir las siguientes instrucciones:

En primer lugar, antes de que la persona autorice es necesario informarle de forma clara y expresa lo siguiente:

- El tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
- El carácter facultativo de la respuesta a las preguntas que le sean formuladas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.
- Los derechos que le asisten como Titular, previstos en el artículo 8 de la ley 1581 de 2012.
- La identificación, dirección física o electrónica de la CGR.

En segundo lugar, obtendrá el consentimiento del Titular a través de cualquier medio que pueda ser objeto de consulta posterior, tal como página web, formularios, formatos, actividades, presenciales o en redes sociales, PQRS, mensajes de datos o Apps.

Se deberá dejar prueba del cumplimiento de la obligación de informar, así como del consentimiento.

La autorización también podrá obtenerse a partir de conducta(s) inequívoca(s) del Titular del dato que permita(n) concluir, de manera razonable, que éste otorgó su consentimiento para el tratamiento de su información. Dichas) conducta(s) debe(n) ser muy clara(s), de manera que no admita(n) duda o equivocación sobre la voluntad de autorizar el tratamiento.

9.2 Autorización para tratamiento de datos sensibles

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

- La autorización debe ser explícita o mediante conductas inequívocas claras, específicas y comprobables.
- Se debe informar al Titular que no está obligado a autorizar el tratamiento de dicha información.
- Se debe informar de forma explícita y previa al Titular cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad de dicho tratamiento.

Con respecto del tratamiento de datos sensibles, para el caso de la CGR, podrá hacer tratamiento atendiendo lo previsto en los siguientes escenarios:

- El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares[17].

- La información sea requerida por autoridades públicas en ejercicio de sus funciones legales o por orden judicial[18].

- La información sea suministrada a las autoridades públicas en ejercicio de sus funciones legales o por orden judicial[19].

- Podrá acceder a información amparada por reserva legal, incluida la relacionada con datos personales[20].

9.3 Autorización de tratamiento de datos de niños, niñas y adolescentes (NNA)[21]

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

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

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

10. Seguridad

La CGR adoptará las medidas técnicas, físicas, legales, humanas, administrativas y organizativas correspondientes, que guarden relación con las leyes de privacidad y seguridad de los datos personales para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Si los Titulares consideran que su interacción con la CGR ya no es segura (por ejemplo, si creen que la seguridad de su información personal podría estar comprometida), deberán notificar inmediatamente a la CGR a través de los canales de atención indicados en el numeral 15 de la presente Política.

Cuando la CGR transmita o transfiera información personal a un proveedor de bienes y/o servicios, el cual deberá contar con las medidas adecuadas para proteger la confidencialidad y seguridad de la información personal.

[17] Literal e) del artículo 6 de la Ley Estatutaria 1581 de 2012.
[18] Literal a) del Artículo 10 de la Ley Estatutaria 1581 de 2012.
[19] Literal b) del Artículo 13 de la Ley Estatutaria 1581 de 2012.
[20] Artículo 267 de la Constitución Política, artículo 136 de la Ley 1955 de 2019, artículo 3, literal k) y el artículo 90 del Decreto 403 de 2020
[21] Artículo 12 del Decreto 1377 de 2013.

11. Retención de Información Personal

La CGR adopta medidas razonables para garantizar que la información personal sea confiable para el uso pretendido, preciso y completo, según sea necesario, para llevar a cabo los fines descritos en el numeral 5 de esta Política de Tratamiento de Datos Personales. La Entidad mantendrá la información personal de los Titulares durante el período de tiempo que sea necesario para cumplir con los fines establecidos en esta política, salvo que la ley vigente exija o permita un periodo de retención mayor.

12. Transferencia Nacional o Internacional de Datos Personales

La CGR podrá realizar la transferencia de datos a otros Responsables del tratamiento cuando así esté autorizado por el Titular de la información, por la ley o por un mandato administrativo o judicial.

13. Transmisiones Nacionales o Internacionales de Datos a Encargados del Tratamiento

La CGR podrá enviar o transmitir datos a uno o varios Encargados del Tratamiento ubicados dentro o fuera del territorio de la República de Colombia en los siguientes casos:

- Cuando cuente con autorización de Titular.
- Cuando, sin contar con la autorización del Titular, exista entre el Responsable del Tratamiento y el Encargado del Tratamiento un contrato o acuerdo de transmisión de datos[22].

14. Ejercicio de los Derechos de los Titulares

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

Los derechos de los Titulares a conocer, actualizar, rectificar o suprimir información o revocar la autorización podrán ejercerse por las siguientes personas, legitimadas de conformidad con el artículo 2.2.2.25.4.1 del Decreto Único Reglamentario 1074 de 2015[23].

- Por el Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición la CGR.
- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante o apoderado del Titular, previa acreditación de la representación o apoderamiento.

[22] Literal e) del artículo 26 de la Ley 1581 del 2012.
[23] Modificó lo dispuesto por el artículo 20 del Decreto 1377 de 2013.

- Por estipulación a favor de otro o para otro.

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

Todas las consultas y reclamos a la CGR se podrán realizar a través de los siguientes mecanismos:

- Correo electrónico cgr@contraloria.gov.co
- En la siguiente dirección física: Avenida Carrera 69 No 44 – 35. Piso 1, Bogotá D.C., Colombia.

Estas son las pautas para atender consultas y reclamos:

14.1 Consultas

Todas las consultas que realicen las personas legitimadas para conocer los datos personales que reposen en la CGR se canalizarán **EXCLUSIVAMENTE** a través de los canales que la Entidad tiene destinados para el efecto, correo electrónico cgr@contraloria.gov.co, y dirección física Avenida Carrera 69 No. 44 – 35, Bogotá, Colombia. En todo caso, es necesario dejar prueba de lo siguiente:

- Fecha de recibo de la consulta.
- Identidad del solicitante.
- Datos de contacto y notificación del solicitante.

Una vez verificada la identidad del Titular, se le suministrarán los datos personales requeridos. La respuesta a la consulta deberá comunicarse al solicitante en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.[24]

14.2 Reclamos

Los reclamos tienen por objeto corregir, actualizar, o suprimir datos o elevar una queja por el presunto incumplimiento de cualquiera de los deberes establecidos para el régimen de protección de datos personales y en esta política.

En todo caso, el trámite de respuesta tendrá el seguimiento del Oficial de Protección de Datos Personales de la CGR, a quien se podrá acudir directamente cuando la respuesta que brinde la dependencia directamente concernida con el asunto sea negativa a los intereses del peticionario.

[24] Artículo 14 de la Ley 1581 de 2012.

El reclamo debe presentarse mediante solicitud dirigida a la **Contraloría General de la República – Protección de Datos Personales** que contenga la siguiente información:

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

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo para que subsane las fallas, complemente o aclare su solicitud. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.[25]

Si el reclamo está completo o cuando se complete en el evento en que no lo haya estado inicialmente, se incluirá en la base de datos o sistema de información una leyenda que diga "*reclamo en trámite*", así como el motivo del mismo, en un término no mayor a dos (2) días hábiles. Ésta deberá mantenerse hasta que el reclamo sea decidido.

El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual, en ningún caso, podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

15. Dependencia Oficial de Protección de Datos Personales de la CGR.

La Unidad de Seguridad y Aseguramiento Tecnológico e Informático - USATI es la dependencia designada por la Resolución Organizacional OGZ-0765-2020, como Oficial de Protección de Datos Personales en la CGR y, por tanto, la encargada de velar por la protección al ejercicio del derecho de habeas data por parte de los titulares de los datos personales, a quien se puede contactar a través de email cgr@contraloria.gov.co

16. Videovigilancia

La CGR utiliza sistemas de videovigilancia instalados en diferentes sitios, internos y externos de nuestras instalaciones ubicadas en las distintas sedes de la Entidad, como lo son la Sede Principal, ubicada en la Avenida Carrera 69 No. 44 – 35 en Bogotá D. C., Colombia, y las Gerencias Departamentales Colegiadas ubicadas en las ciudades capitales de los departamentos de la República de Colombia, excepto en el departamento de Cundinamarca[26].

[25] Articulo 15 de la Ley 1581 de 2012.
[26] https://www.contraloria.gov.co/web/guest/directorio-de-dependencias

La CGR informa sobre la existencia de estos mecanismos mediante la difusión, en sitios visibles, de anuncios de videovigilancia, principalmente en los accesos peatonales y vehiculares de sus instalaciones.

La información recolectada se utilizará para fines de seguridad de las personas, los bienes e instalaciones, el cumplimiento de disposiciones legales y el cumplimiento de disposiciones contractuales. Esta información puede ser empleada como prueba en cualquier tipo de proceso ante cualquier tipo de autoridad y organización.

17. Vigencia de la Política de Tratamientos de Datos Personales de la Contraloría General de la República y de la Base de Datos

Esta Política tiene vigencia desde la fecha de su publicación en el Portal Institucional de la CGR, por parte de la Oficina de Comunicaciones y Publicaciones; y de la comunicación acerca de su publicación en el aplicativo SIGECI, por parte de la Dirección de la Oficina de Planeación a los servidores públicos y contratistas de prestación de servicios de la CGR.

La vigencia de la base de datos personales será el tiempo razonable y necesario para cumplir las finalidades del tratamiento, teniendo en cuenta lo dispuesto en el artículo 2.2.2.25.2.8 del Decreto Único Reglamentario 1074 de 2015[27].

18. Datos del Responsable del Tratamiento

Razón social: CONTRALORÍA GENERAL DE LA REPÚBLICA

Dirección: Avenida Carrera 69 No. 44 - 35 Bogotá D.C., Colombia

Correo Electrónico: cgr@contraloria.gov.co

Teléfono: en Bogotá (57-601) 518 7000

Página web: www.contraloria.gov.co

[27] Modificado por el artículo 11 del Decreto 1377 de 2013.

Elaborado por el (los) servidor(es)	Presentado por el Directivo:	Aprobador por:	Validado en el contexto del SIGECI por (Servidor(es) del GTSIGECI)	Validación en el contexto del SIGECI revisada por (Líder del GTSIGECI)	Validación en el contexto del SIGECI aprobada por (Administrador del SIGECI)
Jairo Hernán Barragán Gómez, Unidad de Seguridad y Aseguramiento Tecnológico e Informático – USATI. Diana Patricia Murillo Calderón, Unidad de Seguridad y Aseguramiento Tecnológico e Informático – USATI.	José Antonio Poveda Montes Jefe de Unidad de Seguridad y Aseguramiento Tecnológico e Informático – USATI.	Líder de Proceso Gestión Integral de Seguridad: Margarita María Márquez Figueroa, Directora de la Unidad de Seguridad y Aseguramiento Tecnológico e Informático – USATI. Líder del Macroproceso de Gestión de Riesgo, Seguridad y Continuidad del Negocio: José Antonio Poveda Montes, Jefe de Unidad de Seguridad y Aseguramiento Tecnológico e Informático – USATI y Vanessa Varón Garrido, Directora Oficina de Planeación.	Paola Tatiana Tovar, Contratista de la Oficina de Planeación.	José Neheman Gómez Lozada, Asesor de Gestión de la Oficina de Planeación.	Vanessa Varón Garrido, Directora Oficina de Planeación.