RESOLUCIÓN ORGANIZACIONAL OGZ-0531-2016 DE 2016

(diciembre 28)

Diario Oficial No. 50.103 de 31 de diciembre de 2016

CONTRALORÍA GENERAL DE LA REPÚBLICA

Por la cual se crea el Sistema de Gestión de Seguridad, se crea el Comité de Seguridad de la Contraloría General de la República, se adopta la política general de seguridad, la política de seguridad y privacidad de la información, la política de tratamiento de datos personales y se dictan otras disposiciones.

EL CONTRALOR GENERAL DE LA REPÚBLICA,

en ejercicio de sus facultades constitucionales y legales, y de conformidad con las normas consagradas en los artículos 2o, 119, 267 y 268 de la Constitución Política de Colombia, la Ley 1474 de 2011, en especial las consagradas en los numerales 2 y 4 del artículo 35 del Decreto-ley número 267 de 2000 y,

CONSIDERANDO:

Que el numeral 2 del artículo 35 del Decreto-ley número 267 de 2000 faculta al Contralor General de la República para adoptar las políticas, planes, programas y estrategias necesarias para el adecuado manejo administrativo de la Contraloría General de la República.

Que el numeral 4 del artículo 35 del Decreto-ley número 267 de 2000 asigna al Contralor General de la República la función de dirigir como autoridad superior las labores administrativas de las diferentes dependencias de la Contraloría General de la República, de acuerdo con la ley.

Que el artículo 76 del Decreto-ley número 267 de 2000 faculta al Contralor General de la República para reglamentar consejos, comités, comisiones y juntas, "…tanto para los órganos de creación legal como para los que él decida conformar para suplir las necesidades del servicio".

Que el artículo 128 de la Ley 1474 de 2011 crea la Unidad de Seguridad y Aseguramiento Tecnológico e Informático de la Contraloría General de la República con la finalidad de prestar apoyo profesional y técnico para la formulación y ejecución de las políticas y programas de seguridad de los servidores públicos, de los bienes y de la información de la entidad; llevar el inventario y garantizar el uso adecuado y mantenimiento de los equipos de seguridad adquiridos o administrados por la Contraloría; promover la celebración de convenios con entidades u organismos nacionales e internacionales para garantizar la protección de las personas, la custodia de los bienes y la confidencialidad e integridad de los datos manejados por la institución.

Que en el numeral 1 del artículo 4o de la Resolución Reglamentaria número 0205 de 2012 de la Contraloría General de la República, establece dentro de las funciones de la Unidad de Seguridad y Aseguramiento Tecnológico e Informático, la de dirigir y adoptar las políticas, planes, programas y estrategias para el desarrollo de la seguridad y aseguramiento tecnológico en el cumplimiento de la misión organizacional de la Contraloría General de la República.

Que la utilización de tecnología en el procesamiento, almacenamiento, recuperación y transmisión de la información, implica importantes riesgos de seguridad en cuanto a disponibilidad, confidencialidad e integridad, por lo que la Contraloría General de la República

debe asegurar tales atributos en su información institucional en el cumplimiento de sus funciones constitucionales y legales.

Que mediante el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones número 1078 de 2015, se definieron los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea.

Que el numeral 4 del artículo 2.2.9.1.2.1, del Decreto número 1078 de 2015 establece como uno de los cuatro componentes de la estrategia de Gobierno en Línea, la Seguridad y Privacidad de la Información.

Que los objetivos del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, son:

1. Contribuir al incremento de la transparencia en la gestión pública.

2. Dar lineamiento para la implementación de la gestión de la seguridad y privacidad de la información, en las entidades del Estado.

3. Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de ciberseguridad en la entidad.

4. Alinear el marco de referencia de arquitectura empresarial con los principios de seguridad y privacidad de la información.

Que el parágrafo del artículo 2.2.9.1.1.2 del Decreto número 1078 de 2015, establece que la implementación de la estrategia de Gobierno en Línea en los órganos de control, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en el artículo 209 de la Constitución Política.

Que el artículo 2o, del Título I, de la Ley Estatutaria 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales, establece que “los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública…” se regirán por los principios y disposiciones contenidos en dicha normatividad.

Que a su vez el literal g), del artículo 4o, del Título II de la Ley Estatutaria 1581 de 2012 establece el principio de seguridad como principio rector en materia de tratamiento de datos personales, por lo que los mismos se deben 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.

Que el literal a) del artículo 5o, del Título I de la Ley 1712 de 2014, “por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional”, establece la calidad de sujeto obligado de toda entidad pública y por ende el deber de regirse por los principios y disposiciones que regulan el derecho de acceso a la información pública.

Que el artículo 2o, del Título I, de la Ley 1712 de 2014, establece el principio de máxima publicidad para el titular universal, según el cual toda información en posesión, bajo control o custodia de un sujeto obligado se considera pública y no podrá ser reservada o limitada sino por disposición constitucional o legal.

Que en cumplimiento de la regulación en materia de tratamiento de datos personales y del derecho de acceso a la información pública se pueden presentar conflictos jurídicos y riesgos de seguridad, en la protección de dichos derechos, así como en la garantía de disponibilidad, confidencialidad e integridad de la información al interior de la Entidad; por lo que la Contraloría General de la República debe establecer las políticas, procedimientos, mecanismos y demás métodos requeridos en el cumplimiento de sus funciones constitucionales y legales.

Que el Plan Estratégico 2014-2018 “Control fiscal eficaz para una mejor gestión pública” contempla en su objetivo corporativo 5, “Asegurar el funcionamiento y la organización de la CGR para lograr resultados”, el producto 16 “Plan de fortalecimiento de Seguridad Física y Tecnológica”.

Que el Código de Buen Gobierno de la Contraloría General de la República adoptado mediante Resolución Organizacional OGZ 350 de diciembre de 2015, establece políticas generales en donde la alta dirección manifiesta su compromiso con aspectos relacionados con la seguridad, tales como: Compromiso frente a la Administración de Riesgos, Compromiso frente a Gobierno en Línea, Compromiso frente a la Gestión Documental, Compromiso frente a la Seguridad de la Información y Compromiso frente a la Confidencialidad de la Información.

Que con el fin de dar cumplimiento a las anteriores previsiones y a lo ordenado por la Ley 87 de 1993, artículo 2o, en cuanto a la protección de los recursos de la entidad, buscando su adecuada administración ante posibles riesgos que la afecten, así como la definición y aplicación de medidas para prevenir los riesgos; detectar y corregir las desviaciones que se presentan en la entidad y que puedan afectar el logro de sus objetivos, se hace necesario disponer lo pertinente al interior de la entidad.

Que los numerales 5 y 21 del artículo 34, de la Ley 734 de 2002, Código Único Disciplinario, establece el deber de los servidores públicos de custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos; así como, el de vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a que han sido destinados.

Que en el Capítulo 2o, Título 1o, Parte 4o, Libro 2o del Decreto número 1066 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector Administrativo del Interior, y en cuyo contenido se organiza el Programa de Prevención y Protección de los derechos a la vida, la libertad, la integridad y la seguridad de personas, grupos y comunidades del Ministerio del Interior y de la Unidad Nacional de Protección, establece que todos los servidores públicos pondrán en conocimiento de la Unidad Nacional de Protección y las demás entidades competentes, las situaciones de riesgo o amenaza contra las personas, de manera urgente, por medio físico, vía telefónica o correo electrónico, con el fin de activar los procedimientos establecidos en los programas de protección o para el despliegue de actividades tendientes a garantizar la seguridad de las personas por parte de la Fuerza Pública.

En mérito de lo expuesto;

RESUELVE:

ARTÍCULO 1o. SISTEMA DE GESTIÓN DE SEGURIDAD. Créase el Sistema de Gestión de Seguridad, a cargo de la Unidad de Seguridad y Aseguramiento Tecnológico e Informático, a

través del cual se administrará y publicará la documentación, con carácter público, relativa a la seguridad de personas, bienes e información, conformada por políticas, normas, guías, instructivos, formatos, listas de chequeo y todos los demás que sean pertinentes.

PARÁGRAFO. En relación con la documentación de procedimientos sobre seguridad y aseguramiento tecnológico e informático, la preparación de propuestas de creación, actualización y eliminación, su presentación formal a la Oficina de Planeación para su revisión como Administradora del SIGCC, validación si procede desde el punto de vista del SIGCC y su publicación en el Aplicativo SIGCC, se cumplirán de conformidad Resolución Reglamentaria número 109 de julio 23/10 y procedimiento de mejora vigente publicado en el SIGCC.

ARTÍCULO 2o. CREACIÓN DEL COMITÉ DE SEGURIDAD. Créase el Comité de Seguridad de la Contraloría General de la República.

ARTÍCULO 3o. CONFORMACIÓN DEL COMITÉ DE SEGURIDAD. El Comité de Seguridad de la Contraloría General de la República estará conformado por:

1. El Contralor General de la República o su delegado.

2. El Jefe de la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (USATI).

3. El Gerente Administrativo y Financiero o su delegado.

4. El Director de la Oficina de Sistemas e Informática o su delegado.

5. El Gerente de Talento Humano o su delegado.

6. El Director de la Oficina de Planeación o su delegado.

PARÁGRAFO 1o. Será invitado permanente al Comité, con voz pero sin voto, un representante de la Oficina de Control Interno.

PARÁGRAFO 2o. El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

PARÁGRAFO 3o. Los servidores públicos de la Contraloría General de la República que asistan al Comité de Seguridad en calidad de delegados de sus jefes inmediatos deberán presentar ante el Comité, el documento que los acredite para participar en las decisiones que se tomen al respecto.

PARÁGRAFO 4o. La documentación aprobada por el Comité de Seguridad tendrá carácter vinculante a partir de su comunicación.

ARTÍCULO 4o. FUNCIONES DEL COMITÉ DE SEGURIDAD. Serán funciones del Comité de Seguridad las siguientes:

1. Recomendar para su aprobación, las políticas de seguridad, sus cambios y las responsabilidades generales en materia de seguridad.

2. Aprobar las normas técnicas, los controles, tecnologías, metodologías y demás documentos relativos al Sistema de Gestión de seguridad.

3. Apoyar las campañas de sensibilización en temas de seguridad dentro de la Entidad.

4. Evaluar y proponer a la alta dirección, iniciativas de inversión que permitan fortalecer las medidas de seguridad de la Entidad.

5. Adoptar los indicadores de gestión de seguridad.

6. Monitorear, analizar, garantizar el control y mitigación de incidentes de seguridad presentados en la entidad.

ARTÍCULO 5o. SECRETARÍA TÉCNICA DEL COMITÉ DE SEGURIDAD. La Secretaría Técnica del Comité de Seguridad de la Contraloría General de la República estará a cargo del Director de Seguridad y Aseguramiento Tecnológico e Informático (USATI). La Secretaría Técnica del Comité deberá cumplir con las siguientes funciones:

1. Convocar a los miembros del Comité e invitados a las sesiones ordinarias y extraordinarias, con la debida antelación.

2. Preparar el orden del día de las sesiones del Comité, remitiendo a los miembros e invitados a la sesión, a través de cualquier medio y dejando constancia de los envíos, la agenda de trabajo y los documentos que deban analizarse.

3. Elaborar para la firma de los miembros del Comité la(s) acta(s) de la(s) sesión(es) anterior(es), que será(n) sometida(s) a la aprobación y suscripción de los mismos, como primer punto del orden del día en cada sesión.

4. Preparar los informes que soliciten los miembros del Comité para el estudio de los asuntos de su competencia y/o aquellos que se soliciten de forma externa sobre las actividades del mismo. En este sentido, la Secretaría podrá solicitar la información que requiera a las diferentes dependencias y servidores o contratistas de la Entidad.

5. Preparar los informes del estado de la seguridad y la efectividad de los controles de la seguridad para realizar la revisión periódica para asegurar que la definición de políticas de seguridad permanece conforme a las necesidades de la Entidad y se identifican mejoras sobre el mismo.

6. Llevar el archivo y custodia de las Actas y demás documentos que se produzcan en el Comité, de forma sistemática y organizada.

7. Las demás que le asigne el Comité.

ARTÍCULO 6o. SESIONES DEL COMITÉ DE SEGURIDAD. El Comité de Seguridad de la Contraloría General de la República sesionará de manera ordinaria una vez (1) cada semestre y extraordinariamente cuando se estime pertinente, por convocatoria de la Secretaria Técnica.

ARTÍCULO 7o. ADOPCIÓN DE POLÍTICAS. Mediante la presente resolución se adopta la Política general de seguridad identificada con Código SGS-PO-001 versión 1.0, la Política de seguridad y privacidad de la información identificada con código SGS-I-A5-PO-001 versión 1.0 y la Política de tratamiento de datos personales de la Contraloría General de la República identificada con Código SGS-I-A18-PO-001.

ARTÍCULO 8o. VIGENCIA Y DEROGATORIA. La presente Resolución rige a partir de la fecha de su publicación y deroga todas las disposiciones que le sean contrarias.

Comuníquese, publíquese y cúmplase.

Dada en Bogotá D. C., a 28 de diciembre de 2016.

El Contralor General de la República,

EDGARDO JOSÉ MAYA VILLAZÓN.

SISTEMA DE GESTIÓN DE SEGURIDAD.

POLÍTICA GENERAL DE SEGURIDAD.

Declaración de Política

La seguridad es uno de los procesos esenciales de la Contraloría General de la República - CGR y en su cumplimiento la Entidad se compromete a diseñar, implantar, mantener y mejorar constantemente las estrategias que aseguren, en un marco de equilibrio, el buen uso y protección de los recursos asociados al talento humano, los bienes y la información, satisfaciendo en su preservación leyes, normas, estándares y mejores prácticas nacionales e internacionales.

Ámbito de Aplicación

Todos los niveles de la administración, así como los funcionarios, contratistas, proveedores, ciudadanos y, en general, todos aquellos que tengan relación con personas, los bienes o la información de la Entidad, que dan soporte a sus procesos, son responsables de garantizar la confidencialidad y disponibilidad de la información así como el cuidado e integridad de los bienes, información y personas; por consiguiente, son también responsables del cumplimiento de la Política General de Seguridad enunciada en este documento.

Enunciado

En la CGR, la seguridad incluye las prácticas orientadas a establecer, evaluar y gestionar los riesgos a que se encuentran sometidos las personas, los bienes y la información de la Entidad, por lo que su ámbito de aplicación está relacionado con:

– Diseñar una estrategia de seguridad que permita a la CGR reaccionar ante las amenazas y vulnerabilidades que puedan afectar a las personas, bienes o información.

– Apoyar la gestión de la seguridad mediante el suministro de todos los recursos que fortalezcan la seguridad de la organización a fin de fomentar prácticas efectivas en armonía con los sistemas de gestión existentes en la Entidad.

– Asegurar que se dispone del talento humano con conocimientos y capacitación suficientes para poner en práctica las estrategias y procesos de seguridad definidos.

– Obtener la trazabilidad de las acciones de todas las partes interesadas a fin de monitorear, analizar, documentar y decidir sobre todas las actividades realizadas por las mismas, orientadas a preservar la seguridad.

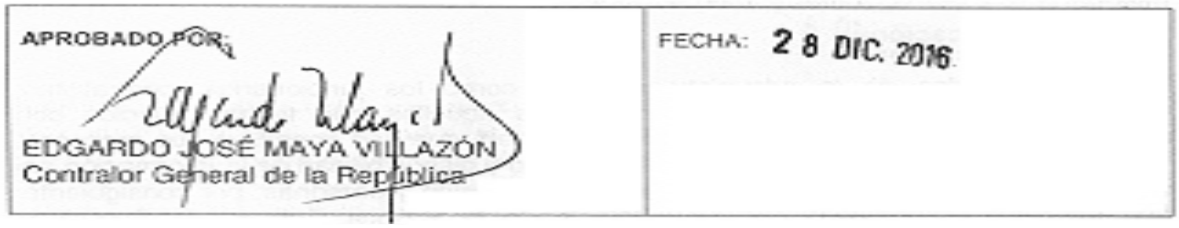
– Establecer y medir la eficacia de la seguridad con respecto a los indicadores definidos por la Entidad en el marco de los sistemas de gestión implementados.

– Mejorar continuamente la eficacia de la seguridad mediante un proceso de gestión que asegure que se adoptan las medidas de seguridad pertinentes.

El incumplimiento de esta Política traerá consigo las consecuencias legales, establecidas en el ordenamiento jurídico vigente, en lo que respecta a seguridad.

Vigencia

El presente documento rige a partir de su aprobación, comunicación y publicación.



SISTEMA DE GESTIÓN DE SEGURIDAD

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Declaración de Política

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la Contraloría General de la República con respecto a la protección de los activos de información de la Entidad.

La seguridad de la información está relacionada con el cumplimiento de las siguientes dimensiones de la información:

- Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidad o procesos no autorizados.

- Integridad: Propiedad de salvaguardar la exactitud y completitud de los activos de información.

- Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de un individuo, entidad o proceso debidamente autorizado.

Ámbito de Aplicación Todos los niveles de la administración así como los funcionarios, contratistas, proveedores, ciudadanos y en general todos aquellos que tengan relación con las fuentes, recursos y tecnologías de información (incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la generación, procesamiento y entrega de la información, quienes son responsables de mantener la confidencialidad, integridad y disponibilidad de la misma.

Por tanto son también responsables del cumplimiento de la Política de Seguridad y Privacidad de la Información.

Enunciado

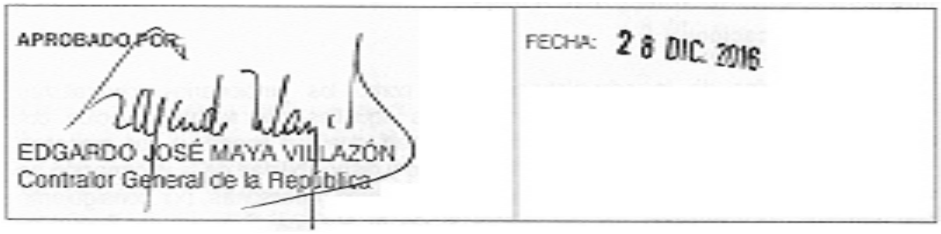
En la CGR la información constituye el activo principal para la prestación de los servicios y la

toma de decisiones, razón por la cual existe una política de seguridad orientada a protegerla a fin de garantizar la continuidad de la operación en el marco de una cultura de seguridad tendiente a administrar el riesgo operacional. Por tanto la Entidad debe elaborar, implantar, mantener y mejorar constantemente las estrategias de seguridad existentes con una asignación equilibrada de recursos dirigidos a lograr el nivel más elevado de la seguridad con la aplicación de normas nacionales e internacionales.

El incumplimiento de esta Política traerá consigo las consecuencias legales, establecidas en el ordenamiento jurídico vigente, en lo que respecta a seguridad y privacidad de la información.

Vigencia

El presente documento rige a partir de su aprobación, comunicación y publicación.



SISTEMA DE GESTIÓN DE SEGURIDAD.

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Conforme al artículo 128 de la Ley 1474 de 2011, Estatuto Anticorrupción, y el artículo 4o de la Resolución Reglamentaria número 205 de 2012, la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (USATI) de la Contraloría General de la República (CGR) es la encargada de prestar el apoyo profesional y técnico para formulación y ejecución de políticas y programas de seguridad de la información de la entidad, así, como la de garantizar la confidencialidad e integridad de los datos manejados por la institución.

En cumplimiento de la Ley Estatutaria 1581 de 2012 y su Decreto Reglamentario número 1377 de 2013, la CGR adopta la presente política para el tratamiento de datos personales, la cual será informada a todos los titulares de los datos recolectados o que en el futuro se obtengan en el ejercicio de las funciones y competencias de la Contraloría General de la República, en cumplimiento de la misión de esta.

Por lo anterior, el marco normativo que se desarrolla con esta política es el siguiente:

- Constitución Política de Colombia de 1991, artículos 15 y 20, relativos a derecho constitucional de las personas a conocer, actualizar y rectificar la información que de ellas se haya recogido en bancos de datos y derecho de acceso a la información.

- Ley Estatutaria 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”.

- Ley Estatutaria 1581 de 2012, “por la cual se dictan disposiciones generales para la protección de datos personales”.

- Decreto 1377 de 2013, “por el cual se reglamenta parcialmente la Ley 1581 de 2012”.

- Decreto 886 de 2014, “por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos”.

- Ley 1712 de 2014, “por medio de la cual se crea la Ley de Transparencia y del Derecho de acceso a la Información Pública Nacional y se dictan otras disposiciones”.

- Decreto 103 de 2015, “por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”.

- Ley 734 de 2002, “por la cual se expide el Código Disciplinario Único”.

- Decreto-ley número 267 de 2000, “por el cual se dictan normas sobre organización y funcionamiento de la Contraloría General de la República, se establece su estructura orgánica, se fijan las funciones de sus dependencias y se dictan otras disposiciones”.

- Sentencia Corte Constitucional, C-748 de 6 de octubre de 2011. M. P.: Jorge Ignacio Pretelt Chaljub.

- Sentencia Corte Constitucional, C-274 de 9 de mayo de 2013. M. P.: María Victoria Calle Correa.

En la aplicación de esta política deberán observarse las excepciones del régimen de protección de datos personales, es decir, según las cuales el régimen de la Ley 1581 de 2012 no será aplicable a: (i) los archivos y las bases de datos pertenecientes al ámbito personal o doméstico; (ii) 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, (iii) los que tengan como fin y contengan información de inteligencia y contrainteligencia, (iv) los de información periodística y otros contenidos editoriales, (v) los regulados por la Ley 1266 de 2008 (información financiera y crediticia, comercial, de servicios y proveniente de terceros países) y (vi) los regulados por la Ley 79 de 1993 (sobre censos de población y vivienda). Los servidores deberán acogerse a las inhabilidades, impedimentos, incompatibilidades y conflicto de intereses contemplados en la Ley 734 de 2002 (Código Disciplinario Único, Título IV, Capítulo Cuarto) para el tratamiento de datos personales.

Que ante el ejercicio del derecho de acceso a la información pública en cabeza de la ciudadanía, se tendrá en cuenta lo anterior, y a su vez los criterios de armonización contemplados en la Ley 1712 de 2014 y sus reglamentaciones posteriores, en cada caso concreto que así lo requiera.

1. ÁMBITO DE APLICACIÓN

Esta política debe ser conocida y aplicada por todos los funcionarios y contratistas de la CGR y terceros que tengan acceso a información que contenga datos personales, como pasantes, judicantes, ciudadanos que provean o demanden servicios de la misma.

2. GLOSARIO Y SIGLAS[1]

Para la correcta interpretación y aplicación de la presente política la CGR tomará en cuenta las siguientes definiciones.

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el

tratamiento de datos personales.

Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

Para la aplicación de la presente política, debe distinguirse dos clases de bases de datos; las automatizadas, es decir, aquellas que se almacenan y administran a través de herramientas informáticas y las bases de datos manuales o archivos, donde la información se encuentra organizada o almacenada en medio físico y contienen información personal, tal como nombre, identificación, números de teléfono, correo electrónico, etc., 1 Tomado de la Ley Estatutaria 1581/123, Decreto número 1377 de 2013, Ley 1266 de 2008 y Ley 1712 de 2014.

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

Dato privado: Es el dato que por su naturaleza íntima o reservada, sólo es relevante para el titular

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

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

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Encargado del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

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

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado

de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley de Transparencia.

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

Registro Nacional de Bases de Datos (RNBD): El RNBD es el directorio público de las bases de datos sujetas a tratamiento que operan en el país; el cual es administrado por la Superintendencia de Industria y Comercio y tiene como finalidad la libre consulta por parte de los ciudadanos.

Responsable del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

Sujetos Obligados: Se refiere a cualquier persona natural o jurídica, pública o privada incluida en el artículo 5o de la Ley 1712 de 2014, corregido por el artículo 1 del Decreto Nacional 1494 de 2015, entiéndase de manera específica, la Contraloría General de la Republica y cada uno de sus funcionarios y contratistas.

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.

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera 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.

3. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES

Para el desarrollo y aplicación del tratamiento de datos personales registrados en las bases de datos y archivos de la CGR, se aplicarán los siguientes principios rectores establecidos en el artículo 4o de la Ley 1581 de 2012 y de la Ley 1712 de 2014, los cuales serán objeto de aplicación de criterios de armonización, ante la duda de su aplicabilidad o conflicto entre los mismos, en el caso concreto.

a) Principio de legalidad en materia de tratamiento de datos: En el tratamiento de datos personales de la CGR, se observarán y aplicarán lo establecido en la Ley 1581 de 2012 y demás disposiciones normativas que se desarrollen;

b) Principio de finalidad: El tratamiento de datos personales realizado en la CGR, atenderá a una finalidad legítima de acuerdo con la constitución y la ley;

c) Principio de libertad: El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular en los casos que establezca la ley. Los datos personales no podrán

ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;

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. Los sujetos obligados están en deber de proporcionar y facilitar el acceso a la información en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales o legales;

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 constitución y la ley. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la ley.

Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la ley.

g) Principio de seguridad: La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento a que se refiere la ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

h) Principio de confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley.

i) Principio de responsabilidad demostrada: Los responsables del tratamiento de datos personales deben ser capaces de demostrar, que se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y las demás disposiciones normativas que la desarrollen y complementen.

j) Principio de máxima publicidad para el titular universal: Toda información en posesión, bajo control o custodia de un sujeto obligado es publica y no podrá ser reservada o limitada sino por disposición constitucional o legal.

4. RESPONSABLE Y ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES

La CGR es la responsable del tratamiento de datos personales, registrados en forma presencial (Avenida Carrera 69 número 44-35. Bogotá) o virtual (www.contraloria.gov.co), en bases de datos personales de la Entidad.

Los encargados del tratamiento de los datos personales son los servidores públicos y contratistas

de la CGR que en cumplimiento de sus funciones realicen operaciones sobre datos personales, tales como: recolección, almacenamiento, uso, circulación o supresión.

La Oficina de Sistemas e Informática llevará el inventario de las bases de datos de la CGR que contengan datos personales.

La Unidad de Seguridad y Aseguramiento Tecnológico e Informático realizará la inscripción de las bases de datos de la CGR que contengan datos personales, en el Registro Nacional de Base de Datos cuya administración corresponde a la Superintendencia de Industria y Comercio.

La Contraloría Delegada para la Participación Ciudadana coordinará el trámite de atención de las solicitudes o reclamos relacionados con la ley de protección de datos que realicen los titulares ante la CGR, en lo de su competencia. La respuesta será competencia de la dependencia encargada del tratamiento de los datos referidos en la solicitud o reclamo, y si se considera necesario a causa de la duda o sensibilidad de la información, se remitirá al órgano especializado en la materia que se cree para tal efecto.

5. TRATAMIENTO DE DATOS PERSONALES

5.1 GENERALIDADES

La CGR recolecta y almacena datos personales en sus bases de datos, en uso de su función legal y el tratamiento obedece únicamente a su función misional, es decir, el ejercicio del control y la vigilancia de la gestión fiscal.

La CGR garantiza la protección de derechos como el hábeas data, la privacidad, la intimidad, el buen nombre, la imagen y la autonomía institucional, y a su vez el de acceso a la información, por tanto el tratamiento de datos personales deberá realizarse cumpliendo con la normatividad legal colombiana vigente que establezca disposiciones para la protección de datos personales.

La CGR divulgará a sus servidores públicos, contratistas y terceros encargados del tratamiento las obligaciones que tienen en relación con el tratamiento de datos personales mediante campañas y actividades pedagógicas.

La CGR documentará en el Sistema Integrado de Gestión y Control de Calidad el manual de procedimientos relacionados con el tratamiento de datos personales.

La presente política podrá ser modificada, sin embargo, toda modificación se hará conforme a la normatividad vigente y tendrá efecto a partir de su publicación en los mecanismos que disponga la CGR para dar a conocer a los titulares de la información, los cambios que se produzcan.

5.2. DERECHOS DE LOS TITULARES DE LOS DATOS

En atención y en consonancia con lo dispuesto en la normatividad vigente y aplicable en materia de protección de datos personales, el titular de los datos personales tiene los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a la CGR en su condición de responsable del tratamiento. Este derecho se podrá ejercer, entre otros, ante datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado;

b) Solicitar prueba de la autorización otorgada a la CGR, salvo en los casos expresamente

exceptuados en la ley;

c) Ser informado por la CGR, 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 Ley 1581 de 2012 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. Exceptuando los casos en que el titular tenga un deber legal o contractual de permanecer en la base de datos del responsable o encargado;

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

La información solicitada por el titular podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el titular. La CGR deberá poner a disposición del titular de la información, mecanismos gratuitos y de fácil acceso para presentar la solicitud de supresión de datos o la revocatoria de la autorización.

5.3. AUTORIZACIÓN DEL TITULAR

La Autorización es el consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

La CGR tendrá como soporte de la autorización del titular de los datos personales un documento físico, electrónico, mensaje de datos, internet, sitios web, o en cualquier otro formato que permita garantizar su posterior consulta, o mediante un mecanismo técnico o tecnológico idóneo, que permita manifestar u obtener el consentimiento, mediante el cual se pueda concluir de manera inequívoca, que de no haberse surtido una conducta del titular, los datos nunca hubieren sido capturados y almacenados en la base de datos. El medio para otorgar la autorización será puesto a disposición del titular con antelación y de manera previa al tratamiento de sus datos personales.

La CGR adoptará las acciones tendientes y necesarias para mantener registros o mecanismos técnicos o tecnológicos idóneos de cuándo y cómo obtuvo autorización por parte de los titulares de datos personales para el tratamiento de los mismos. Para dar cumplimiento a lo anterior, se podrán establecer archivos físicos o repositorios electrónicos realizados de manera directa o a través de terceros contratados para tal fin.

Adicionalmente y conforme a lo establecido en la normatividad vigente en la materia, y teniendo en cuenta la aplicabilidad de criterios de armonización ante el conflicto que se pueda presentar entre los principios rectores, la autorización del titular no será necesaria cuando se trate de:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;

b) Datos de naturaleza pública;

c) Casos de urgencia médica o sanitaria;

d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o

científicos;

e) Datos relacionados con el Registro Civil de las Personas.

5.4. REVOCATORIA DE LA AUTORIZACIÓN

Los titulares de los datos personales pueden revocar el consentimiento al tratamiento de los mismos en cualquier momento ante la CGR, siempre y cuando no lo impida una disposición legal o contractual. En caso de proceder la revocatoria de tipo parcial de la autorización para el tratamiento de datos personales para algunas finalidades, la CGR podrá seguir utilizando los datos para las demás finalidades respecto de las cuales no proceda dicha revocatoria.

5.5. AVISO DE PRIVACIDAD

El aviso de privacidad es la comunicación verbal o escrita generada por la CGR, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

El aviso de privacidad, como mínimo, deberá contener la siguiente información:

- La identidad, domicilio y datos de contacto del responsable del tratamiento.

- El tipo de tratamiento al cual serán sometidos los datos y la finalidad del mismo.

- Los mecanismos generales dispuestos por el responsable para que el titular conozca la política de tratamiento de la información y los cambios sustanciales que se produzcan en ella.

5.6. DERECHOS DE LOS NIÑOS, NIÑAS Y ADOLESCENTES

La CGR en el tratamiento de datos personales de los niños, niñas y adolescentes, asegurará el respeto a los derechos prevalentes de este grupo, estableciendo que queda proscrito el tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública; por tanto, la CGR velará por el tratamiento adecuado, de los datos personales de niños, niñas y adolescentes, respetando el interés superior de aquellos y asegurando la protección de sus derechos fundamentales.

Lo mismo se reputara, del tratamiento de datos personales referente a las víctimas de violencia sexual en los términos de la Ley 1719 de 2014, y de las víctimas del conflicto armado en los términos de la Ley 1448 de 2011; por lo que dicho tratamiento en estos casos, se realizara mediante la debida valoración de los mismos, conforme a los mecanismos y procedimientos que se establezcan para ello.

5.7. TRATAMIENTO DE DATOS SENSIBLES

La CGR podrá realizar tratamiento de datos catalogados como sensibles únicamente cuando:

a) El titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;

b) El tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;

c) El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular;

d) El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

e) 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;

f) A pesar de darse los anteriores, y cuando se considere estrictamente necesario, mediante la aplicación de un juicio de razonabilidad y proporcionalidad, se determine que el no tratamiento de dichos datos, sea más nocivo que darles tratamiento, en el caso concreto.

5.8. DEBERES DE LA CGR COMO RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES

Son deberes de la CGR:

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 ley, copia de la respectiva autorización otorgada por el titular. En cuanto a este literal se aplicará la exención prevista en el artículo 10 de la Ley 1581 de 2012;

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, siempre y cuando el titular informe oportunamente sus novedades;

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 este 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 ley y en la presente política;

i) Exigir al encargado del tratamiento en todo momento, el respeto de las condiciones de seguridad y privacidad de la información del titular;

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

presente política;

k) Adoptar un manual interno de procedimiento para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos, en el marco de la presente política;

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 de 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.

5.9. DEBERES DE LOS SERVIDORES PÚBLICOS DE LA CGR COMO ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES

Los encargados del tratamiento de datos personales en la CGR están obligados a:

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

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

c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la normatividad vigente en la materia y lo establecido en la presente política;

d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;

e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la normatividad vigente en la materia y conforme a lo establecido en la presente política;

f) Adoptar un manual interno de procedimientos para garantizar el adecuado cumplimiento de la ley y la presente política, y en especial, para la atención de consultas y reclamos por parte de los Titulares;

g) Registrar en la base de datos las leyenda “reclamo en trámite” en la forma en que lo regula la normatividad vigente en la materia;

h) 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;

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;

k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

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

Los encargados del tratamiento de datos personales en la CGR, a través de su respectivo Jefe inmediato, deberán reportar las bases de datos con información personal que administran e informarán las novedades de su administración a la Oficina de Sistemas e Informática y a la Unidad de seguridad y aseguramiento tecnológico e informático. De igual manera deberán reportar las nuevas bases de datos personales que constituyan.

El incumplimiento de las políticas de tratamiento de la información acarreará las sanciones contempladas en el Código Único Disciplinario y normas concordantes

5.10. GARANTÍAS DE DERECHO DE ACCESO Y CONSULTAS

La CGR garantizará el derecho de acceso a la información, cuando previamente se acredite por el solicitante y/o titular la identidad del mismo, legitimidad, o personalidad de su representante, poniendo a disposición de este, sin costo o erogación alguna, de manera pormenorizada y detallada, los respectivos datos personales a través de todo tipo de medio, incluyendo los medios electrónicos que permitan el acceso directo del titular a ellos.

En el caso de consultas y solicitudes de acceso a información o datos personales que provengan de terceros y/o no titulares de lo solicitado, se tendrá en cuenta la aplicabilidad por parte del responsable del tratamiento, de las excepciones constitucionales y legales que aplican en la materia, y de los resultados que arrojen los juicios de proporcionalidad y razonabilidad que permitan conceder o negar el derecho de acceso a lo solicitado, cuando la sensibilidad del caso estrictamente así lo requiera.

La CGR garantizará el derecho de consulta, suministrando a los titulares o a través de un tercero debidamente autorizado, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.

Los titulares, podrán consultar sus datos de manera directa. En consecuencia, con respecto a la atención de solicitudes de consulta de datos personales la CGR garantiza:

- Habilitar medios de comunicación electrónica u otros que considere pertinentes.

- Establecer formularios, sistemas y otros métodos simplificados, mismos que deben ser informados en el aviso de privacidad.

- Utilizar los servicios de atención al cliente o de reclamaciones que tiene en operación.

5.11. RECLAMOS

El titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la normatividad vigente en la materia o en la presente política, podrán presentar un reclamo ante el responsable del tratamiento o el encargado del tratamiento canalizándola y remitiéndola a través de la dependencia designada para tal fin, la cual ejercerá la función de protección de datos personales al interior de la CGR, conforme a lo que se establezca en el respectivo manual de procedimientos.

La CGR suministrará, actualizará, rectificará 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.

La CGR tiene plena libertad de habilitar mecanismos que le faciliten el ejercicio de este derecho, siempre y cuando éstos beneficien al titular. En consecuencia, se podrán habilitar medios electrónicos u otros que considere pertinentes La CGR podrá establecer formularios, sistemas y otros métodos simplificados, que deben ser informados en el aviso de privacidad y que se pondrán a disposición de los interesados en la página web.

En el evento en que el titular considere que la CGR dio un uso contrario al autorizado y a las leyes aplicables, podrá hacer uso de sus derechos en su sede cuyo domicilio es dirección de correspondencia: Avenida Carrera 69 número 44-35. Piso 1. Bogotá - Colombia y a través del correo electrónico: control_ciudadano@contraloria.gov.co

5.12. SEGURIDAD DE LA INFORMACIÓN Y MEDIDAS DE SEGURIDAD

En desarrollo del principio de seguridad establecido en la normatividad vigente, la CGR adoptará 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.

La CGR efectuará un correcto tratamiento de los datos personales contenidos en sus bases de datos, evitando el acceso no autorizado a terceros que puedan conocer, vulnerar, modificar, divulgar y/o destruir la información que se encuentra almacenada. Para esto aplicará los respectivos protocolos de seguridad y acceso a los sistemas de información, almacenamiento, procesamiento y medidas físicas de control de riesgos de seguridad.

La CGR continuará con la implementación de mecanismos de seguridad adecuados, así como la aplicación de instructivos y el desarrollo de actividades de seguimiento a nivel interno para garantizar el correcto funcionamiento de los esquemas de seguridad técnica;

sin embargo a pesar de estas medidas adoptadas, la CGR no se responsabiliza por cualquier consecuencia derivada del ingreso indebido o fraudulento por parte de terceros a las bases de datos y/o por alguna falla técnica en el funcionamiento.

Los datos personales que no sean públicos serán tratados por la CGR como confidenciales, aun cuando la relación contractual o el vínculo entre el titular del dato personal y la CGR hayan finalizado. A la terminación de dicho vínculo, tales datos personales deben continuar siendo tratados de acuerdo con lo dispuesto por el manual de procedimientos de gestión documental, archivo y correspondencia.

La CGR se reserva, en los eventos contemplados en la ley y en su normatividad interna, la facultad de mantener y catalogar determinada información que repose en sus bases o bancos de datos, como confidencial de acuerdo con las normas vigentes y reglamentos, todo lo anterior y en consonancia con el derecho fundamental y constitucional, y principalmente de la autonomía administrativa.

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

La CGR no publicará datos personales 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.

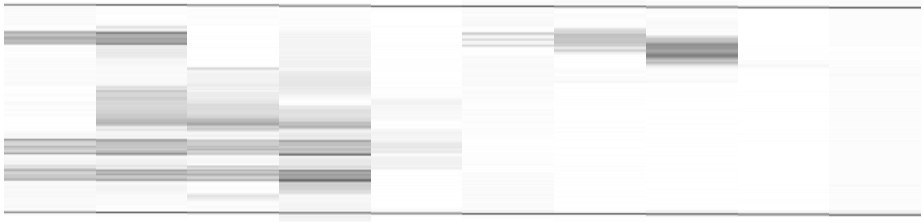
5.13. UTILIZACIÓN Y TRANSFERENCIA DE DATOS PERSONALES E INFORMACIÓN PERSONAL POR PARTE DE LA CGR

La CGR podrá intercambiar información de datos personales con autoridades gubernamentales o públicas tales como autoridades administrativas, de impuestos, organismos de investigación y autoridades judiciales, cuando la soliciten en ejercicio de sus funciones, y atendiendo a las garantías constitucionales y legales, y al contenido de la presente política.

La transferencia internacional de datos personales solo se realizará a países que proporcionen niveles adecuados de protección de datos, de acuerdo a los estándares propuestos y previa declaración de conformidad por parte de la Superintendencia de Industria y Comercio quien verificará la viabilidad de la operación.

Vigencia

El presente documento rige a partir de su aprobación, comunicación y publicación.



Disposiciones analizadas por Avance Jurídico Casa Editorial Ltda.
Normograma del Sena
ISSN Pendiente
Última actualización: 15 de marzo de 2018

logo