# Resolución Reglamentaria Número 022
**(Abril 19 de 2018)**

**"Por la cual se modifican las Políticas de Seguridad y Privacidad de la Información en la Contraloría de Bogotá, D.C."**

**EL CONTRALOR DE BOGOTÁ, D.C.**
**En ejercicio de sus atribuciones constitucionales y legales y en especial las conferidas en el Acuerdo 658 de 2016, modificado parcialmente por el Acuerdo 664 de 2017 expedidos por el Concejo de Bogotá y**

**CONSIDERANDO:**

Que el artículo 2 de la Ley 87 de 1993, *"Por la cual se establecen normas para el ejercicio de control interno en las entidades y organismos del Estado y se dictan otras disposiciones",* señala entre los objetivos fundamentales del diseño y desarrollo del Sistema de Control Interno: a) Proteger los recursos de la Organización, buscando su adecuada administración ante posibles riesgos que los afecten, e) Asegurar la oportunidad y confiabilidad de la información y de sus registros y f) Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos.

Que el artículo 4 ibídem contempla, entre otros, los siguientes elementos del Sistema de Control Interno, bajo la responsabilidad de los directivos de la Entidad: la definición de políticas como guías de acción y procedimientos para la ejecución de procesos, así como, la adopción de normas para la protección y utilización racional de los recursos y la simplificación y actualización de normas y procedimientos.

Que la Resolución 305 del 20 de octubre de 2008, modificada por la Resolución 004 de 2017, expedida por la Comisión Distrital de Sistemas (CDS) de Bogotá D.C. regula lo concerniente a políticas públicas en materia de tecnologías de la información y comunicaciones.

Que el artículo 16 de la Resolución 305 del 2008, modificada por el artículo 6 de la Resolución 004 de 2017, consagra el deber de adoptar políticas de seguridad y custodia de los datos y la información, para las entidades, organismos y órganos de control del Distrito Capital.

Que mediante el Acuerdo 658 de 2016, *"Por el cual se dictan normas sobre organización y funcionamiento de la Contraloría de Bogotá D.C., se modifica su estructura orgánica e interna, se fijan las funciones de sus dependencias, se modifica su planta de personal y se dictan otras disposiciones",* le otorgó a la Dirección de Tecnologías de la Información y las Comunicaciones, entre otras, las funciones de diseñar y proponer la política de uso y aplicación de tecnologías, estrategias, y herramientas, para el mejoramiento continuo de los procesos de la Contraloría de Bogotá D.C. y la de Coordinar la aplicación a todo nivel de la organización de los estándares, buenas prácticas y principios para el manejo de la información.

Que el Decreto 1377 de 2013, reglamenta parcialmente la Ley 1581 de 2012, cuyo contenido establece, el tratamiento de información de datos personales, autorización de uso, políticas de tratamiento, derechos de los titulares y la responsabilidad de los organismos frente al tratamiento de datos personales.

Que a través de la Resolución Reglamentaria No. 006 de 2014 la Contraloría de Bogotá D.C., adoptó la Política de Tratamiento de Datos Personales.

Que mediante la Resolución Reglamentaria No. 022 de 2016 la Contraloría de Bogotá D.C., adoptó las Políticas de Seguridad y Privacidad de la Información en la Contraloría de Bogotá, D.C.

Que la Ley 1712 de 2014 expedida por el Congreso de la República, tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.

Que el Decreto Único Reglamentario No. 1078 de 2015, Título 9 Capítulo 1, Sección 2, Artículo 2.2.9.1.2.1 en su numeral 4 define el componente Seguridad y Privacidad de la Información, como las acciones transversales tendientes a proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

Que la Resolución No. 019 de 2018 reglamenta el Comité de Seguridad de la Información y Gobierno en Línea- SIGEL de la Contraloría de Bogotá D.C, en su artículo 3 numeral 1º, establece dentro de sus funciones la de: definir, aprobar y difundir las políticas en materia de Seguridad de la Información aplicables al interior de la Contraloría de Bogotá, D.C., emitiendo las directrices y recomendaciones relacionadas con la Seguridad de la Información.

Que para el cumplimiento de sus funciones, la Contraloría de Bogotá ha desarrollado e implementado una plataforma tecnológica sobre la cual se registra, procesa, transmite y almacena información mediante

los Activos de información que interactúan con la ciudadanía y los funcionarios. Así mismo, la Contraloría de Bogotá D.C., reconoce que la información que genera es un activo valioso y un bien estratégico para llevar a cabo el cumplimiento de sus funciones y que por lo tanto requiere ser protegida y de un adecuado y seguro manejo de la misma para garantizar un óptimo y oportuno servicio a la ciudadanía y funcionarios de la Contraloría.

Que en sesión ordinaria del Comité de Seguridad de la Información y Gobierno en Línea- SIGEL, cebrada el 26 de octubre de 2017, se presentó y aprobó la Política de Seguridad Privacidad de la Información de la Contraloría de Bogotá D.C.

Que de acuerdo a la anterior, es necesario actualizar las Políticas de Seguridad y Privacidad de la Información en la Contraloría de Bogotá D.C, para ajustarlas a los lineamientos vigentes en la normatividad.

**RESUELVE:**

**ARTÍCULO PRIMERO.** Modificar las Políticas de Seguridad y Privacidad de la Información en la Contraloría de Bogotá D.C., adoptando las políticas contenidas en el documento anexo, el cual hace parte integral de la presente resolución.

**ARTÍCULO SEGUNDO:** El Comité de Seguridad de la Información y Gobierno en Línea- SIGEL, será el encargado de realizar la difusión, seguimiento al cumplimiento y actualización de las Políticas de Seguridad y Privacidad de la Información.

**ARTÍCULO TERCERO:** Es responsabilidad de los Directores, Subdirectores, Jefes de Oficina y Gerentes velar por la divulgación y aplicación de las POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION CONTRALORÍA DE BOGOTÁ D.C, adoptadas mediante la presente resolución.

**ARTÍCULO CUARTO.** La presente resolución rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias, en especial la Resolución Reglamentaria No. 022 de14 de julio de 2016.

**PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.**

**Dada en Bogotá, D.C., a los diecinueve (19) días del mes de abril de dos mil dieciocho (2018).**

**JUAN CARLOS GRANADOS BECERRA**
Contralor de Bogotá, D.C.

# POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN CONTRALORÍA DE BOGOTÁ D.C.

**JUAN CARLOS GRANADOS BECERRA**
**Contralor de Bogotá, D.C.**

**ANDRÉS CASTRO FRANCO**
**Contralor Auxiliar**

**CARMEN ROSA MENDOZA**
**Directora de Tecnologías de la Información y las Comunicaciones**

**Bogotá, D.C.**

**Abril 2018**

# TABLA DE CONTENIDO

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN....3
INTRODUCCIÓN....3
1. OBJETIVO GENERAL....3
1.1 OBJETIVOS ESPECÍFICOS....4
2. ALCANCE....4
3. BASE LEGAL....5
4. TÉRMINOS Y DEFINICIONES....6
5. ASPECTOS GENERALES....8
6. POLÍTICA GENERAL....9
6.1 CUMPLIMIENTO....9
6.2 ROLES Y RESPONBILIDADES....9
6.3 MODIFICACIÓN....11
6.4 COMUNICACIÓN....11
6.5 MONITOREO....12
7. POLÍTICAS ESPECÍFICAS....12
7.1. DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN....12
7.2 DE LA GESTIÓN DE LOS ACTIVOS....13
7.3. DE CONTROL DE ACCESO....16
7.4. DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS RECURSOS HUMANOS....17
7.5. DE LA CRIPTOGRAFÍA....18
7.6. DE LA SEGURIDAD FÍSICA Y DEL AMBIENTE....18
7.8. DE LA SEGURIDAD DE LAS COMUNICACIONES....21
7.9. DE LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA....21
7.10. DE LAS RELACIONES CON EL PROVEEDOR....22
7.11. DE LA GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN...23
7.12. DE LA GESTIÓN DE LA INFORMACIÓN DE LA CONTINUIDAD DEL NEGOCIO..23
7.13. DEL CUMPLIMIENTO....24
7.14. POLÍTICA DE PRIVACIDAD DE LA INFORMACIÓN....24

# POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## INTRODUCCIÓN

La Contraloría de Bogotá, D.C. como entidad que vigila la gestión fiscal de la Administración Distrital y de los particulares que manejan fondos o bienes públicos, en el ejercicio de sus deberes constitucionales se encuentra comprometida con la seguridad de la información como parte fundamental de la protección y confianza con el Estado y los ciudadanos, todo enmarcado en el cumplimiento de las leyes y en concordancia con una gestión confiable y efectiva en la vigilancia y control del uso adecuado de los recursos públicos.

En la Contraloría de Bogotá, D.C., la información es un activo fundamental para la prestación de servicios y toma de decisiones eficientes, razón por la cual, existe un compromiso expreso en su protección, como parte de una estrategia orientada a la administración de riesgos y consolidación de una cultura de seguridad, con el aseguramiento de la información se busca identificar y minimizar los riesgos a los que se expone y disminuir el impacto generado sobre sus activos, con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad, disponibilidad y privacidad de la información, acorde con las necesidades del Estado, ciudadanía, funcionarios, terceros, contratistas, proveedores, sujetos de control y en cumplimiento de las normas legales vigentes.

De esta manera, se establece la política de seguridad que será revisada con regularidad, como parte del proceso de revisión estratégica, o cuando se identifiquen cambios en la Entidad, en su estructura, sus objetivos o en alguna condición que la afecte, para asegurar que dicha política siga siendo adecuada y ajustada a los requerimientos de la Entidad.

## 1. OBJETIVO GENERAL

Establecer lineamientos de propósito general para asegurar una adecuada protección a los activos de información de la Contraloría de Bogotá D.C, permitiendo que los recursos de información que maneja la Entidad, sean

accedidos sólo por personas autorizadas que tienen una necesidad legítima para la realización de funciones propias del Ente de Control (Confidencialidad), que estén protegidos contra modificaciones no planeadas o realizadas con o sin intención (Integridad), que se aplique la protección de datos sensibles (Privacidad) y que estén disponibles cuando éstos sean requeridos para el desarrollo de las actividades propias de la Entidad (Disponibilidad).

### 1.1 OBJETIVOS ESPECÍFICOS

1. Propender por el cumplimiento de los objetivos estratégicos de la Entidad.
2. Mantener la confianza en la seguridad de la información en los usuarios internos y externos en el manejo de los procesos, trámites y servicios de la Entidad.
3. Definir un correcto acceso, uso y manejo de los recursos de información.
4. Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos de la Entidad.
5. Establecer los canales de comunicación que permitan la divulgación y conocimiento de la seguridad de la información.
6. Proteger la imagen, los activos de información y el buen nombre de la Entidad.
7. Propender por el debido cumplimiento de mejores prácticas en seguridad de la información.

## 2. ALCANCE

Esta política, aplica a toda la Entidad, funcionarios, contratistas, terceros, sujetos de control fiscal, ex funcionarios, ex contratistas, usuarios internos y externos que acceden o hacen uso de cualquier activo de información independientemente de su ubicación, medio o formato de la Contraloría de Bogotá D.C., así como a la ciudadanía en general.

Las políticas otorgan las directrices requeridas para implantar un Modelo de Seguridad de la Información confiable y definen el marco básico que guiará la implantación y operación de cualquier requisito normativo, proceso, procedimiento, estándar y / o acción, relacionados con la Seguridad de la Información.

## 3. BASE LEGAL

El marco normativo externo e interno sobre el cual se basan las políticas definidas está determinado por la siguiente base legal:

| TIPO DE NORMA | FECHA | DESCRIPCIÓN |
|---|---|---|
| Ley 527 | 18/08/1999 | Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. |
| Ley 734 | 05/02/2002 | Por la cual se expide el Código Disciplinario Único. |
| Resolución 305 | 20/10/2008 | Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre |
| Ley 1341 | 30/07/2009 | Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones - TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones |
| Ley 1437 | 18/01/2011 | Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. |
| Ley 1474 | 12/07/2011 | Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. |
| Ley 1581 | 17/10/2012 | Por la cual se dictan disposiciones generales para la Protección de Datos Personales. |
| Decreto 1377 | 27/06/2013 | Por el cual se reglamenta parcialmente la Ley 1581 de 2012 |
| Ley 1712 | 06/03/2014 | Por medio de la cual se crea la Ley de Transparencia y |

| TIPO DE NORMA | FECHA | DESCRIPCIÓN |
|---|---|---|
| | | del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. |
| Decreto 1081 | 26/05/2015 | Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República. |
| Decreto 1078 | 26/05/2015 | Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. |
| Decreto 124 | 26/01/2016 | Por el cual se sustituye el Título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015 relativo al Plan Anticorrupción y Atención al Ciudadano. |
| Resolución 004 | 28/11/2017 | Por lo cual se modifica la Resolución 305 de 2008 de la CDS |

## 4. TÉRMINOS Y DEFINICIONES

**Activo de información:** Es una pieza de información definible e identificable, almacenada en cualquier medio, es reconocido como valioso para la Entidad (Bases de datos, sistemas de información, servidores, recurso humano, documentos, archivos, recursos tecnológicos).

**Acuerdo de Confidencialidad**: Documento donde se plasma el compromiso para mantener la confidencialidad de la información de la Entidad, a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud del desarrollo de las funciones desempeñadas en la Entidad.

**Área segura:** Espacio en el que se trata la información de carácter sensible o determinados equipos informáticos que deben ser protegidos de accesos no autorizados.

**Autenticación:** Procedimiento informático que permite asegurar que un usuario de un sitio web u servicio informático es auténtico o quien dice ser.

**Cookie:** Es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

**Confidencialidad**: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

**Control**: Son todas aquellas políticas, procedimientos, lineamientos, practicas organizacionales establecidas para evitar o mitigar riesgos de seguridad de la información.

**Dirección IP:** Número que identifica, de manera lógica y jerárquica en una red informática a un dispositivo (computadora, tableta, portátil, Smartphone).

**Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

**Estándar**: Regla que especifica una acción o respuesta que se debe seguir a una situación dada.

**Incidente de seguridad:** Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información.

**Información**: Todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración[1]

Por otra parte, la Ley 1712 de 2014, artículo 6, la define como: “un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen”.

[1] Tomada de http://www.iso27000.es/sgsi.html

**Integridad**: Propiedad de garantizar el mantenimiento, la exactitud y completitud de la información.

**Medios removibles:** Dispositivos tecnológico de almacenamiento de información diseñados para ser extraídos del computador.

**Mejor Práctica**: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta.

**Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

**Privacidad**: Aquello que no es público, que lleva a cabo en un ámbito reservado.

**Seguridad de la información**: Según [ISO/IEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

**Segregación de tráfico:** Separación de transito de la información que fluye a través de la red informática de la Entidad.

**Smartphone: Teléfono** celular que disponen de un hardware y un sistema operativo propio capaz de realizar tareas y funciones similares a las realizadas por los ordenadores fijos o portátiles.

**Vulnerabilidad:** Debilidad de un activo o control que pueda ser explotada por una a mas amenazas.

## 5. ASPECTOS GENERALES

La información y la tecnología utilizada para su procesamiento, son activos fundamentales para la prestación de los servicios de la Entidad y para la toma de

decisiones de manera eficiente, razón por la cual la Contraloría de Bogotá D.C., protege estos recursos de las amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la información y garantizar la continuidad de los procesos de la entidad, minimizando los riesgos identificados y aportando al correcto complimiento de los objetivos organizacionales.

Las Políticas de Seguridad de la Información, surgen como una herramienta institucional de obligatorio cumplimiento y como parte integral de la gestión de la seguridad de la información en la aplicación del Modelo de Seguridad y Privacidad de la Información definido por del Ministerio de las Tecnologías de la Información y las Comunicaciones.

## 6. POLÍTICA GENERAL

La Contraloría de Bogotá D.C. reconoce la importancia de la protección de los activos de Información que soportan los procesos de la Entidad, por ello se encuentra comprometida con la implementación de medidas para asegurar su confidencialidad, integridad, disponibilidad y privacidad de acuerdo con las normas legales vigentes, para lo cual, adopta políticas, procedimientos, lineamientos y asigna responsabilidades para la adecuada gestión de la seguridad de la información.

### 6.1 CUMPLIMIENTO

Todas las personas mencionadas dentro del alcance deberán dar cumplimiento al 100% de las políticas descritas.

El incumplimiento a las Políticas de Seguridad de la Información de la Contraloría de Bogotá D.C., traerá consigo, las consecuencias disciplinarias, fiscales y penales que apliquen a la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a Seguridad y Privacidad de la Información.

### 6.2 ROLES Y RESPONBILIDADES

**Comité de Seguridad de la Información - SIGEL**

Define, aprueba y difunde las políticas en materia de Seguridad de la Información aplicables al interior de la Contraloría de Bogotá, D.C., emitiendo las directrices y recomendaciones relacionadas con la Seguridad de la Información.

**Directores, Subdirectores, Jefes De Oficina y Gerentes**
Velar por la divulgación y aplicación de las políticas de seguridad y privacidad de la información.

**Funcionarios, contratistas, sujetos de control fiscal, terceros, ex funcionarios, ex contratistas, la ciudadanía en general.**

- Aplicar y dar cumplimiento a las políticas de seguridad y privacidad de la información de la Contraloría de Bogotá D.C.
- Los ex funcionarios y ex contratistas deben mantener la debida confidencialidad sobre la información de la Entidad después de que se ha terminado la relación contractual o vinculante con la Contraloría de Bogotá D.C.
- Dar cumplimiento a los procedimientos adoptados por la Contraloría de Bogotá que dan aplicación a las políticas, normas y demás directrices de seguridad de la información.
- Informar y reportar situaciones, eventos en las que se vea afectada la seguridad de la información o recursos asociados a la Entidad.
- Participar activamente de las campañas y actividades entorno a la generación de cultura en seguridad y protección de la información.

**Director de Tecnologías de la Información y las Comunicaciones**
Establecer los recursos que en concordancia con las políticas de la Seguridad de la Información, adopte e implemente los controles computacionales y tecnológicos, para dar cumplimiento a las disposiciones señaladas en las políticas, normas, estándares y procedimientos de seguridad de la información.

**Director de Talento Humano**
Establecer desde la gestión y capacitación del talento humano la aplicación y divulgación de las políticas de seguridad de la información.

**Oficina de Control Interno**
Ejercer seguimiento y control al cumplimiento de las políticas de seguridad la información.

**Oficina Asesora Jurídica**
Realizar cuando corresponda las revisiones, observaciones, sugerencias a la política de seguridad y sus modificaciones desde el ámbito jurídico que aseguren el pleno cumplimiento con las normativas y legislaciones vigentes.

Ejercer cuando corresponda la representación judicial de la Entidad ante la inobservancia de la aplicación de las políticas y normas de Seguridad de la Información por parte de terceros, contratistas y proveedores, que repercutan en pérdidas para la Entidad, por materialización de riesgos de tipo reputacional, operacional, financiero, estratégicos, de cumplimiento y de corrupción, cuando a ello haya lugar.

**Oficina de Asuntos Disciplinarios**
Realizar cuando corresponda las investigaciones, establecer y ejecutar medidas de carácter disciplinarios, ante cualquier inobservancia de aplicación de las políticas y normas por parte de los funcionarios de la Contraloría de Bogotá D.C.

**Oficina Asesora Comunicaciones**
Difundir a través de los canales de comunicación institucionales las políticas, normas y procedimientos de seguridad de la información que permita la divulgación, concientización y generación de cultura en la protección de la información.

## 6.3 MODIFICACIÓN

La Contraloría De Bogotá D.C., podrá modificar las Políticas de seguridad de la información aquí contenidas, a su libre elección, en cualquier momento cuando las circunstancias lo exijan y las mismas estarán vigentes una vez se hayan adoptado por acto administrativo y divulgado por los diferentes mecanismos de comunicación institucional.

## 6.4 COMUNICACIÓN

La Contraloría de Bogotá D.C establece los siguientes mecanismos de difusión de la política de seguridad:

- Publicación de la política de seguridad en la página web institucional en lugar de fácil acceso.
- Socialización a personal a la entidad (contratistas, funcionarios, y responsables de la seguridad de la información) y partes interesadas.
- Socialización al personal de la entidad cuando haya lugar a modificaciones y/o actualizaciones de las políticas de seguridad que hayan sido aprobadas por el Comité SIGEL.
- Publicidad a través de canales de comunicación institucional.

### 6.5 MONITOREO

Los responsables verificarán el cumplimiento de las políticas de seguridad de la información y los demás mecanismos de protección de la información a través de diversos métodos, incluyendo, pero no limitado al seguimiento periódico, monitoreo, reportes, auditorías internas y externas.

Comité SIGEL revisara las políticas periódicamente, mínimo una vez en el año o cuando las condiciones de la Entidad lo requieran, para asegurar su conveniencia, adecuación y eficacia continúas.

## 7. POLÍTICAS ESPECÍFICAS

### 7.1. DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

En la Contraloría de Bogotá D.C., se definen los roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información, en los cuales se segregarán las funciones y las áreas de responsabilidad, para prevenir que se presenten conflictos de intereses que conlleven a oportunidades de modificaciones no autorizadas o el uso inadecuado de los activos de la información.

**Directrices:**

- El Comité Técnico de Seguridad de la Información y Gobierno en Línea - SIGEL, establece las políticas generales para garantizar la seguridad y la integridad de la información, la implementación de la Estrategia de Gobierno en Línea, conforme a los nuevos lineamientos del orden Nacional y Distrital relativos a la seguridad de la información, los sistemas informáticos, el uso adecuado de la información y su integración y coordinación con el proceso de gestión documental de la Entidad.
- La Dirección de Tecnologías de la Información y las Comunicaciones establecerá los roles, funciones y responsabilidades de operación y administración de los sistemas de información de la Contraloría de Bogotá D.C, estos roles, funciones y responsabilidades, deberán estar debidamente documentadas y distribuidas.
- La Contraloría de Bogotá D.C, establecerá acuerdos de cooperación de seguridad de información con entidades de seguridad del estado.
- Los funcionarios de la Contraloría de Bogotá D.C asistirán a foros, conversatorios, conferencias de interés especial en seguridad de la información.
- Los proyectos desarrollados en la Contraloría de Bogotá D.C deberá incorporar dentro de la planeación y desarrollo, el cumplimiento de la política de seguridad de la información, valoración de riesgos y los controles a estos.

## 7.2 DE LA GESTIÓN DE LOS ACTIVOS

Establecer lineamientos frente a la identificación, clasificación, uso, administración y responsabilidad frente a los activos de información

**Identificación, clasificación y etiquetado de activos:**

- La Contraloría de Bogotá D.C. establecerá la metodología y/o procedimiento para la identificación, clasificación y etiquetado de los activos de información, donde se determinará los responsables y la forma para la elaboración del inventario de activos de información.
- La Contraloría de Bogotá D.C. mantendrá un inventario actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por la Dirección de Tecnología de la Información y las Comunicaciones.

- La Contraloría de Bogotá D.C. es la dueña de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.
- Cada activo de información de la Contraloría de Bogotá D.C, debe tener asignado un propietario quien velará por su protección y correcta gestión.
- Toda la información producida, tratada, procesada, almacenada o transmitida en la Contraloría de Bogotá D.C., debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad según metodología y/o procedimiento establecido por la Entidad en el Subsistema de Gestión de Seguridad de la Información.

**Devolución de los activos:**

Los funcionarios y contratistas deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por la Contraloría de Bogotá D.C. en el proceso de desvinculación o finalización de la relación laboral o contractual, de igual manera deberán documentar y entregar a la Entidad los conocimientos importantes que posee de la labor ejecutada.

**Gestión de medios removibles:**

La Contraloría de Bogotá D.C., adoptará un procedimiento formal para la gestión de medios removibles. Los medios removibles deberán ser supervisados, estos serán de acceso y uso restringido en la entidad. El procedimiento de gestión de medios removibles, contendrá las pautas que abarquen todo el ciclo de vida de estos medios, así como un protocolo de eliminación de forma segura que no ponga en riesgo la información y produzca el menor impacto ambiental posible. Ninguna información en la Contraloría de Bogotá D.C., deberá ser divulgada o modificada sin autorización de la Entidad, so pena de incurrir en falta la cual será sancionada de acuerdo a la normatividad vigente.

**Disposición de los activos:**

- La Contraloría de Bogotá D.C. establecerá procedimiento mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o re uso cuando ya no se requieran los activos.

- Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

**Dispositivos Móviles**

Con el objetivo de establecer directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes "smartphones", tabletas), entre otros, suministrados por la entidad y personales que accedan a través de redes inalámbricas y hagan uso de los servicios de información de la Contraloría de Bogotá D.C, se dispone:

- La Contraloría de Bogotá D.C., establecerá lineamientos para el acceso a redes inalámbricas, la instalación de chats corporativos y/o correos electrónicos de la entidad mediante el uso de este tipo de dispositivos y establecerá las responsabilidades que deben tener los funcionarios, contratistas o terceros frente al uso de la información almacenada en los dispositivos móviles.
- En la Contraloría de Bogotá D.C., se adoptarán medidas de apoyo en la seguridad para ejercer correctamente gestión de los riesgos que se presenten al utilizar dispositivos móviles, así como en el acceso a la información, el procesamiento o almacenamiento en lugares de trabajo remotos.
- La instalación y configuración de las cuentas institucionales de correo y redes sociales tendrán el apoyo del área de tecnologías de la información y las comunicaciones.
- Los dispositivos móviles institucionales deben tener contraseña de ingreso y bloqueo del equipo de manera automática y manual, tener activado la función de borrado remoto, cifrar la memoria de almacenamiento.
- Los dispositivos móviles institucionales deben tener únicamente la tarjeta sim asignada por la entidad, la cual, no puede instalarse en otro equipo diferente la asignando.
- Ante la pérdida del equipo institucional, ya sea por extravío o hurto, deberá informar de manera inmediata a la Dirección Administrativa y continuar con el

procedimiento administrativo por pérdida de elementos establecido por la entidad.

- Los teléfonos móviles y/o teléfonos inteligentes institucionales, debe permanecer encendidos y cargados durante las horas laborales o de acuerdo con la responsabilidad y requerimientos propios del cargo.
- Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por la Contraloría de Bogotá D.C. con el fin de realizar actividades propias de su cargo o funciones asignadas en la entidad, deben evitar hacer uso de estos en lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo.

### 7.3. DE CONTROL DE ACCESO

- En la Contraloría de Bogotá D.C., se establecerán medidas de control de acceso a la información en los niveles de sistema operativo, red, sistemas de información y demás servicios de TI, estos controles deben limitar el acceso a la información de acuerdo a las funciones y cargos que desempeñen los funcionarios, contratistas y terceros. Siempre se brindarán accesos de acuerdo al principio de privilegio más bajo, con los cuales todos los funcionarios, contratistas y terceros puedan desempeñar correctamente sus funciones sin brindar accesos de mayor alcance a los que se requiere.
- En la Contraloría de Bogotá D.C, se establecerá un procedimiento mediante el cual se brinden las pautas para una correcta gestión de usuarios y accesos a la información en todos sus niveles, este procedimiento debe contemplar la restricción y control de los accesos privilegiados a la información y los sistemas de información, así como establecer las definiciones para el monitoreo de las acciones desde cuentas de usuarios y súper usuarios.
- Todo código fuente perteneciente a la Contraloría de Bogotá D.C., o del cual se haga uso a nivel corporativo tendrá tratamiento de información confidencial y su acceso será restringido. El uso de programas utilitarios que estén en capacidad de anular el sistema y sus controles, así como ingresar al código fuente está prohibido en todos los niveles de la entidad, su uso será autorizado en única instancia por la Dirección de Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá D.C., previa validaciones de riesgo de la seguridad de la información y su pertinencia.

## 7.4. DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS RECURSOS HUMANOS

- En la Contraloría de Bogotá D.C., se implementarán mecanismos para asegurar que los funcionarios, contratistas, sujetos de vigilancia y control fiscal, conozcan y comprendan sus responsabilidades con la seguridad de la información, en los casos pertinentes se perfeccionarán acuerdos de confidencialidad con funcionarios, contratistas y terceros en donde se establezcan las responsabilidades en cuanto a la seguridad de la información, estos acuerdos tendrán vigencia aun si se producen cambios de estado en la relación funcionario/contratistas-entidad.
- En la Contraloría de Bogotá D.C, se fijarán mecanismos de verificación de antecedentes necesarios para asegurar que todos los candidatos a empleos se encuentren en cumplimiento con las leyes y regulaciones vigentes antes del inicio de relación laboral, así mismo se efectuarán actividades de concienciación periódicas que aseguren el conocimiento y cumplimiento de las políticas, normas, estándares y procedimientos de seguridad de la información al personal de la Entidad.
- Funcionarios y contratistas durante su vinculación laboral con la Contraloría de Bogotá D.C darán cumplimiento a las políticas, normas, estándares y procedimientos de seguridad de la información adoptadas por la Entidad, asimismo la Contraloría de Bogotá D.C pude realizar verificaciones de antecedentes del personal en cumplimiento con las leyes y regulaciones vigentes durante la relación laboral.
- Después de finalizada la vinculación laboral del personal con la Contraloría de Bogotá D.C se retiraran y/o desactivaran los permisos de acceso a los servicios informáticos de la Entidad, para lo cual Dirección de Talento Humano informará a la Dirección de Tecnologías de la Información y las Comunicaciones las novedades de retiro de funcionarios y se revocaran los privilegios de acceso como funcionario a las instalaciones de la Entidad.
- Ex funcionarios y ex contratistas darán cumplimiento a las políticas de seguridad de la información después de la terminada la relación laboral con la Contraloría de Bogotá D.C.

## 7.5. DE LA CRIPTOGRAFÍA

- En la Contraloría de Bogotá D.C., la información transmitida o almacenada será cifrada de acuerdo a su criticidad, para lo cual se establecerán lineamientos de cifrado de información, los cuales debe incluir las pautas para la gestión de llaves criptográficas y los servicios que se implementen con medidas de seguridad a los que se les apliquen controles criptográficos.

## 7.6. DE LA SEGURIDAD FÍSICA Y DEL AMBIENTE

- En la Contraloría de Bogotá D.C., se identificaran las áreas que almacenen, manejen o generen información sensible sobre las cuales se crearán perímetros de seguridad que permitan controlar el acceso solo de personal autorizado, así como aplicar mecanismos de seguridad física que permita prevenir daños por desastre natural, ataques maliciosos o accidentales.
- La Contraloría de Bogotá D.C. definirá los perímetros físicos de seguridad donde se encuentre la información crítica, sensible o se realice almacenamiento y/o procesamiento de la información y aplicará los controles de acceso según la restricción de las zonas definidas.
- En la Contraloría de Bogotá D.C., se deberá establecer lineamientos para el trabajo en áreas seguras, el cual debe incluir controles para los puntos de acceso a estas áreas, definir la ubicación y protección del equipamiento y elementos de soporte, fijar un estándar interno para la seguridad del cableado, el mantenimiento al equipamiento y la seguridad de los mismos fuera de las instalaciones de la entidad.
- En la Contraloría de Bogotá D.C., toda la información marcada como sensible o crítica debe estar resguardada en áreas seguras y su acceso debe ser restringido.

### Políticas de escritorio

- Los funcionarios al ausentarse de su lugar de trabajo, junto con bloquear su estación de trabajo, debe guardar en lugar seguro (gabinetes, mobiliario protegido con llave, caja fuerte, gabinete a prueba de incendios) cualquier documento físico (hojas impresas, carpetas, cuadernos, libretas de apuntes), medio magnético u óptico removible (Memorias Flash, Discos Duros Externos,

CD ROM, DVD) que contenga información pública reservada, publica clasificada, confidencial, sensible de la Contraloría de Bogotá D.C.

- Bloquear las impresoras multifuncionales, protegerlas de uso no autorizado, retirar inmediatamente la información pública reservada, pública clasificada, confidencial, sensible de la Contraloría de Bogotá D.C. una vez impresa.
- Los funcionarios de la Contraloría de Bogotá D.C. deben conservar su escritorio libre de información pública reservada y/o pública clasificada, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- Los usuarios a los que la Contraloría de Bogotá D.C. les asigne equipos móviles como computadores, teléfonos inteligentes, tablets, deben activar el bloqueo de teclas o pantalla, que permita evitar el acceso no autorizado a estos dispositivos.
- Desconectar de la red/ sistema /servicio los equipos de cómputo, terminales, impresoras cuando estén desatendidas por largos periodos de tiempo. Los mismos deben estar protegidas bajo llave o controles de seguridad cuando no estén en uso.

**Políticas de pantalla limpia**

- Las estaciones de trabajo y equipos portátiles deben tener aplicado el protector de pantalla estándar institucional de la contraloría de Bogotá D.C., que se active en un tiempo sin actividad del equipo.
- La pantalla de autenticación a la red de la Contraloría de Bogotá D.C. debe requerir solamente la identificación de la cuenta y contraseña.
- Los usuarios de los sistemas de información y comunicaciones de la Contraloría de Bogotá D.C., deberán cerrar las aplicaciones y servicios de red cuando ya no los necesite.
- Los funcionarios deben bloquear los equipo de cómputo (PC y portátiles) cuando se dejen desatendidos (desplazamiento del puesto de trabajo, horario de almuerzo, participación de pausas activas, retiro de impresiones, atención de visitas, salidas a los servicios sanitarios).

## 7.7. DE LA OPERACIÓN

- En la Contraloría de Bogotá D.C., se establecerán procedimientos necesarios para asegurar la operación correcta y segura de las instalaciones de

procesamiento de la información, así como protocolos para controlar los cambios en la entidad, gestionar la capacidad para adaptar el uso de recursos y realizar proyecciones futuras que aseguren una respuesta oportuna a los requerimientos de la entidad.

- Se deberá de igual forma, registrar, mantener y revisar con regularidad los registros de los eventos de los usuarios, excepciones, fallas y eventos de seguridad de la información de la entidad. Estos registros se deben proteger contra cualquier alteración o accesos no autorizados, en concordancia se deben registrar las actividades de los administradores y operadores de los sistemas de información de la entidad.
- Todos los sistemas de información de la Contraloría de Bogotá D.C., deben estar sincronizados al servicio de hora legal de Colombia suministrado por el Instituto Nacional de Metrología de Colombia, para lo cual la Dirección de Tecnologías de la Información y las Comunicaciones deberá establecer los mecanismos necesarios para tal fin.
- La Dirección de Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá D.C., establecerá un procedimiento en el cual se regule la instalación de software en la entidad, así como reglas que regulen la instalación de software por parte de los funcionarios, contratistas y terceros en equipos computacionales de la entidad.
- La Dirección de Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá D.C., deberá obtener información de las vulnerabilidades técnicas de forma oportuna, así como evaluar la exposición de la entidad a estas vulnerabilidades y tomar las medidas necesarias para abordar los riesgos asociados.
- La Oficina de Control Interno y la Dirección de Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá D.C., deberán planificar y acordar aspectos sobre las auditorías a los sistemas computacionales de la entidad en aras de minimizar el riesgo de interrupción de la operación de la entidad.
- La información misional de la Contraloría de Bogotá D.C., deberá estar centralizada y se deberá asegurar la ejecución de copias de respaldo ante cualquier afectación por pérdida o degradación.

## 7.8. DE LA SEGURIDAD DE LAS COMUNICACIONES

- La Dirección de Tecnologías de la información y las Comunicaciones definirá mecanismos de protección de la información en las redes de datos de la Contraloría de Bogotá D.C., asegurando su disponibilidad con una adecuada gestión de la seguridad y control del tráfico.
- Los mecanismos que se implementen deberán asegurar el control y gestión de la red de datos, servicios de red, segregación de tráfico por grupos de servicios, usuarios y sistemas de información, transferencia de información y mensajería electrónica.
- Para la transferencia de información entre la Contraloría de Bogotá D.C., y otra entidad de cualquier orden y naturaleza sea pública, privada o mixta, se deberán establecer requisitos de confidencialidad y no divulgación de la información, para lo cual será necesario establecer los respectivos contratos de confidencialidad, enmarcados en las leyes vigentes.

## 7.9. DE LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA

- En la Contraloría de Bogotá D.C., se deberán incluir los requisitos de seguridad para los nuevos sistemas o las mejoras para los sistemas existentes, de igual manera para la información asociada a los servicios expuestos en redes públicas y las transacciones que en estos se realicen, se deben establecer mecanismos de protección contra operaciones fraudulentas, disputas contractuales y el acceso, la divulgación y modificación no autorizada.
- La Dirección de Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá D.C., definirá procedimiento para el desarrollo de software y sistemas de información, estas deben ser aplicadas a los desarrollos y adaptaciones de los sistemas en la entidad, del mismo modo se debe establecer un procedimiento para el control de cambios en los sistemas de información, en el que se debe asegurar que cuando se efectúen cambios en la plataforma de operación no haya impacto adverso en las operaciones y en la seguridad de la información.
- La Dirección de Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá D.C., definirá mecanismos de prueba de aceptación de nuevos sistemas de información, actualizaciones y versiones nuevas, así

como supervisar, monitorear la actividad del desarrollo de los sistemas tercerizados y realizar pruebas de funcionalidad de la seguridad.

- La Dirección de Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá D.C., deberá establecer los mecanismos procedimentales y tecnológicos que aseguren los datos utilizados en los ambientes de prueba.
- Todo nuevo hardware y software que se vaya a adquirir y conectar a la plataforma tecnológica de la Contraloría de Bogotá D.C., por cualquier dependencia o proyecto de la entidad, deberá ser gestionado por la Dirección de Tecnologías de la Información y las Comunicaciones para su correcto funcionamiento.
- El software proporcionado por la Contraloría de Bogotá D.C no puede ser copiado o suministrado a terceros.
- En los equipos de la Contraloría de Bogotá D.C se debe utilizar software licenciado o libre que la Dirección de Tecnologías de la Información y las Comunicaciones, haya adquirido como resultado de proyectos o programas que se encuentran en la Entidad.
- Para la adquisición y actualización de software, es necesario efectuar la solicitud a la Dirección de Tecnologías de la Información y las Comunicaciones.
- El software que se adquiera la Entidad, debe quedar licenciado a nombre de la Contraloría de Bogotá D.C.
- Se encuentra prohibido el uso e instalación de juegos en los computadores de la Contraloría de Bogotá D.C.

## 7.10. DE LAS RELACIONES CON EL PROVEEDOR

- La Contraloría de Bogotá D.C. establecerá lineamientos para el tratamiento de seguridad en los acuerdos con los proveedores donde se establece, aprueba y divulga los requerimientos y obligaciones relacionados con la seguridad de la información, tanto con los proveedores como con la cadena de suministros que estos tengan.
- Los proveedores deben aceptar y firmar los acuerdos de confidencialidad establecidos por la Contraloría de Bogotá.

## 7.11. DE LA GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

- En la Contraloría de Bogotá D.C., se establecerá procedimientos y responsables de gestión que permita evaluar y decidir cuándo un evento de seguridad, corresponde a un incidente de seguridad de la información, así como asegurar una atención que brinde respuesta rápida, eficaz y metódica a los incidentes detectados.
- Todo evento de seguridad ocurrido en la Contraloría de Bogotá D.C., deberán ser comunicados mediante canales de gestión apropiados.
- Los funcionarios, contratistas y terceros que hagan uso de los sistemas de información de la entidad, que tengan conocimiento de cualquier debilidad en la seguridad de la información, en los sistemas o servicios deben informarlo a la Dirección de Tecnologías de la Información y las Comunicaciones.
- En la Contraloría de Bogotá D.C., establecerá procedimiento para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia, así como utilizar todo el conocimiento que se adquiera al analizar y resolver incidentes de seguridad de la información para la reducción de la probabilidad o el impacto de incidentes futuros.

## 7.12. DE LA GESTIÓN DE LA INFORMACIÓN DE LA CONTINUIDAD DEL NEGOCIO

- La Contraloría de Bogotá D.C., destinará los recursos necesarios para brindar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación.
- Se deberá restablecer las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante los eventos catastróficos, de igual manera se deberán mantener canales de comunicación adecuados hacia funcionarios, proveedores y terceras partes interesadas.

## 7.13. DEL CUMPLIMIENTO

- En la Contraloría de Bogotá D.C., se deberán cumplir los requisitos legales regulatorios y contractuales pertinentes y ser actualizados en los sistemas de información y en los procedimientos para asegurar su cumplimiento.
- En la Contraloría de Bogotá D.C., se deberán proteger los registros contra pérdida, destrucción, falsificación, acceso y emisión no autorizados, de acuerdo con la legislación, regulaciones y obligaciones contractuales de la entidad.
- Todos los controles criptográficos que se implementen en la Contraloría de Bogotá D.C., deberán cumplir con los acuerdos, leyes y regulaciones pertinentes.

## 7.14. POLÍTICA DE PRIVACIDAD DE LA INFORMACIÓN

Es interés de la Contraloría de Bogotá D.C. la protección de la privacidad de la información personal del funcionario y/o ciudadano obtenida a través de los diferentes mecanismos de consulta físicos y electrónicos dispuestos por la entidad, para lo cual se compromete a adoptar una política de privacidad de acuerdo con lo que se establece a continuación:

- La Contraloría de Bogotá D.C. implementará acuerdos de confidencialidad en el cual todo funcionario, contratista y/o tercero vinculado a la entidad debe firmar con el compromiso de no divulgar la información interna y externa que conozca de la entidad, así como las funciones que desempeña.
- El ciudadano y/o funcionario reconoce que el ingreso de información personal por cualquiera de los mecanismos establecidos por la entidad, lo realiza de manera voluntaria y ante la solicitud de requisitos específicos por la Contraloría de Bogotá D.C. para llevar a cabo un trámite, una queja o reclamo o una solicitud o para acceder a los mecanismos interactivos que ofrece la entidad.
- El ciudadano y /o funcionario acepta que a través del registro en el Sitio Web de la Contraloría de Bogotá D.C. se recogen datos personales, los cuales no se cederán a terceros sin su conocimiento.
- La recolección y tratamiento automatizado de los datos personales, como consecuencia de la navegación y/o registro por el Sitio Web tiene como finalidades las detalladas a continuación:

- ✓ La adecuada gestión y administración de los servicios ofrecidos en el Sitio Web, en los que el ciudadano y/o funcionario decida darse de alta, utilizar o contratar.
- ✓ El estudio cuantitativo y cualitativo de las visitas y de la utilización de los servicios por parte de los usuarios.
- ✓ El envío por medios tradicionales y electrónicos de información relacionados con la Contraloría de Bogotá D.C. y de cualquier otro proyecto o programa.
- ✓ Poder tramitar servicios de gobierno en línea.

**Derechos de los Titulares**

- ✓ Conocer, actualizar y rectificar sus datos personales frente al responsable y encargado del tratamiento. Este derecho se podrá ejercer entre otros, ante datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado personales y podrá ejercitarlos mediante un formulario de actualización de datos disponible en el sitio web de la Contraloría de Bogotá D.C.
- ✓ Solicitar prueba de la autorización otorgada a la Contraloría de Bogotá D.C. como responsable y encargado del tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012.
- ✓ Ser informado por la Contraloría de Bogotá D.C., como responsable del tratamiento y encargado del tratamiento, previa solicitud, respecto del uso que le ha dado a los datos personales del Titular.
- ✓ Presentar ante la Contraloría de Bogotá D.C. quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.
- ✓ Revocar la autorización y/o solicitar la supresión del dato personal cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Contraloría de Bogotá D.C. haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a la Ley 1581 de 2012 y a la Constitución.
- ✓ Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

**Autorización del titular**: Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa, expresa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.

**Casos en que no es necesaria la autorización.** La autorización del Titular no será necesaria, cuando se trate de:

- ✓ Información requerida por la Contraloría de Bogotá D.C. en ejercicio de sus funciones legales o por orden judicial;
- ✓ Datos de naturaleza pública;
- ✓ Casos de urgencia médica o sanitaria;
- ✓ Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
- ✓ Datos relacionados con el Registro Civil de las Personas.

**Uso de Cookies y del Archivo de Actividad en página Web**

Las cookies utilizadas por la página Web son archivos enviados a un navegador por medio de un servidor web para registrar las actividades del usuario en la página Web y permitirle una navegación más fluida y personalizada. El ciudadano tiene la posibilidad de configurar su navegador personal para impedir la entrada de éstas, bloquearlas o, en su caso, eliminarlas. Para utilizar la página Web institucional, resulta necesario que el usuario permita la descarga o instalación de cookies.

De igual manera, los servidores de la página Web detectan de manera automática la dirección IP y el nombre de la red utilizados por el usuario. Toda esta información es registrada temporalmente en un archivo de actividad del servidor que permite el posterior procesamiento de los datos con el fin de obtener mediciones estadísticas que permitan conocer el número de impresiones de páginas, y el número de visitas realizadas a la página Web, entre otras mediciones.

Además de sistemas propios de monitorización de la página Web, ésta utiliza herramientas estadísticas externas que emplean "cookies", ubicados en el

equipo del usuario, para analizar el uso que hacen los usuarios de la página Web. La información que genera la cookie acerca del uso de la página Web por parte del usuario (incluyendo su dirección IP) será directamente transmitida y archivada en los servidores. Se usará esta información, recopilando informes de la actividad de la página Web y prestando otros servicios relacionados con la actividad y el uso de Internet. Se podrá transmitir dicha información a terceros cuando así se lo requiera la legislación, o cuando dichos terceros procesen la información.

La Contraloría de Bogotá D.C., podrá asociar la dirección del usuario IP con algún otro dato, para asegurar la correcta prestación de los servicios Web.

El ciudadano puede rechazar el tratamiento de los datos o la información, manifestando que no está de acuerdo con el uso de cookies mediante la selección de la configuración apropiada de su navegador personal. Sin embargo, debe saber que de esta manera podría tener una funcionalidad limitada de la página. Al utilizar la página Web el usuario es consciente del tratamiento de la información en la forma y para los fines arriba indicados.

**Cesión de Datos Personales a Terceros**

La Contraloría de Bogotá D.C., no cederá a terceros los datos personales de los usuarios, que se recogen a través de la página Web, sin su consentimiento expreso. Sin perjuicio de lo anterior, el usuario autoriza que se cedan sus datos personales cuando así sea requerido por las autoridades administrativas competentes[2] o por mandato judicial en cumplimiento a las disposiciones legales.

El ciudadano también comprende que los datos por él consignados formarán parte de un archivo y/o base de datos que podrá ser usado por la Contraloría de

---

*2 Según concepto del Consejo de Estado: "…La Sala Plena de lo Contencioso Administrativo ha dicho que es aquella que ejercen quienes desempeñan cargos de la administración nacional, departamental y municipal o de los órganos electorales y de control que impliquen poderes decisorios de mando o imposición sobre los subordinados o la sociedad. La autoridad administrativa, comprende, entonces, las funciones administrativas de una connotación como la descrita y excluye las demás que no alcanzan a tener esa importancia". Fuente: Consejo de Estado, Sala de Consulta y Servicio Civil, «Radicación 1831 de 2007,» Sala de Consulta y Servicio Civil, 05 07 2007. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=26387.*
*Ley 1581 de 2012, Art 19 Autoridad de protección de datos: ""<Artículo CONDICIONALMENTE exequible> La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley"*

Bogotá D.C., para efectos de surtir determinado proceso. El Usuario podrá modificar o actualizar la información suministrada en cualquier momento.

La información personal proporcionada por el servidor público de la entidad está asegurada por una clave de acceso que sólo él conoce. Por tanto, es el único responsable de mantener en secreto su clave. La Contraloría de Bogotá D.C., se compromete a no acceder ni pretender conocer dicha clave. Debido a que ninguna transmisión por Internet es absolutamente segura ni puede garantizarse dicho extremo, el servidor público de la entidad asume el hipotético riesgo que ello implica, el cual acepta y conoce. La Contraloría de Bogotá D.C. adoptará los niveles de seguridad para protección de los datos personales legalmente requeridos, instalando las técnicas y organizativas necesarias para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos facilitados.

**Correo electrónico institucional, Foros, Blogs, Chats y otros espacios de Participación**.

El usuario reconoce que su participación en cualquier correo, foro, chat, comentario, blog y/o cualquier otro espacio de participación institucional, será bajo su exclusiva responsabilidad, y que de igual forma, las opiniones y/o acciones y/o comportamiento de otros usuarios en tales espacios son responsabilidad exclusiva de quienes las emiten o realizan, por lo cual la Contraloría de Bogotá D.C., lo hace responsable de tales conductas, opiniones y de las consecuencias que ellas pudieren acarrear a favor y/o en contra de otros participantes o de terceros.

El diseño, manejo, finalidad y características de los diferentes espacios de participación del Sitio Web, es discrecional de la Contraloría de Bogotá D.C., quien podrá en cualquier momento cambiarlos y/o eliminarlos, y/o determinar la cantidad de participantes admitidos en cada uno de ellos. La participación en los foros, chats, comentarios y otros espacios similares de participación institucional, implican la aceptación y conocimiento por parte del usuario de estas Condiciones de Uso, así como el compromiso irrevocable de cada usuario de respetar dichas condiciones.
Si un usuario no está conforme o de acuerdo con los presentes Términos y Condiciones, la Contraloría De Bogotá D.C. le sugiere no participar en él y/o en los Espacios.

Cada usuario acepta y faculta expresa e irrevocablemente a la Contraloría de Bogotá D.C., para revisar los comentarios u opiniones vertidos en los Espacios y/o

suprimir los que no se adecuen a las normas de convivencia plasmadas en las Condiciones de Uso de la información, así como a interrumpir la comunicación en caso que lo considere conveniente por tales motivos.

De igual forma la Contraloría de Bogotá D.C., se reserva el derecho de ejercer tal facultad cuando así lo estime conveniente, a su discreción, sin que por tal razón sea factible imputar responsabilidad alguna a la Contraloría de Bogotá D.C. por el no ejercicio de la facultad y/o por la existencia, ingreso, participación de usuarios no deseables y/o de comentarios u opiniones que no atienden estas recomendaciones.

Teniendo en cuenta que los comentarios y opiniones vertidas en los foros, comentarios y Blogs no provendrán de la Contraloría de Bogotá D.C. sino de terceros absolutamente ajenos, la Contraloría de Bogotá D.C. no se responsabiliza por el tenor de los mismos, así como tampoco presta conformidad ni discrepa con ellos, siendo entendido que emanan exclusivamente de su autor, y quedan bajo su completa responsabilidad.

Asimismo, queda prohibido ingresar comentarios, mensajes, opiniones, información, o similares, de contenido difamatorio, abusivo, contrario a la moral y las buenas costumbres, discriminatorio, ofensivo, obsceno, intimidatorio, calumnioso, inapropiado, ilegal, violatorio de derechos de terceros de cualquier índole, incluidos los derechos de los menores de edad, que cause daños y/o perjuicios, o impida o limite el derecho propio o ajeno a usar los Espacios y demás capítulos del sitio, constituya un delito o apología a un delito y/o incite a la violencia y/o a la comisión de delitos.

Ahora bien, en el supuesto de que este tipo de comentarios, mensajes, opiniones, información, o similares, ingrese en "los espacios", los usuarios, aceptan en forma expresa e incondicionada que la Contraloría de Bogotá D.C., sus funcionarios, proveedores, o anunciantes, NO serán responsables en modo alguno por las consecuencias de cualquier tipo y alcance que los mismos pudieran generar, frente a cualquier tercero, ya sea en virtud de su inclusión dentro de "los espacios" o por cualquier causa relacionada directa o indirectamente con el uso de los mismos.

Asimismo, la Contraloría de Bogotá D.C., sus servidores, proveedores o anunciantes, NO serán responsables de modo alguno en el supuesto que los comentarios, información, mensajes, opiniones, o similares, se vean afectados, eliminados, alterados, o modificados de alguna manera.

La Contraloría de Bogotá D.C., a su sólo juicio, se reserva el derecho de excluir de los Espacios, a aquellos usuarios que no se atengan a las presentes reglas o que no respeten los principios básicos de sana convivencia. Así como también de interrumpir y/o eliminar y/o excluir, total o parcialmente, en todos los casos, todo mensaje, opinión, información o similares que no se adecuen o resulten violatorios de las reglas y/o principios antes indicados.

Cada usuario deberá denunciar cualquier violación a las Condiciones de Uso de la Información institucional por parte de otros usuarios de la que tenga conocimiento, para lo cual utilizará los mecanismos de comunicación autorizados por la entidad para tales efectos, a fin de que la Contraloría de Bogotá D.C. tome las medidas que estén a su alcance respecto a dicha situación.