

REGISTRO DISTRITAL

RESOLUCIONES DE 2019

SECRETARÍA DISTRITAL DE SALUD DE BOGOTÁ D.C.

Resolución Número 1326 (Mayo 31 de 2019)

Por la cual se aprueba reforma estatutaria de la institución privada sin ánimo de lucro FUNDACIÓN MUJER Y FAMILIA, con domicilio en la ciudad de Bogotá

EL SECRETARIO DEL DESPACHO DE LA SECRETARIA DISTRITAL DE SALUD DE BOGOTÁ D.C.

En ejercicio con sus atribuciones legales y en especial las conferidas por el decreto 780 de 2016 expedido por el ministerio de salud y protección social, la resolución 13565 de 1991 expedida por el ministerio de salud (hoy ministerio de salud y protección social) y el decreto 581 de 1995 expedido por la alcaldía mayor de Bogotá, modificado por el decreto 530 de 2015 y,

CONSIDERANDO:

Que mediante resolución No. 976 de 19 de noviembre de 2012, expedida por la secretaria distrital de salud, se reconoció personería jurídica a la entidad sin ánimo de lucro denominada “FUNDACIÓN MUJER Y FAMILIA”.

Que la directora DALILA GONZÁLEZ ORTIZ, en su calidad de representante legal de la FUNDACIÓN MUJER Y FAMILIA, mediante oficio con radicado No. 2019ER29498 del 12 de abril de 2019, solicitó la aprobación de reforma estatutaria de dicha institución, adaptada por su Asamblea General, la cual consiste en modificar los artículos No. 1,2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28 y la eliminación de los artículos 29,30,31,32,33,34.

Que, para el trámite de aprobación de la reforma estatutaria antes referida, el Representante Legal de la Entidad allegó los siguientes documentos: 1) Acta de sesión extraordinaria de Asamblea No. 003 de fecha 08 de abril de 2019, mediante la cual se reforman los Estatutos de la FUNDACIÓN MUJER Y FAMILIA, 2) Estatutos de los cuales se solicita aprobar reforma, en un solo cuerpo y 3) Estatutos vigentes.

Que realizado el análisis de la solicitud y de los anteriores documentos, la Subdirección de Inspección, Vigilancia y Control de Servicios de Salud de esta Secretaría, expidió concepto técnico favorable, de fecha 29 de mayo 2019, para la aprobación de la reforma estatutaria solicitada por el Representante Legal de la Institución sin ánimo de lucro, denominada FUNDACIÓN MUJER Y FAMILIA, el cual concluyó que:

- a). *La documentación allegada por la institución sin ánimo de lucro denominada FUNDACIÓN MUJER Y FAMILIA, para el trámite de la reforma estatutaria, cuya aprobación solicita la Representante Legal de dicha institución, está conforme a lo establecido en el Acta de sesión extraordinaria de Asamblea No. 003 de fecha de 8 de abril de 2019.*
- b). *Los estatutos cuya aprobación solicita el Representante Legal de dicha institución sin ánimo de lucro denominada FUNDACIÓN MUJER Y FAMILIA, cumplen con las exigencia del decreto 780 de 2016 expedido por el Ministerio de Salud y Protección Social y la Resolución 13565 de 1991, expedida por el Ministerio de Salud (hoy Ministerio de Salud y Protección Social) y no contravienen al orden público, la moral ni las buenas costumbres, ni desvirtúan los fines para los cuales fue creada la referida institución. “*

En mérito de lo expuesto, éste despacho.

RESUELVE:

ARTÍCULO PRIMERO: Aprobar la reforma de los estatutos de la institución sin ánimo de lucro denominada FUNDACIÓN MUJER Y FAMILIA, con domicilio en la ciudad de Bogotá, adoptada por su Asamblea, mediante Acta de sesión extraordinaria No. 003 de fecha 8 de abril de 2019.

ARTÍCULO SEGUNDO: Adoptar el documento de los nuevos Estatutos presentados por la FUNDACIÓN MUJER Y FAMILIA, con las respectivas reformas, de acuerdo con lo expuesto en la parte motiva del presente acto administrativo.

ARTÍCULO TERCERO: En los aspectos no contemplados en los Estatutos de la entidad, se aplicara lo dispuesto en las normas que rigen las instituciones sin ánimo de lucro del sub sector privado del sector salud y demás normas aplicables.

ARTÍCULO CUARTO: Notifíquese personalmente al contenido de la presente Resolución al Representante Legal de la FUNDACIÓN MUJER Y FAMILIA, o a quien haga sus veces, haciéndole saber que, contra la misma solo procede el recurso de reposición ante este Despacho, el cual deberá interponerse por escrito en la diligencia de notificación personal, o dentro de los (10) diez días siguientes a ella, o a la notificación por aviso, o al vencimiento del termino de publicación según el caso.

ARTÍCULO QUINTO: Una vez ejecutoriado, el presente Acto Administrativo deberá ser publicado en la Gaceta Distrital y se deberá allegar copia de la misma a la oficina del Registro de la Secretaria Distrital de Salud.

ARTÍCULO SEXTO: La presente Resolución rige a partir de su publicación.

NOTIFÍQUESE PUBLÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los treinta y ún (31) días del mes de mayo del año dos mil diecinueve (2019).

LUIS GONZALO MORALES SÁNCHEZ
Secretario de Despacho

**SUBDIRECCIÓN INSPECCIÓN VIGILANCIA Y
CONTROL DE SERVICIOS DE SALUD
CONCEPTO TÉCNICO DE FECHA 29 DE MAYO
DE 2019**

Realizado el análisis de la solicitud y de los documentos presentados por la entidad sin ánimo de lucro, denominada “FUNDACIÓN MUJER Y FAMILIA”, para la aprobación de reforma estatutaria, como lo son: 1) Acta de sesión extraordinaria de Asamblea No. 003 de fecha 8 de abril de 2019, mediante la cual se reforman los estatutos de la FUNDACIÓN MUJER Y FAMILIA 2) Estatutos de los cuales se solicita aprobar reforma, en un solo cuerpo. Y 3) Estatutos Vigentes, la Subdirección de Inspección, Vigilancia y Control de Servicios de Salud de esta Secretaria, por cuyo conducto se presentó solicitud de aprobación de reforma estatutaria, expiden concepto técnico favorable al respecto, teniendo en cuenta que:

- a). La documentación allegada por la institución sin ánimo de lucro denominada FUNDACIÓN MUJER Y FAMILIA, para el trámite de reforma estatutaria, cuya aprobación solicita el Representante Legal de dicha Institución, está conforme a lo establecido en el Acta de sesión extraordinaria de Asamblea No. 003 de fecha 08 de abril de 2019.
- b). Los Estatutos cuya aprobación solicita el Representante Legal de dicha institución sin ánimo de lucro denominada FUNDACIÓN MUJER Y FAMILIA, cumplen con las exigencias del Decreto 780 de 2016 expedido por el Ministerio de Salud y Protección Social y la Resolución 13565 de 1991, expedida por el Ministerio de Salud (hoy Ministerio de Salud y Protección Social) y no contraviene el orden público, la moral ni las buenas costumbres, ni desvirtúan los fines para los cuales se fue creada la referida institución.

MARTHA JUDITH FONSECA SUÁREZ
Subdirectora Inspección, Vigilancia y Control de Servicios de Salud

Resolución Número 519 (Septiembre 24 de 2019)

“Por la cual se modifica el Manual Específico de Funciones y de Competencias Laborales para un empleo de la Planta de Personal de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.”

EL SECRETARIO GENERAL (E) DE LA ALCALDÍA MAYOR DE BOGOTÁ, DISTRITO CAPITAL
En ejercicio de sus facultades legales, en especial las previstas en el numeral 9 del artículo 1º del Decreto Distrital 101 de 2004, Decreto 479 de 2019 y

CONSIDERANDO:

Que el artículo 122 de la Constitución Política establece: “No habrá empleo público que no tenga funciones detalladas en ley o reglamento, y para proveer los de carácter remunerado se requiere que estén contemplados en la respectiva planta y previstos sus emolumentos en el presupuesto correspondiente”.

Que mediante Resolución 160 de 2019 se modificó el Manual Específico de Funciones y de Competencias Laborales para los empleos de la planta de personal de la Secretaría General - Alcaldía Mayor de Bogotá, en el sentido de adicionar las competencias funcionales transversales a los empleos pertinentes.

Que en la Resolución en mención para el empleo de profesional universitario código 219, grado 13 con funciones en la Dirección Administrativa y Financiera cuyo propósito principal es: *“Aplicar procesos que permitan la recepción, manejo, consolidación, clasificación, registro, distribución y control de la gestión documental, de acuerdo a las normas y reglamentos que regulan la materia.”*, se cometió un error de transcripción al establecer en el requisito de Estudios Título de Formación Técnica o Tecnológica, en lugar de Título Profesional.

Que el Decreto Distrital 367 de 2014 “Por el cual se actualiza el Manual General de Requisitos para los

empleos públicos correspondientes a los Organismos pertenecientes al Sector Central de la Administración Distrital de Bogotá, D.C. y se dictan otras disposiciones” en su artículo 4º, numeral 4.3 establece como requisito de estudio para los empleos del nivel profesional, título de formación profesional.

Que el artículo 1º del Decreto 051 de 2018 que adiciona el “PARÁGRAFO 3º del artículo 2.2.2.6.1 del Decreto 1083 de 2015 establece “En el marco de lo señalado en el numeral 8 del artículo 8 de la Ley 1437 de 2011, Código de Procedimiento Administrativo y de lo Contencioso Administrativo, las entidades deberán publicar, por el término señalado en su reglamentación, las modificaciones o actualizaciones al manual específico de funciones y de competencias laborales. La administración, previo a la expedición del acto administrativo lo socializara con las organizaciones sindicales.” En este sentido, se realizó la mencionada socialización el día 24 de septiembre de 2019.

Que mediante oficio No. 2019 EE2347 del 23 de septiembre de 2019, la Directora del Departamento Administrativo del Servicio Civil Distrital, expidió concepto técnico favorable para la modificación del Manual Específico de Funciones y de Competencias Laborales de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C, en el sentido de modificar el requisito de estudio para el empleo Profesional Universitario Código 219 Grado 13 de la Dirección Administrativa y Financiera, de la Subsecretaría Corporativa, de conformidad con la normativa vigente.

Que de conformidad con lo anterior, se hace necesario modificar el Manual Específico de Funciones y Competencias Laborales para un Empleo de la planta de personal de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1º:- Modificar el Manual Específico de Funciones y de Competencias Laborales para un Empleo de la Planta de Personal de la Secretaría General de la Alcaldía Mayor de Bogotá D.C, el cual quedará así:

I. IDENTIFICACIÓN DEL EMPLEO	
Nivel:	Profesional
Denominación del Empleo:	Profesional Universitario
Código:	219
Grado:	13
No. de Cargos:	16
Dependencia:	Donde se ubique el cargo
Cargo del Jefe Inmediato:	Quién ejerza la supervisión directa

II. 219-13 DIRECCIÓN ADMINISTRATIVA Y FINANCIERA	
III. PROPÓSITO PRINCIPAL	
Aplicar procesos que permitan la recepción, manejo, consolidación, clasificación, registro, distribución y control de la gestión documental, de acuerdo a las normas y reglamentos que regulan la materia.	
IV. DESCRIPCIÓN DE LAS FUNCIONES ESENCIALES	
1. Realizar la gestión y trámite de los archivos y documentos de la Entidad de acuerdo con las normas y procedimientos vigentes. 2. Efectuar el suministro de los registros bibliográficos, cartográficos y expedientes requeridos por usuarios (as), con el fin de suplir sus necesidades ante los trámites que requieran. 3. Verificar la información que se suministra al usuario, verificando que la información sea veraz y confiable. 4. Aplicar metodologías para la organización, la transferencia, la disposición de documentos, la preservación a largo plazo y la valoración de los archivos, de manera eficiente y de acuerdo con la normatividad vigente. 5. Realizar seguimiento y evaluación al proceso de numeración y fechado de los decretos, resoluciones, circulares, directivas, que hayan sido firmados e impartir las instrucciones para su oportuna distribución en las dependencias, entidades y servidores interesados, de manera eficiente y oportuna. 6. Realizar seguimiento al trámite de correspondencia interna y externa de la entidad y el cumplimiento de las normas, procedimientos y sistemas establecidos, de manera oportuna y eficiente. 7. Realizar seguimiento del cumplimiento de las normas y procedimientos en la elaboración y presentación de las comunicaciones, trámites internos y externos que genera y recibe la secretaría general de la alcaldía mayor de Bogotá, en concordancia con los lineamientos técnicos y normativos. 8. Ejercer actividades de planeación, evaluación y seguimiento de los procesos de garantía de calidad de la dependencia acorde con los lineamientos establecidos y la normatividad vigente. 9. Desempeñar las demás funciones que le sean asignadas por el jefe inmediato, relacionadas con la naturaleza del cargo y el área de desempeño.	
V. CONOCIMIENTOS BÁSICOS O ESENCIALES	
1. Normatividad Gestión Documental. 2. Sistemas y metodología de archivo y gestión documental. 3. Procesos administrativos. 4. Estatuto Anticorrupción. 5. Normas técnicas de calidad. 6. Herramientas ofimáticas.	
VI. COMPETENCIAS COMPORTAMENTALES	
COMUNES	POR NIVEL JERÁRQUICO
• Aprendizaje Continuo. • Orientación a resultados. • Orientación al usuario y al ciudadano. • Compromiso con la organización. • Trabajo en equipo. • Adaptación al cambio.	• Aporte técnico-profesional. • Comunicación efectiva. • Gestión de procedimientos. • Instrumentación de decisiones. • Manejo de la Información y de los recursos. • Uso de tecnologías de la información y la comunicación. • Confiabilidad técnica. • Capacidad de análisis.
VII. COMPETENCIAS ÁREAS TRANSVERSALES	
COMPETENCIAS LABORALES TRANSVERSALES	COMPETENCIAS COMUNES TRANSVERSALES
• Gestión de procedimientos de calidad. • Resolución de conflictos. • Toma de decisiones.	• Transparencia. • Gestión de Procedimientos de Calidad
VIII. REQUISITOS DE ESTUDIO Y EXPERIENCIA	
Estudios	Experiencia
Título de formación profesional en: Administración de Sistemas de Información y Documentación; Administración Documental; Archivística; Archivo; Bibliotecología; Bibliotecología y Archivística; Ciencia de la Información y Bibliotecología; Ciencia de la Información y la Documentación; Ciencia de la Información, Bibliotecología, Documentación y Archivística; Ciencia de la Información-Bibliotecología; Ciencias de la Información y la Documentación; Ciencias de la Información, Documentación y Archivística; Desarrollo de Procesos y Servicios Bibliotecarios; Documentación y Archivística; Documentología; Gestión Bibliotecaria; Gestión Documental; Sistemas de Información y Documentación; Sistemas de Información; Sistemas de la Información, Documentación y Archivística; del núcleo básico de Bibliotecología, otras Ciencias Sociales y Humanas. Tarjeta o matrícula profesional en los casos reglamentados por la Ley.	Treinta y seis (36) meses de experiencia profesional relacionada con las funciones del cargo.

PARÁGRAFO: Para los requisitos de estudio y experiencia previstos en este manual, se aplicarán las equivalencias previstas en el Decreto Ley 785 de 2005 y el Decreto Distrital 367 de 2014, y las demás normas que los modifiquen, complementen o adicionen.

ARTÍCULO 2º- Los demás apartes de la Resolución 160 de 2019 continúan vigentes.

ARTÍCULO 3º- La presente Resolución rige a partir de la fecha de su refrendación por parte de la Directora del Departamento Administrativo del Servicio Civil Distrital y modifica parcialmente la Resolución 160 de 2019.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los veinticuatro (24) días del mes de septiembre de dos mil diecinueve (2019).

JUAN CARLOS MALAGÓN BASTO
Secretario General (E.)

Refrendado,

NIDIA ROCÍO VARGAS
Directora del Departamento Administrativo del Servicio Civil Distrital

Resolución Reglamentaria Número 038 (Septiembre 24 de 2019)

“Por la cual se actualizan las Políticas de Seguridad de la Información de la Contraloría de Bogotá, D.C.”

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

CONSIDERANDO:

Que de conformidad con el artículo 269 Constitucional y con el literal b) del artículo 4 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, las entidades públicas, según la naturaleza de sus funciones, deben implementar políticas como guías de acción, como uno de los elementos del sistema de control interno institucional.

Que mediante el Decreto 1008 del 14 de junio de 2018, se establecieron los lineamientos generales de la Política de Gobierno Digital y se subrogó el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, en cuanto se refiere a la Política Gobierno Digital para Colombia, antes Estrategia de Gobierno en Línea.

Que el artículo No. 2.2.9.1.2.2 del citado Decreto 1008 de 2018, estipula que para la implementación de la Política de Gobierno Digital, las entidades públicas deberán aplicar el Manual de Gobierno Digital que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de esta Política de Gobierno Digital.

Que el Acuerdo 658 de 2016 expedido por el Concejo de Bogotá, D.C., modificado por el Acuerdo 664 de 2017, regula en el artículo 40, las funciones de la Dirección de Tecnologías de la Información y las Comunicaciones, entre otras, correspondiéndole 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.; coordinar la aplicación a todo nivel de la organización de los estándares, buenas prácticas y principios para el manejo de la información y desarrollar estrategias para el flujo eficiente de la información en todos los procesos de la Entidad.

Que de conformidad con el Decreto 1499 de 2017, modificatorio del Decreto 1083 de 2015, Decreto Único Reglamentario del Sector de la Función Pública y con el fin de incorporar la estructura definida en la Dimensión No. 7ª - Control Interno del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG, la Contraloría de Bogotá, D.C., mediante Resolución Reglamentaria No. 038 de 2018, adoptó la nueva versión del Modelo Estándar de Control Interno – MECI para la Entidad.

Que de acuerdo con lo aprobado en el Comité SIGEL, en sesión del 11 de junio de 2019, según Acta No. 03 y en el Comité Coordinador de Teletrabajo, en sesión del 27 de agosto del 2019, según Acta No.06, es necesario actualizar las Políticas de Seguridad de la Información de la Contraloría de Bogotá, D.C., acorde con la normatividad vigente y con lo establecido en la Norma Técnica Colombiana ISO/IEC 27001:2013, en relación con las directrices para proteger la información, asegurando que en ella se cumplan las características de integridad, disponibilidad y confidencialidad, mediante la ejecución de acciones en concordancia con disposiciones operativas y tecnológicas y con los objetivos estratégicos.

Que la metodología utilizada para la actualización y reorganización de estas políticas consistió en la comparación entre lo descrito en la Guía No.2 “*Elaboración de la Política General de Seguridad y Privacidad de la Información*” del Ministerio de la Información y las Comunicaciones – MinTIC, las Políticas de la Seguridad de la Información, establecidas en el anexo A de la Norma Técnica Colombiana ISO/IEC 27001:2013 y las Políticas de Tecnologías vigentes de la Contraloría de Bogotá, D.C., de conformidad con el Decreto 1008 de 2018.

Que en virtud de lo expuesto, es necesario actualizar las Políticas de Seguridad y Privacidad de la Información en la Contraloría de Bogotá, D.C., adoptadas mediante la Resolución Reglamentaria No. 022 del 19 de abril de 2018, debiéndose, entre otros aspectos, modificar el nombre a Políticas de Seguridad de la Información.

RESUELVE:

ARTÍCULO PRIMERO. Actualizar las “*Políticas de Seguridad de la Información de la Contraloría de Bogotá, D.C. – PGTI-16, Versión 3.0*”, las cuales se anexan y hacen parte integral de la presente Resolución.

ARTÍCULO SEGUNDO. El Comité de Política de Gobierno Digital de la Contraloría de Bogotá, D.C. –

PGDIGITAL, será el encargado de realizar la difusión, seguimiento al cumplimiento y actualización de las Políticas de Seguridad de la Información.

PARÁGRAFO. La Dirección de Tecnologías de la Información y las Comunicaciones, apoyará la ejecución de las Políticas.

ARTÍCULO TERCERO. Es responsabilidad de los Directores, Subdirectores, Jefes de Oficina y Gerentes, velar por la aplicación de la normatividad, procedimientos y demás directrices establecidas para la aplicación de las Políticas.

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 del 19 de abril de 2018.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los veinticuatro (24) días del mes de septiembre de dos mil diecinueve (2019).

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

Aprobación		Revisión Técnica
Firma:		
Nombre:	Carmen Rosa Mendoza Suarez	Mercedes Yunda Monroy
Cargo:	Directora Técnica	Directora Técnica
Dependencia:	Dirección de Tecnologías de la Información y las Comunicaciones	Dirección de Planeación
R.R. No.	038	Fecha: SEPTIEMBRE 24 DE 2019

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

MARIA ANAYME BARÓN DURÁN
Contralora Auxiliar

MERCEDES YUNDA MONROY
Directora Técnica de Planeación

CARMEN ROSA MENDOZA SUÁREZ
Directora Técnica de Tecnologías de la Información y las Comunicaciones

Bogotá, D.C., Septiembre 2019

TABLA DE CONTENIDO

1.	INTRODUCCIÓN.....	4
2.	OBJETIVO GENERAL DEL SGSI.....	4
2.1.	OBJETIVOS ESPECÍFICOS DEL SGSI	5
3.	ALCANCE/APLICABILIDAD.....	5
4.	CUMPLIMIENTO	5
5.	TERMINOLOGÍA	6
6.	POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACION	7
7.	POLÍTICAS ESPECIFICAS DE LA SEGURIDAD DE LA INFORMACION	8
7.1.	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.....	9
7.2.	DISPOSITIVOS MÓVILES.....	10
7.3.	TELETRABAJO	11
7.4.	CONTROL DE ACCESO LÓGICO Y FÍSICO	12
7.5.	CONTROLES CRIPTOGRÁFICOS	14
7.6.	ESCRITORIO LIMPIO Y PANTALLA LIMPIA	15
7.7.	COPIAS DE RESPALDO.....	16
7.8.	TRANSFERENCIA DE LA INFORMACIÓN	17
7.9.	DESARROLLO SEGURO.....	18
7.10.	RELACIONES CON LOS PROVEEDORES	19
7.11.	GESTIÓN DE ACTIVOS.....	21
7.12.	NO REPUDIO.....	22
7.13.	PRIVACIDAD Y CONFIDENCIALIDAD.....	22
7.14.	INTEGRIDAD	23
7.15.	DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN.....	24
7.16.	REGISTRO Y AUDITORÍA	25
7.17.	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	26
7.18.	CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN ..	27
8.	APROBACION Y ACTUALIZACIÓN	28
9.	CONTROL DE CAMBIOS.....	28

1. 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 el cumplimiento de las funciones misionales y de apoyo, así como para la toma de decisiones, 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 el 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, la ciudadanía, los funcionarios, terceros, contratistas, proveedores, sujetos de control y en cumplimiento de las normas legales vigentes.

De conformidad con lo anterior, se establece dentro del Subsistema de Gestión de Seguridad de la Información – SGSI de la Contraloría de Bogotá D.C., el documento de políticas de seguridad de la información, el cual expresa el compromiso de la alta dirección con la seguridad de la información, así como, la identificación de las reglas y procedimientos que cada usuario que accede o usa los recursos tecnológicos de la Entidad debe conocer para preservar la confidencialidad, la integridad y la disponibilidad de los sistemas y la información que usan.

Estas políticas serán revisadas 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 dichas políticas sigan siendo adecuadas y ajustadas a los requerimientos de la Entidad.

2. OBJETIVO GENERAL DEL SGSI

Establecer las directrices para la proteger la información de la Contraloría de Bogotá D.C., asegurando que en ella se cumplan las características de integridad, disponibilidad y confidencialidad, mediante la ejecución de acciones en concordancia con disposiciones legales, operativas, tecnológicas y de acuerdo al objetivo estratégico, manteniendo la confianza de los usuarios internos y externos de los procesos, trámites y servicios que presta la Entidad.

2.1. OBJETIVOS ESPECÍFICOS DEL SGSI

Los siguientes son los objetivos de seguridad de la información para la Contraloría de Bogotá D.C.:

- Aplicar controles de seguridad que permitan proteger los activos de información, buscando mantener la confidencialidad, la disponibilidad e integridad.
- Garantizar la integridad, confidencialidad y el acceso a la información de acuerdo a los niveles y criterios de seguridad que establecidos por la Entidad y a los exigidos por la normatividad vigente.
- Identificar mediante una adecuada evaluación del riesgo, el valor de la información, así como las vulnerabilidades y las amenazas a las que están expuestos los activos de información.
- Minimizar, gestionar y dar tratamiento a los riesgos de seguridad de la información, para que sean conocidos y según su impacto sean asumidos, transferidos, minimizados y/o eliminados de forma eficiente y adaptada a los cambios que se produzcan en la Entidad, el entorno y la tecnología.
- Asegurar el mejoramiento continuo de la seguridad de la información para responder a Los cambios futuros.
- Cumplir con los requisitos legales vigentes aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información.

3. ALCANCE/APLICABILIDAD

El alcance del Subsistema de Gestión de la Seguridad de la Información – SGSI, aplica a los activos de información de los procesos que conforman el mapa de procesos de la Contraloría de Bogotá D.C.

Por lo anterior, estas políticas aplican a toda la Entidad, sus funcionarios, contratistas, sujetos de control fiscal, usuarios internos y externos que acceden o hacen uso de cualquier activo de información, así como exfuncionarios y excontratistas que hayan tenido acceso a 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.

4. CUMPLIMIENTO

Tanto la política General del SGSI como las políticas específicas que de esa se desprendan son de obligatorio cumplimiento para todas las personas mencionadas dentro del alcance y deberán dar acatamiento al 100% de las mismas.

El incumplimiento a la política de Seguridad y Privacidad de la Información de la Contraloría de Bogotá D.C., traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las Lineamientos que competen al gobierno nacional y territorial en cuanto a seguridad de la Información se refiere.

5. TERMINOLOGÍA

Activo: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización.

Activo de Información: en relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Activo de información: Conocimiento o datos que tienen valor para el individuo u organización¹.

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.

Autenticación: Asegurar que una característica declarada de una Entidad es correcta.

Autenticidad: Propiedad de que una Entidad es lo que dice ser.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, Entidades o procesos no autorizados.

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

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una Entidad autorizada.

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.

Información²: Es un activo esencial para el negocio de una organización y por consiguiente necesita ser debidamente protegida. La información puede ser almacenada en muchas formas, incluyendo formato digital (por ejemplo, ficheros almacenados en medios electrónicos u ópticos), formato físico (por ejemplo, en papel), así como la información intangible que forma parte del conocimiento de los empleados. La información puede ser transmitida por diferentes medios incluyendo: mensajería, comunicación electrónica o verbal. Independientemente del formato o del medio por el cual se transmite la información, es necesaria siempre una protección adecuada.

¹ ISO/IEC 27032:2012

² NTC-ISO/IEC27000:2016

Integridad: Propiedad de exactitud y completitud de la información.

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

Mejora Continua: El objetivo de la mejora continua de un SGSI es aumentar la probabilidad de lograr los objetivos relativos a la preservación de la confidencialidad, disponibilidad e integridad de la información. El foco de la mejora continua es buscar oportunidades para la mejora y no asumir que las actividades de gestión existentes son suficientemente buenas o tan buenas como podrían ser.

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

Seguridad de la información: Asegura la confidencialidad, integridad y disponibilidad de la información. La seguridad de la Información implica la aplicación y gestión de controles apropiados que involucren la consideración de un amplio rango de amenazas, con el objetivo de asegurar el éxito empresarial sostenido, así como su continuidad, y minimizar las consecuencias de los incidentes de la seguridad de la información.

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

6. POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACION

La siguiente es la Política de Seguridad de la Información establecida para la Contraloría de Bogotá, D.C.:

“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 Lineamientos legales vigentes, para lo cual, adopta políticas, procedimientos, lineamientos y asigna responsabilidades para la adecuada gestión de la seguridad de la información”.

La alta dirección de la Contraloría de Bogotá D.C., entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un subsistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Distrito y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Para la Contraloría de Bogotá D.C., la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, las políticas del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en los procesos de la Entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de la ciudadanía y funcionarios.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y grupos de interés de la Contraloría de Bogotá D.C.
- Garantizar la continuidad del negocio frente a incidentes.

7. POLÍTICAS ESPECÍFICAS DE LA SEGURIDAD DE LA INFORMACION

A continuación, se establecen las políticas específicas de la seguridad de la información que soportan el SGSI de la Contraloría de Bogotá D.C.:

- La Contraloría de Bogotá D.C., ha decidido definir, implementar, operar y mejorar de forma continua un Subsistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la Entidad y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas o terceros.
- La Contraloría de Bogotá D.C., protegerá la información generada, procesada o resguardada por los procesos misionales y activos de información que hacen parte de los mismos.
- La Contraloría de Bogotá D.C., protegerá la información creada, procesada, transmitida o resguardada por sus procesos misionales, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La Contraloría de Bogotá D.C., protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La Contraloría de Bogotá D.C., controlará la operación de sus procesos misionales garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Contraloría de Bogotá D.C., implementará control de acceso a la información, sistemas y recursos de red.
- La Contraloría de Bogotá D.C., garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- La Contraloría de Bogotá D.C., garantizará a través de una adecuada gestión de los incidentes de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La Contraloría de Bogotá D.C., garantizará la disponibilidad de sus procesos misionales y la continuidad de su operación basado en el impacto que pueden generar los incidentes.
- Contraloría de Bogotá D.C., garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
- Con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información, Contraloría de Bogotá D.C., desarrollará e implementará controles de seguridad de la información, los cuales serán establecidos en los procedimientos del Sistema Integrado de Gestión.

A continuación, se describen en detalle las políticas específicas de la seguridad de la información que soportan el SGSI de la Contraloría de Bogotá D.C.

7.1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

En la Contraloría de Bogotá D.C., se definen los roles y responsabilidades los cuales ejecutan actividades de administración, operación y gestión de la Seguridad de la Información, para prevenir que se presenten conflictos de intereses que conlleven a modificaciones no autorizadas o el uso inadecuado de los activos de la información, esto es posible organizando una adecuada comunicación para que la Entidad pueda aprobar los lineamientos de Seguridad de la Información así como coordinar la implementación de la seguridad en todos los procesos de la Entidad.

Lineamientos:

- 7.1.1.** Los diferentes roles y sus responsabilidades del Subsistema de Gestión de Seguridad de la Información están definidos en el numeral 7.4.6. Roles y Responsabilidades del manual del Sistema Integrado de Gestión – SIG de la Entidad.
- 7.1.2.** El Comité Técnico de Seguridad de la Información y Gobierno en Línea – SIGEL o quien haga sus veces, establece las políticas generales para garantizar la seguridad y la integridad de la información, la implementación de la Política de Gobierno Digital, 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.
- 7.1.3.** 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.
- 7.1.4.** Se debe asignar al responsable de cada activo o proceso de Seguridad de la Información, y se deben documentar los detalles de esta responsabilidad.

- 7.1.5. Se deben definir las responsabilidades para las actividades de gestión del riesgo de la Seguridad de la Información
- 7.1.6. La estructura de organización de Seguridad de la Información debe ser publica y clara en sus responsabilidades para cada uno de los roles definidos.
- 7.1.7. Para tener la capacidad de cumplir las responsabilidades en seguridad de la información, los funcionarios designados deberán ser competentes y se les deberá brindar oportunidades de mantenerse actualizados con los avances en este tema.

7.2. DISPOSITIVOS MÓVILES

El uso de dispositivos móviles, limitando el alcance de estos dispositivos inicialmente a los computadores portátiles (notebooks y laptops) y unidades de almacenamiento externo que contengan información de la Entidad y que a su vez se utilicen para el manejo de esta información, deben ser controlados de acuerdo al análisis de riesgo correspondiente, y mitigar el impacto a que se expone la información como su pérdida, alteración y divulgación no autorizada.

Lineamientos:

- 7.2.1. Se debe contar con un inventario actualizado de dispositivos móviles (computadores portátiles y unidades de almacenamiento externo suministrados por la Entidad que no sean de consumo) utilizados para almacenar, procesar y/o transmitir información de la Contraloría de Bogotá D.C.
- 7.2.2. La Contraloría de Bogotá D.C., establecerá lineamientos para el acceso a redes inalámbricas, la instalación de software 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.
- 7.2.3. En la Contraloría de Bogotá D.C., se adoptarán medidas de apoyo en seguridad de la información para ejercer correctamente la gestión de los riesgos en el acceso a la información, el procesamiento o almacenamiento que se presenten al utilizar los dispositivos móviles en lugares de trabajo remotos.
- 7.2.4. Ante la pérdida del equipo institucional, ya sea por extravío o hurto, deberá informar de manera inmediata a la Dirección Administrativa y Financiera y continuar con el procedimiento administrativo por pérdida de elementos establecido por la Entidad.
- 7.2.5. 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, se debe evitar hacer uso de estos para cuestiones personales, así como en lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo.

- 7.2.6. Los dispositivos móviles institucionales deben contar con mecanismos de autenticación para desbloquear el equipo y poder tener acceso a su información y servicios.
- 7.2.7. Si desde el dispositivo móvil se procesa información se debe contar con un software instalado y actualizado contra códigos maliciosos, firewall personal para prevenir incidentes de seguridad.
- 7.2.8. Se deben generar recomendaciones del uso y cuidado de tipo físico cuando el dispositivo se encuentre fuera de las instalaciones de la entidad. El usuario debe propender por el cuidado físico del dispositivo cuando este se encuentre fuera de la entidad, esto es resguardo del dispositivo en lugar seguro, no exposición ni uso en lugares que pueden ser catalogados como inseguros.
- 7.2.9. Es responsabilidad del usuario realizar periódicamente copias de respaldo a la información que se almacena en el dispositivo.

7.3. TELETRABAJO

La Contraloría de Bogotá D.C., según lo establecido en los procedimientos de la Entidad debe proteger la información a la que tienen acceso los funcionarios, por razón y motivo de su cargo, en consecuencia y respecto a los teletrabajadores se indica, el acceso a los diferentes entornos y sistemas informáticos de la Entidad será efectuado siempre y en todo momento bajo el control y responsabilidad del teletrabajador, siguiendo los procedimientos establecidos por la Entidad. El teletrabajador se compromete a respetar la legislación en materia de protección de datos, las políticas de seguridad y privacidad de la información que la Entidad ha implementado, como también con el cumplimiento de:

Lineamientos:

- 7.3.1. El funcionario autorizado para trabajar en la modalidad de teletrabajo deberá acoger las recomendaciones dadas por el Comité Coordinador de Teletrabajo, frente a posibles riesgos tecnológicos, identificados en la visita de valoración y adoptará los controles necesarios para la mitigación de dichos riesgos.
- 7.3.2. Los teletrabajadores deben cumplir con el esquema de licenciamiento de software definido, así como, mantener el antivirus activo y actualizado y respetar los controles que la Contraloría de Bogotá D.C., ha definido y que le apliquen.
- 7.3.3. El acceso remoto únicamente se podrá realizar desde equipos propiedad de la Contraloría de Bogotá, o los aprobados por el Comité Coordinador de Teletrabajo, cumpliendo los requisitos y mecanismos de seguridad establecidos por la entidad, para conexión segura.
- 7.3.4. Los funcionarios utilicen su equipo personal para teletrabajar, deben separar el entorno de teletrabajo del entorno personal, utilizando cuentas diferentes para cada uno de ellos.
- 7.3.5. Los teletrabajadores deben cumplir con las medidas de seguridad que la entidad haya implementado para asegurar la confidencialidad e integridad de los datos de carácter

personal a los que tenga acceso, así como, comprometerse a no ceder en ningún caso a terceras personas los datos de carácter personal a los que tenga acceso.

- 7.3.6.** En el esquema de teletrabajo no se permite almacenar información clasificada en servicios en la nube no licenciados por la entidad.
- 7.3.7.** Los teletrabajadores son responsables de la información utilizada y procesada para el desarrollo de sus funciones, por tal razón deberán realizar de copias de respaldo de la información regularmente para asegurar la continuidad de las funciones realizadas.
- 7.3.8.** La administración, mantenimiento y soporte de equipos que son propiedad de los teletrabajadores, es responsabilidad de los mismos, en ningún momento la Contraloría de Bogotá D.C., se hace responsable por estas actividades; la entidad las asume, para los equipos que suministre al teletrabajador.
- 7.3.9.** En caso de pérdida, suplantación o robo de un equipo portátil o cualquier medio de almacenamiento, utilizado para teletrabajar y que contenga información relacionada con la Contraloría de Bogotá D.C., se deberá realizar de forma inmediata, el respectivo reporte de acuerdo con el procedimiento para la Gestión de Incidentes de Seguridad vigente en la entidad y se deberá poner la denuncia ante la autoridad competente, si aplica.

7.4. CONTROL DE ACCESO LÓGICO Y FÍSICO

En la Contraloría de Bogotá D.C., se establecerán medidas de control de acceso a la información y demás servicios de TI, estos controles deben limitar el acceso a la información de acuerdo a la clasificación de la información, 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.

Lineamientos:

- 7.4.1.** La Contraloría de Bogotá D.C, se aplicará un procedimiento mediante el cual se brinden las pautas para una correcta gestión del control de acceso a usuarios en todos sus niveles; en este procedimiento se 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 periódico de las acciones y los cambios a las cuentas privilegiadas.
- 7.4.2.** Cuando se solicite tener acceso a algún recurso o servicio de la Entidad, se deberá realizar el correspondiente análisis de riesgo con la participación del propietario de la información y de los activos asociados, con el fin de determinar los privilegios a otorgar y definir los mecanismos necesarios para su protección.
- 7.4.3.** En ningún caso se otorgará acceso a terceros, a la información, a las instalaciones, o a centros de procesamiento de información crítica, si previamente no se han cumplido los controles de seguridad establecidos.
- 7.4.4.** Las asignaciones de privilegios en las aplicaciones para los diferentes usuarios estarán determinadas por el procedimiento de control de acceso a usuarios estos

- privilegios deben revisarse a intervalos regulares y ser modificados o reasignados cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.
- 7.4.5.** Se debe usar una identificación de usuario (ID) para permitir que los funcionarios queden vinculados y sean responsables de sus acciones.
- 7.4.6.** Se debe retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado de ser parte de la Entidad.
- 7.4.7.** Los privilegios de administración de cualquier equipo de cómputo (servidor, estación de trabajo, desktop, portátil, o equipo activo de red), deben ser asignados exclusivamente a los administradores del sistema designados en la Dirección de Tecnologías de la Información y las Comunicaciones de la Entidad, en ningún caso se debe autorizar estos privilegios de acceso al usuario del equipo.
- 7.4.8.** Cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debe suministrar de manera segura una contraseña temporal, la cual se debe forzar a cambiar inmediatamente realice el siguiente ingreso al sistema.
- 7.4.9.** Las contraseñas nunca se deben almacenar en sistemas de computador o en otro medio en un formato no protegido.
- 7.4.10.** Las contraseñas predeterminadas por el fabricante se deben cambiar inmediatamente después de la instalación de los sistemas o del software.
- 7.4.11.** Toda contraseña es personal e intransferible, y cada usuario es responsable de las acciones que se ejecuten con el usuario que se le ha asignado.
- 7.4.12.** Todos los usuarios deberán cumplir los siguientes lineamientos para la construcción de sus contraseñas:
- Deben estar compuestas mínimo de ocho (8) caracteres que deben ser combinados (mayúsculas, minúsculas, números y caracteres especiales).
 - No deben ser idénticas o similares a contraseñas que hayan usado previamente, o al nombre o apellido del usuario.
 - La contraseña tendrá una vigencia máxima de 90 días, finalizando este periodo el usuario deberá realizar el cambio correspondiente.
 - No deben ser fáciles de inferir o adivinar.
 - No deben ser susceptibles a ataques de diccionario, es decir, que no incluya palabras que podrían ser encontradas en un diccionario.
- 7.4.13.** Para la selección de controles de las áreas protegidas se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil y otras formas de desastres naturales o provocados por el hombre.
- 7.4.14.** El cableado de energía eléctrica y comunicaciones que transportan datos o brinda apoyo a los servicios de información deben protegerse contra interceptación o daños.
- 7.4.15.** Se debe garantizar la seguridad física de los centros de cableado incluyendo, entre otros, el sistema eléctrico y el control de acceso biométrico.
- 7.4.16.** Todas las puertas que utilicen sistema de control de acceso, deben permanecer cerradas, y es responsabilidad de todos los funcionarios y terceros autorizados evitar que las puertas se dejen abiertas.
- 7.4.17.** Se debe exigir a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado en la Entidad, mientras permanezcan dentro de sus instalaciones.

- 7.4.18.** Los visitantes deberán permanecer acompañados de un funcionario cuando se encuentren dentro de alguna de las áreas identificadas como seguras de la Entidad.
- 7.4.19.** Es responsabilidad de todos los usuarios internos y externos acatar las Lineamientos de seguridad y mecanismos de control de acceso a las instalaciones de la Entidad.
- 7.4.20.** Todas las áreas que se hayan definido como protegidas y activos de información que la componen, deben ser protegidas de acceso no autorizado mediante controles y tecnologías de autenticación fuerte.
- 7.4.21.** Todo acceso físico a las áreas protegidas deberá estar manejado según los lineamientos definidos por los procedimientos designados para el manejo de estas áreas.
- 7.4.22.** En las áreas seguras donde se encuentren activos de información, se debe cumplir como mínimo con los siguientes lineamientos:
- No se deben consumir alimentos ni bebidas.
 - No se deben ingresar elementos inflamables.
 - No se debe permitir el acceso de personal ajeno sin que este acompañado por un empleado durante el tiempo que dure su visita.
 - No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.
 - No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
 - No se permite el ingreso de equipos electrónicos (computadores portátiles, cámaras, celulares, USB, etc.), así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.

7.5. CONTROLES CRIPTOGRÁFICOS

La política de seguridad de controles criptográficos define el uso de controles encaminados a la protección de la información de la Entidad con base en análisis de riesgos que se realicen, con el fin de garantizar una adecuada protección de la confidencialidad, integridad y disponibilidad de la información, esta política aplica a todas las personas que usen mecanismos criptográficos sobre los servicios o información de la Contraloría de Bogotá D.C.

Lineamientos:

- 7.5.1.** La información digital catalogada como, pública reservada y/o pública clasificada, se debe almacenar y/o transmitir bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad, no obstante, en caso de no poderse aplicar un mecanismo criptográfico, se deberá asignar clave de apertura a los archivos digitales que contengan este tipo de información.
- 7.5.2.** Se deben establecer mecanismos para el manejo y la administración de llaves de cifrado; y estándares para la aplicación de controles criptográficos.

- 7.5.3. Se deben implementar controles respecto de la administración de llaves, recuperación de información cifrada en caso de pérdida, compromiso o daño de las llaves y reemplazo de las llaves de cifrado.
- 7.5.4. Al implementar esta política en materia criptográfica, se deben considerar los controles aplicables al cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
- 7.5.5. Al utilizar firmas y certificados digitales, se debe considerar la legislación vigente que describa las condiciones bajo las cuales una firma digital es legalmente válida.
- 7.5.6. Todas las llaves serán protegidas contra modificación y destrucción y las llaves privadas serán protegidas contra uso indebido, copia o divulgación no autorizada.
- 7.5.7. A fin de reducir la probabilidad de compromiso, las llaves tendrán fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por un lapso de tiempo definido, no mayor a 12 meses.
- 7.5.8. La pérdida, robo o posible divulgación no autorizada de la llave de cifrado o mecanismo criptográfico debe de ser reportado inmediatamente a la Dirección de Tecnologías de la Información y las Comunicaciones para su revocación.
- 7.5.9. Para la generación de contraseña para las llaves o mecanismos criptográficos deberán cumplir lineamientos establecidos en el lineamiento 7.4.12. de este documento, para la construcción de contraseñas seguras.
- 7.5.10. La Dirección TIC será responsable y encargada de la activación y revocación de las llaves criptográficas asignadas por la Contraloría de Bogotá, D.C., a los usuarios autorizados.

7.6. ESCRITORIO LIMPIO Y PANTALLA LIMPIA

La Contraloría de Bogotá D.C., establece las reglas para reducir los riesgos de acceso no autorizado, daño o pérdida, o divulgación no autorizada de la información, en cada uno de los puestos de trabajo, equipos y servidores de computo en términos de garantizar la confidencialidad, integridad y disponibilidad de los activos de información.

Lineamientos:

- 7.6.1. Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por la Entidad.
- 7.6.2. Los usuarios siempre al ausentarse del puesto de trabajo deberán bloquear el equipo de cómputo, para evitar que otras personas puedan acceder a la información, de la siguiente manera:
 - Pulsar simultáneamente (tecla Windows + la tecla L) para bloquear el equipo.
 - Pulsar (Ctrl + alt + supr) y seleccionar la opción bloquear equipo.
- 7.6.3. En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deben dejar los medios que contengan información clasificada, reservada o confidencial protegida bajo llave.
- 7.6.4. Los usuarios son responsables por la custodia y las acciones que se realicen sobre los activos de información que le han asignado, por lo tanto, debe estar presente en el

sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.

- 7.6.5.** No se debe dejar en las impresoras documentos expuestos que contengan información sensible, ya que se puede comprometer su confidencialidad.
- 7.6.6.** El usuario no tiene permitido hacer manipulación (traslados, desconexiones.) de las estaciones de trabajo, con excepción de los computadores portátiles asignado para el desarrollo de sus funciones.
- 7.6.7.** No publicar o dejar a la vista, documentos o datos clasificados, reservados o confidenciales para la Entidad, como: nombres de usuario, contraseñas, direcciones IP, contratos, números de cuentas, listas de clientes, archivos de propiedad intelectual, datos personales de los funcionarios Públicos y/o cualquier información importante para la Entidad que no se desea publicar.
- 7.6.8.** Los funcionarios al ausentarse de su sitio de trabajo deben guardar en un lugar seguro (gabinetes, mobiliario protegido con llave, caja fuerte) cualquier documento físico (hojas impresas, carpetas, cuadernos, libretas de apuntes), medio magnético removible (Memorias Flash, Discos Duros Externos, CD ROM, DVD) que contenga información de la Contraloría de Bogotá D.C.
- 7.6.9.** La estación de trabajo y equipos que están asignados a los usuarios, son activos de la Entidad, por lo mismo el usuario no es dueño del mencionado activo.
- 7.6.10.** Desde el momento en que el usuario firma el formato de asignación de inventario individual, la responsabilidad sobre el estado del equipo es completamente del usuario.

7.7. COPIAS DE RESPALDO

La Contraloría de Bogotá D.C., debe realizar copias de respaldo de la información misional la cual deberá estar centralizada y se deberá asegurar la ejecución de copias de respaldo ante cualquier afectación por pérdida o degradación. De igual manera se aclara que cada usuario es responsable de la información que maneja en su equipo de cómputo, en consecuencia, es el responsable de realizar las copias de respaldo de la misma.

Lineamientos:

- 7.7.1.** Los medios de copias se deben almacenar en custodia externa en una sede alterna de la Contraloría de Bogotá D.C., asegurando que tenga implementado mecanismos de protección ambiental.
- 7.7.2.** Realizar pruebas de restauración de la información, de acuerdo a un plan de restauración de copias de respaldo establecido, para asegurar que se puede depender de ellos para uso de emergencia en caso necesario.
- 7.7.3.** Para la información considerada relevante o importante por cada dependencia de la Entidad, se cuenta con una unidad de almacenamiento centralizada, en la cual se almacena dicha información por los funcionarios autorizados; unidad que se encuentra incluida dentro de los esquemas de copias de respaldo implementados por la Dirección de Tecnologías de la Información de la Contraloría de Bogotá, D.C.

- 7.7.4. Definir los tiempos de retención y de protección en instalaciones adecuadas que provean la debida seguridad física y ambiental, permitiendo minimizar el impacto de la operación de la Entidad, en caso de presentarse una falla o desastre y poder contar con la información necesaria en el momento oportuno para responder con los tiempos de restauración de los servicios.
- 7.7.5. Se debe contar con registros exactos y completos de las copias de respaldo.
- 7.7.6. Definir la frecuencia y tipo de copias de respaldo a realizar.
- 7.7.7. Las pruebas de restauración se deberían hacer en medios de prueba dedicados, no sobrescribiendo el medio original, para evitar que se cause un daño o pérdida de la información.

7.8. TRANSFERENCIA DE LA INFORMACIÓN

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 acuerdos de confidencialidad, enmarcados en las leyes vigentes.

La Entidad debe implementar mecanismos y controles que permitan establecer una comunicación segura en la transferencia de la información evitando la interceptación que pueda copiar, modificar, o eliminar la información por parte de terceros.

Lineamientos:

- 7.8.1. Usar técnicas de cifrado de la información para garantizar la confidencialidad e integridad de la información durante la transferencia de la información.
- 7.8.2. Los propietarios de la información a transferir deben asegurar que la clasificación de ésta se encuentre actualizada teniendo en cuenta las propiedades de seguridad: confidencialidad, integridad y disponibilidad, con el fin de permitir el acceso únicamente a los autorizados.
- 7.8.3. Únicamente se entrega información a receptores autorizados quienes garanticen por escrito la reserva legal y protección de la información que se les vaya a suministrar.
- 7.8.4. Cuando proceda, la oficina responsable de dar respuesta legal a un requerimiento de información clasificada, deberá verificar previamente entre otros temas y sin limitarse a:
 - La solicitud se ajuste a la normatividad aplicable vigente.
 - La respuesta identifique el nivel de clasificación, correspondiente a la naturaleza del documento o la información que se ponga en conocimiento de la autoridad competente.
 - La respuesta cumpla con los protocolos de seguridad, acceso y reserva.
 - La respuesta con la información suministrada no debe poner en peligro o riesgo la Seguridad de la Entidad o sus funcionarios.
 - La respuesta no debe dar a conocer capacidades, procedimientos, medios, elementos técnicos, operaciones o actividades que comprometan la seguridad de la Entidad.

- 7.8.5.** Se debe dar cumplimiento a lo establecido en el procedimiento de Gestión de Activos de la Entidad.

7.9. DESARROLLO SEGURO

La Contraloría de Bogotá D.C., debe crear y mantener mecanismos que incluyan los requerimientos de seguridad en todo el ciclo de vida de desarrollo y mantenimiento seguro de las aplicaciones, los desarrolladores revisarán y determinarán la acción a seguir para el tratamiento de las vulnerabilidades, para evitar que tengan brechas de seguridad, esto aplicará tanto para los desarrollos realizados con terceros como los realizados al interior de la Entidad.

Lineamientos:

- 7.9.1.** Se deben identificar y acordar los requisitos de seguridad en todas las fases del ciclo de vida de desarrollo de software, y se deben justificar, acordar y documentar.
- 7.9.2.** Se deben incluir puntos de chequeo de seguridad dentro de las fases del ciclo de vida de desarrollo de software.
- 7.9.3.** El cambio de versión de las aplicaciones implementadas en el ambiente de producción se debe hacer de acuerdo a lo definido en el procedimiento para el control de cambios, además, debe contar con controles de seguridad, para esto se debe hacer una copia de respaldo en caso que se deba realizar marcha atrás, para mantener la integridad y disponibilidad de los datos y de los sistemas de información.
- 7.9.4.** Se deben realizar pruebas de seguridad en un ambiente controlado con el fin de identificar vulnerabilidades, las cuales deben ser resueltas antes del paso a producción.
- 7.9.5.** Los ambientes de desarrollo, pruebas y producción, deben estar separados.
- 7.9.6.** El paso de software de un ambiente a otro debe ser controlado y gestionado de acuerdo a lo definido en el procedimiento de control de cambios.
- 7.9.7.** El ambiente de prueba debe simular el ambiente de producción.
- 7.9.8.** El desarrollo de contratos de mantenimiento deberá contar con la asignación de un supervisor permanente, encargado de controlar que se cumplan los estándares de seguridad tanto en la parte física como lógica de los sistemas. Ningún mantenimiento podrá ser realizado por personal que no tenga cumpla los requisitos definidos por la Dirección de Tecnologías de la Información y las Comunicaciones.
- 7.9.9.** La Dirección de Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá D.C., aplicará el procedimiento para el desarrollo de software y sistemas de información, el cual debe ser aplicado a los desarrollos y adaptaciones de los sistemas en la Entidad, del mismo modo se debe aplicar el procedimiento para el control de cambios, 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.
- 7.9.10.** La Dirección de Tecnologías de la Información y las Comunicaciones de la Contraloría de Bogotá D.C., aplicará 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.

- 7.9.11.** Todo hardware y software que se vaya a adquirir y/o conectar a la infraestructura tecnológica de la Contraloría de Bogotá D.C., por cualquier dependencia o proyecto de la Entidad, deberá ser adquirido por intermedio de la Dirección de Tecnologías de la Información y las Comunicaciones y gestionado por la misma dirección para su correcto funcionamiento.
- 7.9.12.** El software proporcionado por la Contraloría de Bogotá D.C no puede ser copiado o suministrado a terceros.
- 7.9.13.** 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.
- 7.9.14.** Para la adquisición y actualización de software, es necesario efectuar la solicitud a la Dirección de Tecnologías de la Información y las Comunicaciones.
- 7.9.15.** El software que se adquiera la Entidad, debe quedar licenciado a nombre de la Contraloría de Bogotá D.C.
- 7.9.16.** Se encuentra prohibido el uso e instalación de juegos en los computadores de la Contraloría de Bogotá D.C.

7.10. RELACIONES CON LOS PROVEEDORES

La Contraloría de Bogotá D.C., debe identificar requisitos de seguridad para proteger la información, e incluirlos dentro de los acuerdos con proveedores, por medio de un análisis que permita identificar riesgos asociados para implementar planes de acción dependiendo de las actividades a realizar, de igual manera se debe establecer, aprobar y divulgar los requerimientos y obligaciones relacionados con la seguridad de la información, tanto con los proveedores como con la cadena de suministros que estos posean.

Lineamientos:

- 7.10.1.** Los proveedores deben aceptar y firmar los acuerdos de confidencialidad establecidos por la Contraloría de Bogotá D.C.
- 7.10.2.** Se debe tener en cuenta la documentación relacionada con los servicios, infraestructura de TI, sistemas de información y activos a los cuales tendrá acceso los proveedores, esto deberá ser controlado teniendo en cuenta los permisos de acuerdo al trabajo a realizar y los acuerdos firmados, los cuales deben tener requisitos mínimos de seguridad, que se deben hacer cumplir haciendo seguimiento por medio de mecanismos establecidos.
- 7.10.3.** La Entidad debe incluir dentro de los acuerdos a firmar con el proveedor, todos los controles de seguridad aplicables.
- 7.10.4.** Cuando exista la necesidad de otorgar acceso de terceras partes a los sistemas centrales, deberá realizarse siempre con la participación del propietario de la información, una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta entre otros los siguientes aspectos:
 - El tipo de acceso requerido (físico, lógico y a qué recurso)

- Los motivos para los cuales solicita el acceso
 - Los controles empleados por la tercera parte
- 7.10.5.** En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados, se haya firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.
- 7.10.6.** El acceso de los terceros a la información o a cualquier elemento de la infraestructura tecnológica debe ser solicitado por el supervisor, o persona a cargo del tercero, al propietario de dicho activo, éste junto con los encargados de la infraestructura tecnológica, aprobarán y autorizarán el acceso y uso de la información.
- 7.10.7.** Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadores, contemplarán como mínimo los siguientes aspectos:
- Forma en los que se cumplirán los requisitos legales aplicables
 - Medios para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, conocen sus responsabilidades en materia de seguridad.
 - Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos.
 - Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información.
 - Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
 - Niveles de seguridad física que se asignará al equipamiento tercerizado.
- 7.10.8.** Todos los funcionarios y terceros deben firmar la cláusula y/o acuerdo de confidencialidad que deberá ser parte integral de los contratos utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o Entidades externas.
- 7.10.9.** Se deben formalizar los niveles de acuerdo de servicio y los acuerdos de intercambio de información con cada proveedor dentro del contrato realizado, de acuerdo a los lineamientos establecidos por Contraloría de Bogotá. D.C.
- 7.10.10.** Se deben definir las cláusulas por incumplimiento en los contratos de los proveedores, para establecer las situaciones que puedan generar multas o penalizaciones, dentro de los cuales se contempla los acuerdos de confidencialidad y no divulgación de la información.
- 7.10.11.** Los encargados de la infraestructura tecnológica deben verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros.

7.11. GESTIÓN DE ACTIVOS

La Contraloría de Bogotá D.C., debe identificar todos los activos de información, y mantener un inventario actualizado, exacto, consistente y documentado con todos los aspectos relevantes de cada uno, clasificándolos de acuerdo a la Confidencialidad, Integridad y Disponibilidad de la información, para identificar su valor y criticidad, además, cada activo debe tener un propietario que garantice los niveles de seguridad que correspondan según sea el caso.

Lineamientos:

- 7.11.1.** 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.
- 7.11.2.** Los funcionarios de la Entidad se deben comprometer a identificar, clasificar, etiquetar, disponer, devolver, y gestionar los activos de información establecidos como tal, de acuerdo a la presente política y el procedimiento establecido para la gestión de activos.
- 7.11.3.** La identificación, clasificación y valoración de los activos de información se debe realizar de acuerdo al procedimiento establecido.
- 7.11.4.** 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.
- 7.11.5.** Se debe mantener un registro actualizado y exacto de todos los activos de información necesarios para la prestación de servicios, de acuerdo a lo establecido en el procedimiento para la gestión de activos.
- 7.11.6.** Todos los activos de información deben tener asignado un custodio que tiene la responsabilidad de mantener los controles adecuados para su protección.
- 7.11.7.** Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información, de acuerdo a lo establecido en el procedimiento para la gestión de activos.
- 7.11.8.** Los documentos de la Contraloría de Bogotá D.C., que contengan información relacionada con diferentes niveles de clasificación de seguridad, asumirán la del nivel más alto que tenga la información contenida en ellos.
- 7.11.9.** El acceso a carpetas compartidas debe delimitarse a los funcionarios que las necesitan y deben ser protegidas con contraseñas y/o acceso por roles y responsabilidades.
- 7.11.10.** 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 los conocimientos importantes relacionados con la labor ejecutada.

- 7.11.11.** La Contraloría de Bogotá D.C. empleará 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.
- 7.11.12.** Los medios y equipos donde se almacena, procesan 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.

7.12. NO REPUDIO

La política de no repudio comprende la capacidad de definir diferentes mecanismos o estrategias que están encaminadas a que un funcionario o tercero evite negar que ha realizado alguna acción.

Lineamientos:

- 7.12.1.** Para los procesos que se consideren se deben implementar mecanismos en los que no exista la posibilidad de desafiar su validez de una acción por parte de quien la generó.
- 7.12.2.** Algunos mecanismos a implementar deberán contar con un tercero en que todos confíen y quien permita avalar la integridad y origen de los datos.
- 7.12.3.** Se deben contar con registros que permita hacer trazabilidad de las acciones de creación, origen, recepción, entrega de información y otros, que servirán de evidencia para poder garantizar el no repudio.
- 7.12.4.** Estos registros se deben proteger contra pérdida o modificación de tal manera que se garantice su disponibilidad e integridad.
- 7.12.5.** Se deben realizar auditorías continuas a los mecanismos de control y a los procesos, para asegurarse que las partes implicadas nieguen haber realizado una acción.
- 7.12.6.** Los servicios de intercambio electrónico de información deben incorporar mecanismos que sean garantía de no repudio.

7.13. PRIVACIDAD Y CONFIDENCIALIDAD

La política de Privacidad y Confidencialidad determina los lineamientos de tratamiento y protección sobre los datos personales y sobre la información considerada como sensible y sobre la cual se deberán implementar controles de acuerdo a su nivel de clasificación.

Lineamientos:

- 7.13.1.** En la Contraloría de Bogotá D.C. se tienen implementados acuerdos de confidencialidad los cuales todo funcionario, contratista y/o tercero vinculado a la Entidad debe firmar con el compromiso de no divulgar la información clasificada, reservada o confidencial de la Entidad.

- 7.13.2.** 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.
- 7.13.3.** Para la recolección y tratamiento automatizado de los datos personales, como consecuencia de la navegación y/o registro por el sitio web se deberá informar al titular de los datos la finalidad de los mismos.
- 7.13.4.** Todo funcionario, contratista o tercero debe firmar un acuerdo de confidencialidad, el cual debe contener un compromiso del funcionario, contratista y/o tercero vinculado a la Contraloría de Bogotá D.C., de no divulgar la información interna y externa que conozca como parte del desarrollo de las funciones que desempeña o de su vinculación con la Entidad.
- 7.13.5.** Este acuerdo de confidencialidad debe indicar la vigencia del mismo, el cual debe mantenerse por un tiempo adicional que considere Contraloría de Bogotá D.C., luego de terminada la vinculación con la Entidad.
- 7.13.6.** El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
- 7.13.7.** La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- 7.13.8.** La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- 7.13.9.** Presentar quejas ante el área administrativa encargada de la protección de los datos personales.

7.14. INTEGRIDAD

La política de Integridad se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administrada por usuarios internos y externos relacionados con la Contraloría de Bogotá D.C.

Lineamientos:

- 7.14.1.** Toda la información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas autorizadas y a través de los medios correspondientes, sin modificaciones ni alteraciones.
- 7.14.2.** En el caso de vinculación contractual, el compromiso de administración y manejo íntegro e integral de la información interna y externa debe hacer parte de las cláusulas del respectivo contrato, bajo la denominación de cláusula de integridad de la información.
- 7.14.3.** Para la información que se clasifique como Reservada, Clasificada, Pública, y requiera ser transmitida a través de canales de comunicación se deben utilizar mecanismos que permitan garantizar que la información mantiene su integridad mientras es

transmitida por la red, es decir, que la información es completa y exacta de punto a punto en la transmisión.

7.15. DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

La Contraloría de Bogotá D.C., proporcionará los recursos suficientes y desarrollará esfuerzos tendientes a garantizar la continuidad de las operaciones para sus procesos con el fin brindar la disponibilidad de los servicios; así mismo, responderá de manera efectiva ante eventos adversos según la dimensión y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la Seguridad de la Información durante dichos eventos, de igual manera se mantendrán canales de comunicación adecuados hacia los funcionarios y demás partes interesadas.

Para esto La Contraloría de Bogotá D.C., deberá evaluar el impacto de eventos que afectan los procesos de la Entidad y que tienen soporte en la infraestructura tecnológica y en la prestación de terceros, igualmente, deberá desarrollar planes de contingencia y de recuperación ante desastres (DRP) para aquellos servicios que son críticos y misionales, dichos planes deben considerar medidas tanto técnicas como administrativas y deberán probarse y revisarse de manera periódica.

Lineamientos:

- 7.15.1.** La Contraloría de Bogotá D.C., conforme a su misionalidad, establece que debe contar con un Plan de Recuperación ante Desastres (DRP) que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.
- 7.15.2.** Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, deben estar incorporados y definidos en el Plan de Recuperación ante Desastres (DRP).
- 7.15.3.** Los responsables de los procesos de la recuperación serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio a todos los interesados.
- 7.15.4.** Los análisis de riesgos, impacto al negocio y estrategias de recuperación realizados sobre los planes que estén operando, deben ser evaluados por lo menos cada año, para asegurar que continúan reflejando las estrategias y necesidades de la operación, esta labor debe ser coordinada por el oficial de Seguridad de la Información, la Dirección de Planeación con el apoyo de los dueños de procesos críticos y la Dirección de Tecnologías de la Información y las Comunicaciones.
- 7.15.5.** Todos los sistemas de información que soportan las funciones críticas de la Entidad, deben tener un plan de recuperación de TI que le permita garantizar una respuesta efectiva y eficiente ante eventos de desastre o interrupciones mayores, el cual estará a cargo de la Dirección de Tecnologías de la Información y las Comunicaciones.
- 7.15.6.** Los procesos críticos deben soportarse en aplicaciones e infraestructura técnica robusta, software y hardware confiable y en instalaciones alternas o duplicadas.
- 7.15.7.** Se requiere proveer al personal activo la documentación de las acciones a llevar a cabo en el evento de un desastre o una emergencia que puede afectar las

aplicaciones de la operación y la infraestructura técnica, habilitando los procesos críticos de la Entidad, para ser restaurados en escalas de tiempo aceptables.

- 7.15.8.** Los planes de recuperación deben ser probados periódicamente y como resultado de estas pruebas realizar los ajustes correspondientes.
- 7.15.9.** Se debe identificar, acordar y documentar todas las responsabilidades y los procedimientos para la recuperación de los servicios informáticos.
- 7.15.10.** Se debe elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados identificados como críticos y misionales dentro de la Entidad.
- 7.15.11.** Se debe realizar los análisis de impacto a la operación y los análisis de riesgos de continuidad para posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia, con las consideraciones de Seguridad de la Información a que haya lugar.

7.16. REGISTRO Y AUDITORÍA

Esta política de Registro y Auditoría define lo pertinente a las auditorías que se realizan a los procesos que incluyen activos del Sistema de Gestión de Seguridad de la Información e indica temas del registro y conservación de las evidencias de las actividades y acciones que afectan los activos de información.

Lineamientos:

- 7.16.1.** La oficina de Control Interno de la Entidad, debe definir un plan de auditoría y un equipo auditor que lo ejecute, el cual debe cumplir con las capacidades, habilidades y conocimientos para su ejecución.
- 7.16.2.** La oficina de Control Interno de la Entidad, debe asegurar que los resultados de las auditorías se informan al Oficial de Seguridad de la Información y al Director de Tecnología y que se conserva información documentada como evidencia de la implementación del programa de auditoría.
- 7.16.3.** Como parte del programa de auditoría se deben incluir auditorías periódicas al Subsistema de Gestión de Seguridad de la Información.
- 7.16.4.** Los registros de auditoría deben incluir toda la información de registro y monitoreo de eventos de seguridad, estos registros se deben almacenar por lo menos por un periodo de dos años.
- 7.16.5.** Las auditorías se deben realizar acorde a la normatividad y requerimientos legales aplicables a la naturaleza de la Entidad.
- 7.16.6.** Se debe definir a qué es necesario hacer seguimiento y medición dentro del Subsistema de Gestión de Seguridad de la Información.
- 7.16.7.** Se deben desarrollar planes de auditoría interna para evaluar los niveles de aplicabilidad de la seguridad de la información en todos sus ámbitos, tanto digitales como físicos.
- 7.16.8.** Se debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Entidad; así como recomendar lo pertinente sobre las deficiencias detectadas.

- 7.16.9.** El almacenamiento de los registros de las auditorías internas realizadas al Sistema de Gestión de Seguridad de la Información se debe realizar de acuerdo a lo establecido en el procedimiento de Auditorías Internas.

7.17. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Contraloría de Bogotá D.C., debe promover en los usuarios internos y externos el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

Lineamientos:

- 7.17.1.** En la Contraloría de Bogotá D.C., se aplicarán 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.
- 7.17.2.** Todo evento de seguridad ocurrido en la Contraloría de Bogotá D.C., deberán ser comunicados mediante canales de gestión apropiados.
- 7.17.3.** 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.
- 7.17.4.** Se debe reportar al Oficial de Seguridad de la Información los incidentes de seguridad de la información, quien tendrá la responsabilidad de investigar y solucionar los incidentes de acuerdo con su criticidad, junto con la Dirección de Tecnologías de la Información y las Comunicaciones y el equipo de respuesta ante incidentes de seguridad de la información - CSIRT.
- 7.17.5.** Los propietarios de los activos de información, funcionarios y terceros deben informar los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización, de acuerdo al procedimiento “Gestión de Incidentes de Seguridad de la Información”.
- 7.17.6.** Se deben documentar y clasificar los incidentes de acuerdo con las indicaciones especificadas en el procedimiento de “Gestión de Incidentes de Seguridad de la Información”.
- 7.17.7.** Se deben analizar los incidentes de seguridad para identificar cuáles serán escalados y proceder a realizar el contacto con las autoridades, cuando se estime necesario.
- 7.17.8.** Todo aquel evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la Confidencialidad, Integridad, y Disponibilidad de la infraestructura tecnológica deberá ser reportado de acuerdo al procedimiento de Gestión de Incidentes de Seguridad de la Información.
- 7.17.9.** En los casos que sea necesario realizar recolección y preservación de la evidencia de las investigaciones que se realicen durante el análisis de un incidente de seguridad de

la información, la Entidad establecerá un procedimiento para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia.

7.18. CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

La política de Capacitación y Sensibilización en Seguridad de la Información, se centra en formar y dar a conocer a los empleados temas relacionados con la seguridad de la información, cuya finalidad es que puedan identificar y reportar de manera oportuna los incidentes de seguridad de la información y disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

Lineamientos:

- 7.18.1.** Se debe proveer al personal activo las habilidades requeridas a través de entrenamientos para proteger los sistemas y cumplir con las responsabilidades de administración y uso de manera oportuna, correcta y segura los activos de información.
- 7.18.2.** Se debe crear una cultura que promueva la seguridad donde todos los individuos apliquen los controles de seguridad y prevengan que la información sensible de la Entidad se vea comprometida.
- 7.18.3.** A partir de los resultados de pruebas de ingeniería social y/o de análisis de riesgo se deberán determinar los temas y las estrategias de sensibilización para reforzar el nivel de conocimiento en temas de seguridad de la información para todos los funcionarios.
- 7.18.4.** Se debe definir un mecanismo de inducción en Seguridad de la Información para todos los funcionarios que sean destinados a recibir un nuevo cargo, bien sea por nombramiento, traslado o por disposiciones internas.
- 7.18.5.** Se debe definir y desarrollar un programa de capacitación y sensibilización de tal forma que de manera periódica se refuercen los conceptos y amenazas de seguridad para que los funcionarios cuenten con información actualizada y sepan cómo actuar ante incidentes y como reportarlos.
- 7.18.6.** La Contraloría de Bogotá D.C., deberá incluir dentro del Plan Institucional de Capacitación – PIC, los programas de capacitación y sensibilización en seguridad de la información.
- 7.18.7.** La asistencia a las sesiones de capacitación y sensibilización en seguridad de la información son de carácter obligatorio.
- 7.18.8.** Los mensajes de sensibilización deben dar a conocer y entender de fácil manera las políticas de seguridad de la información.
- 7.18.9.** Se debe evaluar a todos los funcionarios de manera periódica, los niveles de sensibilización en temas de seguridad de la información.

Las anteriores políticas se complementan con cada uno de los procedimientos, guías, manuales y demás documentación establecidos por la Contraloría de Bogotá D.C. para la gestión del Subsistema de Gestión de la Seguridad de la Información.

8. APROBACION Y ACTUALIZACIÓN

Las políticas de seguridad de la información, serán aprobadas en sesión del Comité SIGEL o quien haga sus veces y las actualizaciones a que haya lugar, serán aprobadas por la misma instancia y se realizarán cuando se requiera.

9. CONTROL DE CAMBIOS

Versión	R.R. No.	Descripción de la Modificación
1.0	R.R. No.022 14-jul-2016	Se adoptan las Políticas de Seguridad y Privacidad de la Información en la Contraloría de Bogotá, D.C., para efectos de obligatoriedad en su cumplimiento, la cual forma parte de la documentación que soporta el Sistema Integrado de Gestión, en el marco del Subsistema de Seguridad de la Información y de la estrategia del Gobierno en Línea.
2.0	R.R. No. 022 19-abr-2018	Se actualizan las Políticas, conforme a lo aprobado en el Comité SIGEL No.3 realizado el día 11 de junio de 2019, a la normatividad legal vigente y a lo establecido en la Norma Técnica Colombiana ISO/IEC 27001:2013, con las directrices para la proteger la información, asegurando que en ella se cumplan las características de integridad, disponibilidad y confidencialidad, mediante la ejecución de acciones en concordancia con disposiciones legales, operativas, tecnológicas y de acuerdo al objetivo estratégico, debiéndose modificar el nombre a Políticas de Seguridad de la Información
3.0	R.R. No.038 24-sep-2019	

CONTRALORÍA DE BOGOTÁ, D.C.

Resolución Reglamentaria Número 039 (Septiembre 25 de 2019)

**“Por la cual se adopta la Política de
Administración del Riesgo para la Contraloría de
Bogotá D.C.”**

**EL CONTRALOR DE BOGOTÁ D.C.
En ejercicio de las atribuciones constitucionales
y legales, especialmente las conferidas en el
Decreto Ley 1421 de 1993, el Acuerdo 658 de
2016 modificado por el Acuerdo 664 de 2017 y,**

CONSIDERANDO:

Que la Constitución Política establece en su artículo 209, que *“La Administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley”* y en el artículo 269 la obligación de las autoridades correspondientes en las entidades públicas, de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley.

Que la Ley 87 de 1993 *“Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones”*, establece que son objetivos del control interno, entre otros, la protección de los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten y 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 Decreto 1083 de 2015 “*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública*” que compiló el Decreto 1537 de 2001. Establece en su artículo 2.2.21.5.4 la Administración de riesgos. “*Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces, evaluando los aspectos tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizacionales, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos.*”

Que el Departamento Administrativo de la Función Pública expidió la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, según la cual la Alta Dirección debe establecer la Política de Administración de Riesgos, es decir determinar lineamientos precisos acerca del tratamiento, manejo de los riesgos.

Que se hace necesario adoptar la Política de Administración del Riesgo para la Contraloría de Bogotá. D.C. Que la Política de Administración del Riesgo para la Contraloría de Bogotá, D.C., fue aprobada en Comité Institucional de Coordinación de Control Interno como consta en el Acta No. 01 en sesión del 14 de agosto de 2019

En mérito de lo expuesto, el Contralor de Bogotá D.C.

RESUELVE:

ARTÍCULO PRIMERO. Adoptar la Política de Administración del Riesgo para la Contraloría de Bogotá, D.C. que se anexa a la presente Resolución y hace parte integral de esta.

ARTÍCULO SEGUNDO. El seguimiento y actualización de los Riesgos en la Entidad será responsabilidad de los responsables de los Procesos del Sistema Integrado de Gestión SIG.

ARTÍCULO TERCERO. La Oficina de Control Interno, realizará la evaluación de los controles establecidos para evitar que los riesgos se materialicen, así como las acciones preventivas y correctivas establecidas por los Responsables de los Procesos.

ARTÍCULO CUARTO. La Dirección de Planeación brindará apoyo y asesoría en las actividades correspondientes a la Política de Administración del Riesgo en la Contraloría de Bogotá, D.C.

ARTÍCULO QUINTO. Es responsabilidad de los Directores, Subdirectores, Jefes de Oficina y Gerentes velar por la divulgación de la Política de Administración del Riesgo.

ARTÍCULO SEXTO. La presente Resolución rige a partir de la fecha de su publicación y deroga las normas que le sean contrarias.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los veinticinco (25) días del mes de septiembre de dos mil diecinueve (2019).

JUAN CARLOS GRANADOS BECERRA

Contralor de Bogotá D.C.

Aprobación	Revisión Técnica
Firma:	Firma:
Nombre: María Anayme Barón Durán	Mercedes Yunda Monroy
Cargo: Contralora Auxiliar	Directora Técnica
Dependencia: Despacho Contralora Auxiliar	Dirección de Planeación
R.R. No. 039 DE SEPTIEMBRE 25 DE 2019	

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

MARÍA ANAYME BARÓN DURÁN
Contralora Auxiliar

MERCEDES YUNDA MONROY
Directora Técnica de Planeación

MARÍA ANAYME BARÓN DURÁN
Responsable Proceso Direccionamiento Estratégico
Contralora Auxiliar

Septiembre de 2019

INTRODUCCIÓN

Toda actividad está expuesta a situaciones de riesgo que pueden afectar en forma negativa el cumplimiento de la misión, objetivos institucionales, objetivos del proceso o la satisfacción del cliente como consecuencia de la diversidad de riesgos de corrupción, de Gestión y de Seguridad de la información, por lo que se requiere un acercamiento más profundo, metodológico y sistemático a la administración de riesgos para la Contraloría de Bogotá, D.C.

El presente documento técnico toma como referencia la “*Guía para la administración del riesgo y el diseño de controles en entidades públicas*” versión 4.0 expedida por el Departamento Administrativo de la Función Pública – DAFP; por tanto, establece los lineamientos para la identificación, análisis, valoración, evaluación y tratamiento de los riesgos que pudieran afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos, y planes institucionales, los cuales deben ser acatados por todos los servidores públicos de la entidad en el desarrollo de sus funciones y son complemento a la Política identificada en el Plan Estratégico Institucional PEI 2016 – 2020 “*Una Contraloría aliada con Bogotá*”, que establece: “*La Contraloría de Bogotá D.C., asume la Administración del Riesgo como parte integral del Direccionamiento Estratégico, lo que implica un compromiso institucional con la identificación, análisis y valoración de los riesgos que pueden afectar la gestión de los procesos del Sistema Integrado de Gestión - SIG, con miras a controlar sus efectos sobre el cumplimiento de la misión, a través de las acciones implementadas*”¹.

1. OBJETIVO:

Establecer los principios básicos, lineamientos, responsabilidades y directrices que permitan disminuir la probabilidad de ocurrencia y el impacto de todas aquellas situaciones en que se pueda ver expuesta la Contraloría de Bogotá, D.C. en función del desarrollo de un pensamiento basado en riesgos aplicando las normas en materia de riesgos y la metodología expedida por el Departamento Administrativo de la Función Pública DAFP “*Guía para la administración del riesgo y el diseño de controles en entidades públicas*” versión 4.0, con el fin de alcanzar de manera eficaz y efectiva la misión y el cumplimiento de los objetivos institucionales.

¹ Política de Administración del Riesgo. Plan Estratégico Institucional PEI 2016 – 2020.

Alineación con el Plan Estratégico

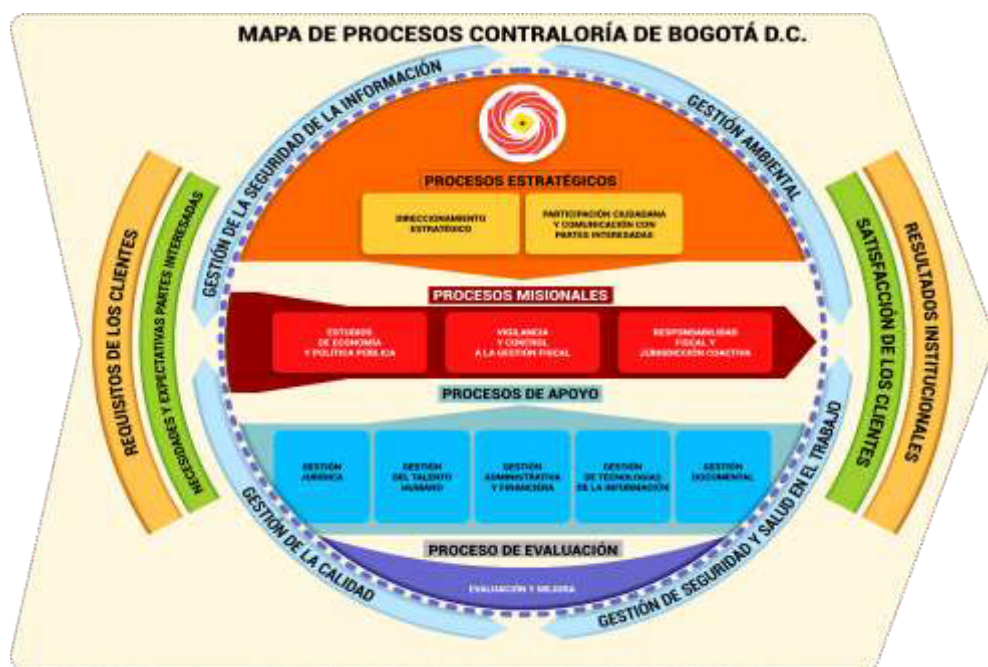
La estrategia organizacional de la Contraloría de Bogotá, D.C., se encuentra formalizada en el Plan Estratégico Institucional - PEI, documento que recoge y difunde las principales líneas de acción y estrategias que se propone adelantar en el corto y medio plazo, orientadas al cumplimiento de su misión bajo los siguientes parámetros:

Misión. La Contraloría de Bogotá, D.C., es la entidad que vigila la gestión fiscal de la Administración Distrital y de los particulares que manejan fondos o bienes públicos, en aras del mejoramiento de la calidad de vida de los ciudadanos del Distrito Capital.

Visión. En el año 2020, la Contraloría de Bogotá, D.C., será reconocida por los ciudadanos como una entidad confiable por su efectividad en la vigilancia y control del uso adecuado de los recursos públicos, fundada en la participación ciudadana, la sostenibilidad y el uso de la tecnología.

Para la Entidad, la administración de los riesgos es una herramienta de control fundamental para el cumplimiento de los objetivos estratégicos y de los procesos internos. Es por esto que la presente política se encuentra armonizada con la misión y visión organizacional, así como con el Sistema Integrado de Gestión - SIG.

Mapa de procesos:



2. ALCANCE.

La política debe ser aplicada por toda la entidad desde el Direccionamiento Estratégico como línea estratégica (Alta Dirección y el Comité Institucional de Coordinación de Control Interno – CICC) hasta el nivel operativo en cumplimiento de las tareas diarias del que hacer de la institución. Aplica a todos los procesos y proyectos de la Entidad y a todas las actividades realizadas por los funcionarios durante el ejercicio de sus funciones y en representación de la Entidad.

Se complementa con los parámetros establecidos en los siguientes procedimientos: “Procedimiento para elaborar el contexto de la organización y Plan Estratégico Institucional – PEI” y “Procedimiento para la Administración Integral de los Riesgos Institucionales”.

3. TÉRMINOS Y DEFINICIONES.

- **Alta Dirección:** Máxima autoridad, es decir el representante legal como responsable del Sistema de Control Interno según la Ley 87 de 1993 quién deberá disponer de los recursos físicos, económicos, tecnológicos, de infraestructura y de talento humano y la responsabilidad del Proceso en General de la Administración de Riesgos
- **Riesgo de gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo de seguridad digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Riesgo inherente:** es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo residual:** nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

- **Gestión del riesgo:** proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Probabilidad:** posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo.
- **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Activo:** en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Control:** medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizado.
- **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.
- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Integridad:** propiedad de exactitud y completitud.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.

- **Tolerancia al riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.
- **Apetito al riesgo:** Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

4. RESPONSABILIDADES Y ROLES

Para la administración integral de los riesgos institucionales se determinan los roles y responsabilidades de las diferentes líneas de defensa, teniendo en cuenta las directrices del Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Modelo Integrado de Planeación y Gestión, entre otras, así:

LÍNEA ESTRATÉGICA	
Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno	
Responsables	Actividades de monitoreo y revisión
Alta Dirección y Comité Institucional de Coordinación de Control Interno – CICC	✓ Revisar, aprobar y socializar la Política de administración del riesgo ✓ Aprobar el Mapa de Riesgos de Gestión, Corrupción y Riesgos de Seguridad de la Información en Comité Directivo ✓ Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo) ✓ Analizar los cambios en el contexto de la organización (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles ✓ Realizar seguimiento y análisis periódico a los riesgos institucionales

1ª. LÍNEA DE DEFENSA	
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.	
Responsables	Actividades de monitoreo y revisión
Responsables de los Procesos	✓ Identificar y valorar los riesgos de Gestión, Corrupción y de la Seguridad de la Información que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera ✓ Diseñar, ejecutar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso. ✓ Establecer la(s) acción(es) asociadas al control que mitigan o reducen cada riesgo, determinando el periodo de ejecución, indicador, área responsable y registro que evidencie el cumplimiento de la acción. ✓ Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo. ✓ Solicitar modificaciones de los diferentes tipos de riesgos de acuerdo con los autoevaluaciones, observaciones o informes de las auditorías internas o externas. ✓ Realizar monitoreo y revisión al Mapa de Riesgos de Gestión, Corrupción y Seguridad de la Información.

2ª. LÍNEA DE DEFENSA	
Tiene a cargo responsabilidades directas frente al monitoreo y evaluación del estado de controles y la Gestión del Riesgo, asegura que la identificación, análisis, valoración, monitoreo y las actividades de control de los riesgos de Gestión, Corrupción y de Seguridad de la Información implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.	
Responsables	Actividades de monitoreo y revisión
Dirección de Planeación,	✓ Asesorar a la línea estratégica en el análisis del contexto de

2ª. LÍNEA DE DEFENSA	
Tiene a cargo responsabilidades directas frente al monitoreo y evaluación del estado de controles y la Gestión del Riesgo, asegura que la identificación, análisis, valoración, monitoreo y las actividades de control de los riesgos de Gestión, Corrupción y de Seguridad de la Información implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.	
Responsables	Actividades de monitoreo y revisión
Supervisores e interventores de contratos o proyectos, comités de contratación, áreas financieras, Tics entre otros	la organización (interno y externo), para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo ✓ Consolidar el Mapa de riesgos institucional y presentarlo para aprobación ante el Comité Directivo ✓ Acompañar, orientar y entrenar a los responsables de los procesos en la identificación, análisis y valoración del riesgo ✓ Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los responsables de los procesos ✓ Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalúe y gestione los riesgos y controles para que se generen acciones. ✓ Evaluar que los riesgos sean consistentes con la actual política de la entidad y que sean monitoreados por la primera línea de defensa ✓ Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlo para aprobación del Comité Institucional de Coordinación de Control Interno ✓ Acompañar, orientar y entrenar a los responsables y gestores de calidad en la identificación, análisis, y valoración del riesgo y definición de controles en los temas a su cargo. ✓ Actualizar la versión del Mapa de Riesgos de Gestión y Corrupción o el Mapa de Riesgos de Seguridad de la Información según sea el caso, con las solicitudes de

2ª. LÍNEA DE DEFENSA	
Tiene a cargo responsabilidades directas frente al monitoreo y evaluación del estado de controles y la Gestión del Riesgo, asegura que la identificación, análisis, valoración, monitoreo y las actividades de control de los riesgos de Gestión, Corrupción y de Seguridad de la Información implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.	
Responsables	Actividades de monitoreo y revisión
	modificación aprobadas por la Alta Dirección para su respectiva publicación en la Página WEB de la Entidad.

3ª. LÍNEA DE DEFENSA	
Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.	
Responsables	Actividades de monitoreo y revisión
Oficina de Control Interno	✓ Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos ✓ Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa ✓ Asesorar de forma coordinada con la Dirección de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles. ✓ Llevar a cabo el seguimiento a los riesgos consolidados y presentar dicho informe de seguimiento al CICCÍ según la programación del Plan Anual de Auditoria o reuniones de este comité ✓ Recomendar mejoras a la política de administración del riesgo. ✓ Realizar seguimiento al Mapa de Riesgos, utilizando el Anexo 1 Mapa de Riesgos de Gestión y Corrupción y Anexo 2 Mapa de Riesgos de Seguridad de la Información y determinar el Estado de los Riesgos, así: • <u>Abierto:</u> El riesgo continúa para seguimiento. • <u>Mitigado:</u> el riesgo se estudia para determinar si este se sigue administrando o se retira del

	mapa de riesgos. • Materializado: el riesgo se lleva al Plan de Mejoramiento para la formulación de acciones correctivas ✓ Verificar la inclusión de los riesgos que se materializan en el plan de mejoramiento.
--	---

5. ETAPAS PARA LA GESTIÓN DEL RIESGO

La gestión de riesgos institucionales comprende las actividades de análisis del contexto interno y externo, identificación y análisis del riesgo, valoración, evaluación, definición de controles para el tratamiento y seguimiento. Las diferentes etapas con sus actividades específicas y responsables se describen en el “*Procedimiento para la Administración Integral de los Riesgos Institucionales*”.

6. NIVELES DE ACEPTACIÓN DEL RIESGO O TOLERANCIA AL RIESGO.

La siguiente tabla presenta el mapa de calor (Riesgo Inherente- sin controles) que contiene los niveles de aceptación y la medida de tratamiento para los riesgos de Gestión, Corrupción y Seguridad de la información. Los riesgos de corrupción son inaceptables.

TABLA No.7 Mapa de Calor					
ZONA DE RIESGO - NO APLICA RIESGOS DE CORRUPCIÓN					
PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Rara vez (1)	B	B	M	A	E
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E
ZONA DE RIESGO					
MEDIDA DE TRATAMIENTO DEL RIESGO					
B: Zona de riesgo baja: ACEPTAR EL RIESGO					
M: Zona de riesgo moderada: REDUCIR EL RIESGO					
A: Zona de riesgo Alta: COMPARTIR EL RIESGO					
E: Zona de riesgo extrema: EVITAR EL RIESGO					
ZONA DE RIESGO - RIESGO DE CORRUPCIÓN					
PROBABILIDAD	IMPACTO				
	Moderado	Mayor	Catastrófico		
Casi Seguro (5)	E	E	E		
Probable (4)	A	E	E		
Posible (3)	A	E	E		
Improbable (2)	M	A	E		
Rara vez (1)	M	A	E		
ZONA DE RIESGO					
MEDIDA DE TRATAMIENTO DEL RIESGO DE CORRUPCIÓN					
M: Zona de riesgo moderada: REDUCIR EL RIESGO					
A: Zona de riesgo Alta: COMPARTIR EL RIESGO					
E: Zona de riesgo extrema: EVITAR EL RIESGO					

7. NIVELES PARA CALIFICAR EL IMPACTO

⇒ Riesgos de gestión:

TABLA 4. Criterios para Calificar el Impacto - NO APLICA CORRUPCIÓN		
NIVEL DEL IMPACTO	CRITERIOS PARA CALIFICAR EL IMPACTO	VALOR DEL IMPACTO
CATASTRÓFICO	Interrupción de las operaciones de la Entidad por más de cinco (5) días.	5
	Intervención por parte de un ente de control u otro ente regulador.	
	Pérdida de Información crítica para la entidad que no se puede recuperar	
	Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.	
MAYOR	Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados	4
	Interrupción de las operaciones de la Entidad por más de dos (2) días.	
	Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.	
	Sanción por parte del ente de control u otro ente regulador	
	Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno	
MODERADO	Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.	3
	Interrupción de las operaciones de la Entidad por un (1) día.	
	Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad	
	Inoportunidad en la información ocasionando retrasos en la atención a los usuarios.	
	Reproceso de actividades y aumento de carga operativa	
	Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos	
MENOR	Investigaciones penales, fiscales o disciplinarias	2
	Interrupción de las operaciones de la Entidad por algunas horas.	
	Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias.	
INSIGNIFICANTE	Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.	1
	No hay interrupción de las operaciones de la entidad.	
	No se generan sanciones económicas o administrativas.	
	No se afecta la imagen institucional de forma significativa.	

⇒ Riesgos de Corrupción:

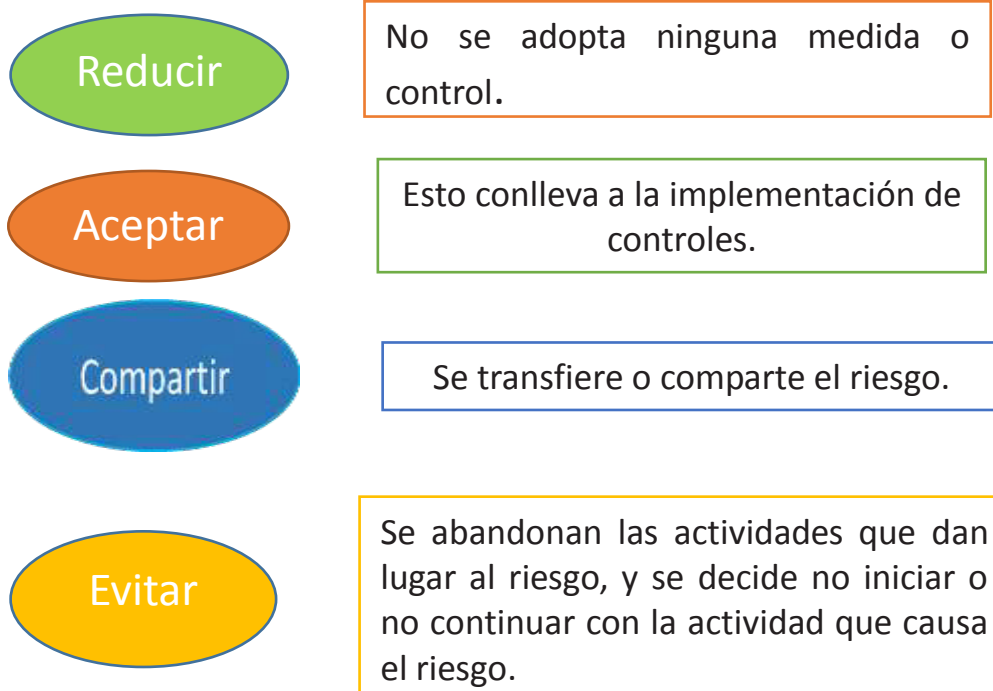
TABLA No.5. CRITERIOS PARA CALIFICAR EL IMPACTO - RIESGOS DE CORRUPCIÓN					
Nº	Pregunta Si el riesgo de corrupción se materializa podría...	Riesgo 1		Riesgo 2	
		Si	NO	Si	NO
1	¿Afectar al grupo de funcionarios del proceso?				
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?				
3	¿Afectar el cumplimiento de misión de la Entidad?				
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?				
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?				
6	¿Generar pérdida de recursos económicos?				
7	¿Afectar la generación de los productos o la prestación de servicios?				
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?				
9	¿Generar pérdida de información de la Entidad?				
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?				
11	¿Dar lugar a procesos sancionatorios?				
12	¿Dar lugar a procesos disciplinarios?				
13	¿Dar lugar a procesos fiscales?				
14	¿Dar lugar a procesos penales?				
15	¿Generar pérdida de credibilidad del sector?				
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?				
17	¿Afectar la imagen regional?				
18	¿Afectar la imagen nacional?				
19	¿Generar daño ambiental?				
TOTAL		0		0	
Clasificación del Impacto: Es la cantidad de respuestas afirmativas, revise la tabla de calificación de riesgo de corrupción					

CALIFICACIÓN IMPACTO RIESGO DE CORRUPCIÓN	
RESPUESTAS POSITIVAS	DESCRIPCIÓN
1 - 5	3-Moderada
6-11	4- Mayor
12-19	5- Catastrófico (Extrema)

⇒ Riesgos de Seguridad de la Información:

TABLA 6. Criterios para Calificar el Impacto - Riesgos de Seguridad Digital		
Descriptor	Descripción	calificación riesgos estratégicos
Insignificante	Sin afectación de la integridad de la información Sin afectación de la disponibilidad de la información Sin afectación de la confidencialidad de la información	1
Menor	Afectación leve de la integridad de la información Afectación leve de la disponibilidad de la información Afectación leve de la confidencialidad de la información	2
Moderado	Afectación moderada de la integridad de la información Afectación moderada de la disponibilidad de la información Afectación moderada de la confidencialidad de la información	3
Mayor	Afectación grave de la integridad de la información Afectación grave de la disponibilidad de la información Afectación grave de la confidencialidad de la información	4
Catastrófico	Afectación muy grave de la integridad de la información Afectación muy grave de la disponibilidad de la información Afectación muy grave de la confidencialidad de la información	5

8. TRATAMIENTO DE RIESGOS



ZONA DE RIESGO	TRATAMIENTO DEL RIESGO	
	RIESGOS DE GESTIÓN Y RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	RIESGOS DE CORRUPCIÓN
BAJA	Se asume el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado, no se adopta ninguna medida de control que afecta la probabilidad o el impacto del riesgo.	Ningún riesgo de corrupción podrá ser aceptado.
MODERADA	Se establecen acciones de control preventivas que permitan REDUCIR o COMPARTIR la probabilidad o el impacto de ocurrencia del riesgo	Se establecen acciones de control preventivas que permitan REDUCIR o COMPARTIR la probabilidad o el impacto de ocurrencia del riesgo
ALTA	Se establecen acciones de Control Preventivas que permitan COMPARTIR, EVITAR o REDUCIR el riesgo se reduce la probabilidad o el impacto del riesgo transferido o compartiendo una parte de este.	Se adoptan medidas para: REDUCIR: la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
EXTREMA	Se establecen acciones de Control Preventivas y correctivas que permitan EVITAR, COMPARTIR o REDUCIR el riesgo con el fin de mitigar la materialización del riesgo.	EVITAR: Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo. TRANSFERIR O COMPARTIR una parte del riesgo para reducir la probabilidad o el impacto del mismo. Los riesgos de corrupción se pueden compartir pero no se puede transferir su responsabilidad.

Para los riesgos de seguridad de la información Identifica en el Registro de Activos de Información del proceso publicado en la página WEB de la entidad aquellos que se

encuentran con criticidad ALTA agrupa los activos de información del mismo tipo y analiza conjuntamente las amenazas y vulnerabilidades que sean comunes y que podrían causar su materialización. Redacta el riesgo orientado a la posibilidad de ocurrencia de un evento teniendo en cuenta la selección anterior:

- ✓ Pérdida de confidencialidad
- ✓ Pérdida de la integridad
- ✓ Pérdida de la disponibilidad

Los procesos que no presentan activos de información con criticidad ALTA deben seleccionar activos de criticidad MEDIA según determinación de la importancia del activo de información para el proceso.

9. PERIODICIDAD PARA EL SEGUIMIENTO

El seguimiento para todos los riesgos será CUATRIMESTRAL y su adecuado control se registra en el ANEXO 1. Mapa de Riesgos de Gestión y Corrupción y ANEXO 2 Mapa de Riesgos de Seguridad de la Información.

10. ACCIONES PARA LA APROPIACIÓN DE LA GESTIÓN DEL RIESGO

En la Contraloría de Bogotá, D.C., se promueve la transparencia y se fortalece la cultura de autocontrol y prevención, lo cual contribuye a la administración integral de riesgos, a través de:

- ✓ Capacitaciones para el fortalecimiento institucional, conceptual y operativo de la gestión integral de riesgos.
- ✓ Asesorías y acompañamiento para el desarrollo del enfoque de administración de riesgos en las actividades diarias.
- ✓ Seguimiento cuatrimestral a todos los riesgos ubicados en las diferentes zonas de riesgo Baja, Moderada, Alta y Extrema de los anexos de la matriz de riesgos, identificada para cada uno de los procesos de la Entidad.
- ✓ Divulgación de los resultados de la administración y gestión de riesgos en los procesos de la Entidad

11. ACCIONES ANTE LA MATERIALIZACIÓN DEL RIESGO

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas a continuación:

- Para cualquier tipo de Riesgo se debe llevar al Plan de Mejoramiento, efectuar el análisis de causas y determinar acciones preventivas y de mejora.
- Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento y actualizar el mapa de riesgos.
- Para los riesgos de corrupción, la Oficina de Control Interno o responsable del Proceso deberá informar al Proceso de Direccionamiento Estratégico o a las autoridades competentes sobre el hecho encontrado realizar la denuncia ante la instancia de control correspondiente de la ocurrencia de un hecho de corrupción.
- Ante la materialización de los riesgos de gestión y de seguridad de la información en zona extrema, alta y moderada se informará al responsable del proceso o al Proceso de Direccionamiento Estratégico según sea el caso, se procede de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso) y documentarlo en el Plan de mejoramiento.
- Para los riesgos de gestión y de seguridad de la información en zona baja informar al responsable del proceso sobre el hecho, así mismo informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el responsable del proceso para revisar el mapa de riesgos establecer acciones correctivas al interior de cada proceso, a cargo del responsable respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos y la verificación por parte de la Oficina de Control Interno que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

CONTROL DE CAMBIOS

Versión	R.R., Acta ² o modificación ³ Día mes año	Descripción de la modificación
1.0	Acta No 01 del 14 de agosto de 2019 Comité Institucional de Coordinación de Control Interno	

² Acta de Comité que aprueba la versión 1.0 del documento.

³ Fecha en la cual el responsable del proceso aprueba la modificación del documento.

Resolución Reglamentaria

Número 040

(Septiembre 25 de 2019)

“Por medio de la cual se adopta la nueva versión del Procedimiento Recepción y Pago de Cuentas dentro del Proceso de Gestión Administrativa y Financiera de la Contraloría de Bogotá, D.C.”

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

CONSIDERANDO:

Que de conformidad con el artículo 269 de la Constitución Política, es obligación de las autoridades públicas, diseñar y aplicar en las entidades públicas, métodos y procedimientos de control interno, según la naturaleza de sus funciones, de conformidad con lo que disponga la ley.

Que según los literales b) y l) del artículo 4 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”*, se deben implementar como elementos del sistema de control interno institucional, la definición de políticas como guías de acción y procedimientos para la ejecución de procesos, así como, la simplificación y actualización de normas y procedimientos.

Que en el artículo 6 del Acuerdo 658 de 2016, por el cual se dictan normas sobre organización y funcionamiento de la Contraloría de Bogotá D.C., se estableció que: *“En ejercicio de su autonomía administrativa le corresponde a la Contraloría de Bogotá, D.C., definir todos los aspectos relacionados con el cumplimiento de sus funciones en armonía con los principios consagrados en la Constitución, las leyes y en este Acuerdo”*.

Que mediante la Resolución Reglamentaria No 038 del 8 de octubre de 2018, se adoptó la nueva versión

del modelo Estándar de Control Interno – MECI, en la Contraloría de Bogotá, D.C, de conformidad al Decreto 1499 de 2017, modificatorio del Decreto 1083 de 2015 -Decreto Único Reglamentario de la Función Pública-, con el fin de incorporar la estructura definida en la dimensión No 7ª- Control Interno del Manual Operativo del Modelo Integrado de Planeación y Gestión - MIPG.

Que se hace necesario ajustar el Procedimiento Recepción y Pago de Cuentas, versión 6.0, código PGAF 06, adoptado mediante Resolución Reglamentaria No.42 del 28 de diciembre de 2017, de acuerdo con las necesidades y solicitudes de quienes intervienen en él, igualmente para ajustarlo a la normatividad vigente.

RESUELVE:

ARTÍCULO PRIMERO. Adoptar la nueva versión del siguiente procedimiento dentro del Proceso de Gestión Administrativa y Financiera – PGAF de la Contraloría de Bogotá, D.C.:

No.	Documento	Código	Versión
1	Procedimiento Recepción y Pago de Cuentas.	PGAF-06	7.0

ARTÍCULO SEGUNDO. Es responsabilidad de los Directores, Subdirectores, Jefes de Oficina y Gerentes, velar por la administración y divulgación del procedimiento adoptado.

ARTÍCULO TERCERO. 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. 042 del 28 de diciembre de 2017.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los veinticinco (25) días del mes de septiembre de dos mil diecinueve (2019).

JUAN CARLOS GRANADOS BECERRA
Contralor de Bogotá D.C.

Aprobación		Revisión Técnica
Firma:		
Nombre:	Lina Raquel Rodríguez Meza	Mercedes Yunda Monroy
Cargo:	Directora Administrativa	Directora Técnica
Dependencia:	Dirección Administrativa y Financiera	Dirección de Planeación
R.R. No.	040	Fecha SEPTIEMBRE 25 DE 2019

1. OBJETIVO(S):

Establecer las actividades y requisitos exigidos por la entidad para realizar los pagos de las obligaciones adquiridas con terceros por la Contraloría de Bogotá, D.C., tales como pago a contratistas, proveedores, servicios de administración, celulares, servicios públicos, nómina, viáticos, avances, aportes en salud, pensiones, riesgos profesionales y aportes parafiscales.

2. ALCANCE:

Este procedimiento contempla el pago a contratistas y proveedores, pago de servicios públicos, de administración y telefonía celular, pagos de nomina, pagos de aportes en salud, pensiones, riesgos profesionales y aportes parafiscales con los siguientes alcances:

Pago de contratistas y proveedores: Inicia cuando el supervisor o interventor del contrato radica los documentos originales de la cuenta en la Subdirección Financiera (área central de cuentas) y termina cuando el Tesorero de la Contraloría de Bogotá ingresa a la plataforma SECOP II y realiza la marcación de pagado.

Pagos de servicios públicos, de administración y telefonía celular: Inicia cuando el Subdirector Técnico de Servicios Generales, Recursos Materiales y/o Auditoría Fiscal diligencia el anexo No 3 junto con la factura o documento equivalente y termina cuando el Auxiliar Administrativo y/o Secretario de Tesorería recibe las ordenes de pago las clasifica por fecha de giro y hace el respectivo cruce con la SDH.

Pagos de nomina: Inicia cuando la secretaria de la Subdirección Financiera Recibe la nomina en medio físico los documentos provenientes de la Dirección de Talento Humano y termina cuando el Auxiliar Administrativo y/o Secretaria de Tesorería entrega el acta de legalización al auxiliar administrativo encargado de generar los comprobantes de egreso, organizar y archivar los informes diarios de tesorería.

Pagos de aportes en salud, pensiones, riesgos profesionales y aportes parafiscales: Inicia cuando la secretaria de la Subdirección Financiera recibe en medio físico los

documentos enviados de la Dirección de Talento Humano y termina cuando el Auxiliar Administrativo y/o Secretario de Tesorería entrega el acta firmada al auxiliar administrativo encargado de generar comprobantes de egreso, organizar y archivar los informes diarios de Tesorería.

3. BASE LEGAL:

TIPO DE NORMA	FECHA (dd/mm/aaaa)	DESCRIPCIÓN
Constitución Política de Colombia	07-jul-1991	Título XII, capítulo cuarto.
Ley 734	05-feb-2002	Por la cual se expide el Código Disciplinario Único hasta el 30 junio de 2021 según ley 1955 de 2019. Artículo 35. Prohibiciones. Numerales 15 y 16. Artículo 48. Faltas gravísimas. Numerales: 20, 21, 22, 23, 24, 25 y 26.
Ley 1150	16-jul-2007	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. Artículo 19, del derecho de turno.
Ley 1819	29-dic-2016	Por medio de la cual se adopta una reforma tributaria estructural, se fortalecen los mecanismos para la lucha contra la evasión y la elusión fiscal, y se dictan otras disposiciones.
Decreto 624	30-mar-1989	Por el cual se expide el Estatuto Tributario de los Impuestos administrados por la Dirección General de Impuestos Nacionales.
Decreto 1421	21-jul-1993	Por el cual se dicta el régimen especial para el Distrito Capital de Santa Fé de Bogotá.
Decreto 807	17-dic-1993	Por el cual se armoniza el procedimiento y la administración de los tributos distritales con el Estatuto Tributario Nacional y se dictan otras disposiciones.
Decreto 111	15-ene-1996	Por el cual se compilan la Ley 38 de 1989, la Ley 179 de 1994 y la Ley 225 de 1995 que conforman el Estatuto Orgánico de Presupuesto.
Decreto Distrital 714	15-nov-1996	Por el cual se compilan el Acuerdo 24 de 1995 y Acuerdo 20 de 1996 que conforman el Estatuto Orgánico del Presupuesto Distrital.
Decreto Distrital 362	21-ago-2002	Por el cual se actualiza el procedimiento tributario de los diferentes impuestos distritales, de conformidad con su naturaleza y estructura funcional.

TIPO DE NORMA	FECHA (dd/mm/aaaa)	DESCRIPCIÓN
Decreto Distrital 216	03-may-2017	Por el cual se reglamentan el Decreto 714 de 1996, Estatuto Orgánico de Presupuesto Distrital y se dictan otras disposiciones.
Acuerdo 658	21-dic-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. Artículo 6.- Autonomía Administrativa.
Acuerdo 664	28-mar-2017	Por el cual se modifica parcialmente el Acuerdo 658 del 21 de diciembre 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 funciones de sus dependencias, se modifica la planta de personal, y se dictan otras disposiciones.
Resolución Ministerio de Hacienda y Crédito Público No. 036	07-may-1998	Por la cual se determinan algunas normas y procedimientos sobre registros presupuestales, suministro de información y su sistematización del Presupuesto General de la Nación: Artículos 2, 3.
Resolución Secretaría De Hacienda Distrital No. 660	29-dic-2011	Por la cual se adopta el Manual de Programación, Ejecución y Cierre Presupuestal de las entidades que conforman el Presupuesto Anual del Distrito Capital.
Resolución Contaduría General de la Nación No. 533	08-oct-2015	Por la cual se incorpora, en el Régimen de Contabilidad Pública, el marco normativo aplicable a entidades de gobierno y se dictan otras disposiciones.
Instructivo 002 de la Contaduría General de la Nación	08-oct-2015	Instrucciones para la transición al marco Normativo para entidades de Gobierno.
Resolución de la Contaduría General de la Nación No.620	26-nov-2015	Por el cual se incorpora el catálogo General de cuentas del Marco Normativo para entidades de Gobierno.

4. DEFINICIONES:

CONTRATISTA¹: La persona natural o jurídica que asume contractualmente ante la Contraloría de Bogotá, con medios humanos y materiales propios o ajenos, el compromiso de ejecutar el objeto contractual pactado de acuerdo a las obligaciones contenidas en el clausulado correspondiente.

FACTURA: Es un título valor que el vendedor o prestador del servicio podrá librar y entregar o remitir al comprador o beneficiario del servicio.

DOCUMENTO EQUIVALENTE: Documento soporte que reemplaza a la factura en operaciones económicas realizadas por personas que no están obligados a facturar (régimen simplificado).

PROGRAMA ANUAL MENSUALIZADO DE CAJA - PAC: Es una herramienta de planeación financiera, con la cual las entidades establecen el monto máximo de pagos en un periodo determinado de tiempo.

PAGO: Es el cumplimiento efectivo de una obligación, o responsabilidad económica adquirida.

RECIBIDO A SATISFACCIÓN: Es el documento que acredita el cumplimiento en debida forma del objeto y obligaciones contractuales.

SUPERVISOR O INTERVENTOR: Funcionario o contratista que en representación de los intereses de la entidad, vigila la debida ejecución del contrato.

SECOP I: Plataforma administrada por Colombia Compra Eficiente para la publicación de todos los procesos contractuales de contratación directa.

SECOP II: Plataforma administrada por Colombia Compra eficiente para la publicación de procesos contractuales diferentes a contratación directa.

5. DESCRIPCIÓN DEL PROCEDIMIENTO:

5.1 PAGO A CONTRATISTAS Y PROVEEDORES

¹ Definición del Proceso de Gestión Administrativa y Financiera.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
1.	Supervisor o Interventor del contrato.	Radica los documentos originales de la cuenta en la Subdirección Financiera (área central de cuentas), para lo cual entrega en medio físico el original de la factura o documento equivalente y los soportes, de acuerdo a lo establecido en el anexo No.1 - radicación de documentos para trámite de cuentas. Cuando se trate de procesos incluidos en la plataforma SECOP I debe radicar una copia de los mismos en la Subdirección de Contratación para que estos obren dentro del expediente contractual.		Punto de Control: Previo a la radicación de la cuenta debe estar programado el PAC del mes de pago. El Supervisor o Interventor, mediante el recibo a satisfacción, informe de supervisión y anexo1 que acreditan el cumplimiento del objeto y las obligaciones contractuales. Observación: El supervisor se quedará con una copia del recibido del anexo 1- (radicación de documentos para trámite de cuentas) por parte del área central de cuentas.
2.	Técnico Profesional Universitario central de cuentas Subdirección Financiera y/o de	Recibe el anexo No.1 - radicación de documentos para trámite de cuentas, con el original de la factura o cuenta de cobro y los soportes para el pago. Radica en el reloj de control del área central de cuentas. Diligencia la información del anexo No. 2 - Hoja de Ruta Interna con los datos pertinentes. Una vez radicada la cuenta entrega al		Punto de Control: Revisa que la documentación se encuentre completa y que corresponda de acuerdo con el tipo de pago establecido en el anexo No.1 - radicación de documentos para trámite de cuentas. Si presenta inconsistencias no se recibe la cuenta. El número de radicación asigna el turno del pago según corresponda.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		supervisor copia del anexo 1. Entrega la documentación al área de Contabilidad de la cuenta y soportes, para su contabilización y posterior pago. Cuando se trate de procesos contractuales incluidos en la plataforma SECOP II verifica que el contratista y el supervisor hayan realizado el cargue de los documentos para tramite de pago y se encuentren aprobados, de ser así radica en el reloj de control del área central de cuentas.		Antes de la recepción de cuenta, revisa que la misma esté programada en el PAC del respectivo mes, si no está en el PAC devuelve la cuenta. Los documentos a radicar con la cuenta son: anexo 1, factura o documento equivalente, recibo a satisfacción, informe de supervisión, informe de actividades con soportes, soporte de pago al SSI de conformidad con la normatividad vigente y en caso de persona jurídica certificación de cumplimiento del pago de SSI y aportes para fiscales suscrita por el revisor fiscal o representante legal según sea el caso. Registrar en el sistema de información vigente las cuentas radicadas.
3.	Profesional Universitario Área Contabilidad	Recibe la relación de cuentas radicadas junto con los soportes. Activa el Procedimiento de gestión contable (ver Elaboración Orden de Pago). Finalizado el procedimiento contable se radica en tesorería.		Punto de Control: Revisa que la documentación se encuentre completa y que corresponda de acuerdo con el tipo de pago establecido en el anexo No.1 - radicación de documentos para trámite de cuentas. Si presenta inconsistencias se hace devolución de la cuenta a la central cuentas.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
4.	Tesorero, Profesional Universitario, (Tesorería) Secretaria (Tesorería)	Recibe la orden de pago aplicativo Contraloría de Bogotá, la copia y sus soportes, activa el Procedimiento de Gestión Tesoral (ver Giro Tesoral y/o Giro de la Orden de Pago) y entrega las ordenes de pago con sus soportes y planillas al auxiliar administrativo y/o secretario de tesorería.	Comprobante de egreso; Órdenes de pago (SICAPITAL y Secretaria de Hacienda); Factura o cuenta de cobro; Anexo No.1 - radicación de documentos para trámite de cuentas, Documentos recibidos en la recepción de cuentas de cobro y/o causación contable.; Anexo No.2 - Hoja de Ruta; Otros soportes.	Punto de Control: Revisa que la documentación se encuentre completa y corresponda al servicio prestado, así mismo verifica los valores de la orden de pago y que el anexo No.2 - Hoja de Ruta Interna se encuentre diligenciado en cada uno de los campos por donde ha pasado la cuenta. Si presenta inconsistencias se devuelve y solicita los ajustes correspondientes.
5.	Auxiliar administrativo y/o secretario de Tesorería.	Recibe las ordenes de pago, las clasifica por fecha de giro y rubros de funcionamiento o proyectos de inversión y hace el cruce con el sistema de la Secretaria Distrital de Hacienda y procede a generar las actas de legalización por concepto de endosos y legalización de impuestos, para revisión y firma del tesorero (a). Una vez firmadas las actas las entrega al	Actas de legalización y comprobantes de egreso.	Punto de Control: Las actas de legalización deben ser entregadas con las órdenes de pago y soportes.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		auxiliar administrativo encargado de generar los comprobantes de egreso, organizar y archivar los informes diarios de tesorería.		
6.	Técnico central de cuentas.	Entrega mediante oficio con radicado de Sigepro a la secretaria de la Subdirección de Contratación original de la orden de pago y original del comprobante de egreso, cuando se trate de contratos incluidos en la plataforma SECOP I. Entrega los informes diarios de tesorería y se activa el procedimiento de Gestión Contable. En el evento que los contratos estén incluidos en la plataforma SECOP II se debe cargar a esta la orden de pago y el comprobante de egreso.	Memorando dirigido a la Subdirección de Contratación de PGD-07-02	
7.	Tesorero (a) de Contraloría de Bogotá.	Ingresar a la plataforma SECOP II para los contratos registrados en esta y realiza la marcación de pagado.		

5.2 PAGOS DE SERVICIOS PÚBLICOS, DE ADMINISTRACIÓN Y TELEFONIA CELULAR.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
1.	Subdirector Técnico de Servicios Generales, Recursos	Diligencia el anexo No.3 Solicitud de CDP y CRP para pago de servicios, junto con la factura o documento equivalente		

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
	materiales y/o auditoría fiscal.	para firma del ordenador del gasto delegado para tal fin.		
2.	Ordenador del Gasto Delegado.	Revisa el Anexo No. 3, si esta de acuerdo lo firma y lo radica en la central de cuentas de la subdirección financiera.	Anexo No. 3 solicitud de CDP y CRP para pago de servicios públicos, administración y celulares. PGAF-06-03	Punto de Control: Previo a la radicación de la cuenta debe estar programado el PAC de pago. Revisa que no haya servicios adicionales no autorizados. En el evento que se evidencie servicios no autorizados en la facturación adjuntar la cuenta de cobro correspondiente.
3.	Técnico Profesional Universitario (Central Cuentas) y/o de	Recibe anexo No.3 debidamente firmado, junto con el original de la cuenta de cobro o factura y soportes requeridos para el pago de los servicios Radica en el reloj de control del área central de cuentas de la subdirección financiera. Diligencia la información del anexo No. 2 - Hoja de Ruta Interna con los datos pertinentes. Entrega al Profesional de Presupuesto, los recibos de servicios públicos, cuenta de cobro o factura, acompañados de la solicitud de CDP y CRP (anexo No.3,) y la hoja de ruta (anexo No.2).		Punto de Control: Verificar que las firmas correspondan a las personas autorizadas y que la documentación se encuentre completa. Si presenta inconsistencias se devuelve. Observación: Verifica que el Tercero se encuentre registrado en la Base de Datos de Terceros del sistema financiero vigente, en caso que el tercero no exista lo registra, de lo contrario revisa que la información existente se encuentre bien diligenciada.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
4.	Profesional Universitario y/o especializado Área Presupuesto	Recibe la solicitud de CDP y CRP (anexo 3) y la hoja de ruta (anexo 2). Diligencia la hoja de ruta (anexo 2), en lo referente al trámite del área de presupuesto. Activa Procedimiento para el Manejo de Presupuesto (ver <i>Expedición de Certificados de Disponibilidad y Certificado de Registro Presupuestal</i>). Entrega la documentación al área de contabilidad para la elaboración de la orden de pago.		Punto de Control: Revisa que la documentación se encuentre completa y corresponda al servicio prestado. Si presenta inconsistencias se devuelve. Observación: La documentación es: ✓ Solicitud de CDP y CRP ✓ Hoja de Ruta (anexo No.2) ✓ Recibo, cuenta de cobro o factura. ✓ Otros soportes.
5.	Profesional Universitario Área Contabilidad	Recibe la documentación, elabora la Orden de Pago (ver Procedimiento para el Manejo de la Contabilidad). Activa el Procedimiento de Gestión Contable (ver Elaboración Orden de Pago). Finalizado el procedimiento contable se activa el procedimiento de Gestión Tesoral.		Punto de Control: Revisa que la documentación se encuentre completa y corresponda al servicio prestado. Si presenta inconsistencias se devuelve.
6.	Tesorero General (a) Contraloría de	Recibe la orden de pago aplicativo Contraloría de Bogotá,	Comprobante de egreso; Órdenes de	Punto de Control: Revisa que la documentación se

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
	Bogotá.	la copia y sus soportes, activa el Procedimiento de Gestión Tesoral (ver Giro Tesoral y/o Giro de la Orden de Pago) y entrega las ordenes de pago con sus soportes y planillas al auxiliar administrativo y/o secretario de tesorería.	pago (SICAPITAL y Secretaria de Hacienda); Factura o cuenta de cobro; CDP y CRP Anexo No.1- radicación de documentos para trámite de cuentas, Documentos recibidos en la recepción de cuentas de cobro y/o causación contable.; Anexo No.2 - Hoja de Ruta; Otros soportes.	encuentre completa y corresponda al servicio prestado, así mismo verifica los valores de la orden de pago y que el anexo No.2 - Hoja de Ruta Interna se encuentre diligenciado en cada uno de los campos por donde ha pasado la cuenta. Si presenta inconsistencias se devuelve y solicita los ajustes correspondientes.
7.	Auxiliar administrativo y/o secretario de Tesorería.	Recibe las ordenes de pago, las clasifica por fecha de giro y hace el cruce con el sistema de la Secretaria Distrital de Hacienda y procede a generar las actas de legalización por concepto de endosos, para revisión y firma del Tesorero (a). Una vez firmadas las actas las entrega al auxiliar administrativo encargado de generar los comprobantes de egreso, organizar y archivar los informes diarios de Tesorería.	Actas de legalización y comprobantes de egreso, generadas por SICAPITAL.	Punto de Control: Las actas de legalización deben ser entregadas con las órdenes de pago y soportes.

5.3 PAGOS DE NOMINA.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
1.	Secretaria de la Subdirección Financiera	Recibe la nómina en medio físico con los siguientes documentos: ✓ Memorando. ✓ Nómina. ✓ Novedades de descuentos, cooperativas, entre otros. ✓ Certificado Registro Presupuestal. Radica en el reloj del área central de cuentas. Entrega la documentación al área de Contabilidad.		Punto de Control: Al inicio de cada vigencia, el Director Técnico de Talento Humano, el Subdirector de Gestión del Talento Humano y el Subdirector Técnico Financiero, elaboran el cronograma para la entrega y pagos de la nómina de funcionarios. Previo a la radicación de la cuenta debe estar programado el PAC de pago. Antes de radicar la nómina, se debe solicitar mediante memorando el Certificado de Disponibilidad y Registro Presupuestal, adjuntando el resumen por centro de costos, del régimen nuevo, antiguo, resumen general, incapacidades incluidas en el periodo, con el fin de activar el Procedimiento para el Manejo de Presupuesto (ver Expedición de Registro Presupuestal). Revisa que la documentación se encuentre completa. En caso que la documentación no corresponda, la devuelve a la Subdirección de Gestión del Talento

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
				Humano para que se subsanen las inconsistencias o se aporte la documentación faltante.
2.	Profesional Universitario Área Contabilidad	Recibe la nómina y los soportes. Activa el Procedimiento de Gestión Contable (ver Elaboración de la relación de autorización-RA). Elabora relación de autorización. Finalizado el procedimiento contable se radica en tesorería.		Punto de Control: Revisa que la documentación se encuentre completa. En caso que la documentación no corresponda, la devuelve a la Subdirección de Gestión del Talento Humano para que se subsanen las inconsistencias o se aporte la documentación faltante.
3.	Secretario y/o Auxiliar Administrativo de Tesorería.	Recibe la RA con los soportes y la planilla, procede a realizar la radicación en el aplicativo de Tesorería de Sicapital. Entrega la RA al Tesorero (a) de la Contraloría de Bogotá.		
4.	Tesorero, Profesional Universitario, (Tesorería) Secretaria (Tesorería)	Recibe la Relación de Autorización - RA y soportes. Activa el Procedimiento para el Manejo de la Tesorería (ver Giro Tesoral y/o Giro de la RA). Entrega el RA con los soportes al auxiliar administrativo y/o secretario de tesorería.		Punto de Control: Revisa que la documentación se encuentre completa y que corresponda. Así mismo verifica los valores de la RA. Si presenta inconsistencias se devuelve y solicita los ajustes correspondientes.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
5.	Auxiliar administrativo y/o secretario de Tesorería.	Recibe el RA de nomina y genera el acta de legalización por concepto de ingreso de los recursos de la nomina, para revisión y firma del Tesorero (a). Una vez firmadas el acta la entrega al auxiliar administrativo encargado de generar los comprobantes de egreso, organizar y archivar los informes diarios de Tesorería.	Acta de legalización y comprobante de egreso, generadas por SICAPITAL.	Punto de Control: El acta de legalización debe ser entregada con el RA y los soportes.

5.4 PAGOS DE APORTES EN SALUD, PENSIONES, RIESGOS PROFESIONALES Y APORTES PARAFISCALES.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
1.	Secretaria de la Subdirección Financiera.	Recibe en medio físico los siguientes documentos. ✓ Memorando ✓ Relación de Autorización ✓ Planilla Única. ✓ Resumen de Pagos debidamente diligenciada y firmada por el Director Técnico de Talento Humano en original. Radica en el reloj del área central de cuentas de la Subdirección Financiera.		Punto de Control: Al inicio de cada vigencia, el Director Técnico de Talento Humano, el Subdirector de Gestión del Talento Humano y el Subdirector Técnico Financiero, elaboran el cronograma para la entrega y pagos de los aportes a seguridad social de funcionarios. Previo a la radicación de la cuenta debe estar programado el PAC de pago.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
		Entrega la documentación al área de Presupuesto, para la expedición del Certificado de Disponibilidad Presupuestal y Certificado Registro Presupuestal.		En caso que la documentación no corresponda, la devuelve a la Subdirección de Gestión del Talento Humano para que se subsanen las inconsistencias o se aporte la documentación faltante.
2.	Profesional Universitario y/o Especializado de Presupuesto	Recibe y revisa la documentación. Activa el Procedimiento Gestión Presupuestal (ver expedición de certificados de disponibilidad y Registros Presupuestales de la Nómina). Entrega la documentación al área de contabilidad para la elaboración de la relación de autorización, junto con el CDP y CRP.		Punto de Control: Revisa que la documentación se encuentre completa. En caso que la documentación no corresponda, la devuelve a la Dirección de Talento Humano para que se subsanen las inconsistencias o se aporte la documentación faltante.
3.	Profesional Universitario Área Contabilidad.	Recibe y revisa la documentación. Activa el Procedimiento de Gestión Contable (ver Elaboración de la Orden de Pago o RA). Elabora la Relación de Autorización-RA. Finalizado el procedimiento contable se radica en tesorería.	Relación de Autorización.	Punto de Control: Revisa que la documentación se encuentre completa y que corresponda. Si presenta inconsistencias se devuelve a la Dirección de Talento Humano para que se subsanen las inconsistencias o se aporte la documentación faltante.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
				Observación: La documentación es: ✓ Formularios de Autoliquidación de Aportes de cada Administradora. ✓ Relación de Autorización. ✓ Planilla Única de Autoliquidación Mensual de Aportes Parafiscales. ✓ Certificado Disponibilidad Presupuestal y, ✓ Certificado Registro Presupuestal.
4.	Secretario y/o Auxiliar Administrativo de Tesorería.	Recibe la RA con los soportes y la planilla, procede a realizar la radicación en el aplicativo de Tesorería de Sicapital. Entrega la RA al Tesorero (a) de la Contraloría de Bogotá.		
5.	Tesorero, Profesional Universitario, (Tesorería) Secretaria (Tesorería)	Recibe la RA con los soportes y activa el Procedimiento de Gestión Tesoral.		Punto de Control: Revisa que la documentación se encuentre completa y que corresponda. Así mismo verifica los valores de la RA. Si presenta inconsistencias se devuelve y solicita los ajustes correspondientes.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL / OBSERVACIONES
6.	Auxiliar Administrativo y/o Secretario de Tesorería.	Recibe el RA de nomina y genera el acta de legalización por concepto de ingreso de los recursos de aportes patronales y parafiscales, para revisión y firma del Tesorero (a). Una vez firmadas el acta la entrega al auxiliar administrativo encargado de generar los comprobantes de egreso, organizar y archivar los informes diarios de Tesorería.	Acta de legalización y comprobante de egreso, generadas por SICAPITAL.	Punto de Control: El acta de legalización debe ser entregada con el RA y los soportes.

6. ANEXOS:

ANEXO No.1 - Radicación de documentos para trámite de cuentas.

	RADICACIÓN DE DOCUMENTOS PARA TRÁMITE DE CUENTAS	Código formato: PGAF-06-01 Versión: 7.0 Código documento: PGAF-06 Versión: 7.0 Página 1 de 1
DATOS GENERALES (1)		
No. DE CONTRATO/CONVENIO:		FECHA DE SUSCRIPCIÓN (DD/MM/AAAA):
CONTRATISTA/ASOCIADO:		ESPACIO EXCLUSIVO PARA CONSECUTIVO DE RADICACIÓN CENTRAL DE CUENTAS - SUBDIRECCIÓN FINANCIERA
VALOR INICIAL DEL CONTRATO/CONVENIO:		
VALOR TOTAL ADICIONADO:		
VALOR TOTAL DEL CONTRATO/CONVENIO: \$ -		
PLAZO CONTRACTUAL:		
PLAZO TOTAL PRORROGADO:		
PLAZO TOTAL DEL CONTRATO/CONVENIO:		
FECHA DE INICIO (DD/MM/AAAA):		
FECHA DE TERMINACIÓN (DD/MM/AAAA):		
INFORMACIÓN DEL PAGO (2)		
TIPO DE PAGO:	No DE PAGO:	
TIPO DE DOCUMENTO:	No.	VALOR TOTAL:
PERIODO CERTIFICADO DEL (DD/MM/AAAA) AL (DD/MM/AAAA)		
DOCUMENTOS NECESARIOS PARA EL TRAMITE DE CUENTAS (3)		
	OBS.	FOLIOS
1. Fotocopia actualizada de Registro Único Tributario - RUT Nota: Aplica solo para el primer pago.		
2. Copia Certificación Bancaria Nota: Aplica solo para el primer pago y/o por cambio de cuenta bancaria.		
3. Original de Factura(s) o Documento Equivalente de conformidad con las normas vigentes.		
4. Formato de recibido a satisfacción debidamente diligenciado y firmado por el supervisor(a) designado en el contrato/convenio del respectivo periodo de pago.		
5. Informe de supervisión debidamente diligenciado y firmado del respectivo periodo de pago.		
6. Certificación de pago de seguridad social y aportes parafiscales expedido por el Revisor Fiscal cuando esten obligados a tenerlo o el Representante Legal del periodo certificado en la cuenta y copia de las respectivas planillas (Persona Jurídica).		
7. Copia de las planillas de pago de salud, pensión y ARL del periodo de pago certificado (Base de cotización igual o superior al 40% del los honorarios mensuales (Persona Natural)).		
8. Copia de personería jurídica (para pertenecientes a régimen especial - Entidades sin ánimo de lucro).		
9. Comprobante de ingreso al almacén (En caso de adquisición de bienes devolutivos o de consumo).		
10. Declaración Juramentada con soportes Nota: Aplica sólo para contratos de prestación de servicios y se debe aportar en el primer pago.		
TOTAL FOLIOS		-
CERTIFICACIÓN		
En mi calidad de Supervisor(a) contractual, certifico que realice la verificación y consistencia de la información de cada uno de los documentos soportes para adelantar el respectivo pago del contrato/convenio y que los mismos se generaron por el cumplimiento del contratista/asociado a entera satisfacción en el período de ejecución certificado y de conformidad con lo establecido en el objeto y obligaciones contractuales y demás normas aplicables.		
NOMBRE DEL SUPERVISOR CARGO DEL SUPERVISOR(A) SUPERVISOR(A)		
ESPACIO EXCLUSIVO PARA SER DILIGENCIADO POR LA SUBDIRECCIÓN FINANCIERA		
OBSERVACIONES:		

INSTRUCTIVO DE DILIGENCIAMIENTO

1. **DATOS GENERALES:** Se diligencia la información de acuerdo al tipo de contrato y el clausulado correspondiente.
2. **INFORMACION DEL PAGO:** Se diligencia la información de acuerdo al tipo de pago que corresponda.
3. **DOCUMENTOS NECESARIOS PARA EL TRÁMITE DE CUENTAS:** Se diligencia la información de acuerdo al tipo de contrato y al tipo de pago.

ANEXO No.2 – Hoja de Ruta Interna:

	HOJA DE RUTA INTERNA	Código formato: PGAF-06-02
		Versión: 7.0
		Código documento: PGAF-06
		Versión: 7.0
		Página 1 de 2

ANEXO 2 DIRECCION ADMINISTRATIVA-SUBDIRECCION FINANCIERA HOJA DE RUTA INTERNA NO: (1) _____					
ENCABEZADO					
NO. RADICADO (2)	_____	FECHA (3)	_____	HORA: (4)	_____
PROVEEDOR (5)	_____				
TIPO DOCUMENTO (6)	_____	No: (7)	_____		
VALOR COMPROMISO (8)	_____	No: Compr. (9)	_____		
ADICIÓN (10)	_____	FECHA (11)	_____		
SALDO PENDIENTE DE PAGO (12)	_____	O. PAGO ANTERIOR (13)	_____		
MENOS ESTE PAGO (14)	_____	(16)	_____		
NUEVO SALDO (15)	_____	Central de Cuentas	_____		
CENTRAL DE CUENTAS ENTREGA A: (17)					
CONTABILIDAD	FECHA	_____	PRESUPUESTO	FECHA	_____
DEVUELVE: (18)	_____	FECHA: (19)	_____		
NO. FOLIOS (20)	_____				
TRAMITE EN LAS AREAS (21)					
PRESUPUESTO REG. DISP Y/O COMPROMISO CONTABILIDAD CAUSACIÓN CGIRO	NO.	MES	DIA	HORA	RESPONSABLE
	_____	_____	_____	_____	_____
	_____	_____	_____	_____	_____
TRAMITE ORDEN DE PAGO (22)	NO.	MES	DIA	HORA	RESPONSABLE
ELABORACIÓN DE ORDEN DE PAGO	_____	_____	_____	_____	_____
FIRMAS (23)					
COORDINADOR PRESUPUESTO COORDINADOR CONTABILIDAD SECRETARIA SUBDIRECCIÓN	MES	DIA	HORA	RESPONSABLE	
	_____	_____	_____	_____	
	_____	_____	_____	_____	
TRAMITE CHEQUE (24)	NO.	MES	DIA	HORA	RESPONSABLE
TESORERIA ELABORACION CHEQUE	_____	_____	_____	_____	_____
FIRMA TESORERO(A) GENERAL FIRMA SUBDIRECTOR(A) (RECIBIDO POR) SECRETARIA TESORERIA	MES	DIA	HORA	RESPONSABLE	
	_____	_____	_____	_____	
	_____	_____	_____	_____	
OBSERVACIÓN ÁREAS : (25)	_____				

INSTRUCCIONES DE DILIGENCIAMIENTO

1. **HOJA DE RUTA INTERNA No:** Es el número consecutivo interno de la hoja de ruta, el cual es asignado en la Central de Cuentas.
2. **No. RADICADO:** Número consecutivo que se genera en la central de cuentas al radicar el documento soporte base para la cancelación del compromiso.
3. **FECHA:** Día, mes y año de la radicación.
4. **HORA:** Hora en que es radicado.
5. **PROVEEDOR:** Persona natural o jurídica que solicita el pago del compromiso.
6. **TIPO DE DOCUMENTO.:** dependiendo el tipo de compromiso puede ser factura, cuenta de cobro, recibo de servicios públicos u otros, el cual va identificado con su numeración.
7. **No.:** Número de Identificación Tributaria o número de la cedula de ciudadanía.
8. **VALOR COMPROMISO:** Valor del registro presupuestal inicial.
9. **No COMPROMISO.:** Número del compromiso.
10. **ADICION:** Valor adicionado al registro presupuestal inicial.
11. **FECHA:** Fecha en que se realiza la adición al compromiso.
12. **SALDO PENDIENTE DE PAGO:** Valor correspondiente al rubro total del compromiso menos los pagos efectuados.
13. **PAGO ANTERIOR:** Valor correspondiente al pago anterior.
14. **MENOS ESTE PAGO:** Valor total de la factura, cuenta de cobro, servicio público u otro.
15. **NUEVO SALDO:** Nuevo saldo del compromiso, diferencia entre el saldo pendiente de pago y el valor del documento soporte del compromiso.
16. **CENTRAL DE CUENTAS:** Funcionario encargado de la central de cuentas.
17. **CENTRAL DE CUENTAS ENTREGA A:** Área de (contabilidad, presupuesto) dando inicio al proceso de causación y/o pago de los compromisos y/u obligaciones que adquiere la Entidad.
18. **DEVUELVE:** Corresponde a quién se le devuelve la cuenta para las correcciones a las que haya lugar.
19. **FECHA:** Fecha en la que es devuelta la cuenta para ser corregida.
20. **NUMERO DE FOLIOS:** Corresponde a la cantidad de paginas que contiene el documento.
21. **TRAMITE EN LAS AREAS:** Se deben diligenciar cada uno de los cuadros y conceptos correspondientes a las diferentes áreas que pasa la factura con los documentos soportes hasta su pago, indicando mes, día, hora y firma del funcionario responsable de cada acción.
22. **TRAMITE ORDEN DE PAGO No.:** Documento que se origina para la cancelación de la obligación y/o compromiso a cancelar.
23. **FIRMAS:** Corresponde a la aprobación del responsable.
24. **TRAMITE CHEQUE.:** Documento que se origina para ser entregado al proveedor o contratista dando cumplimiento al pago del compromiso u obligación que se está tramitando.
25. **OBSERVACIONES AREAS:** Anotaciones que se consideren pertinentes.

ANEXO No.3 - Solicitud de CDP y CRP para pago de Servicios Públicos, Administración y Celulares.

	SOLICITUD DE CDP Y CRP PARA PAGO DE SERVICIOS PÚBLICOS, ADMINISTRACIÓN Y CELULARES	Código formato: PGAF-06-03 Versión: 7.0
		Código documento: PGAF-06 Versión: 7.0
		Página: 1 de 1
1. CODIGO: _____		
2. PARA: _____		
3. DE: _____		
4. ASUNTO: _____		
Cordialmente me permito solicitarle, se sirva expedir Certificado de Disponibilidad y Registro Presupuestal, para amparar los gastos por conceptos de:		
5. Servicio: _____		
6. Factura: _____		
7. Empresa: _____		
8. Nit: _____		
9. Dirección _____		
10. Teléfono: _____		
11. Valor _____		
12. Periodo: _____		
13. Detalle: _____		

Atentamente;		

14. Ordenador del Gasto		

15. VoBo.		

16. Revisó		

17. Elaboró: _____		

**INSTRUCCIONES DE DILIGENCIAMIENTO FORMATO
ANEXO No.3 - SOLICITUD DE CDP Y CRP PARA PAGO DE SERVICIOS PUBLICOS,
ADMINISTRACIÓN Y CELULARES CONTRALORIA DE BOGOTA D.C.**

Casilla	Descripción
1	CÓDIGO: Se coloca el código de la Dirección Administrativa
2	PARA: A quién va dirigido el oficio "cargo del Subdirector Financiero"
3	DE: Cargo del Ordenador del gasto. (Funcionario designado por el Contralor para ejercer la ordenación del gasto y la competencia para la celebración, adjudicación y suscripción de los contratos, comodatos, convenios etc. En cualquier cuantía que se requieran contra el presupuesto de la Contraloría)
4	ASUNTO: Se coloca el objeto del oficio
5	SERVICIO: Nombre del servicio público correspondiente.
6	FACTURA: Número de la factura a pagar
7	EMPRESA: Nombre de la empresa a la que se le va a realizar el pago.
8	NIT: Nit de la empresa a la que se le va a realizar el pago.
9	DIRECCIÓN: Dirección de la empresa.
10	TELÉFONO: Teléfono de la empresa.
11	VALOR: Valor total del recibo del servicio público.
12	PERIODO: Se coloca el día, mes del inicio y el día, mes y año donde termina el cobro del servicio público.
13	DETALLE: Descripción del lugar al que corresponde el servicio
14	ORDENADOR DEL GASTO: nombre y firma del funcionario (Funcionario designado por el Contralor para ejercer la ordenación del gasto y la competencia para la celebración, adjudicación y suscripción de los contratos, comodatos, convenios etc. En cualquier cuantía que se requieran contra el presupuesto de la Contraloría).
15	VO.BO.: Firma del Subdirector de Servicios Generales o quién haya recibido el servicio.
16	REVISOR: Funcionario responsable de la supervisión del consumo y/o servicio
17	ELABORÓ: Responsable de central de cuentas y/o secretaria de la Subdirección Financiera.

7. CONTROL DE CAMBIOS:

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
1.0	R.R. No. 046 22 diciembre 2005	Ver link normatividad.
2.0	R.R. No.035 mayo 2009	Ver link normatividad.
3.0	R.R. No.021 12 octubre 2012	Ver link normatividad.
4.0	R. R. No.051 20 noviembre 2013	Ver link normatividad.
5.0	R.R No.005 31 enero 2017	El procedimiento cambia de versión, dado que mediante memorando No. 3-2017-16522 de junio 27 del 2017, la Alta Dirección comunicó la actualización de la Estructura del Mapa de Procesos de la Entidad y estableció la necesidad de ajustar todos los documentos del Sistema Integrado de Gestión – SIG a este nuevo esquema, generadas por el Acuerdo No. 658 de 2016, modificado parcialmente por el Acuerdo 664 de 2017 y a los cambios surtidos en las normas ISO 9001:2015, ISO 14001:2015, Decreto 1072 de 2015 y demás normas reglamentarias. Adicionalmente, se ajustó con las observaciones de la Auditoría Interna de Calidad y al Plan de Mejoramiento suscrito, así como algunas actividades de las personas que interviene en el procedimiento, especialmente las relacionadas con el supervisor del contrato; control de la información documentada, como es el caso del control de los registros, teniendo en cuenta que los originales de factura y comprobante de egreso reposaran en la tesorería de la entidad, además se suprime la entrega de documentos a la Subdirección de Recursos Materiales, teniendo en cuenta que serán remitidos a la Subdirección de Contratación. Se actualizó el formato del anexo No. 1 con los documentos que se deben verificar en la recepción de cuentas de cobro y/o causación contable en la Subdirección Financiera y se suprime la exigencia de algunos soportes los cuales serán consultados en el SECOP. Se ajustó teniendo en cuenta la estructura definida en el Procedimiento para mantener la información documentada del Sistema Integrado de Gestión – SIG, versión 11.0.
6.0	R.R. No. 042 28-dic-2017	En el OBJETIVO del procedimiento se incluyeron los viáticos y los avances.

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
		Se incluyeron los alcances de cada uno de los procedimientos. En el numeral 4 DEFINICIONES, Se elimina el libro radicador, se modifica la definición de recibido a satisfacción y se incluyen las definiciones de SECOP I y SECOP II. En el procedimiento PAGO A CONTRATISTAS Y PROVEEDORES se modifica la actividad, el punto de control y la observación de la actividad numero uno; se modifica la actividad numero 2 en el punto de control; se modifica la actividad numero 3 en la actividad y el punto de control; se modifica la actividad numero 4, se suprime CDP y CRP de los registros y se incluyen nuevas actividades 5, 6 y 7. En el procedimiento PAGOS DE SERVICIOS PÚBLICOS, DE ADMINISTRACIÓN Y TELEFONIA CELULAR en el numeral 5 renumerar con el numero 1 y modificar la actividad; incluir una nueva actividad como actividad numero 2; renumerar la actividad 6 con el numero 3, renumerar la actividad 7 con el numero 4 y modificar el punto de control, en el numeral 8 renumerar con el numero 5; en el numeral 9 renumerar con el numero 6, modificar el responsable, la actividad y el punto de control; incluir una nueva actividad numero 7. En el procedimiento PAGOS DE NOMINA renumerar la actividad 10 con el numero 1 y modificar la actividad; renumerar la actividad 11 con el numero 2 y modificar la actividad; incluir nuevas actividades 3, 4 y 5 y elimina la actividad numero 12 En el procedimiento PAGOS DE APORTES EN SALUD, PENSIONES, RIESGOS PROFESIONALES Y APORTES PARAFISCALES, se renumeran las actividades 13 y 14 con los números 1 y 2; la actividad 15 se renumera con el numero 3 y se modifica el registro; se suprime la actividad 16, se incluyen las actividades 4, 5 y 6. Se mantienen los anexos 1, 2 y 3. Se modifica el control de cambios.
7.0	R.R. 040 25-spt-2019	

Resolución Reglamentaria

Número 041

(Septiembre 25 de 2019)

“Por la cual se modifica el numeral 1 del artículo primero de la Resolución Reglamentaria No. 021 del 31 de mayo de 2019”

EL CONTRALOR DE BOGOTÁ, D.C.
En ejercicio de sus atribuciones y facultades constitucionales y legales, especialmente las conferidas por el artículo 9 de la Ley 489 de 1998 y el Acuerdo 658 de 2016, modificado por el Acuerdo 664 de 2017, expedido por el Concejo de Bogotá D.C. y,

CONSIDERANDO:

Que el artículo 211 de la Constitución Política consagra la figura de la delegación como mecanismo para que las diferentes autoridades administrativas puedan distribuir, de acuerdo con la ley, las funciones que les han sido asignadas.

Que el artículo 9 de la Ley 489 de 1998, faculta a las autoridades administrativas del orden nacional, transferir el ejercicio de sus funciones, mediante acto de delegación a sus colaboradores de los niveles directivo y asesor, de conformidad con establecido en la Constitución Política y la Ley.

Que el parágrafo del artículo 2 ibídem, dispone que las reglas relativas a los principios propios de la función administrativa sobre delegación se aplicarán a las entidades territoriales, sin perjuicio de la autonomía que les es propia, de acuerdo con la Constitución Política.

Que el artículo 6 del Acuerdo Distrital 658 de 2016 expresa: **“Autonomía administrativa. En ejercicio de su autonomía administrativa le corresponde a la Contraloría de Bogotá, D.C., definir todos los aspectos relacionados con el cumplimiento de sus funciones en armonía con los principios consagrados en la Constitución, las leyes y en este Acuerdo”.**

Que el artículo 21 del Acuerdo Distrital 658 de 2016 determina la facultad de delegación dentro de las reglas generales de funcionamiento de la Contraloría de Bogotá, D.C.: **“Facultades de delegación. Contralor de Bogotá, D.C. mediante acto administrativo, podrá delegar las facultades de ejecución presupuestal, ordenación del gasto, contratación y otras competencias administrativas, técnicas o jurídicas, en los términos de los actos de delegación y de lo dispuesto en el presente Acuerdo. Esta delegación podrá recaer en los servidores públicos de los niveles directivo y asesor de la Contraloría de Bogotá, D.C. (...)”**

Que el artículo 52 del Acuerdo 658 de 2016, determina las funciones a cargo de la Dirección Administrativa y Financiera, dentro de las que se destacan las siguientes:

“(…)”

3. *Dirigir las políticas, planes, programas y demás acciones relacionadas con la gestión presupuestal, contable y de tesorería de la Contraloría de Bogotá, D.C.*

4. *Dirigir la elaboración del Programa Anual de Compras y de Contratación para aprobación de las instancias competentes y efectuar seguimiento permanente al cumplimiento de los mismos.*

“(…)”

8. *Hacer seguimiento a la correcta ejecución, contabilización y rendición de informes y cuentas fiscales, presupuestales y contables, de los recursos asignados a la Contraloría de Bogotá, D.C.*

“(…)”

14. *Las demás funciones asignadas que correspondan a la naturaleza de la dependencia.”*

Que el artículo primero de la Resolución Reglamentaria No. 021 del 21 de mayo de 2019 delega en el Director Técnico de Talento Humano algunas funciones relacionadas con la administración de personal de la Contraloría de Bogotá D.C., afines y complementarias a las enunciadas en el artículo 57 del Acuerdo 658 de 2016, modificado por el artículo 19 del Acuerdo 664 de 2017.

Que de conformidad con las disposiciones precitadas y teniendo en cuenta que en virtud de las funciones asignadas a la Dirección Administrativa y Financiera por el artículo 52 del Acuerdo 658 de 2016 se expidió la Resolución Reglamentaria No. 028 del 6 de septiembre de 2017, a través de la cual se adoptó el Procedimiento de Avances y Comisiones, es pertinente mantener a cargo del titular de dicha dependencia, y de manera excluyente, la ordenación de los viáticos y gastos de viaje que se originen en las comisiones concedidas a los servidores públicos de la Entidad.

Que como consecuencia de ello, se hace necesario modificar el numeral 1 del artículo primero de la Resolución Reglamentaria No. 021 del 31 de mayo de 2019 **“Por la cual se delegan algunas funciones en materia de administración de personal en el Director Técnico de Talento Humano de la Contraloría de Bogotá, D.C.”**, en orden a delegarle exclusivamente las funciones relacionadas con la administración de personal de la Entidad, en consonancia con lo señalado en el artículo 19 del Acuerdo 664 de 2017.

Que en mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO: **Modificar** el numeral 1 del artículo primero de la Resolución Reglamentaria No. 021 del 31 de mayo de 2019, el cual quedará así:

“1. Suscribir los actos administrativos que concedan o nieguen las comisiones de servicio, de estudios y para desempeñar empleos de libre nombramiento y remoción de los servidores públicos de la Contraloría de Bogotá, D.C., de acuerdo con la legislación vigente.”

ARTÍCULO SEGUNDO: Las demás disposiciones contenidas en la Resolución Reglamentaria No. 021 del 31 de mayo de 2019 se mantienen incólumes y por consiguiente conservan plenos efectos.

ARTÍCULO TERCERO: La presente resolución rige a partir de la fecha de su publicación.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los veinticinco (25) días del mes de septiembre de dos mil diecinueve (2019).

JUAN CARLOS GRANADOS BECERRA

Contralor de Bogotá, D.C.