CONTRALORÍA
DE BOGOTÁ, D.C.

**"Al rescate de la moral y la ética pública"**

# MANUAL DE POLÍTICAS PARA LA CONTRALORÍA DE BOGOTÁ, D.C.

## TABLA DE CONTENIDO

# INTRODUCCIÓN

El presente manual contiene las guías generales de acción enfocadas a diferentes aspectos que deben ser tenidos en cuenta y los cuales permiten asegurar el cumplimiento de nuestra misión, la adecuada administración de los recursos, los mecanismos de divulgación de la información a los diferentes grupos de interés, entre otros aspectos.

Ha sido elaborado con la participación de todo el nivel directivo de la entidad; por consiguiente refleja el compromiso con el enfoque y desarrollo de una gestión caracterizada por la transparencia, eficacia, eficiencia y la clara orientación hacia el cumplimiento de la misión institucional así como de los fines esenciales del estado.

Las Políticas documentadas en este manual pretenden lograr una mayor armonización con la política institucional "Fortalecer la ética pública y la moralidad administrativa, como fundamentos del accionar institucional" y ser un instrumento de consulta en forma permanente.

# ALCANCE

De conformidad con la estructura establecida en el Modelo Estándar de Control Interno el presente manual abarca las políticas relacionadas con los siguientes elementos: Desarrollo del Talento Humano, Estilo de Dirección, Políticas de Operación, Información primaria, Información secundaria, Sistemas de Información, Comunicación interna y medios de comunicación. Lo anterior como complemento a las políticas Institucional, de calidad y de Administración del riesgo determinadas en el plan estratégico

Las políticas definidas en este manual deben ser cumplidas por todo el nivel directivo y demás funcionarios de la entidad.

# 1. POLÍTICAS

## *1.1. INSTITUCIONAL*

Fortalecer la ética pública y la moralidad administrativa, como fundamentos del accionar institucional.

## *1.2. DE CALIDAD*

Mejorar el Sistema de Gestión de la Calidad, para obtener productos de calidad, oportunidad y de impacto en la ciudad.

## *1.3. ADMINISTRACIÓN DEL RIESGO*

Establecer la administración del riesgo como un compromiso de todos, garantizando el cumplimiento eficiente de la misión institucional.

## *1.4. ESTILO DE DIRECCIÓN*

El Contralor y su equipo de trabajo se comprometen a responder al mandato ciudadano de defensa de los intereses públicos y la moralidad administrativa en cumplimiento de los fines del Estado.

Las decisiones institucionales y el liderazgo ejercido por el nivel directivo, estarán orientadas por las normas constitucionales y legales vigentes y el protocolo ético de la entidad.

## *1.5. DESARROLLO DEL TALENTO HUMANO*

Garantizar el desarrollo de los programas y procedimientos del proceso de gestión de talento humano, con fundamento en las normas constitucionales y legales vigentes y el protocolo ético de la entidad.

Administrar el recurso humano, promoviendo el respeto de los derechos y el cumplimiento de los deberes de los servidores públicos de la Contraloría de Bogotá.

La operación del proceso se orientará a mejorar la capacidad de transformar permanentemente el capital humano y a gestionar conocimiento para crecer individual e institucionalmente en función de los objetivos estratégicos de la entidad.

### *1.6. OPERACIÓN POR PROCESO*

Las políticas de operación por proceso han sido incorporadas en el Manual de Calidad.

### *1.7. MANEJO DE INFORMACIÓN*

#### *1.7.1. INFORMACION PRIMARIA*

Definir los parámetros y términos para la presentación de la cuenta que deben rendir los sujetos de control a la entidad, así como los requerimientos para la rendición electrónica de cuentas a través del aplicativo SIVICOF, las cuales se determinan en resoluciones reglamentarias que son comunicadas a los interesados y se incorporan en la página WEB institucional.

Constituir espacios de participación ciudadana con el objeto que los grupos plurales de veedurías locales y demás organizaciones ciudadanas que ejercen vigilancia y seguimiento a la gestión de la administración distrital en el ámbito local, se articulen y coordinen para la programación y realización de actividades y acciones de control y auditoria social, a través de los respectivos procedimientos.

Recepcionar, atender y administrar de manera oportuna y eficiente las denuncias, peticiones, quejas y reclamos presentadas de manera verbal, escrita o a través de la página web, de acuerdo con los procedimientos establecidos y haciendo uso de las herramientas tecnológicas dispuestas para ello.

Recepcionar y tramitar las comunicaciones oficiales externas de conformidad con lo establecido en el procedimiento respectivo y haciendo uso de la herramienta tecnológica dispuesta para ello.

### *1.7.2. INFORMACIÓN SECUNDARIA*

Colocar a disposición de la ciudadanía los diferentes informes elaborados producto del desarrollo del ejercicio de control fiscal micro y macro, así como los informes de gestión que permitan reflejar los resultados obtenidos frente a lo programado, a través de la página web de la entidad.

Efectuar las rendiciones de cuentas a la ciudadanía a través de las cuales se informa acerca del cumplimiento de los objetivos y estrategias enmarcados en el plan estratégico de la entidad.

### *1.7.3. POLÍTICA DE SEGURIDAD INFORMÁTICA*

La CB, debe hacer uso de las mejores prácticas en materia de seguridad informática, como herramienta básica para garantizar la confidencialidad, integridad y disponibilidad de la información como soporte de continuidad operacional de la entidad llegado el momento.

**Alcance**

La política de seguridad informática es de aplicación por parte de funcionarios, contratistas, estudiantes en práctica, supernumerarios y en general cualquier persona o entidad que de una u otra forma tenga que ver con el uso de recursos o información suministrados por la CB para el normal desarrollo de sus actividades.

La Dirección de Informática, como dependencia encargada del manejo y administración de los recursos computacionales de la entidad, velará por el estricto cumplimiento de las directrices emanadas del presente documento.

**Objetivos**

- Garantizar que la información de la CB, conserve su confidencialidad, integridad y disponibilidad, sin importar el medio de almacenamiento en el que se encuentre.

- Promover en la CB, el adecuado uso de los recursos de hardware y software como elementos indispensables para el tratamiento y procesamiento de la información.

- Crear en la CB, una cultura de ética y responsabilidad al interior de la organización enfocada hacia la aplicación de la política de seguridad de la información por parte de los servidores públicos, contratistas, estudiantes en práctica, etc.

**Descripción de las políticas**

**Política de seguridad**

a. Proporcionar recursos suficientes para la aplicación de los controles necesarios tendientes a brindar el adecuado aseguramiento de los activos informáticos de la entidad.

b. Los recursos de red, hardware, software y similares con que cuenta la entidad serán de uso exclusivo para la realización de actividades de carácter institucional.

c. La cultura del buen manejo de los recursos informáticos deberá ser una premisa exaltada dentro de las actividades que a diario se realizan en la entidad. Es deber de la CB, emplear mecanismos de difusión y divulgación que pongan de manifiesto la importancia del conocimiento y aplicación de las políticas de seguridad.

d. El tema de seguridad de la información y el aseguramiento de los recursos informáticos debe estar apoyado y correlacionado con la parte normativa y procedimental vigente para tal fin.

**Seguridad organizacional**

a. Contar con un grupo de funcionarios de alto nivel, encargado de la creación, revisión y aprobación de las políticas de seguridad de la información. Será función adicional establecer las responsabilidades sobre la protección de cada uno de los activos informáticos de la entidad y coordinar la divulgación, aplicación y cumplimiento de las políticas por parte funcionarios, contratistas, estudiantes en práctica y demás personas o entes externos que tengan acceso a los recursos de información de la entidad.

b. Buscar apoyo en otras entidades u organizaciones externas de ser necesario, sobre temas de cooperación o asesoramiento especializado en temas de seguridad de la información.

**Clasificación y control de activos**

a. Realizar de manera periódica un inventario de los activos informáticos con que cuenta la CB, de tal forma, que puedan emplearse criterios de clasificación de acuerdo con su nivel de importancia, para así establecer los controles necesarios a la hora de otorgar o denegar el acceso a los mismos.

b. Cada activo informático que haya sido inventariado y clasificado deberá contar con un propietario o responsable quien será el encargado de participar en la definición de los controles de seguridad aplicables, responder por el adecuado uso del recurso y monitorear la efectiva aplicación de la política de seguridad asignada.

**Seguridad del Talento Humano**

a. Contar con un procedimiento de selección de personal que permita la verificación y corroboración de la identidad, referencias personales y profesionales, certificaciones, y demás documentación suministrada a la hora de realizarse los trámites de incorporación de nuevos funcionarios.

b. Establecer un acuerdo de confidencialidad entre la entidad y los funcionarios, contratistas, estudiantes en práctica y demás personas o entes externos que tengan acceso a los recursos informáticos durante, e incluso, después de terminado cualquier tipo de vinculación. El acuerdo debe estar enmarcado dentro de los parámetros del compromiso que se debe tener en materia de seguridad informática.

c. Contar con programas de capacitación y divulgación de las políticas de seguridad informática, así como también de los procedimientos específicos de seguridad aplicables a cada área en particular. Se debe entrenar a los funcionarios en el uso de aplicativos y sistemas que de acuerdo con sus cargos deben utilizar, enfatizando siempre, en la responsabilidad de dar adecuada aplicación de las políticas de seguridad.

d. Reportar por parte de los funcionarios de la entidad al personal encargado de la seguridad informática sobre cualquier incidente, amenaza, violación, debilidad o malfuncionamiento que atente contra

cualquiera de los activos de información de la Contraloría de Bogotá, D.C.

**Gestión de la continuidad del negocio**

a. Garantizar la continuidad del negocio es una actividad que deberá estar enfocada hacia el establecimiento, en el menor tiempo posible, de las operaciones normales de la entidad en caso de presentarse una catástrofe que impida el acceso parcial o total a los sistemas de información.

b. Contar con un plan de contingencia y continuidad teniendo en cuenta el impacto y criticidad de cada sistema de información para la organización. Dicho plan deberá estar soportado en pruebas y/o simulacros periódicos que permitan medir su efectividad.

**Gestión de comunicaciones y operaciones**

a. La gestión de operaciones deberá estar encaminada hacia la estructuración de procedimientos y responsabilidades propios del manejo de los recursos informáticos. Deberán ser de pleno conocimiento por parte de todos los funcionarios encargados, guardando niveles adecuados de segregación de funciones, estableciendo mecanismos de control y seguimiento de cambios y un apropiado tratamiento de incidentes en materia de seguridad de la información.

b. Garantizar la correcta y segura operación de servidores de aplicaciones, bases de datos y demás servicios sensibles para la organización, basados en una correcta planificación de los sistemas requeridos, en una definición adecuada de reglas de protección contra virus y software malicioso, en un apropiado nivel de mantenimiento de la plataforma informática, en una eficiente administración de los recursos de red y en el riguroso cuidado de los medios de almacenamiento de datos, bien sea, físicos o electrónicos.

**Control de acceso**

a. Contar con procedimientos de control establecidos para el acceso a los diferentes recursos informáticos, tales como aplicaciones, redes, sistemas operativos, correo electrónico, Internet, áreas específicas

de la entidad y en general cualquier fuente de información sensible en materia de seguridad.

b. El acceso a las diferentes fuentes de información deberá estar ligado a privilegios o roles de usuario que establezcan lo que puede y no puede hacer un funcionario dentro de los diferentes sistemas. Es importante definir controles de seguimiento y monitoreo de las actividades que los mismos realizan con el fin de detectar de manera anticipada posibles inconvenientes de seguridad. El uso adecuado de las credenciales de acceso y de las herramientas que se proporcionan son de exclusiva responsabilidad de los funcionarios y/o terceros que las utilizan.

**Adquisición, desarrollo y mantenimiento de sistemas**

a. Contar con los mecanismos necesarios que permitan verificar que dentro de los procesos de análisis, diseño, desarrollo e implementación de software, así como de adquisición de aplicaciones a terceros, sean tenidos en cuenta aspectos de seguridad como validación de usuarios, validación de datos de entrada/salida, controles de procesamiento, controles criptográficos, firmas digitales, cambios en el software y en general controles que garanticen la integridad de la información procesada.

**Gestión de incidentes**

a. La gestión de incidentes en materia de seguridad para la CB, deberá estar encaminada hacia el tratamiento de los eventos que afecten directa o indirectamente la confidencialidad, disponibilidad e integridad de la información en la entidad. Se contará con mecanismos que permitan evaluar el impacto sobre el desarrollo normal de las actividades institucionales producto de la vulneración de alguna de las políticas de seguridad, se ejecutarán procedimientos específicos para el tratamiento de los incidentes y se revisarán y ajustarán aquellos procesos afectados, con el ánimo de evitar que se repitan los sucesos.

**Seguridad física y del entorno**

a. Contar con las medidas necesarias tendientes a proteger el entorno físico donde se mantienen los equipos de procesamiento de la información. Deberán establecerse controles que impidan accesos no

autorizados, mecanismos de validación de identificación, implementación de sistemas de soporte de energía, sistemas de detección y extinción de incendios, sistemas de aire acondicionado, y en general, todas aquellas medidas que tengan como fin proteger el perímetro o área sensible donde se encuentren los valores informáticos.

b. El acceso a los puntos de almacenamiento o procesamiento de información por parte de terceros deberá contar medidas especiales de seguridad tales como: autorización previa, registro de acceso (entrada/salida) y supervisión y verificación permanente.

**Seguridad legal**

a. Dentro del esquema de gestión de seguridad de la información, la CB deberá garantizar el cumplimiento de la reglamentación legal vigente a nivel de propiedad intelectual, licenciamiento de software, control de software no autorizado, tiempos de retención documental, privacidad de la información personal, uso indebido de las plataformas de procesamiento, derechos de uso de tecnología criptográfica y recolección de evidencias de incidentes de seguridad.

b. Verificar de forma periódica que los controles y medidas adoptadas a nivel de seguridad de la información correspondan o estén acordes con los diferentes ambientes y/o plataformas tecnológicas con que se cuente.

## *1.8. COMUNICACIÓN*

### *1.8.1. COMUNICACIÓN INTERNA*

Efectuar la comunicación al interior de la entidad por tres medios: escrito (a través de memorandos o circulares), retroalimentación en mesas de trabajo y a través de medios electrónicos.

Determinar los parámetros a tener en cuenta en las comunicaciones por medio de memorandos o circulares en el procedimiento para la recepción y entrega de comunicaciones oficiales internas.

Utilizar el sistema de correo electrónico únicamente para la transmisión de información relacionada con asuntos laborales del usuario y/o asuntos de

interés común que incidan en la buena marcha y en el mejoramiento de la armonía laboral de la entidad.

Mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones.

Evitar el uso inapropiado del correo electrónico: Intentos de acceso y/o accesos no autorizados a otra cuenta de correo, intentos de acceso y/o accesos no autorizados a carpetas, transmisión de mensajes de correo con información sensible o confidencial a personas u organizaciones externas sin autorización, cadenas de mensajes que congestionen la red, transmisión de mensajes obscenos y cualquier actividad no ética que afecte a la organización.

Acoger los demás *parámetros establecidos en el modelo de seguridad informática que implemente la CB*, en relación con la *información que se maneje y transmita por medios electrónicos.*

### *1.8.2. MEDIOS DE COMUNICACIÓN*

Brindar información integral, oportuna, completa, actualizada, clara, veraz y confiable a los diferentes grupos de interés a través de los medios de comunicación tales como: radio, prensa, televisión, *Noticontrol*, página web, para lo cual desarrollará y cumplirá lo establecido en el procedimiento para la divulgación de información institucional.

Dar a conocer a través de los medios formales de la entidad (radio, prensa, televisión, carteleras, boletines informativos, etc.), información veraz y oportuna, la cual debe contar con la autorización del Contralor y /o el Jefe de la Oficina Asesora de Comunicaciones, según sea el caso.

Utilizar la página web únicamente para propósitos institucionales y legales, por tanto, se publicarán temas y actividades relacionadas con la misión, visión y objetivos y las consiguientes funciones correspondientes al objeto social.

Acatar en su totalidad los términos y condiciones establecidos para el uso de la página web.