Resolución 305 de 2008 Secretaría General Alcaldía Mayor de Bogotá D.C. - Comisión Distrital de Sistemas - CDS	
Fecha de Expedición:	20/10/2008
Fecha de Entrada en Vigencia:	
Medio de Publicación:	

Ver temas del documento

Contenido del Documento

RESOLUCIÓN 305 DE 2008

(Octubre 20)

«Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y *Software* Libre»

LA COMISIÓN DISTRITAL DE SISTEMAS (CDS) DE BOGOTÁ, D. C.

en ejercicio de las facultades legales y en especial de las conferidas en los Decretos Distritales 680 de 2001 y 397 de 2002 y la Resolución 256 de 2008 de la Comisión Distrital de Sistemas (CDS) y,

CONSIDERANDO:

Que el Honorable Concejo de Bogotá mediante el Acuerdo Distrital 20 de 1989 (parágrafo 3.º del artículo 18) facultó al Alcalde Mayor para reglamentar la Comisión Distrital de Sistemas, como órgano rector de políticas de sistematización que deben ser adoptadas por las entidades, organismos y órganos de control del Distrito Capital.

Que en tal sentido el Alcalde Mayor expidió el Decreto Distrital 443 de 1990 para establecer la composición, funciones, adscripción y operatividad de la Comisión, el cual se actualizó mediante el Decreto Distrital 680 de 2001.

Que el Acuerdo Distrital 57 de 2002 del Concejo de Bogotá determinó que la Comisión Distrital de Sistemas (CDS) es el organismo rector de las políticas y estrategias que a nivel de Tecnologías de la información y de las comunicaciones, deben adoptar las entidades, los organismos y los órganos de

control del Distrito Capital, para el diseño e implementación del Sistema Distrital de Información (SDI).

Que mediante el Decreto Distrital 397 de 2002, el Alcalde Mayor delegó en el Secretario General de la Alcaldía Mayor de Bogotá, las atribuciones a él conferidas en el Acuerdo Distrital 57 de 2002 como Presidente de la Comisión Distrital de Sistemas, así como las demás funciones que se requieran en este ejercicio.

Que el artículo 5.º del Acuerdo Distrital 257 de 2006, por el cual se realizó la reforma administrativa del Distrito Capital, prevé que en desarrollo de los principios de *Moralidad, Transparencia y Publicidad (...) Las actuaciones administrativas serán públicas, soportadas en tecnologías de información y comunicación, de manera que el acceso a la información oportuna y confiable facilite el ejercicio efectivo de los derechos constitucionales y legales y los controles ciudadano, político, fiscal, disciplinario y de gestión o administrativo, sin perjuicio de las reservas legales.*

Que el artículo 2.° del Acuerdo Distrital 57 de 2002 señala que el Sistema Distrital de Información (SDI) se establece como herramienta fundamental para facilitar a la Administración Distrital el ejercicio de su función, de una manera efectiva y ágil, procurando la consolidación de un *Gobierno Electrónico*.

Que mediante los Decretos Distritales 619 de 2007, 296 y 316 de 2008, se asignaron las funciones relacionadas con el Comité de Gobierno en Línea a la Comisión Distrital de Sistemas, consistentes en adoptar, estructurar, consolidar, coordinar, orientar, divulgar y realizar el seguimiento de la Estrategia Distrital de Gobierno Electrónico, que permita coordinar a todas las entidades, organismos y órganos de control del Distrito Capital que conforman la administración distrital, y que utilicen las Tecnologías de Información y Comunicaciones (TIC) para el uso de mensajes de datos en las actuaciones, actos y procedimientos administrativos, para que gestionen eficazmente su información y provean servicios y trámites enfocados a las necesidades y demandas ciudadanas.

Que la anterior estrategia propenderá por la reducción de los costos de trámites, procesos y procedimientos, para los administrados y la Administración Pública, así como por la consecución de objetivos de desarrollo social, fortalecimiento institucional, gobernabilidad y competitividad.

Que por medio del Decreto Nacional 1151 de 2008 se establecieron los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia y en desarrollo de este el Ministerio de Comunicaciones expidió el Manual para su implementación.

Que en aras de armonizar el Decreto Nacional 1151 de 2008, los Decretos Distritales 619 de 2007 y 316 de 2008, se le asignó mediante el Decreto Distrital 296 de 2008 a la Comisión Distrital de Sistemas, la función de coordinar la implementación de la Estrategia de Gobierno en Línea.

Que el Acuerdo Distrital 308 de 2008 por el cual se adoptó el Plan de Desarrollo Económico, Social, Ambiental y de Obras Públicas para Bogotá, D. C., 2008 – 2012, en su capítulo 6, artículo 27.2 establece el Programa de Ciudad Digital que busca consolidar la gobernabilidad electrónica y los servicios a la comunidad a través del uso articulado de las herramientas y recursos que ofrecen las Tecnologías de la Información y Comunicación (TIC).

Que mediante la Directiva 05 de 2005 expedida por el Alcalde Mayor, se establecieron las siguientes nueve políticas generales de Tecnologías de Información y Comunicaciones: Planeación de Informática, Estandarización, Seguridad y Control, Democratización de la Información, Marco Legal, Calidad, Racionalización del Gasto, Cultura Informática y Compatibilidad de Sistemas, las cuales son aplicables a las entidades, organismos y órganos de control del Distrito Capital.

Que se considera necesario desarrollar cinco de las nueve Políticas Generales expedidas por la Comisión Distrital de Sistemas, a través de Políticas Básicas, en las siguientes temáticas: Planeación de informática, Seguridad y Control, Democratización de la Información, Calidad y Racionalización del Gasto.

Que mediante la resoluciones 185 y 355 de 2007 la Comisión Distrital de Sistemas estableció dos políticas específicas de Tecnologías de Información y Comunicaciones (TIC) relacionadas con Conectividad e Infraestructura Integrada de Datos Espaciales.

Que la Comisión Distrital de Sistemas considera pertinente establecer una nueva política específica en materia de *Software* Libre.

Que es recomendable integrar en un solo acto administrativo las políticas específicas y las políticas básicas que se emiten, con el propósito de facilitar su consulta y aplicación.

Que de conformidad con lo dispuesto en la Resolución 256 de 2008, expedida por la Comisión Distrital de Sistemas (CDS), por la cual se establece el Reglamento Interno de la Comisión, esta será presidida por el Secretario General de la Alcaldía Mayor, y para el desarrollo de su objeto, la Comisión contará con grupos de trabajo.

Que para el cumplimiento de los objetivos y funciones, la Comisión se reúne en sesiones plenarias y mesas de trabajo, de acuerdo con los requerimientos de su Plan de Acción, y las decisiones que se adopten deben quedar en Actas suscritas por quien preside y por uno de sus miembros, nombrado de manera rotativa, previa aprobación por parte de los asistentes a la correspondiente sesión plenaria, mesa de trabajo o reunión de grupo.

Que de acuerdo con lo dispuesto en el artículo 8.º de la Resolución 256 de 2008 las decisiones proferidas por la Comisión Distrital de Sistemas se adoptan mediante *resoluciones*, suscritas por su Presidente y el Secretario Técnico.

Que conforme al artículo 10.º del Acuerdo Distrital 57 de 2002, las políticas, estrategias y recomendaciones de la Comisión Distrital de Sistemas son de obligatorio cumplimiento por parte de las entidades del Distrito Capital.

Que el proyecto de documento de «Políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de Información y Comunicaciones (TIC) respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y *Software* Libre»

emitidas por la Comisión Distrital de Sistemas fue sometido a consideración de sus miembros y aprobado, según consta en certificación del 7 de octubre de 2008 expedida por el Secretario Técnico de la Comisión.

En mérito de lo anterior,

RESUELVE:

TÍTULO I

SOBRE LAS POLÍTICAS BÁSICAS

CAPÍTULO PRIMERO

POLÍTICAS DE PLANEACIÓN DE INFORMÁTICA PARA LA FORMULACIÓN Y ELABORACIÓN DEL PLAN ESTRATÉGICO DE SISTEMAS DE INFORMACIÓN (PESI) EN EL DISTRITO CAPITAL.

ARTÍCULO 1. OBJETIVO DE LA PLANEACIÓN DE INFORMÁTICA. La política de Planeación de Informática busca, fundamentalmente, que las acciones relacionadas con la tecnología de la información y las comunicaciones, como son: la adquisición, contratación, desarrollo, implementación o utilización de nuevos sistemas o cambios tecnológicos, estén definidas y sean producto de un proceso detallado previo, que tienda al fortalecimiento de los esquemas de coordinación tecnológica de cada entidad u organismo distrital, y obedezcan a procesos continuos, ordenados, dinámicos y flexibles, con enfoque en el servicio a la comunidad y a la ciudadanía, y optimicen la toma de decisiones.

ARTÍCULO 2. PLAN ESTRATÉGICO DE SISTEMAS DE INFORMACIÓN (PESI). Es obligación de las entidades, organismos y órganos de control del Distrito Capital, definir,

ejecutar y actualizar su Plan Estratégico de Sistemas de Información (PESI), el cual debe estar dirigido hacia el soporte de los objetivos, planes, políticas y estrategias de cada ente público y debe servir para la racionalización del gasto y el seguimiento de las inversiones en Tecnologías de Información y Comunicaciones (TIC), además ser el insumo para el proceso de evaluación de cada proyecto de inversión que se inscriba y ejecute ante la Secretaría de Planeación Distrital, conforme con la Directiva 02 de 2002 del Alcalde Mayor.

PARÁGRAFO. El PESI debe ser definido por cada ente Distrital y estar actualizado anualmente en lo referente a diagnósticos, línea de base, dimensionamiento de la infraestructura tecnológica y avances en ejecución; ser avalado por la alta dirección de cada ente Distrital y enviado oportunamente al Presidente de la Comisión Distrital de Sistemas para su registro, revisión, seguimiento y coordinación interinstitucional.

ARTÍCULO 3. ALINEACIÓN DEL PESI. El Plan Estratégico de Sistemas de Información debe estar alineado con los planes de: Desarrollo del Distrito, con el institucional por entidad u organismo; con el de acción definido por la Comisión Distrital de Sistemas y con las Estrategias de Gobierno en Línea expedida por el Gobierno Nacional y de Gobierno Electrónico Distrital.

A fin de armonizar, articular, homogeneizar y robustecer el esquema de interoperabilidad para el Distrito y los sistemas de información de los diferentes entes distritales, se precisa que el "Plan Estratégico de Sistemas de Información (PESI)", de cada uno, debe ser elaborado con base en una metodología estándar, esto es, homogénea, consistente, articulada y documentada; que permita, de una parte, aumentar la eficacia en el uso de los datos y la información misional y administrativa; y de otra, optimizar la prestación de servicios y trámites tanto a los ciudadanos como a los usuarios internos de la Administración Distrital.

ARTÍCULO 4. DIRECTRICES E INSTRUMENTOS PARA LA IMPLEMENTACIÓN DEL PESI. De manera general se tendrá en cuenta en el desarrollo, detalle y elaboración de las directrices de implementación del PESI, en cada ente público distrital, lo siguiente: La pertinencia de los proyectos e inversión asociada; la sostenibilidad económica y funcional de los proyectos e infraestructura tecnológica asociada; la interoperabilidad de nuevos proyectos con infraestructura tecnológica existente y la inclusión de todos los costos asociados.

De forma particular, se tendrán en cuenta temas instrumentales como son: La migración de plataformas e información; guías de contenido y elaboración de planes; capacitación para áreas funcionales y técnicas en dichos procesos; generación de gastos recurrentes de mantenimiento y operación; definición de indicadores de gestión y resultados que permitan realizar el seguimiento.

ARTÍCULO 5. METODOLOGÍA DE PLANEACIÓN ESTRATÉGICA. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital, deben adoptar y aplicar las directrices generales establecidas en el documento denominado *"Metodología de Planeación Estratégica"*, el cual hace parte integral de la presente Resolución, incluyendo el instrumento denominado *"Modelo Plan Estratégico de Entidades"*. (Anexo 1).

ARTÍCULO 6. SEGUIMIENTO DE INDICADORES DE LA CDS. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital deben diligenciar los formatos que permiten realizar el seguimiento a los indicadores definidos por la Comisión Distrital de Sistemas para las entidades distritales. Los formatos debidamente diligenciados por los entes distritales, deben ser

consolidados por cada jefe de organismo cabeza de sector, quien por medio de la herramienta dispuesta por la CDS, los presentará al Presidente de la Comisión.

Para el efecto, la Comisión Distrital de Sistemas adelantará un programa de capacitación para ilustrar los indicadores definidos, así como sobre el uso de la herramienta que permite hacer el seguimiento a los mismos.

PARÁGRAFO. Las directrices y los instrumentos contenidos en el anexo citado de la presente Resolución serán difundidos, incorporados y acogidos al interior de cada ente del Distrito Capital.

ARTÍCULO 7. TÉRMINOS PARA LA PROMULGACIÓN DE LA POLÍTICA E INFORMES. Las políticas básicas de planeación de informática para la formulación y elaboración del *"Plan Estratégico de Sistemas de Información (PESI)"*, en todos las entidades, organismos y órganos de control del Distrito Capital, deben ser promulgadas por el Jefe al interior de cada ente, y ser difundidas y aplicadas por el responsable de área, grupo de trabajo e intervinientes en los procesos y procedimientos asociados con las Tecnologías de Información y Comunicaciones (TIC), dentro de los ciento veinte (120) días calendario siguientes a la expedición de esta Resolución, debiendo cada ente público enviar copia del documento adoptado del PESI, al Presidente de la Comisión Distrital de Sistemas para su consolidación y armonización.

De la misma forma cada entidad u organismo debe remitir el 30 de Junio de cada año un documento actualizado que consolide los cambios y ajustes implementados al Plan estratégico de Sistemas.

ARTÍCULO 8. RESPONSABLES DE LA IMPLEMENTACIÓN Y DIVULGACIÓN DEL PESI. Será responsabilidad del nivel directivo de los diferentes entes distritales, así como de los encargados de área e intervinientes en los procesos y procedimientos asociados con las Tecnologías de Información y Comunicaciones (TIC), garantizar la implementación, divulgación, aplicación y seguimiento de las políticas básicas de planeación de informática, en particular la prevista en esta Resolución.

CAPÍTULO SEGUNDO

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL DISTRITO CAPITAL.

ARTÍCULO 9. OBJETIVO. La utilización creciente de las Tecnologías de la Información y las Comunicaciones -TIC-, genera beneficios para las entidades, organismos y órganos de control del Distrito Capital, mejorando el cumplimiento de la misión y la prestación de servicios a la ciudadanía. Sin embargo, por ser la información el activo más importante de la organización, es necesario protegerla frente a los posibles riesgos derivados del uso de las nuevas tecnologías, para garantizar la seguridad de la información, en aspectos tales como disponibilidad, confiabilidad, accesibilidad e integridad de la misma, en los términos de la Directiva 05 de 2005 del Alcalde Mayor de Bogotá.

ARTÍCULO 10. DEFINICIONES.

10.1. Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

10.1.1. Confidencialidad: Aseguramiento de que la información es accesible sólo para quienes están autorizados.

10.1.2. Integridad: Salvaguardia de la exactitud y completitud de la información y sus métodos de procesamiento.

10.1.3. Disponibilidad: Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando se requiera.

10.2. Activos de información: Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

ARTÍCULO 11. MARCO LEGAL. Las entidades, organismos y órganos de control del Distrito Capital disponen de un marco de referencia de las mejores prácticas para el desarrollo e implementación del Sistema de Gestión de Seguridad de la Información, basados en las recomendaciones de las normas internacionales: NTC-ISO/IEC 27001 que establece los requisitos del Sistema de Gestión de Seguridad de la Información y la norma NTC/ISO IEC 17799 con su equivalente NTC-ISO/IEC 27002 que establece las mejores prácticas para la implementación del Sistema de Gestión de Seguridad de la Información y demás normas concordantes, las cuales son de obligatoria observancia por parte de los entes públicos distritales.

ARTÍCULO 12. LA INFORMACIÓN PATRIMONIO DISTRITAL. Los datos y la información utilizada por todos las entidades, organismos y órganos de control del Distrito Capital para su funcionamiento administrativo y el cumplimiento de sus funciones misionales, constituyen un patrimonio con valor económico que requiere las garantías administrativas y jurídicas para su conservación y ejercicio del derecho pleno de uso, por parte de la Administración Distrital, y en tal sentido, es un "bien público" de valor estratégico y patrimonial.

PARÁGRAFO. Es responsabilidad de las entidades, organismos y órganos de control del Distrito Capital gestionar los recursos tecnológicos y administrativos que permitan el manejo de los datos y la información, así como controlar el uso de dichos recursos por parte de los funcionarios y contratistas que las conforman.

ARTÍCULO 13. ALINEACIÓN DE SISTEMAS DE GESTIÓN. Las directrices y lineamientos definidos deben ser difundidos, incorporados y acogidos al interior de cada uno de las entidades, organismos y órganos de control del Distrito Capital, que junto con las normas

internacionales generalmente aceptadas, son la base para que se implemente el Sistema de Gestión de Seguridad de la Información (SGSI), el cual debe estar alineado con el Sistema Integrado de Gestión, en cada uno de sus componentes, esto es, los Sistemas de Gestión de Calidad, Control Interno, Desarrollo Administrativo y Gestión Ambiental.

ARTÍCULO 14. DEFINICIÓN DE POLÍTICA DE SEGURIDAD. Una política de seguridad es una regla de definición general, independiente de los ambientes tecnológicos y físicos, que representa los objetivos sobre los que se sustenta el Sistema de Gestión de Seguridad de los Activos de Información.

Se establecen las políticas sobre las cuales se debe direccionar el desarrollo futuro del Sistema de Gestión de Seguridad de la Información en el Distrito Capital, así como los principios de actuación de todo el personal que tenga acceso o responsabilidades sobre la información.

La política de seguridad es de obligatorio cumplimiento para todos los servidores públicos y particulares que accedan a la información del respectivo ente público, así como a los espacios físicos del mismo que conlleven un componente de seguridad de información.

ARTÍCULO 15. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD. La Comisión Distrital de Sistemas (CDS), con el fin de formalizar las políticas de seguridad de la información y los estándares planteados en las normas NTC-ISO/IEC 27001, que señala los requisitos del Sistema de Gestión de Seguridad de la Información y NTC/ISO IEC 17799 con su equivalente NTC-ISO/IEC 27002, que establece las mejores prácticas para la implementación del Sistema de Gestión de Seguridad de la Información, define los objetivos, alcances e importancia de la seguridad, como mecanismo para proteger la información y determinar las responsabilidades generales y específicas para la gestión de dicha seguridad, definir y adoptar los lineamientos a seguir para la implementación del Sistema de Gestión de Seguridad de la Información.

Este modelo contiene los procedimientos y estándares adecuados a la arquitectura de seguridad que incluye el aseguramiento de una plataforma tecnológica y los controles y administración de los activos que garanticen la seguridad de la información del organismo.

ARTÍCULO 16. POLÍTICAS DE SEGURIDAD. Las entidades, organismos y órganos de control del Distrito Capital deben adoptar políticas de seguridad y custodia de los datos y la información, y establecer los procedimientos para el adecuado uso y administración de los recursos informáticos de los cuales se valgan para cumplir con sus funciones administrativas, operativas y misionales.

ARTÍCULO 17. FORMULACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. Los proyectos que hagan uso de Tecnologías de Información y Comunicaciones (TIC) deben incluir, a lo largo de todas las fases de desarrollo e implantación, los mecanismos de seguridad y control necesarios que permitan garantizar la confiabilidad de la información que le es provista a los diferentes tipos de usuario.

ARTÍCULO 18. PLANES DE CONTINGENCIA. Los Jefes de las áreas de informática de las entidades, organismos y órganos de control del Distrito Capital deben formular "Planes de Contingencia" que garanticen la continuidad de las operaciones ante una situación crítica que pueda amenazar, parcial o totalmente, la prestación de servicios.

PARÁGRAFO 1º. El Plan de contingencia que se adopte debe ser formulado conforme a una metodología específica para tal fin, contemplar todos los tipos de riesgo posibles para la entidad, establecer el plan de manejo del riesgo y los planes de acción específicos en cada caso, ser avalado por la Alta Dirección, socializado en todos los niveles de la organización estableciendo las responsabilidades correspondientes y revisado periódicamente de acuerdo con el "Plan Estratégico de Sistemas de Información" y con cambios en las condiciones operativas de la entidad.

PARÁGRAFO 2º. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital deben estimular la creación de una Cultura de Seguridad de la información para garantizar la "adecuada implementación del Plan de Contingencia".

ARTÍCULO 19. ASPECTOS DE SEGURIDAD PARA LA IMPLEMENTACIÓN DE PROYECTOS. Las metodologías que se utilicen para el desarrollo e implantación de proyectos de Tecnologías de Información y Comunicaciones (TIC) deben considerar aspectos de seguridad y control que incluyan, entre otros: Acceso a la información, definición y autenticación de usuarios, mecanismos de detección de intrusos, definición de mecanismos de encriptación, administración de la información y su confidencialidad e integridad, administración de la seguridad física de la información.

ARTÍCULO 20. DIRECTRICES DE SEGURIDAD DE LOS DATOS Y LA INFORMACIÓN. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital para efectos de facilitar la Gestión de la Seguridad de la Información al interior de cada una de sus entidades y teniendo en cuenta las normas internacionales generalmente aceptadas, deben establecer un Comité de Seguridad de la Información así como la aplicación de los dominios de control a que se refiere la norma NTC-ISO/IEC 27001, que establece los requisitos del Sistema de Gestión de Seguridad de la Información y la norma NTC/ISO IEC 17799 con su equivalente NTC-ISO/IEC 27002 y demás normas concordantes.

ARTÍCULO 21. COMITÉS DE SEGURIDAD DE LA INFORMACIÓN (CSI). Las entidades, organismos y órganos de control del Distrito Capital dispondrán lo necesario para la creación del Comité de Seguridad de la Información (CSI) o una instancia semejante, que deben validar las Políticas de Seguridad de la Información, así como los procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los recursos informáticos y físicos, asignados a los servidores públicos de cada ente público.

PARÁGRAFO. El Comité de Seguridad de la Información (CSI) o una instancia semejante definida por las entidades, organismos y órganos de control del Distrito Capital, tiene como objetivo asegurar que exista una dirección y apoyo gerencial, para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

ARTÍCULO 22. DOMINIOS DE CONTROL. La norma NTC-ISO/IEC 27001 que establece los requisitos del Sistema de Gestión de Seguridad de la Información define los dominios de control, como una guía que permite garantizar la seguridad de la información, mediante el empleo de los 11 dominios de control.

Para cada dominio de control, se ha definido una política de seguridad.

DOMINIOS DE CONTROL	POLÍTICAS
1. Política de seguridad. Controles para proporcionar directivas y consejos de gestión para mejorar la seguridad de los activos de información.	Preservar la seguridad de los activos de información de cada organismo, para lo cual dispondrá de los recursos necesarios para garantizar el correcto desarrollo de los lineamientos planteados en cada política propuesta.
2. Organización de la Seguridad. Controles para facilitar la gestión de la seguridad de la información en el seno de la organización.	Garantizar que existan responsabilidades claramente asignadas en todos los niveles de la organización, para la gestión de la seguridad de los activos de información y contar con un Comité de Seguridad de la Información conformado por personal de alto nivel de cada una de las entidades, organismos y órganos de control del Distrito Capital que se apoyará en un asesor interno de seguridad. Todos los servidores públicos, contratistas y particulares que tengan acceso a los activos de información del organismo, tendrán el compromiso de cumplir las políticas y normas que se dicten en materia de seguridad de la información, así como reportar los incidentes que detecten. Con el objetivo de direccionar y hacer cumplir los lineamientos del organismo en cada materia y revisar las posibles incidencias y acciones que se deban tomar, el Comité de Seguridad de la Información y el Asesor Interno de Seguridad de la Información, designado por la Jefatura de Informática y Sistemas, podrán apoyarse con recursos externos, mejores prácticas, etc.
3. Gestión de Activos. Controles para catalogar los activos y protegerlos eficazmente.	Toda la información sensible de cada organismo, así como los activos donde ésta se almacena o procesa, deben ser inventariados, asignárseles un responsable y clasificarlos de acuerdo con los requerimientos en materia de seguridad de la información y los criterios que dicte el Comité de Seguridad de la Información del organismo. A partir de esta clasificación se deben establecer los niveles de protección orientados a determinar, a quién se le permite el manejo de la información, el nivel de acceso a la misma y los procedimientos para su manipulación. La clasificación debe revisarse periódicamente y atender a los cambios que se presenten en la información o la estructura que puedan afectarla.
4. Seguridad de los Recursos Humanos. Controles para reducir los riesgos de error humano, robo, fraude y utilización abusiva de los equipamientos.	Desde la vinculación del personal a la entidad u organismo público, se deben tener controles que permitan verificar la idoneidad e identidad, ética profesional y conducta. Los términos y condiciones de empleo o trabajo debe establecer la responsabilidad de los servidores públicos y contratistas, por la seguridad de los activos de información, que van más allá de la finalización de la relación laboral o contractual, por lo que se debe firmar un acuerdo de confidencialidad que se hace extensivo a los contratistas y terceros que tengan acceso a la información. Deben existir mecanismos de información y capacitación para los usuarios en materia

	de seguridad, así como de reporte de incidentes que puedan afectarla. Los servidores públicos deben cooperar con los esfuerzos por proteger la información y ser responsables de actualizarse en cada materia, así como consultar con el encargado de la seguridad de la información, en caso de duda o desconocimiento de un procedimiento formal, ya que esto no lo exonera de una acción disciplinaria que deba llevarse a cabo cuando se incurra en violaciones a las políticas o normas de seguridad.
5. Seguridad Física. Controles para impedir la violación, deterioro y la perturbación de las instalaciones y datos industriales.	Deben establecerse áreas seguras para la gestión, almacenamiento y procesamiento de información en el organismo o entidad pública; éstas deben contar con protecciones físicas y ambientales acordes a los activos que protegen, incluyendo perímetros de seguridad, controles de acceso físicos, controles especiales en áreas de mayor sensibilidad, seguridad de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales de operación y sistemas de contención, detección y extinción de incendios adecuados que preserven el medio ambiente. Esta seguridad debe mantenerse en los momentos de mantenimiento, cuando la información o los equipos que la contienen deben salir del organismo o cuando se deben eliminar o dar de baja, para lo cual deben existir procedimientos especiales.
6. Gestión de las Telecomunicaciones y Operaciones. Controles para garantizar un funcionamiento seguro y adecuado de los dispositivos de tratamiento de la información.	Deben documentarse los procedimientos y responsabilidades de administración y seguridad que sean necesarios en cada ambiente tecnológico y físico, garantizando un adecuado control de cambios y el seguimiento a estándares de seguridad que deben definirse, así como el seguimiento a los incidentes de seguridad que puedan presentarse. Debe buscarse una adecuada segregación de funciones. Deben garantizarse una adecuada planificación y aprobación de los sistemas de información que consideren o provean las necesidades de capacidad futura. Deben considerarse protecciones contra software malicioso y un adecuado mantenimiento y administración de la red, así como un adecuado cuidado de los medios de almacenamiento y seguridad en el intercambio de información.
7. Control de Acceso a los Datos. Medios para impedir accesos no autorizados y registro de los accesos efectuados.	Deben establecerse medidas de control de acceso a las dependencias de cada entidad u organismo y a los diferentes niveles de la plataforma tecnológica, tales como la red, sistema operativo y aplicaciones, así como a la información física que tenga un componente de seguridad. Estas medidas estarán soportadas en el desarrollo de la cultura de seguridad de las personas que laboran en el organismo y buscarán limitar y monitorear el acceso a los activos de información requeridos para el trabajo, de acuerdo con su clasificación y manejando controles, en dispositivos y servicios que permitan identificar los niveles de acceso que los usuarios deben tener. Los usuarios serán responsables de realizar un adecuado uso de las herramientas de seguridad que se ponen a su disposición.
8. Adquisición, Desarrollo y Mantenimiento de Software. Controles para garantizar que la Política de Seguridad esté incorporada a los sistemas de información.	Asegurar que se haga un adecuado análisis e implementación de los requerimientos de seguridad del software desde su diseño, ya sea interno o adquirido, que incluya garantías de validación de usuarios y datos de entrada y salida, así como de los procesos mismos, de acuerdo con la clasificación de los activos a gestionar en la herramienta. Además se establecerán controles para cifrar la información confidencial y se buscará evitar la posibilidad de una acción indebida por parte de un usuario del sistema. Igualmente, se deben asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan presentarse. La implantación de nuevas herramientas de Hardware y Software, de sistemas de información y de otros recursos informáticos, deben cumplir con las políticas definidas.
9. Gestión de Incidentes. Procedimiento a seguir en caso de ocurrencia de incidentes. Existe una clasificación de los incidentes según el grado en que afecten el normal	Asegurar que se haga una adecuada evaluación del impacto en el organismo frente a los eventos de seguridad relevantes, en los cuales las políticas de seguridad hayan sido desatendidas o traspasadas y realizar planes de atención de incidentes y mejora de procesos, para aquellos eventos que resulten críticos para la supervivencia del mismo. Estos planes deben considerar medidas técnicas, administrativas y de vínculo con

uncionamiento del negocio. Controles para gestionar las incidencias que afectan a la seguridad de la Información.	entidades externas; deben probarse y revisarse periódicamente; y deben estar articulados en todo el organismo con los diferentes tipos de recursos tecnológicos y no tecnológicos.
10. Continuidad del Negocio. Controles para reducir los efectos de las interrupciones de actividad y proteger los procesos esenciales de la empresa contra averías y siniestros mayores.	Se debe evaluar el impacto de los diferentes procesos en el organismo y realizar planes de mitigación y continuidad para aquellos que resulten críticos. Los planes de mitigación y continuidad deben considerar medidas tanto técnicas como administrativas y de vínculo con entidades externas; deben probarse y revisarse periódicamente, y deben permanecer articulados con los diferentes recursos tecnológicos y no tecnológicos existentes en todo el organismo.
11. Cumplimiento y Normatividad Legal. Controles para prevenir los incumplimientos de las leyes penales o civiles, de las obligaciones reglamentarias o contractuales y de las exigencias de seguridad.	Garantizar que la gestión de la seguridad dé cumplimiento adecuado a la legislación vigente para lo cual analizará los requisitos legales aplicables a la información que se gestiona incluyendo los derechos de propiedad intelectual, los tiempos de retención de registros, privacidad de la información, uso inadecuado de recursos de procesamiento de información, uso de criptografía y recolección de evidencias. Así mismo, debe garantizarse que el direccionamiento y los controles relacionados con la seguridad de la información se cumplan y sean compatibles técnicamente con los diferentes ambientes y tecnologías. Se debe garantizar la posibilidad de llevar a cabo auditorias, manteniendo los registros necesarios, para que éstas respondan adecuadamente a la disminución del riesgo de discontinuidad de cada tarea o servicio propio de cada entidad u organismo público distrital.

ARTÍCULO 23. RESPONSABLES DE LA PROMULGACIÓN, DIFUSIÓN E IMPLEMENTACIÓN DE LAS POLÍTICAS DE SEGURIDAD. Es deber del Comité de Seguridad de la Información (CSI), o una instancia semejante, de cada una de las entidades, organismos y órganos de control del Distrito Capital, promulgar las políticas básicas y específicas de seguridad de los datos y la información; procurando su difusión y aplicación por el área que éste designe, dentro de los ciento veinte (120) días calendario siguientes a la expedición de esta Resolución, debiendo enviar al Presidente de la Comisión Distrital de Sistemas copia de los documentos de políticas adoptadas por el respectivo ente público, para su consolidación y armonización. Así mismo, deben remitir semestralmente el 1º de junio y 1º de diciembre de cada año, un documento actualizado que consolide los cambios y ajustes implementados respecto a las políticas de seguridad.

PARÁGRAFO. Corresponde a los jefes de dependencia, responsables de área, grupo de trabajo e intervinientes en los procesos y procedimientos asociados con las Tecnologías de Información y Comunicaciones (TIC), garantizar la implementación, la divulgación, la aplicación y el seguimiento de las políticas básicas de seguridad de la información al interior del organismo o entidad.

ARTÍCULO 24. CAPACITACIÓN Y DIVULGACIÓN. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital deben propiciar la capacitación necesaria dirigida a sus servidores públicos y contratistas.

PARÁGRAFO. Corresponde a las Jefaturas de Informática y Sistemas de las entidades, organismos y órganos de control del Distrito Capital coordinar la divulgación de las políticas de seguridad establecidas al interior de cada ente público, para garantizar el conocimiento de los servidores públicos y contratistas, identificar los deberes, derechos e implicaciones por el uso indebido de los recursos de tecnología y comunicaciones, con el fin de que

apoyen y cumplan los preceptos, los cuales ayudan y redundan en beneficio y mejora de los niveles de seguridad de la información.

ARTÍCULO 25. PROCEDENCIA DE OTRAS POLÍTICAS. Mediante el presente capítulo se 0cubren los aspectos básicos que en primera instancia deben adoptar las entidades, organismos y órganos de control del Distrito Capital en materia de seguridad de la información, sin perjuicio de que con posterioridad se planeen y/o adopten otras fases, siempre que se soporten en la normatividad nacional e internacional vigente y tengan previa aprobación de la Comisión Distrital de Sistemas.

CAPÍTULO TERCERO

POLÍTICAS DE DEMOCRATIZACIÓN DE LA INFORMACIÓN, INTEROPERABILIDAD E INTERCAMBIO DE INFORMACIÓN HOMOGÉNEA A TRAVÉS DE SERVICIOS WEB EN EL DISTRITO CAPITAL

ARTÍCULO 26. OBJETIVO. Mediante el uso de la tecnología actual y futura, en los diferentes servicios de información y en especial con Internet, cada entidad u organismo debe disponer e implementar un esquema de interacción e intercambio de información, basado en Tecnologías de Información y Comunicaciones (TIC), que facilite el acceso de la Administración y del ciudadano, de una manera estándar, homogénea y segura, debidamente documentada, a fin de garantizar la interoperabilidad y la consecuente calidad en la prestación de servicios de carácter misional y administrativo, respecto de los servicios de información de interés, manteniendo los principios de privacidad establecidos.

PARÁGRAFO. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital deben garantizar, administrativa y jurídicamente, el tratamiento, conservación y aseguramiento de los datos y la información, por su valor estratégico y económico, en la medida que ellos sirven para el cabal cumplimiento de las políticas de inversión pública y cobertura social que los diferentes proyectos y programas del Plan de Desarrollo vigente prevean.

ARTÍCULO 27. DIRECTRICES DE IMPLEMENTACIÓN DE LA POLÍTICA. Las políticas en esta materia deben promover el uso de la intranet (red de comunicación interna) y el uso institucional de Internet entre los funcionarios distritales bajo el presupuesto de abrir espacios de socialización de la información; habilitar mecanismos que faciliten los procesos de veeduría ciudadana como un componente dentro del SDI; promover programas para que los grupos de población menos favorecidos del Distrito Capital tengan oportunidades de acceso a los servicios distritales, que implica la inclusión de ciudadanos independientemente de sus capacidades físicas.

ARTÍCULO 28. INSTRUMENTOS PARA LA POLÍTICA. Para la consolidación de la Democratización de la Información se requiere de la implementación y seguimiento de los lineamientos de la Agenda de Conectividad Distrital; de la formulación e implementación de la Estrategia de Gobierno Electrónico del Distrito; del Website de la CDS como medio para difundir información; de

talleres que permitan la identificación de trámites y servicios que se requiere poner en la Web y de un instrumento para oficializar el registro.

PARÁGRAFO 1º. En coordinación con las entidades distritales, la Comisión Distrital de Sistemas (CDS), en el área de políticas y estándares informáticos y de comunicaciones debe fijar estándares para la normalización de los datos y el intercambio de información y servicios entre entidades distritales y entre éstas y la ciudadanía.

PARÁGRAFO 2º. Los instrumentos y directrices antes señalados deben ser difundidos, incorporados y acogidos al interior de cada uno de las entidades, organismos y órganos de control del Distrito Capital.

ARTÍCULO 29. INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN**.** Los Jefes de las entidades, organismos y órganos de control del Distrito Capital deben garantizar la integridad y el derecho de uso pleno de sus datos e información misional, administrativa y operativa por parte de la Administración Distrital y de todos los ciudadanos, para lo cual deben definir los reglamentos y lineamientos internos para cumplir con tal fin, dentro del marco de lo establecido en la Ley 527 de 1999, el Decreto Nacional 1151 de 2008 y los Decretos Distritales 619 de 2007 y 185 de 2008 y cualquier otra disposición que establezca a nivel nacional o distrital en la materia.

PARÁGRAFO 1º. El uso que terceros le puedan dar a los datos y a la información en virtud de contratos de cualquier naturaleza que suscriban con las entidades, organismos y órganos de control del Distrito Capital y que presupongan la utilización de datos e información de carácter misional o administrativa, requerirá de la formulación de las condiciones contractuales necesarias que permitan que estos datos e información puedan ser utilizados, asegurando su integridad, seguridad y oportunidad.

PARÁGRAFO 2º. En todo caso, los datos y la información de las entidades, organismos y órganos de control del Distrito Capital deben quedar salvaguardados en poder del Distrito conforme a las políticas y lineamientos que la Administración Distrital dicte, de manera que sean fácilmente legibles y auditables en cualquier momento, con los recursos propios de las entidades, organismos y órganos de control del Distrito Capital.

ARTÍCULO 30. DIAGNÓSTICO DE LAS APLICACIONES MISIONALES Y ADMINISTRATIVAS. Es fundamental e indispensable que cada entidad u organismo del Distrito Capital tenga el diagnóstico detallado de todas las aplicaciones misionales y administrativas que utiliza, el cual puede ser publicado en sus páginas web, caracterizadas en su calidad, tráfico y en su transaccionalidad, de tal manera que se puedan dimensionar realmente las capacidades propias para su manejo y operación y así alcanzar un alto nivel de desarrollo de los servicios y trámites bajo un principio de oferta unificada de servicios distritales, y poder asegurar una verdadera democratización de la información.

ARTÍCULO 31. DIAGNÓSTICO DE INTEROPERABILIDAD**.** Con el fin de iniciar la implementación de un esquema de democratización de la información del Distrito y avanzar en la construcción de una oferta unificada de servicios distritales, se debe adelantar por parte de todos las entidades, organismos y órganos de control del Distrito Capital un proceso de diagnóstico interno detallado que permita identificar en qué estado se encuentra la entidad u organismo en materia de interoperabilidad y cuáles son los servicios y trámites estratégicos que puede ofrecer a la ciudadanía o a la Administración Distrital.

ARTÍCULO 32. FASES DEL GOBIERNO EN LÍNEA. Dentro del marco de lo establecido en el literal c) del artículo 3º del Decreto Distrital 619 de 2007 sobre Estrategia de Gobierno Electrónico Distrital y lo definido por el Gobierno Nacional a través de la Agenda de Conectividad, del artículo 5º del Decreto 1151 de 2008 sobre estrategias de Gobierno en Línea, se definen cinco (5) fases:

Fase 1 – Información.	Fase inicial en la cual las entidades, organismos y órganos de control del Distrito Capital habilitan sus propios sitios Web para proveer información básica vía Internet.
Fase 2 – Interacción	Fase en la cual los sitios Web permiten una comunicación simple de dos vías entre las entidades, organismos y órganos de control del Distrito Capital y el ciudadano, ofreciendo mecanismos de acercamiento que posibilitan hacer uso de la información que proveen las entidades, organismos y órganos de control del Distrito Capital en sus sitios Web.
Fase 3 – Transacción	Fase en la cual la interacción electrónica bidireccional entre el ciudadano y las entidades, organismos y órganos de control del Distrito Capital permite gestionar y completar actividades en línea, haciendo uso eficiente de las TICs como canales para la provisión de servicios y trámites en línea, e implementando esquemas de seguridad más robustos a fin de garantizar que las personas pueden remitir información personal y adelantar transacciones.
Fase 4 – Transformación	Fase en la cual los servicios y trámites que proveen las entidades, organismos y órganos de control del Distrito Capital se organizan alrededor de las necesidades de los ciudadanos y las empresas, agrupándose en cadenas según lineamientos comunes para ser provistos mediante una única interfaz multicanal (Oferta Unificada de Servicios), lo cual exige que las entidades, organismos y órganos de control del Distrito Capital se encuentren interconectadas y sus sistemas de información integrados para permitir el flujo de la información, con las características de seguridad, calidad, disponibilidad y confiabilidad necesarias.
Fase 5 – Participación o Democracia	Fase en la cual las entidades, organismos y órganos de control del Distrito Capital están en capacidad de proveer los mecanismos para que el ciudadano participe activa y colectivamente en la toma de decisiones de la Administración, a través de un esquema totalmente integrado y en línea, mediante el uso de herramientas para el trabajo colaborativo, la discusión interactiva y la consulta en tiempo real, facilitando así el consenso con la ciudadanía en la formulación de políticas, planes y programas inherentes al mejoramiento de la ciudad y de sus habitantes.

ARTÍCULO 33. INTERCAMBIO HOMOGÉNEO DE INFORMACIÓN. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital a fin de iniciar la implementación de un esquema de intercambio efectivo y seguro de

información en el Distrito, deben adoptar y aplicar lo establecido en el documento denominado *"Metodología para la creación de servicios Web en el Distrito Capital"*, el cual hace parte integral de la presente Resolución. (Anexo 2).

ARTÍCULO 34. METODOLOGÍA PARA ESTABLECER PATRONES DE USO DE CORREO ELECTRÓNICO E INTERNET. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital deben adoptar y aplicar lo establecido en el documentos denominado *"Metodología para establecer patrones de uso de correo electrónico e internet"*, la cual hace parte integral de la presente Resolución. (Anexo 3).

ARTÍCULO 35. RESPONSABLES DE LA PROMULGACIÓN, DIFUSIÓN Y APLICACIÓN DE LAS POLÍTICAS DE DEMOCRATIZACIÓN DE LA INFORMACIÓN. El Jefe de cada entidad y organismo debe difundir y aplicar las políticas básicas de democratización de la información e interoperabilidad señaladas, por el área que éste designe, dentro de los ciento veinte (120) días calendario siguientes a la expedición de esta Resolución y dentro del mismo plazo deben remitir al Presidente de la Comisión Distrital de Sistemas los documentos correspondientes a los diagnósticos requeridos en los artículos 30 y 31 de la presente Resolución, así como el informe de avance de la implementación de cada una de las fases del Gobierno en Línea en la entidad.

Adicionalmente, remitirá durante los primeros sesenta (60) días calendario de cada año, un documento actualizado que consolide los cambios y ajustes implementados respecto a las políticas de democratización de la información.

PARÁGRAFO. Corresponde a los jefes de dependencia, responsables de áreas, grupos de trabajo e intervinientes en los procesos y procedimientos asociados con las Tecnologías de Información y Comunicaciones (TIC), garantizar la implementación, la divulgación, la aplicación y el seguimiento de las políticas básicas de democratización de la información previstas en la presente Resolución.

ARTÍCULO 36. PROCEDENCIA DE OTRAS POLÍTICAS. Mediante el presente capítulo se regulan los aspectos básicos que en primera instancia deben adoptar las entidades, organismos y órganos de control del Distrito Capital como políticas básicas de democratización de información, a nivel de interoperabilidad e intercambio de información homogénea a través de servicios Web; por ello, la consolidación de los procesos de democratización de la información debe ser planeada y ejecutada en diferentes pasos e instancias, de conformidad con la normatividad vigente.

CAPÍTULO CUARTO

POLÍTICA DE CALIDAD PARA LA FORMULACIÓN Y GERENCIA DE PROYECTOS CON COMPONENTE DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES EN EL DISTRITO CAPITAL

ARTÍCULO 37. OBJETIVO DE LA POLÍTICA. El objetivo es la implementación de procesos formales, coherentes e integrados, que garanticen la oportunidad, seguridad y calidad de los servicios de información ofertados por la Administración Distrital, a fin de que cubran las exigencias y expectativas del ciudadano, en relación con los requisitos de costo, tiempo, estandarización y funcionalidad, como lo dispone la Ley 872 de 2003 al establecer para las entidades prestadoras de servicios, la creación del *Sistema de Gestión de Calidad* como herramienta que permita dirigir y evaluar el desempeño institucional en términos de calidad y satisfacción social, en la prestación de los servicios a cargo de las entidades y agentes obligados, la cual estará enmarcada en los planes estratégicos y de desarrollo.

En tal sentido, los servicios de información, datos, software, hardware y contenidos, se deben enmarcar en procesos que conlleven al cumplimiento de las especificaciones de presentación, diferenciación, fiabilidad, conformidad, duración, estética, utilidad y asistencia aplicables en cada caso.

ARTÍCULO 38. VERIFICACIÓN DE PROYECTO CON COMPONENTE TECNOLÓGICO*.* Los Directores de Planeación de cada entidad y organismo distrital, deben verificar que los proyectos, con componente de tecnología de información y comunicaciones, estén enmarcados en los principios y parámetros del Sistema de Gestión de Calidad (Acuerdo Distrital 122 de 2004), reglamentado por la Administración Distrital mediante el Decreto Distrital 387 de 2004.

ARTÍCULO 39. DIRECTRICES DE IMPLEMENTACIÓN. La Administración Distrital desarrollará los instrumentos necesarios para el fortalecimiento del Sistema de Gestión de Calidad en la prestación de servicios que utilicen TIC's, en cumplimiento de la Ley 872 de 2003. La Administración Distrital adelantará en coordinación con la Comisión Distrital de Sistemas la divulgación y uso de los estándares de calidad nacionales e internacionales aplicables a las tecnologías de información.

ARTÍCULO 40. REQUERIMIENTOS DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE CALIDAD. Dentro de los requerimientos de implementación del Sistema de Gestión de Calidad reglamentado por la Administración Distrital, se hace indispensable que las entidades, organismos y órganos de control del Distrito Capital:

1. Identifiquen y prioricen aquellos procesos estratégicos y críticos de la entidad u organismo, que resulten determinantes para desarrollar su función misional con calidad.

2. Determinen los criterios y métodos necesarios para asegurar que estos procesos sean eficaces, tanto en su operación como en su control.

3. Documenten y describan de forma clara, completa y operativa, los procesos identificados.

4. Ejecuten los procesos propios de cada entidad u organismo, de acuerdo con los procedimientos documentados.

5. Realicen el seguimiento, análisis y medición de estos procesos.

Corresponderá a las entidades, organismos y órganos de control del Distrito Capital de talleres para la difusión y capacitación en la implementación de estándares de calidad en servicios y la formulación de Indicadores de seguimiento y control de calidad en la prestación de servicios que utilicen TIC 's.

ARTÍCULO 41. MEDIOS DE INSTRUMENTACIÓN. Para el efecto de lo señalado en el artículo anterior la Comisión establece mediante esta Resolución las directrices generales para la formulación de proyectos informáticos y una documento de definición e implantación de metodología de gerencia de proyectos con componente de tecnología de información y comunicaciones.

ARTÍCULO 42. DIRECTRICES GENERALES PARA LA FORMULACIÓN DE PROYECTOS INFORMÁTICOS. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital deben adoptar y aplicar lo establecido en el documento denominado *"Directrices generales para la formulación de proyectos informáticos"*, el cual hace parte integral de la presente Resolución (Anexo 4) y contiene los lineamientos y aspectos necesarios para la evaluación de proyectos por parte de la Comisión Distrital de Sistemas en el marco de la Directiva 02 de 2002 del Alcalde Mayor.

ARTÍCULO 43. DEFINICIÓN E IMPLANTACIÓN DE METODOLOGÍAS DE GERENCIA DE PROYECTOS. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital deben adoptar y aplicar lo establecido en el documento denominado *"Definición e implantación de Metodología de Gerencia de Proyectos"*, el cual hace parte integral de la presente Resolución (Anexo 5); aplicable para la formulación de proyectos con componente de TIC´s, que debe ser elaborado en cada una de las fases del mismo y cuyos componentes se encuentran distribuidos de acuerdo a la siguiente relación:

1. Guía de pasos a seguir para utilizar la metodología de Gerencia de Proyectos.

2. Modelo de Procesos.

a) Glosario de Términos (forma parte del Modelo).

b) Ciclo de Vida de Proyectos.

3. Proceso Gestión de Integración.

a. Plan del Proyecto.

b. Formatos Plan del Proyecto (Firmas de Aprobación, Declaración del Riesgo, Indicadores de Calidad, Descripción de roles, perfiles y responsabilidades).
c. Formatos Procesos de Integración (Declaración Preliminar del Alcance, Informes de desempeño del trabajo).
d. Modelo Carta del Proyecto.

4. Proceso Gestión de Alcance.

a. Formatos Procesos de Alcance (Declaración Preliminar del Alcance, Definición del Alcance, Lista de Entregables, Diccionario Estructura Detallada de Trabajo).
b. Guías para el diligenciamiento de los siguientes formatos: Declaración Preliminar del Alcance, Definición del Alcance, Lista de Entregables y Diccionario Estructura Detallada de Trabajo.

5. Proceso Gestión de Tiempo.

a. Formatos Procesos de Tiempo: Lista de Actividades, Lista de Puntos de Verificación o eventos claves, Disponibilidad de Recursos y Atributos de las Actividades.
b. Guías para el diligenciamiento de los siguientes formatos: Lista de Actividades, Lista de Puntos de Verificación o eventos claves, Disponibilidad de Recursos y Atributos de las Actividades.

6. Proceso Gestión de Costos.

a. Formatos Procesos de Costos: Estimación de Costos, Justificación de la Estimación de Costos, Presupuesto de Costos y Valor Ganado.
b. Guías para el diligenciamiento de los siguientes formatos: Estimación de Costos, Justificación de la Estimación de Costos, Presupuesto de Costos y Valor Ganado.

7. Proceso Gestión de Calidad.

a. Formatos Procesos de Calidad: Mediciones de Control de Calidad, Listas de chequeo, Auditorías Internas y Métricas de Calidad.

8. Proceso Gestión del Recurso Humano.

a. Formatos Procesos de Recurso Humano: Plan Gestión de Personal, Evaluación de desempeño, Requerimientos de personal, Plan de entrenamiento al personal del proyecto, Definición de roles del proyecto, Definición de responsabilidades del equipo del proyecto, Plan de reconocimiento al personal del proyecto, Asignaciones de personal, Disponibilidad del Recurso Humano, Recomendaciones sobre el equipo de trabajo del proyecto y Directorio del personal del proyecto.

9. Proceso Gestión de Comunicaciones.

a. Formatos Proceso de Comunicaciones: Plan de Gestión de las comunicaciones, Informe Semanal de estado, Relación comunicaciones, Requerimientos de comunicaciones de los interesados, Estado de requerimientos de comunicaciones de los interesados, Identificación del tipo de comunicaciones con los Interesados del Proyecto y Matriz de comunicaciones.

10. Proceso Gestión de Riesgos.

    a. Formatos Proceso de Riesgos: Categorías de riesgos, Cuantificación de riesgos, Clasificación del impacto, Probabilidad de ocurrencia, Registro de riesgos y Análisis cuantitativo de riesgos.

11. Proceso Gestión de Adquisiciones.

    a. Formatos Proceso de Adquisiciones: Plan de Gestión de Adquisiciones, Documentación de Adquisiciones, Declaración de trabajo, Criterios de evaluación y Lista de Proveedores seleccionados.

12. Formato Requerimientos de Cambios.

    a. Guía para el diligenciamiento del Formato Requerimientos de Cambios.

ARTÍCULO 44. APLICACIÓN DE METODOLOGÍA EN LA FORMULACIÓN DE PROYECTOS. Corresponde a las entidades, organismos y órganos de control del Distrito Capital, cuando formulen y desarrollen proyectos de fortalecimiento institucional con componentes de Tecnología de Información y Comunicaciones (TIC), que sean de impacto interinstitucional y de mayor costo, de conformidad con los rangos previstos en la Directiva 02 de 2002, la cual establece que los proyectos de impacto interinstitucional son todos aquellos cuya realización involucra dos o más instituciones, o cuyo producto es utilizado por dos o más instituciones y/o su costo sea igual o superior a quinientos (500) SMLV, aplicar la metodología de gerencia de proyectos, citada en la presente resolución el instrumento equivalente definido por parte de la entidad.

Lo anterior sobre el presupuesto de que los procesos y procedimientos estratégicos y críticos que utilizan las entidades, organismos y órganos de control del Distrito Capital para desarrollar su función misional se soportan y se apoyan en Tecnologías de Información y Comunicaciones (TIC).

ARTÍCULO 45. RESPONSABLES DE LA IMPLEMENTACIÓN DE POLÍTICAS DE CALIDAD. El Jefe de cada entidad u organismo debe implementar las políticas básicas de calidad para la formulación y gerencia de proyectos con componente TIC´s, previstas en este capítulo, dentro de los ciento ochenta (180) días calendario siguientes a la expedición de esta Resolución, en lo aplicable a cada una de las fases del ciclo de vida de un proyecto con componente de TIC´s.

De la misma forma, cada entidad y organismo debe remitir un documento donde especifique la metodología de gerencia de proyectos adoptada y

aplicada al interior de la misma, para aquellos proyectos con componente de tecnología de información y comunicaciones.

PARÁGRAFO. Las directrices y los instrumentos contenidos en los anexos, deben ser difundidos, incorporados y acogidos al interior de cada una de las entidades, organismos y órganos de control del Distrito Capital.

ARTÍCULO 46. PROCEDENCIA DE OTRAS POLITICAS. Este capítulo da cobertura, a los aspectos que en primera instancia deben adoptar las entidades, organismos y órganos de control del Distrito Capital como políticas básicas de calidad, para la formulación y gerencia de proyectos con componente de Tecnología de Información y Comunicaciones. En todo caso el desarrollo de esta política debe estar enmarcada en la dinámica del Sistema de Gestión de Calidad conforme a la normatividad vigente.

CAPÍTULO QUINTO

POLÍTICAS DE RACIONALIZACIÓN DEL GASTO PARA LA ADMINISTRACIÓN E IMPLEMENTACIÓN DE BIENES Y RECURSOS DE INFRAESTRUCTURA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES EN EL DISTRITO CAPITAL.

ARTÍCULO 47. OBJETIVO. Para la Administración Distrital es preciso racionalizar la utilización de Tecnologías de Información y Comunicaciones (TIC) de manera que se rentabilicen plenamente las inversiones y se eviten altos costos en el desarrollo de proyectos, en la duplicidad de sistemas de información, generando una mecánica de cooperación interinstitucional, actuando no como entidades independientes sino integralmente como Distrito, de manera que se genere valor agregado para las instituciones y se ofrezca un servicio eficiente a los ciudadanos.

ARTÍCULO 48. *COORDINACIÓN PARA LA RACIONALIZACIÓN DEL GASTO.* La Comisión Distrital de Sistemas en desarrollo de su función de coordinación de la gestión informática, esto es, de construir y mantener actualizada la información sobre los bienes, recursos, proyectos, planes y servicios informáticos y de comunicaciones de las entidades, organismos y órganos de control del Distrito Capital y facilitar su uso estratégico, considera pertinente racionalizar la utilización de Tecnologías de Información y Comunicaciones (TIC), de manera que se rentabilicen plenamente las inversiones y se eviten altos costos en el desarrollo de proyectos y en la duplicidad de sistemas de información de conformidad con los parámetros establecidos en la Directiva 005 de 2005 del Alcalde Mayor.

Lo anterior presupone un conocimiento detallado de la infraestructura de tecnología existente al interior de las entidades, organismos y órganos de control del Distrito Capital, con el fin de hacer un mejor aprovechamiento de los recursos públicos y optimizar los procesos de contratación de bienes y servicios en materia de tecnología.

Por lo tanto, es indispensable que las entidades, organismos y órganos de control del Distrito Capital tengan la máxima claridad sobre la capacidad técnica y funcional de los recursos tecnológicos y la infraestructura sobre los que se implementan los sistemas de información que las apoyan a nivel administrativo y misional.

ARTÍCULO 49. LINEAMIENTOS GENERALES PARA LA POLÍTICA. Los presupuestos en la formulación de lineamientos de la política de racionalización del gasto en materia de tecnología de información y comunicación son los siguientes:

1. Los gerentes de proyecto deben identificar los proyectos adelantados por otras áreas dentro de la misma entidad u otras entidades, organismos y órganos de control del Distrito Capital y evaluar si son complementarios o sustitutos en lo relacionado con la utilización de TIC's y con base en ello, formular la alternativa de solución conveniente a su entidad y al Distrito.

2. En todas las entidades, organismos y órganos de control del Distrito Capital los funcionarios responsables de los proyectos que tengan componente de tecnología de información y comunicaciones, deben identificar los costos directos e indirectos que se generan en las diferentes etapas de ejecución del proyecto.

3. Los funcionarios responsables de los proyectos, desde la etapa de pre-inversión, deben identificar los elementos que permitan evaluar y garantizar la sostenibilidad del mismo en el largo plazo.

4. La Comisión Distrital de Sistemas debe liderar la negociación de convenios distritales con proveedores de tecnología de información y comunicaciones que permitan obtener economías de escala para el Distrito.

ARTÍCULO 50. DIRECTRICES DE IMPLEMENTACIÓN DE RACIONALIZACIÓN DEL GASTO EN EL D.C. Se destacan como directrices para la implementación de la racionalidad del gasto en materia de administración de bienes y recursos de infraestructura de tecnología de información y comunicaciones, los siguientes:

1. En materia de sistemas de apoyo administrativo, todas las entidades distritales en el momento de realizar una adquisición, deben evaluar como alternativa los sistemas de propiedad de otra entidad distrital que hayan sido homologados por la CDS. En particular se debe considerar como primera alternativa el Sistema de Información Hacendario.

2. Las compras en materia de tecnología informática que realicen las entidades deben ajustarse a los precios obtenidos en los convenios firmados por el Distrito con los proveedores de tecnología.

3. El Distrito establecerá los servicios que puedan ser prestados por entidades distritales y que no se contratarán con proveedores externos.

4. El costo del acceso a internet debe ser registrado por las entidades en el presupuesto de funcionamiento.

5. Los proyectos de implementación de sistemas de información deben garantizar una buena relación costo beneficio teniendo en cuenta aspectos como la oportunidad, la calidad, la integridad, posibilidad de masificación y evolución tecnológica.

ARTÍCULO 51. INSTRUMENTACIÓN DE LA POLITICA DE RACIONALIZACIÒN DEL GASTO.

Debe contar con lo siguiente:

1. Metodología de Formulación y Evaluación de Proyectos de Tecnología de Información y Comunicaciones.

2. Modelo de términos de referencia que contemple los aspectos mínimos que deben ser tenidos en cuenta para la contratación de sistemas de información con el fin de que el proyecto sea sostenible en el tiempo.

3. Lista actualizada de servicios estandarizados y rango de tarifas para cada uno.

4. Lista de servicios y entidades distritales que lo prestan; plan de incentivos para las entidades distritales que prestan servicios a otras entidades distritales.

5. Identificación de servicios al ciudadano o entidades diferentes al Distrito que sean susceptibles de cobro como medio de sostenibilidad del proyecto.

PARÁGRAFO. Los instrumentos previstos en los numerales 2 al 5 deben ser objeto de desarrollo por esta Comisión Distrital, dentro del año siguiente a la suscripción de la presente Resolución.

ARTÍCULO 52. DIAGNÓSTICO E INVENTARIO DE SERVICIOS INFORMÁTICOS. La Comisión Distrital de Sistemas, en desarrollo de su función de coordinación de la gestión informática, esto es, de construir y mantener actualizada la información sobre los bienes, recursos, proyectos, planes y servicios informáticos y de comunicaciones de las entidades, organismos y órganos de control del Distrito Capital y facilitar su uso estratégico, considera pertinente racionalizar la utilización de Tecnologías de Información y Comunicaciones (TIC), de manera que se rentabilicen plenamente las inversiones y se eviten altos costos en el desarrollo de proyectos y en la duplicidad de sistemas de información de conformidad con los parámetros establecidos en la Directiva 005 de 2005.

Lo anterior presupone un conocimiento detallado de la infraestructura de tecnología existente al interior de las entidades, organismos y órganos de control del Distrito Capital, con el fin de hacer un mejor aprovechamiento de los recursos públicos y optimizar los procesos de contratación de bienes y servicios en materia de tecnología.

Por lo tanto, es indispensable que las entidades, organismos y órganos de control del Distrito Capital tengan máxima claridad sobre la capacidad técnica y funcional de los recursos tecnológicos y la infraestructura sobre los que se implementan los sistemas de información que las apoyan a nivel administrativo y misional.

ARTÍCULO 53. INVENTARIOS DE LOS SISTEMAS DE INFORMACIÓN Y DE LA INFRAESTRUCTURA DE TECNOLOGÍA. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital deben actualizar la información correspondiente a los siguientes inventarios: "Inventario de los sistemas de información administrativos y misionales" e "Inventario de la infraestructura de tecnología relacionada con informática y comunicaciones", aplicativos que se encuentran publicados para su actualización y diligenciamiento en la página web de la CDS, www.bogota.gov.co/cds.

PARÁGRAFO. Las directrices y los instrumentos contenidos en los anexos ya citados en este capítulo, deben ser difundidos, incorporados y acogidos al interior de cada una de las entidades, organismos y órganos de control del Distrito Capital.

ARTÍCULO 54. LINEAMIENTOS PARA LA IMPLEMENTACIÓN Y ADMINISTRACIÓN DE INFRAESTRUCTURA DE TECNOLOGÍA DE CONECTIVIDAD. Las entidades, organismos y órganos de control del Distrito Capital deben adoptar y aplicar lo establecido en el documento denominado "Lineamientos para la implementación y administración de infraestructura de tecnología de conectividad", los cuales hacen parte integral de la presente Resolución (Anexo 6).

ARTÍCULO 55. METODOLOGÍA DE AUTODIAGNÓSTICO DE INFRAESTRUCTURA DE CONECTIVIDAD. Las entidades, organismos y órganos de control del Distrito Capital deben adoptar y aplicar lo establecido en el documento denominado "Metodología de auto-diagnóstico de infraestructura de conectividad", la cual hace parte integral de esta Resolución. (Anexo 7).

ARTÍCULO 56. RESPONSABLES DE LA PROMULGACIÓN, APLICACIÓN E INFORMES. Los Jefes de cada entidad, organismo y órganos de control del Distrito Capital, deben disponer lo pertinente para la promulgación, difusión y aplicación, por el área que éstos designen, de las políticas básicas de racionalización del gasto para la administración e implementación de bienes y recursos de infraestructura de tecnología de información y comunicaciones, previstas en la presente resolución.

Dentro de los ciento veinte (120) días calendarios siguientes a la expedición de esta Resolución, las entidades, organismos y órganos de control del Distrito Capital deben enviar copia de los documentos sobre los avances en su implementación, al Presidente de la Comisión Distrital de Sistemas para su consolidación.

Así mismo, las entidades, organismos y órganos de control del Distrito Capital deben diligenciar semestralmente con corte a 30 de junio y 31 de diciembre y

dentro de los 30 días siguientes a las mencionadas fechas, los inventarios solicitados en los artículos precedentes para su consolidación y armonización; así como remitir el 1º de junio y el 1º de diciembre de cada año, un documento actualizado que consolide los resultados generados por cada organismo o entidad, respecto a las políticas de racionalización del gasto.

TÍTULO II

SOBRE LAS POLÍTICAS ESPECÍFICAS

CAPÍTULO PRIMERO

POLÍTICAS DE CONECTIVIDAD PARA LOS ENTES PÚBLICOS EN EL DISTRITO CAPITAL.

ARTÍCULO 57. COHERENCIA EN LA IMPLEMENTACIÓN DE LA RED DISTRITAL DE CONECTIVIDAD. Cada entidad, organismo y órgano de control del Distrital Capital, debe aplicar en el desarrollo de su gestión de tecnología, las políticas, lineamientos y metodologías para la contratación, implementación y gestión de servicios de conectividad (canales de comunicaciones y acceso a Internet), con las cuales se pretende sentar bases para que la Administración Distrital logre un mejoramiento sustancial en sus sistemas de comunicaciones y un real acercamiento a la ciudadanía, a través de una eficiente prestación de servicios apoyados en la tecnología. Lo anterior permite una mayor coherencia en la implementación de la Red Distrital de Conectividad.

ARTÍCULO 58. APROBACIÓN DE POLÍTICAS DE CONECTIVIDAD. Adóptanse las políticas específicas de conectividad que fueron aprobadas por la Comisión Distrital de Sistemas, en las Mesas de Trabajo de Mayo 30 y Julio 7 de 2006 y Febrero 1 de 2007, las cuales se encuentran contenidas en el Acta No. 2 del 13 de Marzo de 2007.

ARTÍCULO 59. POLÍTICA EN MATERIA DE CONECTIVIDAD. Los Jefes de cada entidad y organismo Distrital deben adoptar como política en materia de conectividad, los lineamientos de orden técnico para la contratación, implementación y gestión de servicios de conectividad, contenidos en los documentos aprobados por la Comisión Distrital de Sistemas, denominados:

a) *"Lineamientos Técnicos y Metodología para la Contratación, Implementación y Gestión de Servicios de Conectividad", (*Anexo 8).

b) *"Formato Modelo para la Elaboración de Anexos Técnicos de Contratos de Servicios de Conectividad", (*Anexo 9).

c*) "Procedimiento de implementación de los servicios de conectividad", (*Anexo 10)

d) *"Procedimiento para la homologación de proveedores de servicios de conectividad y comunicaciones y sus formularios.", (*Anexo 11).

e) *"Procedimientos técnicos de ingeniería de tráfico.", (*Anexo 12).

f) *"Procedimiento de Caracterización Técnica de aplicaciones, desde la perspectiva de tráfico y conectividad.", (*Anexo 13).

CAPÍTULO SEGUNDO

POLÍTICA DE INFRAESTRUCTURA INTEGRADA DE DATOS ESPACIALES DEL DISTRITO CAPITAL. IDEC@

ARTÍCULO 60. POLÍTICA DE INFRAESTRUCTURA INTEGRADA DE DATOS ESPACIALES EN EL DISTRITO CAPITAL. La Comisión Distrital de Sistemas -CDS-, en cumplimiento del artículo 4º del Acuerdo Distrital 130 de 2004, establece los lineamientos técnicos y las políticas de la infraestructura integrada de datos espaciales para el Distrito Capital, la cual será coordinada por la Unidad Administrativa Especial de Catastro Distrital.

PARÁGRAFO. La Unidad Administrativa Especial de Catastro Distrital debe establecer los estándares para la gestión y el manejo de la información espacial georeferenciada, participar en la formulación de las políticas para los protocolos de intercambio de información espacial e igualmente generar y mantener actualizada la Cartografía Oficial del Distrito Capital.

ARTÍCULO 61. RESPONSABLES. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital deben adoptar las políticas especificas para la construcción de la Infraestructura Integrada de Datos Espaciales del Distrito Capital IDEC@, que hacen parte integral de esta Resolución así:

a. *"Guía de elaboración de metadatos"*, (Anexo 14).
b. *"Catálogo de objetos geográficos"*, (Anexo 15).
c. *"Datos fundamentales"*, (Anexo 16).
d. *"Políticas específicas para IDEC@"*, (Anexo 17).

ARTÍCULO 62. COORDINACIÓN. Los proyectos que acometa cualquier entidad u organismo Distrital, relacionado con la elaboración de cartografía, toma de fotografías aéreas, imágenes satelitales o cualquier tecnología de captura de información del territorio deben coordinarse con la Unidad Administrativa Especial de Catastro Distrital.

ARTÍCULO 63. INTEROPERATIVIDAD CON EL GEOPORTAL. Los sistemas de información de las entidades, organismos y órganos de control del Distrito Capital, donde se involucren componentes geográficos y/o cartográficos, deben incluir funcionalidades que permitan interoperar con el Geoportal de IDEC@.

PARÁGRAFO. La Unidad Administrativa Especial de Catastro Distrital prestará asesoría técnica a las entidades, organismos y órganos de control del Distrito Capital que lo requieran.

CAPÍTULO TERCERO

SOBRE LA POLÍTICA PARA PROMOCIONAR EL USO DEL SOFTWARE LIBRE EN LAS ENTIDADES DEL DISTRITO CAPITAL.

ARTÍCULO 64. OBJETIVO Y NATURALEZA. Ante la rápida evolución y la dinámica actual de las Tecnologías de Información y Comunicaciones (TIC) se ha venido identificando la necesidad de contar con soluciones tecnológicas cada vez más costo-eficientes, que permitan obtener beneficios y resultados tangibles en la prestación de servicios a los ciudadanos y en la gestión pública.

ARTÍCULO 65. SOBRE LA PROMOCIÓN Y USO DE SOFTWARE LIBRE EN EL DISTRITO CAPITAL. La Comisión Distrital de Sistemas formula la política orientada a la promoción y uso de software libre en los sectores central, descentralizado y las localidades del Distrito, conforme con lo establecido en el artículo 1º del Acuerdo 279 de 2007 y dentro de su función de apoyo a la formulación y desarrollo de proyectos informáticos y de comunicaciones relacionada con investigar, evaluar, proponer y generar espacios para el aprovechamiento de nuevas soluciones tecnológicas en las entidades, organismos y órganos de control del Distrito Capital.

La política se enmarca dentro de una estrategia orientada a la racionalización del gasto público y a la búsqueda de soluciones alternativas que provean las funcionalidades que el Distrito requiere, a fin de obtener ahorro en la inversión y en el funcionamiento administrativo.

ARTÍCULO 66. PRINCIPIOS EN EL ACCESO A LA POLÍTICA DE PROMOCIÓN DEL *SOFTWARE LIBRE.* La política general de promoción de *Software Libre* no pretende imponer su uso en las entidades, organismos y órganos de control del Distrito Capital, sino que debe ser considerada como una alternativa a la par con otras soluciones del mercado, dependiendo de la equivalencia funcional y tecnológica que corresponda.

Para la implementación de esta política es necesario que las entidades, organismos y órganos de control del Distrito Capital tengan en cuenta los principios que se enumeran a continuación y que deben primar a la hora de evaluar la adquisición y compra de tecnologías:

1. Neutralidad Tecnológica. Consiste en que el marco normativo general que se aplique dentro del comercio telemático no debe optar por un tipo de tecnología en particular.

La neutralidad tecnológica implica hacer uso de estándares, tanto para almacenar información, como para interactuar con otros sistemas, sobre el presupuesto de un uso no coercitivo de la tecnología, que garantice la inclusión digital, la tecnología accesible y la interoperabilidad vertical y horizontal en la Administración Pública; lleva consigo la existencia de una sana competencia e igualdad de concurrencia de los proveedores en el mercado, en la medida que la Administración no debe otorgar ventajas a unos actores por sobre otros.

La neutralidad tecnológica no implica de forma general preferir una tecnología sobre otra. Pero aunque así fuera, la Administración debe ser *imparcial* frente a

los proveedores, con el uso de su potestad de imponer las condiciones necesarias requeridas por ella, para alcanzar sus objetivos y metas previstas.

2. Interoperabilidad. Las soluciones tecnológicas que las entidades, organismos y órganos de control del Distrito Capital deseen adquirir, deben procurar la interoperabilidad con otros sistemas existentes en la misma o diferentes entes distritales, así como soportar estándares abiertos buscando reducir las barreras de acceso y comunicación, sin comprometer la seguridad de la información. Se entiende por interoperabilidad la conexión de personas, datos y diversos sistemas de información.

3. Independencia del Distrito. entidades, organismos y órganos de control del Distrito Capital propenderán por la independencia de soluciones, productos tecnológicos o plataformas de proveedores únicos.

4. Propiedad Intelectual. Las entidades, organismos y órganos de control del Distrito Capital deben considerar cuidadosamente las posibilidades y limitaciones del modelo de licenciamiento de la solución seleccionada. De igual manera, propender por mitigar los riesgos o contingencias legales derivados del uso de plataformas o soluciones que involucren innovación protegida por derechos de propiedad intelectual.

5. Seguridad. Las entidades, organismos y órganos de control del Distrito Capital en la adquisición de Sistemas de Información deben tener en cuenta la vulnerabilidad de dichos sistemas durante un tiempo específico, entre ellos, los tiempos de respuesta de los proveedores a dichas vulnerabilidades, el grado de severidad de dichas vulnerabilidades y la capacidad de los proveedores para corregir las fallas que se presenten.

6. Confiabilidad. Las entidades, organismos y órganos de control del Distrito Capital deben propender por incrementar al máximo la disponibilidad de las soluciones tecnológicas, aumentando su confiabilidad al realizar la actividad en un mayor número de veces con el menor tiempo de interrupciones.

ARTÍCULO 67. POLÍTICAS, DIRECTRICES Y LINEAMIENTOS PARA EL USO DE SOFTWARE LIBRE EN EL DISTRITO CAPITAL. Los Jefes de las entidades, organismos y órganos de control del Distrito Capital a fin de iniciar la implementación de esta política, deben adoptar y aplicar lo establecido en el documento denominado *"Políticas, directrices y lineamientos generales para la utilización de software libre en el Distrito"*, el cual hace parte integral de la presente Resolución. (Anexo 18).

PARÁGRAFO 1º. Los Jefes, o sus delegados, de las entidades, organismos y órganos de control del Distrito Capital que son referidos de manera específica en el anexo 18, y que son responsables de apoyar directamente la promoción de esta política a nivel distrital, deben adelantar y desarrollar sus actividades conforme lo explica dicho anexo y presentar un informe trimestral al Presidente de la Comisión Distrital de Sistemas, los cuales se consolidarán y utilizarán para la presentación del informe semestral de que trata el artículo 2º del Acuerdo 279 de 2007.

PARÁGRAFO 2º. Las políticas, directrices y lineamientos, contenidos en el anexo citado, deben ser difundidos y acogidos al interior de cada una de las entidades y organismos del Distrito Capital.

ARTÍCULO 68. RESPONSABLES DE LA PROMULGACIÓN, DIFUSIÓN Y APLICACIÓN DE LAS POLÍTICAS PARA LA PROMOCIÓN Y USO DEL SOFTWARE LIBRE EN EL DISTRITO CAPITAL. El Jefe de cada entidad y organismo distrital debe acoger, difundir y aplicar las políticas para promocionar el uso del software libre en las entidades del Distrito Capital, la cual será difundida y aplicada por el área que éste designe.

Todas las entidades, organismos y órganos de control del Distrito Capital deben enviar un informe el 1º de junio y 1º de diciembre de cada año, al Presidente de la Comisión Distrital de Sistemas, en el cual se reflejen los avances y resultados obtenidos respecto a la política de promoción y uso del software libre.

PARÁGRAFO. Corresponde a los jefes de dependencia, responsables de área, grupos de trabajo e intervinientes en los procesos y procedimientos asociados con las Tecnologías de Información y Comunicaciones (TIC), garantizar la implementación, la divulgación, la aplicación y el seguimiento de la política de promoción y uso del software libre prevista en este capítulo.

ARTICULO 69. VIGENCIA Y DEROGATORIA. La presente resolución rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias y en especial las Resoluciones 185 y 355 de 2007 de la Comisión Distrital de Sistemas (CDS).

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D. C., a los 20 días de octubre de 2008

YURI CHILLÁN REYES

Presidente

CARLOS MAURICIO CORREDOR VERA

Secretario Técnico