ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE HACIENDA

ESTUDIOS Y DOCUMENTOS PREVIOS
CONTRATACIÓN DE MÍNIMA CUANTÍA

A continuación, presento el estudio de conveniencia y necesidad requerido conforme a lo dispuesto en los numerales 7 y 12 del artículo 25 de la Ley 80 de 1993 (modificado por el art. 87 de la Ley 1474 de 2011) y los artículos **2.1.1°** y **3.5.2°**, del Decreto Reglamentario 734 de 2012, para adelantar un proceso de selección de mínima cuantía y la consecuente celebración del contrato requerido.

1. DESCRIPCIÓN DE LA NECESIDAD QUE SE PRETENDE SATISFACER CON LA CONTRATACIÓN.

Para la Secretaría Distrital de Hacienda es conveniente la celebración de un contrato con el objeto registrado, teniendo en cuenta que el Concejo de Bogotá D. C., requiere garantizar el funcionamiento, seguridad, disponibilidad, operación de la infraestructura tecnológica, lo cual se logra mediante la adquisición, mantenimiento, y soporte de las Licencias de antivirus.

A partir del año 2002, la Secretaría Distrital de Hacienda asumió las funciones que venía desarrollando el Fondo Rotatorio del Concejo, en razón a que mediante Acuerdo Distrital No. 59 del 2002, el Concejo de Bogotá, D.C., dispuso lo siguiente:

"Artículo 3. Subrogación de derechos y obligaciones. El Distrito Capital de Bogotá – Secretaría Distrital de Hacienda subrogará al Fondo Rotatorio del Concejo de Bogotá, D.C. en la titularidad de los derechos que a éste corresponden y en el cumplimiento de las obligaciones a su cargo, incluidas las pecuniarias"

Así mismo, el artículo 6° del Acuerdo antes citado preceptuó:

"Creación del Fondo Cuenta del Concejo de Bogotá, D.C. Créase el Fondo Cuenta del Concejo de Bogotá D.C., para el manejo presupuestal, contable y de tesorería de los recursos financieros destinados a la administración, funcionamiento y operación del Concejo de Bogotá, D.C.

El Fondo Cuenta del Concejo de Bogotá, D.C. no tendrá personería jurídica y el ordenador del gasto de los recursos será el Secretario de Hacienda Distrital, quien podrá delegar dicha facultad en un funcionario del nivel directivo de la Secretaría Distrital de Hacienda."

Igualmente, el parágrafo del artículo 7° del Acuerdo 59 de 2002, estableció:

"Los gastos que se deriven de la administración y funcionamiento del Fondo Cuenta del Concejo de Bogotá, D.C., serán con cargo al presupuesto de la Secretaría Distrital de Hacienda."

A su vez el Decreto Distrital No. 260 del 24 de junio de 2002, en su artículo 1°, señaló:

"Créase en el Presupuesto de la Secretaría Distrital de Hacienda, la Unidad Ejecutora 04 «Fondo Cuenta Concejo de Bogotá, D.C.».

Sobre la base de lo anterior, corresponde a la Secretaría Distrital de Hacienda contratar con cargo a los recursos asignados al "*Fondo Cuenta del Concejo de Bogotá. D.C.*" los bienes o servicios que requiera el Concejo de Bogotá, D.C.

Por lo tanto, y de acuerdo con el requerimiento del Concejo de Bogotá emitido mediante cordis 2013ER37165, se inicia el proceso precontractual para llevar a cabo la celebración del contrato con el objeto descrito en el numeral 2.1.

Con el propósito de garantizar la protección y seguridad de la información, ante los posibles riesgos informáticos que se presentan constantemente a través de virus, troyanos, spam y demás tipos de ataques, que pueden ingresar a la red corporativa ocasionando daños o perdidas de información institucional, se ha generado un esquema de seguridad para el Concejo de Bogotá, con el fin de prevenir el riesgo de contaminación de virus informático a través de los diferentes medios de propagación como son: Conexiones de red, correo electrónico, Internet, unidades extraíbles (CD, flash

memory, etc.). Así mismo, se requiere de una protección efectiva que detecte y remueva o bloquee el software malicioso y los objetos infectados en los escaneos de acceso, como de las herramientas de prevención y contención que posibilitan la toma de acciones prontas y adecuadas de los administradores para prevenir daños mayores. Actualmente el Concejo de Bogotá tiene implementada como solución de Antivirus en todas las máquinas clientes y servidores la suite McAfee.

De igual manera, este antivirus ofrece protección a usuarios remotos y portátiles utilizados en el Salón Comuneros, la biblioteca y demás áreas que se encuentran fuera de las oficinas y los cuales se conectan a través de la red inalámbrica. La administración centralizada de este antivirus ha permitido la instalación de la solución en las estaciones de trabajo; configuración de los parámetros de protección; manejo de las actualizaciones bases de datos, módulos de programas y respuesta efectiva a eventos potencialmente peligrosos.

La necesidad concreta que el Concejo de Bogotá pretende satisfacer es la de brindar las herramientas, que permitan el buen funcionamiento de los equipos, a través de la adquisición, mantenimiento y soporte de las licencias del software antivirus para la plataforma informática de esta Corporación, razón por la cual el requerimiento se encuentra incluido dentro del Plan de Contratación aprobado para esta vigencia.

2. DESCRIPCIÓN DEL OBJETO A CONTRATAR CON SUS ESPECIFICACIONES ESENCIALES.

2.1. OBJETO

Adquisición, mantenimiento y soporte de las licencias de software antivirus para la plataforma del Concejo de Bogotá.

2.2. ALCANCE DEL OBJETO

Para este proceso se requiere la adquisición, configuración, mantenimiento, capacitación, puesta en operación y servicio de soporte, de acuerdo con lo descrito a continuación:

Descripción	Cantidad
Adquisición, configuración, mantenimiento, capacitación, puesta en operación y servicio de soporte de las licencias de software antivirus para las **estaciones de trabajo** que conforman la plataforma tecnológica del Concejo de Bogotá.	520
Adquisición, configuración, mantenimiento, capacitación, puesta en operación y servicio de soporte de las licencias de software antivirus, para los **servidores** que conforman la plataforma tecnológica del Concejo de Bogotá.	21
Adquisición, configuración, mantenimiento, capacitación, puesta en operación y servicio de soporte de las licencias de software antivirus para los **buzones de correo** que hacen parte de la plataforma tecnológica del Concejo de Bogotá	650
Mantenimientos Preventivos (Tres durante la ejecución del contrato) y los mantenimientos correctivos necesarios, durante la ejecución del contrato.	3

2.3. VALOR ESTIMADO DEL CONTRATO

El valor estimado del contrato que se derive del presente proceso de selección, incluido el Impuesto al Valor Agregado (I.V.A.), cuando a ello hubiere lugar y demás impuestos, tasas, contribuciones de carácter nacional y/o distrital legales, costos directos e indirectos, es la suma de Treinta y Ocho Millones Ochocientos Cincuenta y Siete Mil Quinientos Cincuenta y Un Pesos ($38.857.551.00) M/cte, INCLUIDO IVA.

El anterior valor se encuentra respaldado con el siguiente Certificado de Disponibilidad Presupuestal:

No. 93
Fecha: 27-06-2013
Código presupuestal: 3-1-2-01-00-0000-00
Valor: Treinta y Nueve Millones de Pesos M/cte ($39.000.000)
Vigencia 2013

El análisis para calcular el valor estimado del contrato que se derive del presente proceso de selección, así como su monto y el de posibles costos asociados al mismo se encuentra contenido en el estudio de mercado.

2.4. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de doce (12) meses y diez (10) días hábiles, a partir de la firma del acta de inicio, discriminado así:

a) Diez (10) días hábiles para la entrega, instalación, puesta en operación y capacitación de las licencias de software antivirus contados a partir de la fecha de firma del acta de iniciación del contrato, firmada por el contratista y el supervisor designado por la Secretaría Distrital de Hacienda.

b) Doce (12) meses para el mantenimiento y soporte de las licencias, contados a partir de la entrega e instalación de las mismas.

La vigencia del contrato será por el plazo de ejecución del contrato y hasta los cuatro (4) meses siguientes a la finalización del plazo de ejecución.

2.5. FORMA DE PAGO

La Secretaría Distrital de Hacienda efectuará:

a) Un pago inicial correspondiente al 100% del valor total de las licencias, contra entrega del documento para la instalación de las licencias y funcionamiento del software antivirus de forma satisfactoria.
b) Tres pagos iguales, uno cada cuatro (4) meses, correspondientes al valor destinado para los mantenimientos preventivos y los correctivos que sean necesarios, de acuerdo con el valor ofertado para este ítem, para lo cual el contratista deberá adjuntar el soporte de las actividades realizadas de mantenimiento.

Los pagos se efectuarán dentro de los diez (10) días hábiles siguientes a la radicación en la Subdirección Financiera de la certificación de cumplimiento a satisfacción del objeto y obligaciones, expedida por el supervisor del contrato, acompañada de los respectivos recibos de pago por concepto de aportes al Sistema de Seguridad Social Integral (Salud, Pensión y ARL), aportes parafiscales: Sena, ICBF y Cajas de Compensación Familiar, cuando corresponda.

Los pagos se efectuarán a través del sistema SAP en la cuenta de ahorros o corriente de la entidad financiera que indique el contratista, de la cual sea titular éste. Sin perjuicio de lo anterior queda entendido que la forma de pago supone la prestación real y efectiva de la contraprestación pactada.

2.6. SITIO DE ENTREGA

El sitio de entrega e instalación de las licencias será en las instalaciones del Concejo de Bogotá Calle 36 No. 28ª 41, en la ciudad de Bogotá, D.C.

2.7. COMITÉ DE OBRA:

N/A

2.8. CLÁUSULAS SANCIONATORIAS Y COSTOS A CARGO DEL CONTRATISTA: El proponente deberá tener en cuenta que el contrato incluirá cláusula de multas, cláusula penal pecuniaria, cláusulas excepcionales (si hay lugar a ellas). Igualmente, deberá asumir los costos de expedición de la garantía así como todos los impuestos, tasas y contribuciones del orden nacional y distrital que gravan los contratos estatales.

3. CONDICIONES TÉCNICAS EXIGIDAS.

No.	REQUERIMIENTO TÉCNICO MÍNIMO REQUERIDO
1.	**SOFTWARE DE PROTECCION ANTIVIRUS DEBE CUMPLIR LOS SIGUIENTES REQUISITOS:**
1.1.1	El contratista deberá suministrar una (1) solución de antivirus corporativo; con 520 licencias para estaciones de trabajo y 650 licencias para buzones de correo, las cuales serán instaladas en los equipos de cómputo (que incluyan Sistema Operativo MS Windows XP, 7 y 8. Server 2003, 2008, 2012, y Linux Opensuse, Red Hat Enterprise Linux 5.4, Suse Linux Enterprise Server 10.) Para uso continuo con derecho a actualizaciones y nuevas versiones (upgrade) por un término de un (1) año y que cumpla las siguientes características.
1.1.2	La protección antivirus debe tener compatibilidad con los sistemas operativos Windows y Linux Opensuse, Red Hat Enterprise Linux 5.4, Suse Linux Enterprise Server 10.), incluyendo las nuevas versiones de estos. Contar con versiones para estaciones de trabajo, servidores de archivos, servidores de correo electrónico y una herramienta de administración remota.
1.1.3	El licenciamiento debe ser instalado y en perfecto funcionamiento en los servidores Windows Server 2003, 2008, 2012 y superiores, clientes con Windows XP, Service Pack 3 o superior, Windows 7, 8 o superior en 32 y 64 bits incluyendo las nuevas versiones de estos sistemas operativos.
1.1.4	El antivirus debe contar con un mecanismo de actualización que garantice la integridad, que evite la manipulación o alteración de las definiciones de virus por medio de encripción (cifrамiento) y firmas digitales.
1.1.5	El antivirus debe contar con la opción de realizar un rollback de las definiciones que permita regresar a la actualización anterior, en caso de que los archivos instaladores ocasionen fallas en el sistema; este proceso también debe ser administrado desde la consola administrativa.
1.1.6	Módulo de detección en tiempo real que proteja contra: virus, gusanos, troyanos, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, herramientas de control remoto y otros programas potencialmente peligrosos.
1.1.7	El antivirus deberá ser estable, de tal forma que no afecte ni deteriore el rendimiento de la máquina y otros aplicativos o software que estén instalados en la misma.
1.1.8	El antivirus debe tener la capacidad de generar reglas para evitar que programas de software malicioso alteren, abran, eliminen llaves y valores del registro.
1.1.9	El antivirus debe permitir aseguramiento de archivos, carpetas, elementos compartidos y evitar el desbordamiento de buffer.

1.1.10	El antivirus debe tener la capacidad de poder configurar procesos de alto riesgo, bajo riesgo y procesos predeterminados, generando distintas propiedades de exploración de virus para los diferentes tipos de procesos.
1.1.11	El antivirus debe permitir el acceso, en demanda, en segundo plano, proactivo, sub-sistema de prevención de brotes de virus y filtrado de contenido, protección sobre los protocolos HTTP, FTP y SMTP.
1.1.12	El antivirus debe contar con un módulo de exploración en tiempo real, el cual ofrezca protección continua frente a los virus que llegan a través de dispositivos de almacenamiento extraíbles, en la red y de las diversas fuentes en INTERNET.
1.1.13	El antivirus debe tener la capacidad de explorar los procesos que están corriendo en memoria.
1.1.14	El antivirus debe tener el control de la utilización de la CPU para tareas de exploración en demanda.
1.1.15	El antivirus debe explorar múltiples formatos de compactación de archivos (zip, rar, tar, gzip entre otros).
1.1.16	El antivirus debe tener la capacidad de configurar tareas calendarizadas de revisión y limpieza del sistema de archivos.
1.1.17	El antivirus debe tener la capacidad de poder configurar una segunda opción de actualización de firmas, en caso de que la primera opción falle.
1.1.18	El antivirus debe tener la capacidad para analizar Scripts de Java Script y VBScript antes de que se ejecuten.
1.1.19	El motor de exploración deberá utilizar distintas tecnologías de detección antivirus: Exploración de firmas y exploración heurística. La exploración de firmas busca un conjunto de código hexadecimal característico de cada virus y la exploración heurística busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos.
1.1.20	Por cada producto se debe entregar la última versión disponible en el mercado que esté soportada por la casa matriz o fabricante.
1.1.21	El antivirus debe proteger la plataforma de correo electrónico que actualmente posee la entidad Exchange Server Versión 2007, 2012 o Superior.
1.1.22	Anti-Virus de Archivos, Anti-Virus de Correo, Anti-Virus Web, Anti-Hacker, Anti malware de mensajería instantánea Spyware blocker, Defensa Proactiva, Remoción de Malware.
1.1.23	Integrarse con Microsoft Outlook, bloquear publicidad (banners, ventanas emergentes "popup"), dialers y proteger contra phishing, Protección en tiempo real para servidores de correo Exchange 2007, 2010 o superior, El antivirus de servidor de correo debe permitir bloqueo de subject o direcciones de correo personalizados.
1.2	**FUNCIONALIDAD DE LA CONSOLA DE ADMINISTRACIÓN ANTIVIRUS.**
1.2.1	Debe disponer de un filtrado de vistas de las estaciones de trabajo y servidores instalados.
1.2.2	Posibilidad de realizar detección del sistema operativo de cualquier equipo que tenga el antivirus instalado.
1.2.3	La consola debe seleccionar los eventos clasificándolos por críticos informativos y de error.
1.2.4	Detección y bloqueo remoto de equipos infectados, no permitiéndole mayor comunicación con la red.
1.2.5	La consola administrativa debe tener la capacidad de administrar y forzar políticas de seguridad del antivirus directamente a los productos antivirus instalados en los servidores y estaciones de trabajo.
1.2.6	La consola administrativa debe tener la capacidad de descargar las actualizaciones desde Internet a través de los protocolos FTP y/o HTTP, colocándolas en múltiples repositorios distribuidos donde los clientes puedan buscar las definiciones localmente ahorrando ancho de banda.
1.2.7	La consola administrativa debe tener la capacidad de programar las actualizaciones para que sean realizadas en diferentes momentos y horas específicas (diaria, semanal, mensual, cuando la máquina este inactiva, inmediatamente, entre otras).
1.2.8	La consola administrativa debe tener la capacidad de cambiar la configuración, programación de tareas exploración, tareas de actualización, parametrización de la exploración en tiempo real, determinación de acciones ante la detección de un virus y alertas de todas las estaciones.
1.2.9	La consola debe correr sobre un motor de bases de datos donde se encuentre almacenada toda la información acerca del funcionamiento del producto en los servidores y estaciones de trabajo de la red.
1.2.10	La consola administrativa debe mostrar información de todos los ataques generados por estaciones y servidores desplegados en forma gráfica y en detalle.

1.2.11	La consola debe generar informes que permitan realizar un seguimiento del funcionamiento de las medidas antivirus en la institución.
1.2.12	La consola administrativa debe tener la facilidad de integrarse al Directorio Activo de Microsoft, de tal forma que se puedan heredar los grupos y unidades organizacionales.
1.2.13	La consola administrativa debe tener la capacidad de actualizar automáticamente los archivos de definiciones de virus, motor antivirus, ficheros de firmas y actualizaciones del producto antivirus de forma: automática, centralizada e incremental.
1.2.14	La consola administrativa debe ofrecer la generación de reportes gráficos y en detalle en tiempo real que reflejen la situación referente a: **Infecciones**: Virus detectados, archivos implicados, fecha y hora, en que máquinas y las acciones que tomo el producto antivirus (eliminar, limpiar y/o cuarentena, etc.) **Cubrimiento**: Máquinas actualizadas, versiones de productos antivirus de toda la red, de tal forma que se minimice la aparición de brotes de virus por máquina sin actualizar o desprotegidas.
1.2.15	La consola administrativa debe detectar o importar automáticamente las máquinas de la red que van a ser administradas.
1.2.16	La consola administrativa debe proveer la siguiente información de cada una de las máquinas administradas: • Nombre Máquina • Dirección IP • Tipo de SO • Plataforma del SO (Server, Workstation) • Producto antivirus instalado • Versión del producto antivirus instalado • Versión de las firmas de virus • Versión del motor de exploración de virus.
1.2.17	La consola administrativa debe ofrecer una manera centralizada de desplegar el antivirus a las estaciones de trabajo y servidores.
1.2.18	La consola administrativa debe tener la capacidad de que las estaciones de trabajo y servidores tomen la actualización de su sitio más cercano de acuerdo a política definida.
1.2.19	La consola administrativa debe tener la capacidad de configurar los repositorios del software antivirus de una forma centralizada o distribuida para evitar impacto en el ancho de banda cuando se va a realizar la distribución del software antivirus a sitios remotos.
1.2.20	La herramienta administrativa debe tener la capacidad de realizar labores de mantenimiento a la base de datos.
1.2.21	La consola administrativa deberá permitir realizar respaldo de las políticas o directivas implementadas en la consola de administración.
1.2.22	Capacidad para remover remotamente soluciones antivirus (propias o de terceros) que esté presente en las estaciones y servidores.
1.2.23	Capacidad de instalar remotamente la solución de antivirus en las estaciones y servidores Windows a través de recursos administrativos, Login scripts, GPO de Active Directory o medios removibles.
1.2.24	Capacidad de analizar la estructura de Active Directory para descubrir equipos
1.2.25	Capacidad de monitorear diferentes subredes para encontrar equipos no administrados.
1.2.26	Capacidad de monitorear grupos de trabajo para descubrir equipos no administrados.
1.2.27	Capacidad de que una vez que el equipo fue detectado en Active Directory, Sub red o grupo de trabajo, sea reubicado a la estructura administrativa de la consola de acuerdo a reglas personalizables. De ser necesario debe instalar el agente y/o antivirus automáticamente.
1.3	**FUNCIONALIDAD ANTIVIRUS EN WINDOWS SERVER**
1.3.1	Disponer de un motor antimalware o antispyware que detecte infecciones y analice virus, gusanos, y otras amenazas ubicadas en los servidores.
1.3.2	Anticiparse a los virus desconocidos e intrusos de una manera proactiva.
1.3.3	Actualización diaria, incremental y automáticamente del archivo de identificadores de virus, así como de las

	reglas de detección de patrones de comportamiento de los nuevos virus.
1.3.4	Gestión centralizada y remota de la red con múltiples vistas gráficas de los servidores para un fácil reparto de las tareas entre los administradores.
1.3.5	Posibilidad de exclusión del análisis de extensiones o ficheros no deseados.
1.3.6	Posibilidad de elegir el nivel de carga en los análisis programados.
1.3.7	Análisis de ficheros comprimidos en varios niveles de compresión.
1.3.8	En los casos que un fichero no se pueda desinfectar, en análisis de tiempo real o bajo demanda, debe permitir renombrar, borrar y/o enviar a cuarentena dicho fichero.
1.3.9	Informes claros, concisos y detallados e integrados con la consola de administración, pudiéndose ordenar o borrar.
1.3.10	Monitorización tanto del tiempo real, como los realizados bajo demanda y programado.
1.4	**FUNCIONALIDAD DEL ANTIVIRUS PARA ESTACIONES DE TRABAJO**
1.4.1	Disponer de un motor antimalware que detecte infecciones y analice virus, gusanos, spyware y otras amenazas ubicadas en las estaciones de trabajo.
1.4.2	Debe estar diseñado para optimizar el rendimiento de los equipos y el consumo de ancho de banda.
1.4.3	Proteger las estaciones contra infección a través de disquetes, descargas de internet, archivos adjuntos de e-mail, redes, archivos compartidos, CD-ROM's, USB, dispositivos extraíbles y servicios en línea.
1.4.4	El antivirus debe ser instalado en cada estación de forma centralizada desde los servidores, sin tener que pasar puesto por puesto.
1.4.5	El antivirus debe ser configurable la acción a tomar ante la detección de virus, tales como: Preguntar al usuario, limpiar, borrar, denegar acceso, e inclusive manejar carpeta de cuarentena para archivos infectados que se detecten a través de reglas y lista predefinidas y/o personalizadas por el administrador.
1.4.6	El antivirus debe tener la capacidad de generar exclusiones por nombre de archivos, carpetas y tipos de archivos.
1.4.7	El antivirus debe contar con medidas de seguridad para que el usuario cliente no pueda modificar políticas corporativas efectuadas desde la consola de administración.
1.4.8	El antivirus debe ser capaz de detectar el 100% de los virus conocidos (reportados en listas), contra programas malignos especificados.
1.4.9	El antivirus debe contar con un componente que permita explorar mensajes, archivos adjuntos y carpetas públicas, carpetas personales de todo tipo de correo, almacenadas localmente, mensajes de correo electrónico entrante y saliente, los archivos deben ser revisados en tiempo real y/o por demanda. (Como MS Outlook y Lotus domino), directamente sobre la estación de trabajo.
1.4.10	El antivirus debe contar con un módulo de exploración bajo demanda que permita iniciar una exploración en cualquier momento, especificar los objetivos (discos duros, disquetes, carpetas, memoria, unidades extraíbles) y las exclusiones de la exploración, así como también determinar cómo debe responder el explorador cuando detecte un virus y ver informes detallados.
1.4.11	El antivirus debe tener la opción de realizar actualización diaria, incremental y automática, el archivo de identificadores de virus, así como de las reglas de detección de patrones de comportamiento de los nuevos virus.
1.4.12	Debe anticiparse a los virus desconocidos e intrusos mediante herramientas que supervisen los procesos en ejecución en busca de comportamientos maliciosos.
1.4.13	Filtrado de contenidos para discriminar los correos en base a sus elementos y protección antispam.
1.4.14	Tener la capacidad de detectar malware en base a las acciones que el proceso solicita del sistema operativo.
1.4.15	El antivirus debe tener la capacidad de detectar, detener y eliminar códigos o aplicaciones maliciosas como gusanos o troyanos, spyware, ad-ware, keyloggers y programas potencialmente peligrosos.
1.4.16	El antivirus debe contar con un sistema de alertas el cual envíe notificaciones inmediatamente, siempre que el explorador detecte un virus en el computador por medio de correo electrónico, capturas de SNMP, enviar alertas al registro del sistema (Log de Eventos de Windows) y mensajes de red.
1.4.17	Pluging de correo que proporcione detección y desinfección al inicio, bajo demanda y con un residente en buzones de correo de Outlook y Outlook Express.

1.4.18	El antivirus deberá detectar virus en el correo electrónico incluso dentro de archivos comprimidos.
1.4.19	Proteger contra códigos hostiles, tales como ActiveX o aplicaciones Java, permitir configurar la detección sobre todos los archivos o tipo de archivos comprimidos (cualquier formato de compresión, rar, zip, cab, arj, arz entre otrs), ocultos y archivos en ejecución.
1.4.20	Bloqueo de servicios (ftp, http, etc.) y puertos de comunicaciones (puerto 25 para SMTP).
1.4.21	Análisis heurísticos.
1.4.22	Posibilidad de exclusión del análisis de extensiones o ficheros no deseados.
1.4.23	En los casos que un fichero no se pueda desinfectar, en tiempo real o bajo demanda, debe permitir renombrar, borrar y/o enviar a cuarentena dicho fichero.
1.4.24	Informes detallados con los datos referentes a la detección de virus tanto en tiempo real como en análisis bajo demanda y programado.
1.4.25	Monitoreo de programas de mensajería instantánea, analizando todos los datos adjuntos transmitidos.
1.4.26	El agente debe ser flexible en la instalación por medio de login script, ejecutable y/o vía remota.
1.4.27	Se debe realizar un análisis en tiempo real en los dispositivos extraíbles antes de tener acceso a ellos una vez conectado.
1.5	**FUNCIONALIDAD DEL ANTIVIRUS PARA SERVIDORES EXCHANGE**
1.5.1	Debe incluir políticas corporativas que garanticen un filtrado de contenidos por asunto, cuerpo, nombre del fichero adjunto o extensión del fichero y ser capaz de hacer frente al spam y los ataques de phising identificando, bloqueando y destruyendo el correo no solicitado antes de llegar a los buzones de sus destinatarios.
1.5.2	Actualización diaria, incremental y automática del archivo de Identificadores de virus, para una protección contra aquellos virus y correos basura aparecidos desde la última actualización.
1.5.3	Debe vigilar los mensajes que utilizan los protocolos POP3 y SMTP.
1.5.4	Debe tener un sistema de notificación de infecciones y alertas en tiempo real, totalmente configurable.
1.5.5	Monitorización de análisis en tiempo real y bajo demanda.
1.5.6	Debe proteger tanto el correo entrante y saliente, como la copia de mensajes a las carpetas públicas.
1.5.7	La consola de administración debe permitir la instalación, configuración y mantenimiento de varios servidores simultáneamente.
1.5.8	Análisis y desinfección de mensajes anidados a cualquier nivel de anidamiento.
1.6	**FUNCIONALIDAD PREVENCIÓN DE INTRUSOS Y FIREWALL EN HOST**
1.6.1	La solución debe ser administrada desde la misma consola que administra todas las soluciones de antivirus, antispyware.
1.6.2	Reconocimiento de anomalías, detección y bloqueo de ataques de tipo reconocimiento ejemplo: Host Sweep, TCP or UDP port Scan, CGI Holes.
1.6.3	Detección de ataques de tipo Exploits hacia vulnerabilidades de sistema operativo como también de aplicaciones diferentes de Microsoft
1.6.4	La solución debe incluir un sistema de detección y prevención de intrusos basados en host que proteja los recursos del sistema y las aplicaciones de ataques internos y externos.
1.6.5	Debe ofrecer protección frente a la puesta en peligro de los recursos del sistema, de la red, de las aplicaciones que almacenan y proporcionan información.
1.6.6	La solución de prevención de intrusos debe integrarse totalmente con la consola general de administración del antivirus sin necesidad del uso de consolas adicionales.
1.6.7	La solución debe contar con un Firewall personal (Cortafuegos).
1.6.8	La solución debe proporcionar un módulo de bloqueo de aplicaciones para proporcionar un mayor nivel de protección, seguridad y control a los usuarios.
1.6.9	Debe brindar la posibilidad de crear y asignar directivas IPS independientes a varios dominios, sitios, grupos y nodos. La asignación de directivas puede heredarse de una directiva principal y ser editada o aplicarse directamente sobre una estación de trabajo o servidor.
1.6.10	La solución debe permitir realizar una validación de seguridad por niveles de tal forma que pueda realizar un

	seguimiento de los posibles ataques.
1.6.11	El módulo de firewall debe incluir un método de aprendizaje en el que se registre la actividad en cada máquina y sea opcional para el administrador el permitir o denegar dichas conexiones.
1.6.12	El modulo debe permitir su configuración desde la consola principal de administración del antivirus y tener un módulo de reportes propietario en dicha consola para revisión de administrador.
1.6.13	El firewall personal debe tener la opción de permitir o denegar el tráfico entrante, saliente o en ambas direcciones, en conexiones originadas por cualquier puerto local y con destino a cualquier puerto remoto.
1.6.14	El firewall personal debe tener la opción de bloquear tráfico a nivel de aplicación.
1.6.15	Las reglas creadas en el firewall personal deben tener la opción de habilitarse o deshabilitarse.
1.6.16	Permitir la generación de reglas para la protección para carpetas, servicios y archivos del sistema operativo.
1.6.17	Protección basada en el comportamiento que proteja los endpoints frente a las nuevas amenazas de día cero.
1.7	**FUNCIONALIDAD Y REQUISITOS DEL ANTISPYWARE**
1.7.1	El antispyware debe permitir incorporarse a consola de administración y enviar la instalación de forma automática a todas las computadoras de la red.
1.7.2	El antispyware debe Integrarse al antivirus y trabajar de forma conjunta en un solo motor.
1.7.3	El antispyware debe instalarse sobre sistema Operativo Windows XP, 7, 8, en 32 y 64 bits, incluyendo las nuevas versiones.
1.7.4	El antispyware debe escanear y bloquear en tiempo real cualquier acceso e instalación de cualquier spyware, adware, PUPs, malware, keylogger, herramientas de administración remota, Dialer, etc.
1.7.5	El antispyware debe escanear llaves del registro y eliminar las llaves creadas por los spyware o cualquier PUP sin afectar la estructura del registro a nivel de sistema operativo.
1.7.6	El antispyware debe revisar en memoria si se encuentra un spyware, adware, entre otros.
1.7.7	La solución debe ser capaz de explorar, bloquear y eliminar el Spyware de las llaves del registro de Windows y eliminación cookies.
2.1	**SERVICIOS DE IMPLEMENTACIÓN**
2.1.1	La herramienta ofertada deberá ser instalada por el contratista en todas las consolas de antivirus 520 que hay en el Concejo de Bogotá, esta actividad será realizada por el contratista. El contratista además deberá: • Instalar y configurar la consola principal, realizando el despliegue del producto en las estaciones de trabajo del Concejo de Bogotá Configurar políticas, reportes y estadísticas. • Configurar la protección sobre servidores de correo.
2.1.2	El contratista informará periódicamente vía e-mail a la entidad, acerca de los nuevos virus, suministrando los medios para combatirlos y evitar próximos ataques.
2.1.3	El contratista estará obligado a recomendar y acompañar en su implementación, los continuos afinamientos en servidores y clientes (patches, fixes, bloqueo de puertos. Etc.), que contribuyan con la minimización de riesgos y vulnerabilidades, previendo ataques de virus y/o amenazas.
2.1.4	El contratista deberá garantizar total compatibilidad con la infraestructura de red, sin degradar el rendimiento de los equipos bajo las diferentes plataformas tanto de estaciones de trabajo como de servidores e infraestructura de red que se encuentran instalados. Para lo cual deberá soportar técnicamente mediante la realización de pruebas.
2.1.5	El contratista deberá suministrar todos los equipos y software para pruebas en caso de ser necesario.
2.2	**TRANSFERENCIA DE CONOCIMIENTOS**
2.2.1	El antivirus debe incluir capacitación al personal de soporte técnico (6 personas) en el uso y administración del software antivirus.
2.2.2	Se requiere Capacitación sobre la administración del producto para el personal de Sistemas (3 personas) del Concejo de Bogotá
2.3	**LICENCIAMIENTO**
2.3.1	El software debe ser licenciado de manera perpetua a nombre del Concejo de Bogotá.
2.4	**SOPORTE Y MANTENIMIENTO**
2.4.1	El contratista deberá cumplir con el objeto del contrato, con personal idóneo calificado y certificado el cual

	debe estar conformado por ingenieros y técnicos de soporte en el producto ofertado.
2.4.2	El contratista deberá brinda una solución integral de asesoría y acompañamiento en implementación de cualquier solución de seguridad
2.4.3	Soporte técnico Online por parte de Ingenieros del Fabricante, durante el período contratado, ya sea por medio telefónico, correo electrónico o en línea -chat- (Página Web). El servicio de soporte se debe prestar en forma ininterrumpida (24hx7dx365d). El contratista deberá contar con una línea de servicio al cliente como: PBX, Celular, Call Center, Help Desk o similar de tal manera que la Entidad pueda hacer contacto con él fácilmente, para consulta o solución de problemas menores durante la ejecución del contrato.
2.4.4	La disposición del recurso humano se refiere al traslado de un (1) Ingeniero al sitio (instalaciones del Concejo de Bogotá) dentro de las tres (3) horas siguientes al reporte del incidente, bajo un modelo de servicio 5x8x3; es decir, cinco (5) días a la semana, ocho (8) horas al día y con un máximo tiempo de solución de tres (3) horas en el sitio.
2.4.5	El contratista garantizará la instalación, configuración y gestión de los productos que componen la solución de protección antivirus en la totalidad de las maquinas.
2.4.6	El Soporte y mantenimiento de las licencias de antivirus será por un término de Un (1) año a partir de la aprobación de la garantía única y será realizada por la casa matriz y/o representante en Colombia.
2.4.7	El mantenimiento y actualización debe permitir de manera proactiva y centralizada desde la consola de gestión mantener la plataforma tecnológica de la entidad debidamente asegurada, mediante actividades que permitan validar los niveles de actualización y cobertura de los productos implementados en todas las estaciones y servidores que tengan conectividad con la consola, y atender los requerimientos de los usuarios ante posibles ataques de virus, y también se incluye la planeación y ejecución de pilotos para nuevas funcionalidades y productos liberados por el fabricante, previo acuerdo con el supervisor del contrato.
2.4.8	El software antivirus debe tener representación en Colombia y adicionalmente el contratista debe tener la certificación como canal del fabricante del software.
2.5	**GARANTÍA**
2.5.1	La garantía debe iniciar a partir de la fecha del acta de recibido a satisfacción de la solución, emitida por el supervisor del contrato, por un término igual al derecho de las actualizaciones Un (1) año.
2.5.2	De presentarse un brote de virus, infección de equipos por algún virus, clase o subclase de éste, el contratista debe garantizar la correcta eliminación del virus de los equipos infectados y/o de la red en un plazo máximo cuatro (4) horas después de haberse realizado el reporte y solicitado el soporte, garantizando que estos quedaran en perfecto funcionamiento.
2.5.3	El contratista debe garantizar que el soporte, y el mantenimiento se realizará por personal capacitado y certificado en el producto ofrecido.
2.5.4	Garantizar la instalación de las nuevas versiones que sean liberadas por casa matriz durante el tiempo de vigencia de la garantía de calidad y correcto funcionamiento
2.6	**CENTROS MAYORISTAS AUTORIZADOS DE SERVICIO**
2.6.1	Con el fin de garantizar a la entidad: La calidad del servicio, el personal calificado y entrenado para el soporte del software, la garantía por fallas y/o errores de implementación y la atención satisfactoria durante la ejecución del contrato, la firma responsable deberá manifestar que el fabricante cuenta con un (1) centro mayorista autorizado de servicio en Bogotá D.C.
2.6.2	Además, deberá presentar una autorización expresa del fabricante al momento de la firma del acta de inicio del contrato, para que la entidad pueda utilizar este centro, sin costo alguno, cuando el contratista incumpla las condiciones del plan de garantía. Lo anterior, no exonera al contratista de la responsabilidad que le atañe, ni de las multas a que se hiciera acreedor.
2.7	**RESPALDO DE OTROS CANALES**
2.7.1	El fabricante deberá tener respaldo directo en Colombia, permitiéndole a la entidad la selección de otro canal

	especializado que pueda garantizar la calidad del servicio, el personal calificado y entrenado para el soporte del software y llevar a cabo la garantía por fallas y/o errores de implementación y atención satisfactoria durante la ejecución del contrato.
2.7.2	En el periodo de ejecución del contrato se deben realizar tres (3) mantenimientos preventivos al servicio contratado. Las actividades que se deben realizar en el mantenimiento son: verificación y/o actualización de las versiones de los productos, verificación y/o ajuste de parámetros de configuración de la herramienta, verificación y/o ajuste de los reportes de información programados.

3.1 OBLIGACIONES GENERALES DEL CONTRATISTA

1 Acatar la Constitución, la ley, las normas legales y procedimentales establecidas por el Gobierno Nacional y Distrital, y demás disposiciones pertinentes.

2 Cumplir lo previsto en las disposiciones de las especificaciones esenciales, así como en la propuesta presentada.

3 Dar cumplimiento a las obligaciones con los sistemas de seguridad social., salud, pensiones y aportes parafiscales, cuando haya lugar, y presentar los documentos respectivos que así lo acrediten, conforme lo establecido por el artículo 50 de la Ley 789 de 2002, la Ley 828 de 2003, la Ley 1122 de 2007, Decreto 1703 de 2002, Decreto 510 del 5 de marzo de 2003, artículo 23 de la ley 1150 de 2007, Ley 1562 de 2012 y demás normas que las adicionen, complementen o modifiquen.

4 Dentro de los cinco (5) días hábiles siguientes a la fecha en que se le entregue la copia del contrato y las instrucciones para su legalización, deberá constituir las garantías pactadas en el contrato.

5 Garantizar la calidad de los servicios contratados y responder por ello.

6 Colaborar con la entidad contratante para que el objeto contratado se cumpla y que este sea el de mejor calidad.

7 Acatar las órdenes que durante el desarrollo del contrato la entidad le imparta, y de manera general, obrar con lealtad y buena fe en las distintas etapas contractuales evitando las dilaciones y entrabamiento que pudieran presentarse.

8 Reportar de manera inmediata cualquier novedad o anomalía, al supervisor o interventor del contrato, según corresponda.

9 Guardar total reserva de la información que por razón del servicio y desarrollo de sus actividades obtenga. Esta es de propiedad de la Secretaría Distrital de Hacienda de Bogotá, D.C. y sólo salvo expreso requerimiento de autoridad competente podrá ser divulgada.

10 Acatar las instrucciones que durante el desarrollo del contrato le imparta La Secretaría Distrital de Hacienda de Bogotá, D.C por conducto del supervisor o interventor del contrato.

11 Responder por la conservación, el uso adecuado, deterioro o pérdida de los elementos en el evento en que le sean entregados por la entidad para la prestación del servicio.

12 Suscribir y cumplir durante la ejecución del contrato la declaración de aceptación de "POLÍTICAS DE USO Y SEGURIDAD DE LA TECNOLOGÍA DE INFORMACIÓN DE LA SECRETARÍA DISTRITAL DE HACIENDA, previa a la asignación de usuario y el otorgamiento de permisos para la utilización de servicios informáticos, que tienen como fin salvaguardar y preservar la integridad, confidencialidad, oportunidad y disponibilidad de la información.

13 En cumplimiento de la Directiva Distrital No. 003 de 2012 el contratista se obliga a: a) Velar por el respeto de los derechos constitucionales y laborales de los trabajadores que utilice para la ejecución del contrato, para lo cual, eliminará formas de contratación lesivas para los derechos laborales de los trabajadores. b) Velar por el respeto de la legislación laboral vigente e incentivar la mejor oferta laboral y prestacional que garantice el acceso a mejores oportunidades de trabajo. El incumplimiento de las obligaciones contractuales incluidas en el presente numeral, ocasionará el inicio de procesos sancionatorios, conforme con la normatividad vigente, esto es, la imposición de multas o la declaratoria de incumplimiento haciendo efectiva la cláusula penal pecuniaria, si es del caso.

14 Dar cumplimiento a lo dispuesto en la Circular No. 1 de 2011 de fecha19 de enero DE 2011, expedida por el Alcalde Mayor de Bogotá D.C., en el sentido de no contratar a menores de edad, en cumplimiento de los pactos, convenios y convenciones internacionales ratificados por Colombia, según lo establece la Constitución Política de 1991 y demás normas vigentes sobre la materia, en particular aquellas que consagran los derechos de los niños.

3.2. OBLIGACIONES ESPECIALES DEL CONTRATISTA.

1. Cumplir a cabalidad el objeto del presente contrato, en los términos y condiciones señaladas en el mismo.
2. El contratista realizará la entrega del documento de adquisición de las licencias en las instalaciones del Concejo de Bogotá, dentro de los diez (10) días hábiles a partir de la fecha de inicio del contrato.
3. Asumir los costos de transportes, fletes, seguros y similares, que se ocasionen en razón de la entrega de los bienes suministrados.
4. El contratista deberá cumplir con el soporte telefónico y remoto ilimitado durante los doce (12) meses destinados para la ejecución del contrato, sobre la solución, en la modalidad 24hx7dx365d, sin costo adicional durante la vigencia del contrato.
5. El contratista brindará soporte y mantenimiento en sitio sobre la solución en la modalidad 5x8 en un máximo de tiempo de 3 horas, a solicitud del Concejo de Bogotá, las veces que sea requerido durante el tiempo de vigencia del contrato.
6. El contratista deberá atender todos los servicios correctivos necesarios para mantener la solución del software de protección y seguridad, objeto del contrato en condiciones normales de funcionamiento las veces que sea necesario durante la vigencia del contrato.
7. El contratista deberá actualizar nuevas versiones del software antivirus sin ningún costo para la entidad.
8. El contratista realizará la actualización, activación de las licencias, software, firmas y/o bases de datos requeridas para el óptimo funcionamiento de los sistemas especificados, durante el plazo de ejecución del contrato.
9. El contratista deberá proveer personal Calificado (Certificado en el producto a contratar) para cumplir con los mantenimientos preventivos y correctivos, durante el plazo de ejecución del contrato.
10. El contratista se compromete a mantener en forma confidencial todos los datos e información a los cuales tuviere acceso durante la ejecución del contrato. Esta confidencialidad será continua y no vence ni por terminación, ni por caducidad del contrato. La violación de ésta obligación dará lugar a la terminación unilateral por parte del Concejo de Bogotá.
11. El contratista deberá entregar la documentación, manuales técnicos, informes de logs, vulnerabilidades, ataques, recomendaciones, entre otros, en cada visita de actualización, mantenimiento preventivo y/o correctivo.
12. El contratista deberá contar con los mecanismos de redundancia y contingencia cuando se esté ejecutando una labor de mantenimiento.
13. Atender los mantenimientos preventivos acordados durante la ejecución del contrato.
14. El contratista tomará todas las medidas preventivas para la correcta ejecución de las actividades necesarias en el cumplimiento del objeto del contrato, tendientes a minimizar cualquier daño a equipos, enseres y bienes en general. En caso de presentarse daño alguno, el contratista está en la obligación de repararlo.
15. Mantener los precios unitarios fijos durante la ejecución del contrato
16. El contratista realizará la capacitación respectiva una vez se realice la instalación de las licencias de antivirus, al personal que designe el Concejo de Bogotá.
17. El contratista deberá contar con personal suficiente que se encuentre calificado técnicamente en el conocimiento y manejo del software antivirus, para atender los servicios solicitados por la Entidad.
18. Establecer en conjunto con el supervisor del contrato o quien éste designe el cronograma de mantenimientos preventivos, una vez instalada y puesta en funcionamiento la solución de antivirus.
19. Los mantenimientos preventivos se realizaran uno cada cuatro meses, para lo cual el contratista deberá adjuntar el soporte de las actividades efectuadas en dicho mantenimiento

3.3. OBLIGACIONES ESPECIALES DEL SUPERVISOR

El supervisor además de las funciones establecidas en el procedimiento de Supervisión e Interventoría, 38.P-01, tendrá las siguientes:

1 Proporcionar los medios logísticos y respectivas autorizaciones que se requieran para que el contratista pueda desarrollar las actividades objeto del contrato.

4. FUNDAMENTOS QUE SOPORTAN LA MODALIDAD DE SELECCIÓN.

Efectuado el análisis de que trata el numeral ***6 "Condiciones Generales"*** del procedimiento 37-P.01, se determinó que corresponde a la modalidad de **SELECCIÓN DE MINIMA CUANTIA**, de conformidad con lo establecido en el artículo 94 de la Ley 1474 de 2011 y mediante el procedimiento establecido en el Título III capítulo V del Decreto Reglamentario 734 de 2012.

5. JUSTIFICACIÓN DE CAPACIDAD FINANCIERA COMO REQUISITO HABILITANTE.

Por la naturaleza del contrato, las obligaciones que se derivan del mismo y el presupuesto asignado, se considera necesario solicitar capacidad financiera como requisito habilitante, con el fin de proveer la solvencia económica del contratista que le permita la ejecución de requisitos y condiciones previamente acordados en la relación contractual y como consecuencia se garantice el adecuado desarrollo del contrato.

6. EL ANÁLISIS QUE SUSTENTA LA EXIGENCIA DE MECANISMOS DE COBERTURA DEL RIESGO QUE GARANTIZAN LA SERIEDAD DEL OFRECIMIENTO, EL CUMPLIMIENTO DE LAS OBLIGACIONES QUE SURJAN DEL CONTRATO Y DE SU LIQUIDACIÓN Y LA RESPONSABILIDAD EXTRACONTRACTUAL.

6.1 EL ANÁLISIS QUE SUSTENTA LA EXIGENCIA DE GARANTÍAS DESTINADAS A AMPARAR LOS PERJUICIOS DE NATURALEZA CONTRACTUAL O EXTRACONTRACTUAL, DERIVADOS DEL OFRECIMIENTO.

Cada proponente deberá constituir a favor de BOGOTA D. C.- SECRETARIA DISTRITAL DE HACIENDA, con NIT. 899.999.061-9, una garantía de seriedad de la propuesta y su vigencia será por el término mínimo de tres (3) meses, contados a partir de la fecha de cierre del presente proceso.

La garantía de seriedad se constituirá por un valor igual o superior al diez por ciento (10%) del valor total del presupuesto oficial.

6.2 EL ANÁLISIS QUE SUSTENTA LA EXIGENCIA DE GARANTÍAS DESTINADAS A AMPARAR LOS PERJUICIOS DE NATURALEZA CONTRACTUAL O EXTRACONTRACTUAL, DERIVADOS DEL INCUMPLIMIENTO DEL CONTRATO.

Para garantizar las obligaciones que se adquieren en virtud del contrato, el contratista otorgará a favor del DISTRITO CAPITAL – SECRETARÍA DISTRITAL DE HACIENDA, una garantía que ampare los siguientes riesgos:

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE HACIENDA

ESTUDIOS Y DOCUMENTOS PREVIOS
CONTRATACIÓN DE MÍNIMA CUANTÍA

El principal riesgo que se puede presentar en la ejecución del objeto contractual es que el contratista no cumpla a cabalidad con las obligaciones establecidas en el contrato, para lo cual éste deberá constituir el amparo de ***Cumplimiento*** por el treinta por ciento (30%) del valor del contrato, vigente por el término de ejecución del mismo y cuatro (4) meses más. Este amparo debe constituirse a partir de la fecha de suscripción del contrato y debe garantizar el cumplimiento del contrato, el pago de la cláusula penal y de las multas.

Otro de los riesgos que se podrían presentar en esta contratación es que el servicio no se cumpla bajo los parámetros establecidos en el contrato y en la Invitación Pública, por lo que constituye un riesgo que debe ser amparado mediante la cobertura de ***Calidad del Servicio***, el cual deberá establecerse por el diez por ciento (10%) del valor total del contrato, vigente por el término de ejecución del mismo y cuatro (4) meses más.

Calidad de los bienes suministrados (Calidad y correcto funcionamiento de los bienes suministrado): Para garantizar la calidad y correcto funcionamiento de los bienes suministrados que pueden presentar eventuales defectos durante la ejecución de las obligaciones derivadas del contrato, el cual deberá establecerse por el diez por ciento (10%) del Valor total de los bienes suministrados, vigente por el termino de ejecución del mismo y cuatro (4) meses más.

La Secretaría Distrital de Hacienda al responder solidariamente con el contratista frente al cumplimiento en el pago de salarios y prestaciones sociales del personal asignado al contrato, considera que un riesgo que se puede presentar en esta contratación es que el contratista no cumpla con dichas obligaciones, por tanto es necesario amparar dicho riesgo mediante la cobertura De ***Salarios, Prestaciones Sociales e indemnizaciones laborales***: Por el cinco por ciento (5%) del valor total del contrato, vigente por el plazo de ejecución del mismo y tres (3) años más.

Se debe proteger patrimonialmente a la Entidad frente a los daños que se pueden producir a terceros con ocasión de la ejecución del objeto contractual, para lo cual se debe constituir una póliza de Responsabilidad Civil Extracontractual la cual deberá establecerse por el valor equivalente a 200 SMLV, vigente por el término de ejecución del contrato, con los siguientes amparos, límites y porcentajes, según lo establecido en el Articulo 5.2.1.2.2 del Decreto 0734 de 2012.

Amparos y porcentajes de cobertura: Conforme al Artículo 5.2.1.2.2. Del decreto 0734 de 2012 y la póliza de Responsabilidad Civil Extracontractual deberá contener como mínimo los siguientes amparos señalados, en adición de la cobertura básica de Predios, Labores y Operaciones recomendamos los siguientes:

Asegurado: La Entidad y el Contratistas y/o Subcontratistas
Beneficiario: La Entidad y los terceros afectados

CONTRATO: Adquisición, mantenimiento y soporte de las licencias de software antivirus para la plataforma del Concejo de Bogotá.			**38.857.551**	
Cobertura Mínimas Recomendadas		**% Recomendado de Cobertura**	**Vr. Asegurado Evento**	**Vr. Asegurado Vigencia**
Predios, Labores y Operaciones - PLO	Mínimo	MINIMO 200 smmlv	117.900.000	117.900.000
Daño Emergente y Lucro Cesante	Mínimo	10% Del valor del PLO evento y 20% vigencia	11.790.000	23.580.000
Perjuicios Extra patrimoniales	Mínimo	10% Del valor del PLO evento y 20% vigencia	11.790.000	23.580.000

ESTUDIOS Y DOCUMENTOS PREVIOS
CONTRATACIÓN DE MÍNIMA CUANTÍA

Contratistas y Subcontratistas	Mínimo	10% del valor del PLO por Evento y 20% del valor del PLO por vigencia.	11.790.000	23.580.000
Amparo Patronal	Mínimo	10% del valor del PLO por Evento y 20% del valor del PLO vigencia.	11.790.000	23.580.000
Vehículos Propios y No Propios	Mínimo	10% del valor del PLO por Evento y 20% del valor del PLO vigencia.	11.790.000	23.580.000
*Bienes bajo Cuidado Tenencia y Control	Mínimo	10% del valor de PLO por evento / 20%del valor del PLO vigencia.	11.790.000	23.580.000
**Responsabilidad Civil Cruzada	Mínimo	10% del valor del PLO por evento / 20%del valor del PLO vigencia.	11.790.000	$ 23.580.000
Gastos Médicos		$3 millones por persona / 12 millones por evento y 20 millones por vigencia.	$ 12.000.000	$ 20.000.000

Es necesario que en el contrato se establezca que los deducibles de la póliza deben ser asumidos por el contratista y no por la Entidad, e igualmente debe incluir las siguientes cláusulas:

- Revocación de la póliza a 60 días, con previo aviso a la Entidad
- Ampliación de aviso de siniestro a 30 días
- Restablecimiento automático del valor asegurado por ocurrencia de siniestro por una vez
- No cancelación o revocación por no pago de prima

De acuerdo con el análisis anterior la garantía debe cubrir los siguientes amparos:

Modalidad	Porcentaje	Vigencia de amparos
Cumplimiento de las obligaciones surgidas del contrato estatal incluyendo el pago de multas y cláusula penal pecuniaria	Por el 30 % del valor total del contrato.	El término de ejecución del contrato más 4 meses.
Calidad y correcto funcionamiento de los bienes suministrados	Por el 10 % del Valor total de los bienes suministrados	El término de ejecución del contrato más 4 meses.
Responsabilidad Extracontractual1	Por el equivalente a 200 SMLV.	El termino de ejecución del contrato.

Modalidad	Porcentaje	Vigencia de amparos
Calidad del servicio	Por el 10% del Valor total de los servicios prestados	El término de ejecución del contrato más 4 meses.
Pago de Salarios, prestaciones sociales e indemnizaciones laborales.	Por el 5% por ciento del valor total del contrato	El término de ejecución del contrato y 3 años.

[1] La Póliza de Responsabilidad Extracontractual sólo puede ser amparada mediante póliza de seguro y debe cumplir con los requisitos establecidos en el Art. 5.2.1.2° del Decreto Reglamentario 734 de 2012.

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE HACIENDA

ESTUDIOS Y DOCUMENTOS PREVIOS
CONTRATACIÓN DE MÍNIMA CUANTÍA

Las clases de garantías, los riegos a amparar derivados del incumplimiento del contrato, el cubrimiento de otros riesgos y la suficiencia de la garantía están consagradas en el Decreto Reglamentario 734 de 2012.

7. EL SOPORTE QUE PERMITA LA TIPIFICACIÓN, ESTIMACIÓN Y ASIGNACIÓN DE LOS RIESGOS PREVISIBLES QUE PUEDAN AFECTAR EL EQUILIBRIO ECONÓMICO DEL CONTRATO.

Decreto 734 de 2012, dispone:

*"**Artículo 2.1.2. Determinación de los riesgos previsibles.** Para los efectos previstos en el artículo 4° de la Ley 1150 de 2007. se entienden como riesgos involucrados en la contratación todas aquellas circunstancias que de presentarse durante el desarrollo y ejecución del contrato, tienen la potencialidad de alterar el equilibrio económico del contrato, pero que dada su previsibilidad se regulan en el marco de las condiciones inicialmente pactadas en los contratos y se excluyen así del concepto de imprevisibilidad de que trata el artículo 27 de la Ley 80 de 1993. El riesgo será previsible en la medida que el mismo sea identificable y cuantificable en condiciones normales. ...(...)"*

En las modalidades de Licitación Pública, Selección Abreviada y Concurso de Méritos, la entidad deberá tipificar en el proyecto de pliego de condiciones, los riesgos que puedan presentarse en el desarrollo del contrato, con el fin de estimar cualitativa y cuantitativamente la probabilidad e impacto, y señalará el sujeto contractual que soportará, total o parcialmente, la ocurrencia de la circunstancia prevista en caso de presentarse, a fi de preservar las condiciones iniciales del contrato.

De lo anterior concluye el área de origen que la contratación que se pretende celebrar, no se encuentra incluida dentro de la norma citada, en el entendido de que la misma se trata de una contratación de mínima cuantía, por lo cual no se hace necesaria la emisión de la matriz de estimación, tipificación y asignación de riesgos previsibles que puedan afectar el equilibrio económico del contrato.

8. DIRECTIVA DISTRITAL No. 008 de 2012

Esta entidad distrital no ha encontrado técnicamente viable la posibilidad de incluir en estos estudios previos la obligación del contratista o asociado de vincular población beneficiaria de la Directiva Distrital No. 001 de 2011, y en consecuencia, pasa a dejar CONSTANCIA de las razones extrajurídicas de tal inviabilidad, de acuerdo con el literal c) del punto 4) de la citada Directiva, en los siguientes términos:

- El personal requerido para la ejecución de las actividades debe ser calificado, toda vez que se requiere conocimiento específico y experiencia en el manejo de este tipo de elementos y en el soporte para el servicio.

- El presente proceso de contratación no contiene características de tipo social, dado que se trata de un proceso cuyo componente es netamente tecnológico.

Lo anterior en cumplimiento, con lo establecido en la Directiva 001 de enero 31 de 2011 y Directiva 018 del 09 de septiembre de 2011.

9. RECOMENDACIÓN

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE HACIENDA

ESTUDIOS Y DOCUMENTOS PREVIOS
CONTRATACIÓN DE MÍNIMA CUANTÍA

Con la presentación de este estudio, queda evidencia de la necesidad del contrato tendiente a cumplir con los propósitos establecidos para la buena marcha y efectivo cumplimiento de los cometidos de la Secretaría Distrital de Hacienda, por consiguiente, se solicita adelantar el proceso contractual respectivo.

ÁREA DE ORIGEN	DIRECTOR DEL AREA DE ORIGEN
Nombre: **LORENA JEISEL ARIAS PINZÓN** Cargo: Subdirectora Servicios y Atención al Usuario	Nombre: **JOSE ANTONIO VALDERRAMA SANCHEZ** Cargo: Director de Sistemas e Informática

Elaboró:	Ana Vilma Quevedo
Revisó:	Lorena Jeisel Arias Pinzón