FICHA TÉCNICA

1. SOFTWARE ANTIMALWARE PARA EL CONCEJO DE BOGOTÁ D.C.	
Denominación del Bien:	Prestar los servicios de soporte, actualización y configuración de la plataforma ANTIMALWARE del Concejo de Bogotá D.C.
Denominación Técnica:	Prestar los servicios de soporte, actualización y configuración de la plataforma ANTIMALWARE del Concejo de Bogotá D.C.
Objeto:	Prestar los servicios de soporte, actualización y configuración de la plataforma ANTIMALWARE del Concejo de Bogotá D.C.

1.1 Justificación:

La Oficina de Tecnología del Concejo de Bogotá D.C., es responsable de administrar y soportar la infraestructura tecnológica de la Corporación, la cual incluye las plataformas de seguridad de la información, redes y comunicaciones. Asimismo, el Proceso de Tecnologías de la Información debe implementar, administrar y mantener la infraestructura tecnológica (hardware y software), redes y comunicaciones con el fin de garantizar la disponibilidad de la información, fortalecer el cumplimiento de las funciones misionales y administrativas de la corporación. Para ello, se debe garantizar la protección y seguridad de la información generada por los concejales y demás dependencias del Concejo de Bogotá D.C.
La seguridad informática es de gran importancia en el desarrollo de las labores diarias de toda entidad. La constante aparición y sofisticación de programas maliciosos, conocidos como malware, representan una amenaza significativa y persistente para la estabilidad y el rendimiento óptimo de los equipos de cómputo, la integridad y confidencialidad de la información, y la continuidad de las operaciones de la Corporación. Con el firme propósito de mitigar estos riesgos y fortalecer la postura de seguridad, durante el año 2024, se contó con el software antimalware *Bitdefender GravityZone Business Security* en los equipos del Concejo de Bogotá D.C.

Mantener licenciamiento del software antimalware activo es fundamental para preservar la seguridad de la infraestructura tecnológica. La renovación oportuna de este licenciamiento es crucial para asegurar que las defensas se mantengan actualizadas y sean capaces de hacer frente a las últimas y más sofisticadas amenazas cibernéticas que surgen constantemente en el panorama digital actual. Esta renovación es esencial para garantizar la continuidad ininterrumpida de las operaciones del Concejo de Bogotá D.C. Al contar con un software antimalware permanentemente actualizado, se minimiza de manera significativa el riesgo de incidentes de seguridad que podrían comprometer información sensible y la operación de la Corporación.

En el marco de la estrategia para fortalecer la gestión institucional del Concejo de Bogotá D.C., la Oficina de Tecnología de la Corporación, a través del proceso de Tecnologías de la Información, ha proyectado para la presente vigencia la renovación del licenciamiento del software antimalware Bitdefender o equivalente. Esta acción no es solo una medida preventiva, sino una necesidad para garantizar el correcto funcionamiento y la protección integral de los equipos de cómputo con los que cuenta el Concejo de Bogotá D.C.

ÍTEM	CARACTERÍSTICA	MÍNIMO REQUERIDO
2. CONDICIONES GENERALES		
2.1.	Cantidades	El contratista deberá garantizar el correcto licenciamiento del software antimalware GravityZone Business Security Enterprise o equivalente y su actualización a la última versión estable, tanto para estaciones de trabajo como para servidores y la consola de administración, incluyendo mejoras del producto y correcciones durante el tiempo de vigencia del licenciamiento, sin costo adicional para un mínimo de: • 750 estaciones de trabajo. • 70 servidores (físicos y virtuales). • 1290 buzones de correo Outlook 365. La consola y licencias de antimalware deben ser de la última versión estable y vigente del producto ofertado.
2.2.	Tiempo de vigencia del licenciamiento y/o suscripciones	Las licencias deberán estar vigentes por un término no inferior a doce (12) meses a partir de la entrega y activación efectiva de las licencias adquiridas, y no podrá traslaparse con el licenciamiento actual de la Corporación. Una vez vencido el tiempo de licenciamiento contratado, el software quedará en la Corporación, pero con las limitaciones propias de la suscripción.
2.3.	Tipo de licenciamiento	Licenciamiento y/o suscripción para entidades de Gobierno (si aplica)
2.4.	Titularidad de las licencias y/o suscripciones	Todo licenciamiento y/o suscripción deberá quedar a nombre del Concejo de Bogotá D.C., y asociado a la cuenta de correo licenciascbta@concejobogota.gov.co o la que el supervisor del contrato defina para tal fin.
2.5.	Certificados de fabricante	Con el fin de garantizar que el proponente cuenta con el debido respaldo del producto, la Corporación requiere que el Contratista sea canal autorizado para Colombia del fabricante o desarrollador de la solución antimalware. Por lo cual, se debe entregar junto con la propuesta una certificación expedida por la casa matriz del software, con fecha no mayor a 30 días anteriores a la fecha de cierre del proceso, y la cual deberá estar vigente durante la ejecución del contrato. Si la casa matriz tiene sucursales en Colombia o subsidiarias, estas podrán expedir la Certificación. Si dentro de las políticas de comercialización de la casa matriz está contemplado que un distribuidor mayorista para Latinoamérica o para Colombia otorgue la Certificación, esta será aceptada siempre

		y cuando se anexe la autorización de la casa matriz al distribuidor mayorista para otorgar dicha certificación. En caso de proponentes plurales, uno de los integrantes del proponente plural (consorcio o unión temporal) deberá presentar la certificación.
3. CARACTERÍSTICAS DEL SOFTWARE ANTIMALWARE		
3.1.	Gestión y administración	**Consola de Administración Centralizada:** Plataforma de gestión unificada, intuitiva y basada en la nube para la administración de todos los componentes de seguridad. **Dashboards e Informes:** Generación de informes detallados sobre el estado de la seguridad, amenazas detectadas y actividades del sistema. **Notificaciones y Alertas:** Sistema de alertas configurable para eventos críticos de seguridad. **Integración SIEM:** Capacidad de integrar datos de seguridad con sistemas SIEM (Security Information and Event Management). **Gestión de Políticas Flexible:** Creación y aplicación de políticas de seguridad detalladas y adaptables a diferentes grupos de usuarios y equipos. **Soporte Multi-Idioma.**
3.2.	Protección de Endpoints (Estaciones de Trabajo y Servidores)	Defensa Multi-Capa: • **Anti-Malware Avanzado:** Detección de amenazas conocidas y de día cero mediante machine learning (local y en la nube), firmas y heurísticas. • **Anti-Ransomware:** Protección específica contra ataques de ransomware, incluyendo mitigación de impacto y capacidad de revertir cambios. • **Defensa contra Exploits:** Prevención de ataques que explotan vulnerabilidades en aplicaciones y sistemas operativos. • **Protección contra Ataques sin Archivos (Fileless Attacks):** Detección y bloqueo de técnicas que operan directamente en memoria sin dejar rastros en disco. • **Análisis Automatizado en Sandbox:** Capacidad de detonar archivos sospechosos en un entorno aislado para determinar su comportamiento malicioso. • **Firewall Bidireccional:** Control del tráfico de red entrante y saliente con detección y prevención de intrusiones (IPS/IDS). • **Control de Dispositivos (Device Control):** Gestión granular del acceso a dispositivos externos (USB, CD/DVD, etc.).

		• **Control de Aplicaciones (Application Control):** Permite la creación de listas blancas y negras para ejecutar aplicaciones. • **Protección Web y Anti-Phishing:** Bloqueo de sitios web maliciosos, phishing y contenido fraudulento. • **Cifrado de Disco Completo (Full-Disk Encryption):** Integración para el cifrado y la gestión del cifrado de unidades de disco completo.
3.3.	Compatibilidad con sistemas operativos (Agentes de Endpoint)	La solución debe ser compatible con una amplia gama de sistemas operativos para estaciones de trabajo y servidores, incluyendo, pero no limitándose a: • Windows: Windows 10, Windows 11, Windows 8.1, Windows 7, Windows Server 2019, 2016, 2012 R2, 2012, 2008 R2. • macOS: macOS Big Sur (11.x) y versiones posteriores, así como versiones anteriores comunes (Catalina, Mojave, High Sierra, Sierra). • Linux: Distribuciones principales como Ubuntu, Red Hat Enterprise Linux (RHEL)/CentOS, SUSE Linux Enterprise Server, Debian, Fedora, Oracle Linux, Amazon Linux.
3.4.	Gestión de riesgos y vulnerabilidades	**Análisis de Riesgos de Endpoint (Endpoint Risk Analytics):** Identificación y evaluación de riesgos asociados a configuraciones erróneas, vulnerabilidades de software y comportamientos de usuarios. **Gestión de Parches (Patch Management):** Funcionalidad para identificar vulnerabilidades de software en los endpoints y facilitar la implementación de parches y actualizaciones de seguridad para sistemas operativos y aplicaciones de terceros.
3.5.	Detección y respuesta (EDR/XDR)	**Visibilidad Completa:** Recopilación y análisis de telemetría detallada de los endpoints para una visibilidad profunda de la actividad. **Detección de Anomalías:** Identificación de comportamientos inusuales o sospechosos que puedan indicar un ataque. **Análisis de Causa Raíz (Root Cause Analysis):** Herramientas para investigar y comprender el origen y el alcance de los incidentes de seguridad. **Correlación entre Endpoints (Cross-Endpoint Correlation):** Capacidad de correlacionar eventos de seguridad de múltiples endpoints (estaciones de trabajo, servidores, contenedores) para detectar ataques avanzados con movimiento lateral. **Investigación y Remediación:** Shell de Comando Remoto: Acceso seguro y remoto a los endpoints para realizar investigaciones y ejecutar comandos de remediación.

		Respuesta Automatizada: Capacidades de respuesta automática ante amenazas detectadas. **Capacidades Forenses:** Herramientas para recopilar evidencia y realizar análisis forense. **Reglas personalizadas para EDR:** Posibilidad de crear reglas de detección personalizadas.
3.6.	Seguridad de correo electrónico	**Protección Integral de Email:** Filtros avanzados contra spam, phishing, malware y amenazas de compromiso de correo electrónico empresarial (BEC).
4. SERVICIOS		
4.1.	Actividades iniciales	Al inicio del contrato, el contratista deberá entregar la matriz de comunicaciones y escalamiento para los servicios contratados. Diez (10) días hábiles después de la firma del acta de inicio, se deberá presentar un informe del estado inicial de la solución y un plan de trabajo. El informe deberá incluir como mínimo la siguiente información: • Un inventario y diagnóstico general de la solución instalada, analizando cada uno de sus componentes, con el fin de determinar necesidades de: actualización, reconfiguraciones y/o redefinición de políticas. • Revisión de la consola de administración. • Análisis de los eventos y alarmas. • Cronograma de actividades que contemple las actividades requeridas para la corrección de errores y afinamiento del software y/o actualización de ser necesaria. • Recomendaciones para garantizar el buen funcionamiento de la solución de antimalware objeto del contrato y los elementos que lo componen.
4.2.	Instalación e implementación	El contratista o proveedor, durante la vigencia del contrato, deberá realizar las instalaciones, configuraciones y/o migraciones que se requieran para garantizar el correcto funcionamiento de los componentes de la solución suministrada. Esto incluye, pero no se limita a: • Configurar y parametrizar la consola de administración. • Instalar e integrar la solución a los equipos de cómputo con que cuenta el Concejo de Bogotá D.C. (estaciones de trabajo, servidores físicos y virtuales). • Realizar la integración con los equipos de monitoreo de la Corporación (SIEM, Firewall, etc) en caso de requerirse.

		• Renovar el licenciamiento del software necesario para la operación de los equipos conforme a las configuraciones, funcionalidades implementadas y requeridas por la arquitectura actual. • Informar a la Oficina de Tecnología de la Corporación la configuración realizada durante la instalación Todas las actividades deberán ser concertadas y programadas con la Oficina de Tecnología del Concejo de Bogotá D.C. **NOTA 1:** En caso de suministrar una solución equivalente, el contratista deberá realizar la desinstalación de todos los agentes actuales en los diferentes equipos de la corporación, y proceder a instalar y configurar los nuevos agentes, así como realizar las configuraciones que se requieran en las consolas y plataformas del concejo de Bogotá con el fin de garantizar el correcto funcionamiento de la solución y todas las funcionalidades solicitadas, esta actividad no deberá representar un costo adicional para la entidad. **NOTA 2:** En caso de daño lógico de los computadores o servidores debido a las labores de instalación o migración por parte del proveedor o uno de sus ingenieros o técnicos, este deberá realizar todas las actividades y acciones necesarias para restaurar el sistema al estado en el que se encontraba antes de ser intervenido, garantizando la restauración de la información. Esto en ninguna circunstancia deberá generar un costo adicional al contrato.
4.3.	Configuración	El contratista o proveedor deberá realizar todas las configuraciones y parametrizaciones necesarias para garantizar la puesta en operación de la solución, siguiendo las mejores prácticas del fabricante y de acuerdo con los requerimientos del Concejo de Bogotá D.C. Se deberán tener en cuenta los siguientes ítems: • Recolectar la información sobre los usuarios y la infraestructura actual de la Corporación, sí aplica. • Instalar y configurar las herramientas necesarias para sincronizar los directorios, los buzones de correo, actualizaciones automáticas, entre otras. • Crear perfiles, usuarios y grupos, sí aplica. • Configurar los servicios requeridos por la Corporación. • Asesorar e informar a la Oficina de Tecnología de la Corporación en la configuración definida.
4.4.	Actualizaciones	Durante el plazo de ejecución del contrato, se debe mantener actualizado a la última versión estable liberada por el fabricante el software, de tal forma que permitan mantener las funcionalidades de la solución de antimalware hasta la fecha de vencimiento del plazo

		de ejecución del contrato, sin que esto represente un costo adicional para el Concejo de Bogotá D.C. El personal asignado al contrato debe estar en la capacidad de realizar las actualizaciones de la solución antimalware a nuevas versiones estables que se encuentren liberadas por el fabricante, así como la migración a servidores y consolas de administración que sean propiedad de la Corporación en caso de ser necesario. Las actividades de actualización deberán ser concertadas con el proceso de Sistemas y Seguridad de la Información de la Corporación.
4.5.	Soporte	El contratista y/o fabricante deberán prestar el servicio de soporte técnico remoto o en sitio para la atención y solución a requerimientos e incidentes que se reporten, así como para evaluar y solucionar fallas que se presenten en la solución objeto del contrato, por llamado del Concejo de Bogotá y sin costo adicional para el mismo. En caso que una actividad de mantenimiento o actualización programada generé una indisponibilidad de los servicios prestados, se podrá solicitar que la misma se realice fuera del horario laboral sin que esto implique un costo adicional para la Corporación. Por incidente se entenderá todas las eventualidades que generen problemas técnicos como fallas, daños, degradación del desempeño, mal funcionamiento o anomalías que se presenten en el hardware, software o licenciamiento y que afecten las funcionalidades o impidan que estos cumplan con su óptimo desempeño. El servicio de soporte comprende la realización de las siguientes actividades: a. Prestar un servicio de un centro de registro y atención de llamadas de servicio en el que recibirá y registrará los requerimientos e incidentes reportados por el Concejo de Bogotá. El registro incluirá mínimo los datos de fecha, hora, descripción y número de caso asignado; este último se utilizará para identificar y hacer seguimiento del caso. b. Recibir y gestionar las solicitudes de los incidentes reportados por el Concejo de Bogotá dentro de los plazos estipulados en el ítem acuerdos de niveles de servicio del presente documento. c. Realizar las actualizaciones de nuevas versiones de software, Parches o Fixes liberadas y estables en los bienes objeto del contrato. Se entiende que las versiones son estables si han sido instaladas, probadas y funcionan sin inconvenientes. d. Con el fin de garantizar las correctas condiciones de funcionamiento y la disponibilidad de los servicios, previo a la ejecución de una actualización o cualquier otro cambio en el

		software, hardware o configuraciones, el contratista evaluará y presentará al supervisor del contrato un informe que contenga los riesgos y el impacto derivados de las actividades que demande el cambio; las actividades necesarias para su ejecución; los tiempos de no disponibilidad del servicio; las pruebas y/o mediciones posteriores al cambio para garantizar la correcta prestación de los servicios; y las acciones de retorno, en el evento que se presente algún inconveniente técnico con las funcionalidades implementadas. e. En cualquier momento y durante la ejecución del contrato, el Concejo de Bogotá podrá revisar la trazabilidad de los incidentes y requerimientos escalados por el contratista a fábrica y conocer la solución ofrecida por el fabricante para los mismos. f. Suministrar todas las herramientas y recursos necesarios para la prestación del servicio de soporte. g. Realizar y actualizar el levantamiento de información de las configuraciones implementadas, de tal forma que se disponga de un registro actualizado de las mismas. h. Brindar las recomendaciones para contribuir en el mejoramiento de los procesos realizados por el Concejo de Bogotá D.C. Estas recomendaciones deberán reflejarse en el informe mensual de ejecución del contrato.
4.6.	Soporte en sitio y remoto	El contratista y/o fabricante debe tener la capacidad de brindar servicio de soporte técnico remoto y en sitio para los servicios contratados. En caso de que el servicio de soporte se realice de forma remota, este se debe hacer en coordinación con la Oficina de Tecnología de la Corporación. El soporte será en sitio para los casos en que no sea posible resolver el problema de forma remota. El servicio en sitio no significa costos adicionales para la Corporación. La atención en sitio deberá ser realizada por un equipo de soporte técnico conformado por especialistas certificados en la solución de antimalware y personal técnico de la Corporación.
4.7.	Mantenimiento preventivo	Se debe realizar durante la vigencia del contrato mínimo una (1) visita para practicar labores de mantenimiento preventivo y puesta a punto de sistema y elementos que integran el contrato; este mantenimiento podrá ser ejecutado por el contratista con personal calificado. Estas actividades se ejecutarán durante la vigencia del contrato, previa aprobación por parte de la supervisión, con quien se establecerán de común acuerdo las fechas para las ventanas de

		trabajo, teniendo en cuenta que estas podrán ser en horario no laboral con el fin de no afectar la operación de la Corporación. El servicio de mantenimiento preventivo comprende todas aquellas actividades proactivas y/o predictivas, que permitirán el correcto funcionamiento del sistema objeto del contrato. En estas visitas se verificarán algunos de los parámetros que conduzcan a detectar y prevenir posibles amenazas o fallas futuras. Involucra por lo menos los siguientes aspectos: • La realización de una copia de respaldo (Backup) de los elementos a intervenir. • La revisión de las bitácoras (LOG's) y alarmas de los diferentes componentes y la entrega de los informes con su respectivo análisis que permitan conocer el estado de los mismos. • Realizar el diagnóstico de la solución objeto del contrato, analizando cada uno de sus componentes, para determinar las necesidades de reconfiguración y/o redefinición de parámetros del sistema que permitan el buen funcionamiento. • Identificar y corregir posibles fallas de seguridad, desempeño, configuración y/o disponibilidad de manera oportuna con el fin de prevenir posibles afectaciones en sus operaciones críticas. • Actualización de los niveles de firmware, microcódigo y sistema de monitoreo a su último nivel liberado por el fabricante, de los componentes del equipo que así lo requieran. • Una vez realizado el servicio de mantenimiento preventivo, el Contratista debe entregar probado a satisfacción y en funcionamiento la solución objeto del contrato. • El contratista deberá presentar un informe al supervisor del contrato para conocer el estado de la solución objeto del contrato después de efectuado el servicio de mantenimiento preventivo, explicando los cambios realizados y las razones de los mismos, las recomendaciones de configuración y las alertas de monitoreo. Documentar toda la información de la infraestructura intervenida y generar los esquemas correspondientes.
4.8.	Soporte correctivo	El contratista o proveedor deberá atender las fallas presentadas en la solución antimalware durante la vigencia del contrato. El contratista deberá atender los requerimientos en sitio con base en los acuerdos de niveles de servicio definidos.
4.9.	Niveles de servicio	El Contratista o proveedor debe contar con una plataforma para registro y monitoreo de tiquetes de soporte; se debe garantizar que exista un tiquete por cada reporte que realice la Corporación.

		El soporte durante el período del contrato para la solución de problemas técnicos debe contemplar los siguientes niveles de servicio: • Soporte Nivel 1: Email y/o telefónico: Se deberá suministrar un email y número telefónico de contacto. A través de email o teléfono, los usuarios autorizados solicitarán la resolución de dudas o incidentes con la instalación, uso, configuración y activación de productos. Si la naturaleza de la incidencia lo requiere, se pasará al nivel 2. • Soporte Nivel 2: Soporte presencial para atender incidentes por medio de ingenieros especializados en la solución objeto del contrato. • Soporte Nivel 3: Para atender incidentes en la solución objeto del contrato que no pueden ser atendidos a través del soporte en nivel 1 y 2, y que requieren apoyo directo del fabricante. En cualquiera de los niveles anteriores debe contarse con el acompañamiento del contratista o el fabricante. Los servicios serán recibidos por el Concejo de Bogotá en oportunidad y calidad en las siguientes condiciones: a. Para el servicio de soporte técnico, el contratista recibirá y registrará los casos reportados por el Concejo de Bogotá D.C. Debe ser prestado en la modalidad 5x8x4; es decir: cinco (5) días a la semana (lunes a viernes), ocho (8) horas al día (08:00 a.m. a 05:00 p.m.), con un tiempo máximo de respuesta de cuatro (4) horas hábiles a partir del reporte de la solicitud del servicio, para la atención del incidente en sitio o de manera remota, por todo el plazo de ejecución del contrato. b. Con el objeto de atender el caso reportado, dentro de un plazo no mayor a cuatro (4) horas, contado a partir del registro del mismo, un ingeniero de soporte del proveedor debe contactar al supervisor del contrato, o a quien designe el Concejo de Bogotá. El ingeniero de soporte tiene la opción de solucionar el caso de manera telefónica, sesión remota o presencial. c. En caso de brindar soporte telefónico, si pasada una (1) hora de soporte no se soluciona el problema, el incidente se atenderá en sesión remota o en sitio en las sedes del Concejo de Bogotá. Para el desplazamiento, el contratista contará con un plazo no mayor de cuatro (4) horas, contado a partir del reporte del incidente. d. El Contratista debe garantizar la recuperación estable de los Servicios en máximo ocho (8) horas contadas a partir del registro del incidente, reservándose el derecho de proporcionar una solución provisional sin deterioro de la calidad de los

		servicios ni costos adicionales para la Corporación. La solución definitiva no debe superar los treinta (30) días calendario. Todo cambio será documentado y se deberá entregar un informe al supervisor del contrato con la información del soporte prestado.
5. GARANTÍA		
5.1.	Garantía de fabricante	La garantía será de por lo menos doce (12) meses desde la entrega y activación de las licencias. El proveedor deberá garantizar el acceso a nuevas actualizaciones y soporte, mediante la garantía técnica, por el tiempo que duren vigentes las suscripciones.
6. RECURSO HUMANO		
6.1.	Gerente de cuenta	El proveedor, al inicio de la ejecución del contrato, deberá asignar un profesional gerente de cuenta (Nombre del profesional, cargo, correo electrónico y número de celular de contacto), el cual será responsable de las liquidaciones, aplicaciones de ANS, facturación y demás solicitudes generales que la Corporación requiera que permitan garantizar la correcta ejecución del contrato durante su vigencia. En caso de ajustes o cambios del personal para esta labor, el representante legal del proveedor notificará al supervisor los cambios correspondientes.
6.2.	Equipo de trabajo	El contratista deberá garantizar que cuenta con el personal técnico debidamente capacitado para atender los requerimientos solicitados por el Concejo de Bogotá D.C. El personal deberá estar disponible para desplazarse a las sedes del Concejo de Bogotá D.C. para apoyar labores de instalación de las aplicaciones objeto del contrato y relacionadas en la presente ficha, en caso de ser necesario.
7. MANEJO DE RESIDUOS (Si aplica)		
7.1.	Realizar la gestión de todos los elementos, partes, desechos tecnológicos y residuos peligrosos que se generen durante la ejecución del contrato, de acuerdo con lo establecido en la normatividad vigente. Previamente, se debe presentar una carta o convenio actual entre el Proveedor y la empresa encargada del programa de disposición final. a. Debe presentar licencia ambiental de la empresa que realizará el tratamiento, aprovechamiento y/o disposición final según corresponda, y cuando se realice la gestión, el certificado de disposición final de los residuos en kilogramos. b. Realizar el pesaje y etiquetado del residuo peligroso generado de acuerdo con los lineamientos establecidos en la Corporación. c. Diligenciar la bitácora de generación de residuos peligrosos establecida por el Concejo cada vez que se realice el ingreso del residuo al área de almacenamiento de residuos peligrosos de la Corporación.	

	d. Remitir de forma trimestral un registro de los residuos peligrosos generados de forma mensual. e. Presentar las fichas de datos de seguridad de los insumos utilizados durante la ejecución del contrato. f. Dar cumplimiento a lo establecido en el Decreto 1079 de 2015, en lo referente al transporte de mercancías peligrosas. g. Dar cumplimiento a los lineamientos establecidos en el Plan Institucional de Gestión Ambiental de la Corporación.	
7.2.	Residuos peligrosos	El contratista está en la obligación de realizar la gestión integral de los residuos peligrosos (RESPEL), de acuerdo con el Decreto 4741 de 2005 y el Anexo 1 del mismo decreto. Estos deben ser gestionados a través de una de las empresas gestoras de residuos peligrosos con licencia ambiental otorgada por una autoridad ambiental. Al momento de la firma del acta de inicio, debe presentar la copia de la licencia vigente. En caso de que el contratista no cumpla directamente con este requisito, podrá hacerlo a través de un tercero que si cumpla con los requisitos para el manejo de los residuos tóxicos.
7.3.	Residuos de aparato eléctricos y electrónicos	Para la gestión de RAEE (cableado, conectores, tomas eléctricas y los que se generen en ejecución del contrato), se deberá dar cumplimiento a lo establecido en el Decreto 1076 de 2015, Título 7A, Capítulo IV de Disposiciones Finales de RAEE. De igual forma, tendrá a su cargo la recolección, transporte y disposición final con empresas o entidades autorizadas por la autoridad competente. Asimismo, presentará al supervisor del contrato copia de los formatos diligenciados del transporte y copia de la disposición de los residuos, dando cumplimiento a la normatividad vigente. El contratista deberá almacenar los residuos peligrosos generados en el área de almacenamiento que disponga el Concejo de Bogotá D.C., dando cumplimiento a lo establecido en el Plan de Gestión Integral de Residuos Peligrosos. Asimismo, deberá informar al responsable del Sistema de Gestión Ambiental de la Corporación la fecha para el retiro de dichos residuos, con el fin de realizar el acompañamiento de entrega de los residuos peligrosos y una lista de verificación del cumplimiento del Decreto 1609 de 2012, compilado en el Decreto 1079 de 2015 y/o la normatividad que le aplique. Los costos asociados o derivados del desarrollo de estas actividades serán asumidos por el contratista, quien también informará al funcionario responsable del programa de Gestión Ambiental de la Corporación, para que se lleve a cabo el registro de

		dicha gestión y la cuantificación de la generación del material asociado. En caso de que se generen residuos sólidos aprovechables durante la ejecución del contrato, estos deberán ser separados en la fuente por el contratista, labores que se efectuarán siguiendo el código de colores adoptado por la Corporación, en cumplimiento con lo establecido en el Plan Institucional de Gestión Ambiental.
8. SEGURIDAD DE LA INFORMACIÓN		
8.1.	Políticas	El contratista debe salvaguardar la Confidencialidad, Integridad y Disponibilidad de la Información, de acuerdo con la Política de Seguridad de la Información y la Política de Protección de Datos Personales, para todos los activos que administre y/o maneje dentro del Concejo de Bogotá D.C. durante la vigencia del contrato. Asimismo, deberá realizar la respectiva devolución de la información digital y/o física que le fue entregada al momento de iniciar el contrato y durante la vigencia del mismo hasta su finalización, por lo que se deberán acatar todas las directrices establecidas por el Concejo de Bogotá D.C. y el Gobierno Nacional, para el manejo seguro de la información.
8.2.	Confidencialidad	El contratista y el personal que este designe para realizar las diferentes labores en la Corporación deberán garantizar la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que generen como producto de la ejecución de las actividades, y por tanto, en ningún caso podrán divulgarla, copiarla, reproducirla o suministrarla a terceros. El contratista deberá suscribir el Compromiso de Confidencialidad de la Corporación antes de iniciar actividades.
9. GESTIÓN DE CONOCIMIENTO		
9.1.	Documentación	El contratista deberá entregar toda la documentación que se genere con ocasión de la ejecución del contrato y, como mínimo, los siguientes ítems: • Documento expedido por el fabricante en el cual se pueda verificar la legalidad del software, la cantidad de licencias suministradas, la vigencia y que las mismas se encuentren a nombre del Concejo de Bogotá D.C. Se acepta la validación a través del portal WEB del fabricante. • Manuales de usuario y de administración de la solución suministrada o la URL del fabricante o proveedor donde se puedan consultar.

		• Medios magnéticos (CD o DVD) o URL con acceso para la Corporación en la cual se pueda descargar el software para su reinstalación en caso de ser necesario. • Acta de entrega e instalación de la solución. • Documentación de los soportes realizados durante la ejecución del contrato. • Evidencia de la realización de las transferencias de conocimiento (videos, lista de asistencia, memorias, entre otros). Los formatos de entrega serán concertados con el Concejo de Bogotá D.C.
9.2.	Transferencia de conocimiento para usuario técnico o administrador	El contratista o proveedor debe llevar a cabo capacitaciones presenciales o virtuales para un grupo de usuarios técnicos o administradores definidos por la Corporación, con una intensidad mínima de cuatro (4) horas distribuidas en un máximo de dos (2) sesiones, las cuales permitan administrar, mantener y soportar todas las funcionalidades de la solución suministrada. Las capacitaciones deberán abarcar al menos las siguientes temáticas: • Solución de problemas que se presenten en la solución objeto del contrato. • Transferencia de conocimientos acerca de la administración y operación de la consola de administración. • Transferencia de conocimientos relacionados con nuevas funcionalidades de la solución. El contratista deberá tener en cuenta lo siguiente: • Brindar el apoyo pedagógico necesario para la transferencia de conocimiento a su público objetivo. • Proponer actividades educativas para aplicar las herramientas apropiadas a las necesidades identificadas, utilizando diversas metodologías y canales (presencial, web, escrita, entre otros). • Identificar y programar los recursos logísticos y tecnológicos necesarios para cada actividad educativa. • Elaborar y presentar un informe sobre los resultados de las actividades de capacitación, con el fin de brindar insumos para correctivos y la toma de decisiones. • Identificar necesidades de formación.

		El contratista o proveedor debe proporcionar el material de capacitación de acuerdo con el tema definido (estructura curricular, material de apoyo, recursos audiovisuales o multimedia). Las capacitaciones se podrán realizar de forma no presencial previa concertación con la supervisión del contrato y se deberá levantar un registro de los participantes. **NOTA 1:** En caso de suministrar una solución equivalente, el contratista deberá realizar una capacitación adicional de mínimo ocho (8) horas, dirigida a cuatro (4) funcionarios de la Corporación en al cual se profundice la instalación, configuración, administración y operación de los productos ofertados, esta capacitación deberá ser teórico-practica y debe ser certificada por el fabricante de la solución.

Proyectó: Francisco Javier Bernal García Firmado digitalmente por Francisco Javier Bernal García
Revisó: David Mateo Rivera
Oficina de Tecnología