OBJETO: ADQUIRIR EL LICENCIAMIENTO DE SOFTWARE ESPECIALIZADO PARA REALIZAR ANALISIS DE VULNERABILIDAD DE SEGURIDAD DE LA INFORMACIÓN EN LOS SISTEMAS MISIONALES Y DE APOYO PARA LA SECRETARIA DISTRITAL DE AMBIENTE SDA, ASÍ COMO LOS SERVICIOS DE SOPORTE TÉCNICO ESPECIALIZADO.

ALCANCE DEL OBJETO: El licenciamiento tiene por objeto contar con una herramienta de software para evaluar la condición de seguridad de la Secretaría Distrital de Ambiente – SDA mediante el monitoreo y análisis de vulnerabilidades sobre sus principales activos tecnológicos, identificando riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, para fortalecer el Sistema de Gestión de Seguridad de la Información conforme a la norma ISO/IEC 27001:2022.

El proveedor deberá realizar la entrega de los siguientes productos y servicios:

Licenciamiento de software especializado para realizar análisis de vulnerabilidad técnica de seguridad de la información en la infraestructura tecnológica que soporta los sistemas misionales y de apoyo para la Secretarí a Distrital de Ambiente para mínimo 128 activos internos y externos (Red LAN y WAN) por un (1) año, con soporte 5x8 (cinco días a la semana, 8 horas al día) durante la vigencia de la licencia.

DESCRIPCIÓN GENERAL DE LA NECESIDAD

Con la transformación digital y el aumento de dispositivos, sistemas conectados a Internet y aplicaciones en nube, el número de ciberataques se ha incrementado, obligando a las entidades públicas y privadas a implementar soluciones que permitan identificar, analizar y mitigar vulnerabilidades que puedan en un futuro afectar la seguridad en su infraestructura de TI y en sus sistemas de información. Estas soluciones permiten identificar, evaluar, detectar y mitigar los diferentes riesgos de seguridad de manera eficaz.

El objeto del proceso está encaminado a la protección de los servicios tecnológicos y de la información, teniendo como base las normas ISO 27001, 27002, 31000, 19770, 55001 y las regulaciones del Ministerio de las Tecnologías de la Información y las Comunicaciones, relacionadas con seguridad Informática y ciberseguridad en Colombia.

La contratación se orienta a fortalecer la gestión de la seguridad de la información, permitiendo avanzar en la madurez de los controles, así como en la capacidad de monitoreo y respuesta ante eventos de seguridad. Para ello, se requiere la ejecución de actividades especializadas relacionadas con el análisis de vulnerabilidades, la correlación de eventos, la atención y mitigación de alertas, la remediación de brechas y la mejora continua de los controles de seguridad.

Así mismo, permitirá asegurar la correcta operación, mantenimiento y optimización de las plataformas de monitoreo y correlación, fortaleciendo la capacidad de detección, análisis y respuesta ante eventos de seguridad, así como la trazabilidad de las acciones realizadas. De manera complementaria, se contempla la transferencia de conocimiento al personal de la Entidad y la disponibilidad de documentación técnica, contribuyendo a la continuidad operativa y al fortalecimiento institucional.

Por lo anterior, la contratación resulta necesaria para fortalecer la gestión de la seguridad, garantizando una operación estable, controlada y alineada con las necesidades técnicas y operativas definidas por la Entidad.

Dado que para la SDA constituye una necesidad detectar cuáles son las vulnerabilidades que pueden amenazar de manera inminente nuestros sistemas, herramientas y plataformas, compuestos por ordenadores institucionales, sitios y aplicaciones web, servidores Windows y Linux, telefonía IP, switches, routers, entre otros, resulta imperativo obtener un software licenciado que nos permita correr (ejecutar) el análisis de vulnerabilidades.

De conformidad a lo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI) expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea, se define como vulnerabilidad "la debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001)."

Teniendo en cuenta la noción de vulnerabilidad expuesta, la entidad requiere adquirir un software especializado para realizar el análisis de vulnerabilidad que permitirá identificar y tratar los riesgos que puedan comprometer la seguridad de la información en los sistemas ("activos" en términos del Modelo de Seguridad y Privacidad de la Información (MSPI)) misionales y de apoyo de la Secretaría Distrital de Ambiente y con ello reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas expuestas a través del software especializado que se pretende contratar.

Al referirnos a Software Especializado se habla de un software cuya funcionalidad está dedicada en su totalidad al cumplimiento de su misionalidad, en este caso es el descubrimiento de vulnerabilidades, recomendaciones para su remediación (acciones para solucionar o reducir la vulnerabilidad), seguimiento a la remediación (seguimiento a las actividades de los responsables de la remediación), y monitoreo de las vulnerabilidades; en otras palabras, el software licenciado no realiza otra actividad fuera de las relacionadas con vulnerabilidades, lo cual permite un grado alto de especialización en la actividad que realiza.

Así mismo, el MPSI alineado a la norma técnica colombiana NTC-ISO/IEC 27001:2022 respecto del control de vulnerabilidades técnicas, para el efecto establece: "La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el análisis de vulnerabilidades de la infraestructura tecnológica, a través de un plan de pruebas que permita identificar y tratar los riesgos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de TI."

Según lo expuesto en el párrafo anterior, se precisan los siguientes conceptos de conformidad con lo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI) expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea, así:

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27001).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27001).

A fin de dimensionar la gravedad de la situación ante el desconocimiento de las vulnerabilidades, es importante conocer cuáles son los Tipos de Vulnerabilidades que pueden llegar a presentarse:

- **Amenazas de Malware.** Los programas maliciosos son una de las mayores ciber amenazas a la que se exponen las entidades. Dentro del malware existen distintos tipos de amenazas, siendo las principales:
    - **Virus**: Los virus informáticos son un software que se instalan en un dispositivo con el objetivo de ocasionar problemas en su funcionamiento. Para que un virus infecte un sistema es necesaria la intervención de un usuario (intencionada o inintencionadamente).
    - **Gusanos**: Es uno de los malware más comunes que infectan los equipos y sistemas de una entidad, ya que no requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo. El objetivo de los gusanos es el de replicarse e infectar el mayor número de dispositivos posibles utilizando la red para ello. Son una amenaza para las redes empresariales, porque un solo equipo infectado puede hacer que la red entera se vea afectada en muy poco tiempo. Troyanos: Los troyanos son programas que se instalan en un equipo y pasan desapercibidos para el usuario. Su objetivo es el de ir abriendo puertas para que otro tipo de software malicioso se instale. Ransomware: Consiste en cifrar toda la información de la entidad, impidiendo el acceso a los datos y los sistemas y se pide un rescate para poder liberar la información (normalmente en criptomonedas como bitcoins). Keylogger: Se instalan a través de troyanos y se encargan de robar datos de acceso a plataformas web, sitios bancarios y similares".

- **Vulnerabilidades de los sistemas**. Los sistemas y aplicaciones informáticas por lo general contienen algún error en su diseño, estructura o código que genera alguna vulnerabilidad. Por pequeño que sea ese error, siempre podrá generar una amenaza sobre los sistemas y la información, siendo la puerta de entrada para recibir ataques externos o internos. Las principales vulnerabilidades suelen producirse en: Errores de configuración; Errores en la gestión de recursos.; Errores en los sistemas de validación; Errores que permiten el acceso a directorios; Errores en la gestión y asignación de permisos; Amenazas de ataques de denegación de servicio.
  Un ataque de denegación de servicio distribuido (DDoS) se produce cuando un servidor recibe muchas peticiones de acceso, sobrecargando el sistema y haciendo que el servidor caiga o funcione de forma incorrecta (acceso lento o rebotando mensajes de errores). Para realizar este tipo de ataques se utilizan muchos ordenadores (bots) que de forma automatizada hacen peticiones a ese servidor.
  Los ataques DDoS son muy habituales contra servidores o servidores web de entidades, por lo que para la ANLA resulta indispensable disponer de medidas protectoras contra esta peligrosa amenaza que puede dejar fuera de servicio la actividad de la entidad, lo que exige en primera medida la posibilidad de identificar tal vulnerabilidad.

- **Vulnerabilidades producidas por contraseñas**. Con el teletrabajo y el cloud computing la gestión de contraseñas se ha convertido en uno de los puntos más importantes en ciberseguridad. Para acceder a las plataformas de trabajo de la entidad se requiere un usuario y contraseña, cuando se utilizan contraseñas poco seguras se generan vulnerabilidades en los sistemas, pues si son fácilmente descifrables pueden generar incursiones de terceros no autorizados que pueden robar, modificar o eliminar información, cambiar configuraciones si disponen de los privilegios apropiados, o incluso realizar el apagado de equipos, la generación de contraseñas seguras es una de las claves para incrementar el nivel de ciberseguridad de la Entidad.

- **Vulnerabilidades producidas por usuarios**. Los ataques informáticos están relacionados directamente con el uso incorrecto o negligente por parte de un usuario. Una mala asignación de privilegios o permisos puede hacer que un usuario tenga acceso a opciones de administración o configuración para las que no está preparado, cometiendo errores que suponen una amenaza para la empresa.

- **Otras amenazas informáticas.** Existen muchas otras amenazas informáticas que afectan a las empresas como los ataques por Inyección SQL que afectan a servidores de bases de datos empresariales, red de equipos zombies (utilizando recursos de la empresa para actividades ilícitas), ataques MITM (man in the middle) para espionaje de información, etc.

El error humano es otra causa de riesgos en ciberseguridad. El usuario siempre tiene el riesgo de cometer un error que pueda generar una vulnerabilidad que suponga una amenaza informática. Por esta razón se deben automatizar los procesos críticos para minimizar o eliminar el factor de riesgo del error humano.

Las malas prácticas o la falta de formación en ciberseguridad también generan vulnerabilidades, como la apertura de ficheros de dudosa procedencia, engaños por publicidad falsa, apertura de correos fraudulentos y similares. Estas acciones son una amenaza de ataques como el phishing (suplantación de identidad) o similares.

La identificación oportuna de vulnerabilidades permite prevenir futuras materializaciones de eventos, generando incidentes que pueden afectar la Disponibilidad, Integridad y Confidencialidad de la información de la Secretaría Distrital de Ambiente, las cuales corresponden a la triada del sistema de gestión de seguridad de la información.

La misión institucional de la SDA le exige, no solamente orientar la gestión ambiental de Bogotá para reducir la vulnerabilidad climática, conservar la biodiversidad y controlar el deterioro de los recursos naturales, sino que además requiere que la información que se genera en la ejecución de esta se encuentre protegida, no solo en lo relativo a la privacidad sino sobre todo en cuanto a la conservación de la misma, que permita el debido seguimiento a las actividades desarrolladas en tal sentido.

Así mismo, en el evento de algún tipo de dificultad en su utilización, ante una eventual desconfiguración sin que sea posible su restauración por parte de los administradores, se requiere soporte técnico de tercer nivel para ayudar a los administradores por parte de la entidad a solucionar estos inconvenientes y recuperar el normal funcionamiento del software licenciado.

Actualmente, la Entidad no cuenta con soluciones de software de vulnerabilidades contratado; no obstante, genera nuevos desarrollos y publica información en el Portal Web y expone servicios tecnológicos en Internet que requieren de este tipo de verificaciones y validaciones según lo establecido en el Modelo Integrado de Planeación y Gestión (MIPG) y el Plan de Seguridad y Privacidad de la Información del Decreto 612 de 2018, los análisis de vulnerabilidades deben realizarse todos los años.

En este orden de ideas, la SDA requiere de un software licenciado por medio del cual se puedan identificar las vulnerabilidades de las plataformas, sistemas y/o herramientas tales como FOREST, SIPRES, SIPSE, ARCGIS, Bases de datos, servicios Web, y demás con las que cuenta hoy en día la entidad.

Para la vigencia 2026, se requiere contratar la adquisición de la licencia de software especializada para realizar análisis de vulnerabilidad de seguridad de la información en los sistemas misionales y de apoyo de la Secretaría Distrital de Ambiente - SDA, así como los servicios de soporte técnico especializado, que permita identificar el estado seguridad de todos los sistemas de información de la entidad, aclarando que, como ya se mencionó, corresponde a una adquisición toda vez que no se cuenta actualmente con una herramienta de estas características que ofrezca el adecuado cumplimiento de funcionalidades técnicas y de seguridad de la información frente a las amenazas existentes en el entorno digital del que somos parte como entidad distrital.

OBLIGACIONES ESPECÍFICAS:

1. Elaborar y cargar en la plataforma SECOP II, el informe de ejecución de la gestión adelantada debidamente firmado por el supervisor, con los soportes para adelantar el respectivo pago, que evidencie el cumplimiento de las obligaciones pactadas en el contrato, en las fechas establecidas en el mismo.
2. Cumplir con las especificaciones técnicas previstas en el ANEXO - FICHA TÉCNICA y demás documentos que hacen parte del contrato.
3. Entregar la carta de licenciamiento de software de acuerdo con las condiciones de la ficha técnica del proceso contractual a nombre de la Secretaría Distrital de Ambiente – SDA dentro de los **5 días hábiles siguientes** al cumplimiento de los requisitos de perfeccionamiento y firma del acta de inicio del contrato.
4. Brindar soporte remoto en la modalidad 5x8 (cinco días a la semana, ocho horas al día) cuando sea requerido por la Entidad; este servicio lo debe prestar el contratista durante la vigencia de la licencia, de acuerdo a las condiciones establecidas en la cláusula 2.1.7 del presente anexo técnico.
5. Resolver las solicitudes e incidentes del software especializado licenciado asociado a parametrizaciones o mal funcionamientoconforme a los términos establecidos en el numeral 2.1.7 de este anexo técnico
6. Mantener la herramienta de escaneo de vulnerabilidades con las actualizaciones vigentes hasta el término de doce (12) meses a partir de la fecha de activación de las licencias documentada en la carta de licenciamiento de software.
7. Entregar los informes definidos en los numerales 2.1.5.22 y 2.1.6.24 del presente anexo técnico, con una periodicidad mensual.
8. Las demás que se deriven de la naturaleza del contrato y que garanticen su cabal y oportuna ejecución.

PLAZO DE EJECUCIÓN:

El plazo de ejecución del contrato será de dos (2) meses, contado a partir del cumplimiento de los requisitos de ejecución, previo perfeccionamiento y legalización del contrato y la suscripción del acta de inicio. El plazo no podrá sobrepasar el 31 de diciembre de la vigencia presupuestal 2026.

NOTA: La vigencia del licenciamiento y el soporte técnico tendrán un plazo de duración de doce (12) meses contados a partir de la activación de la licencia de software correspondiente.

CLASIFICACIÓN UNSPSC:

El objeto está codificado en el clasificador de bienes y servicios UNSPSC (The United Nations Standard Products and Services Code / Codificación de Bienes y Servicios de Acuerdo con el Código Estándar de Productos y Servicios de Naciones Unidas) como se indica a continuación:

Clasificación UNSPSC	Segmento	Familia	Clase
Equipo de seguridad de red	43000000	43220000	43222500
Servicios de sistemas y administración de componentes de sistemas	81000000	81110000	81111800

CONDICIONES TÉCNICAS

Ítem	Descripción técnica del bien, obra o servicio a contratar	Cantidad	Unidad de medida
1.1	Licenciamiento de software especializado para realizar análisis de vulnerabilidad técnica de seguridad de la información en la infraestructura tecnológica que soporta los sistemas misionales y de apoyo para la Secretarí a Distrital de Ambiente para mínimo 128 activos internos y externos (Red LAN y WAN) por un (1) año, con soporte 5x8 (cinco días a la semana, 8 horas al día) durante la vigencia de la licencia.	1	Unidad

2.1 Especificaciones técnicas:

2.1.1 Generalidades

ITEM	CARACTERISTICA
2.1.1.1	La plataforma debe contar con alguna de las siguientes certificaciones: SSAE 18 SOC 2 FedRAMP Moderate EU-U.S. Data Privacy Framework (DPF) **CSA STAR** (PCI ASV ISO/IEC 27001: 2022 ISO/IEC 27017: 2015 ISO/IEC 27018: 2019
2.1.1.2	La solución debe tener la capacidad de evaluar aplicaciones internas, externas y APIs y ésta se debe licenciar por número de aplicaciones y APIs.

2.1.1.3	La solución debe estar catalogada como Leader o Challenger en el reporte de Application Security Testing de GigaOm Radar, correspondiente al año 2025 o superior. Se establece este requerimiento como una medida de control de calidad técnica del bien y/o servicio a adquirir. Algunos aspectos para la justificación técnica del requerimiento: ● Garantía de Madurez e Innovación: A diferencia de otros reportes, el GigaOm Radar evalúa el equilibrio entre la madurez del producto (estabilidad y despliegue en entornos empresariales y gubernamentales) y su capacidad de innovación (respuesta ante nuevas amenazas como ataques a APIs o vulnerabilidades de día cero). Una empresa calificada como "Líder" ha demostrado excelencia en ambos frentes. ● Reducción de Falsos Positivos: Las soluciones líderes en el reporte de 2025 destacan por el uso de Inteligencia Artificial y Machine Learning para el filtrado de resultados. Para una entidad de gobierno, esto se traduce en un ahorro significativo de horas-hombre, evitando que el equipo de seguridad pierda tiempo en alertas irrelevantes. ● Cobertura de Arquitecturas modernas de Software: El reporte de GigaOm para 2025 pone especial énfasis en la capacidad de evaluar microservicios, APIs y aplicaciones móviles. Adquirir una solución fuera de este rango pondría en riesgo la seguridad de las aplicaciones modernas de la entidad.

2.1.2 Monitoreo continuo

ITEM	CARACTERISTICA
2.1.2.1	Incorporar un motor de cálculo de riesgo, que automáticamente ayude a priorizar los activos.
2.1.2.2	Permitir personalizar el perfil de monitoreo asociado a una lista específica de criterios
2.1.2.3	Permitir la asignación de diferentes destinatarios para cada alerta.

2.1.3 Cálculo del riesgo y priorización

ITEM	CARACTERISTICA
2.1.3.1	Enviar notificaciones para usuarios específicos y grupos de usuarios para el perfil de monitoreo o múltiples perfiles de monitoreo.

2 1.3.2	El cálculo de riesgo deberá estar calculado teniendo en cuenta las siguientes variables como mínimo: - Vulnerabilidades asociadas al activo - Criticidad del activo - Ubicación del activo - Amenazas/Ataques asociados a las vulnerabilidades halladas - Problemas - Configuración - Controles compensatorios - Certificados asociados al activo - Obsolescencia del software. Nota: Si **además** de las variables listadas, el software considera otras adicionales, el requerimiento se entenderá también cumplido.
2.1.3.3	Permitir priorizar acciones de remediación basándose en este cálculo de riesgo.
2.1.3.4	El cálculo de riesgo debe ser dinámico y no estático, contemplando variaciones en las amenazas o variables contempladas en el cálculo de riesgo a lo largo del tiempo, en el caso de que alguna variable cambie a lo largo del tiempo, esta misma debería modificar el cálculo de riesgo de la vulnerabilidad y el activo.
2.1.3.5	Permitir crear flujos de trabajo automatizados para acciones de evaluación y remediación sin necesidad de código y mediante el uso de una interfaz gráfica del tipo “drag and drop”.

2.1.4 Gestión de Activos

ITEM	CARACTERISTICA
2.1.4.1	Tener la capacidad de generar un inventario de las aplicaciones y APIs que se identifiquen, entregando información como: - URL - Listado de vulnerabilidades - Información sensible - Certificados - Nivel de riesgo basado en contexto
2.1.4.2	Entregar un catálogo de los sitios web detectados a través de los escaneos con el fin de incluir nuevos sitios Web al inventario, generar listas blancas y negras, mostrar información relacionada con el FQDN, dirección IP, puerto y NetBios sin que esto consuma licencias.
2.1.4.3	Permitir la asignación de diferentes destinatarios para cada alerta.
2.1.4.4	Entregar un mapa de los sitios identificados resaltando: - Aplicaciones / URL relacionadas - Nombre de la aplicación

	- Propietario - Modo de descubrimiento - Dominio - Perfil

2.1.5 Gestión de vulnerabilidades

ITEM	CARACTERISTICA
2.1.5.1	Tener la capacidad de mostrar en una vista simple el riesgo asociado a cada aplicación y/o API evaluado.
2.1.5.2	Entregar estadísticas del estado de vulnerabilidades clasificadas en: - Nuevas - Cerradas - Activas - Re-abiertas
2.1.5.3	Permitir la creación de perfiles de escaneo donde se especifique: - Tags - Tipo de solicitud: Post, Get o Post & Get - Cantidad máxima de Links to Crawl Bruteforcing list
2.1.5.4	Permitir la configuración de hasta 8.000 crawl por escaneo
2.1.5.5	Permitir en los perfiles la inclusión de criterios de búsqueda como: - Números de tarjetas de crédito - Números de servicio social (USA) - Contenido personalizado a través de expresiones regulares con mínimo 5 caracteres y un máximo de 200
2.1.5.6	Permitir la inclusión de criterios de búsqueda de palabras claves basado en expresiones regulares como mínimo 5 caracteres y un máximo de 200 en los perfiles de escaneo.
2.1.5.7	Permitir la ejecución de análisis autenticados, a través de la configuración de perfiles de autenticación, en el cual es posible configurar: - Login estándar (usuario y contraseña) - Personalizada (nombre y valor) - Selenium Script
2.1.5.8	Permitir la creación de lista de fuerza bruta (Bruteforce List) y listas de búsqueda (SearchList).
2.1.5.9	Permitir la creación de listas dinámicas que permitan incluir automáticamente vulnerabilidades a través de criterios de búsqueda como el nivel de criticidad, reglas de búsquedas, clasificación, nombre de la vulnerabilidad, etc. Con el objetivo de realizar re-escaneos o escaneos puntuales sobre las aplicaciones.

2.1.5.10	Permitir el DNS override en las aplicaciones donde por su naturaleza no sea posible la identificación basada en DNS.
2.1.5.11	Permitir escaneos en profundidad dinámicos para descubrir, catalogar todas las aplicaciones web y APIs en el perímetro de la red empresarial, redes internas e instancias en la nube.
2.1.5.12	Permitir escaneo autenticados, complejos y progresivos.
2.1.5.13	Soportar escaneos programados de servicios API SOAP y REST.
2.1.5.14	Contar con una API e integración con Jenkins para automatizar el escaneo en un entorno de CI/CD.
2.1.5.15	Detectar, identificar, evaluar, rastrear y remediar los 10 riesgos principales de OWASP, como inyección de SQL, secuencias de comandos entre sitios (XSS), entidades externas XML (XXE), autenticación interrumpida y configuraciones incorrectas, también las amenazas de WASC, las debilidades de CWE y los CVE asociados en aplicaciones web.
2.1.5.16	Encontrar aplicaciones web homologadas y no homologadas en su red generando un proceso continuo de catalogación y descubrimiento de aplicaciones web.
2.1.5.17	Generar etiquetas para facilitar la búsqueda y el uso de los activos de aplicaciones web hallados.
2.1.5.18	Escanear aplicaciones web de gran tamaño haciendo uso de un mecanismo de escaneo progresivo, que debe permitir escanear en etapas incrementales y evitar cualquier restricción que pueda generarse al intentar escanear una aplicación de una sola vez.
2.1.5.19	Establecer la hora de inicio y la duración exactas de los escaneos.
2.1.5.20	Permitir gestionar múltiples escaneos de aplicaciones web combinando múltiples escáneres para acelerar el proceso de escaneo y obtener resultados de forma más rápida.
2.1.5.21	Consolidar los datos de escaneo automatizado de la solución con datos de herramientas que permiten la evaluación manual de vulnerabilidades a través de Burp Suite y Bugcrowd, para obtener una vista unificada de las vulnerabilidades de la aplicación Web detectadas automática y manualmente.
2.1.5.22	Proporcionar informes resumidos y de escaneo del sitio que se puedan exportar a formato HTML y PDF.
2.1.5.23	Admitir la creación de roles y ámbitos definidos por el usuario y permitir la asignación de los permisos adecuados a cada rol.

2.1.5.24	Permitir la integración con herramientas como: - Jenkins - Bamboo - TeamCity - Azure - Jira

2.1.6 Análisis de malware

ITEM	CARACTERISTICA
2.1.6.1	Tener la capacidad de escanear e identificar infecciones de malware a partir de las propiedades Web.
2.1.6.2	Admitir la capacidad de detección de malware de día cero.
2.1.6.3	Proporcionar una vista completa de la actividad de los escaneos, las páginas infectadas y las tendencias de infección de malware.
2.1.6.4	Proporcionar informes interactivos con un análisis potente y una distribución segura de los resultados del análisis.
2.1.6.5	Admitir la capacidad de etiquetado con fines de categorización.

2.1.7 Soporte técnico especializado

Tipo de asistencia y tiempo de respuesta	Para los servicios descritos la asistencia será en Modalidad 5x8 por un (1) año a partir de la activación del licenciamiento.
Certificado de licenciamiento	El contratista debe realizar acompañamiento técnico durante la instalación del software y tener la capacidad de escalar los casos directamente al fabricante de la solución, en los casos que sea necesario, durante la vigencia del licenciamiento. - Incluir certificado del licenciamiento con la vigencia indicada.

Soporte técnico	Soporte Remoto en los casos que se requiera, de lunes a viernes (días hábiles) de: 8:00 AM a 12:30 PM y de 1:30 PM a 5.30 PM. Suministrar un número de PBX y/o Línea Nacional. Soporte por correo electrónico, 8:00 AM a 5.30 PM, suministrar un correo electrónico para efecto de formular peticiones de soporte. Soporte a través de Página Web, radicación de problemas e Inquietudes por medio del mecanismo de correo electrónico, celular o registro de tickets. Para los tiempos de respuesta remitirse a la tabla No. 1 Tiempos de respuesta y solución de incidentes, según criticidad. Los servicios deben ser prestados en las sedes de la Secretaría Distrital de Ambiente, ubicadas en: Principal - Av. Caracas # 54-38 en la ciudad de Bogotá D.C., o donde se ubique alguna de las sedes de la Secretaría Distrital de Ambiente en la ciudad de Bogotá D.C., con personal local para atender los requerimientos en los tiempos requeridos.

Tiempo de respuesta y solución de incidentes:

Prioridad	Detalle	Tiempo de respuesta	Tiempo de solución
Crítico	Falla de la plataforma que hace imposible administrar la solución. Requiere atención virtual o visita en sitio.	1 hr.	3 hr.
Alto	Problema de amenazas de gran impacto donde continúa operando la plataforma, pero de una manera imperfecta; impacto significativo para la Secretaría Distrital de Ambiente, amenaza aspectos de seguridad futura. Requiere atención virtual o visita en sitio.	2 hr.	4 hr.
Medio	La plataforma continúa funcionando con impedimentos menores. Las tareas pueden continuar con una mínima disminución de performance. Requiere atención virtual o visita en sitio.	4 hr.	8 hr.
Bajo	Consulta técnica y/o de uso. Las tareas se desarrollan normalmente.	8 hr.	16 hr.
Planificado	Implementación de una solicitud de cambios que no es requerida de manera urgente. Las tareas se desarrollan normalmente.	Planificado	Planificado

Tabla No. 1

NOTA: Sin perjuicio de la aplicación de la consecuencia establecida en el ANS, en caso de que la empresa contratista incumpla con los tiempos de respuesta para los ANS estipulados en el numeral 2.4.3, la Secretaría Distrital de

Ambiente evaluará la necesidad de realizar las gestiones tendientes a iniciar el proceso administrativo sancionatorio con el fin de imponer las sanciones pertinentes y de ser el caso hacer efectiva la póliza de cumplimiento.

2.1.8 Certificación distribuidor autorizado

El contratista debe ser distribuidor autorizado en Colombia y estar autorizado para vender, renovar, instalar, soportar técnicamente y cumplir con las garantías solicitadas de la solución ofertada, así como tener certificación de alguno de los dos niveles más altos en las categorías ofrecidas por el fabricante de la solución.

Dicha certificación debe ser expedida por el fabricante en una fecha no superior a treinta (30) días calendario anteriores a la fecha de cierre del proceso, dirigida a la Secretaría Distrital de Ambiente.

GARANTÍAS:

En cumplimiento de la Ley 80 de 1993, Ley 1150 de 2007, Decreto Nacional 1082 de 2015 y demás normas concordantes, el CONTRATISTA se obliga a constituir garantías a favor de **BOGOTÁ D.C - SECRETARÍA DISTRITAL DE AMBIENTE, NIT 899.999.061 -9**, con ocasión de la ejecución del contrato y de su liquidación a través de cualquiera de los mecanismos de cobertura del riesgo señalados en el artículo 2.2.1.2.3.1.2. del Decreto Nacional 1082 de 2015, que cubran los siguientes riesgos:

En cumplimiento de la Ley 80 de 1993, Ley 1150 de 2007, Decreto Nacional 1082 de 2015 y demás normas concordantes, el CONTRATISTA se obliga a constituir garantías a favor de **BOGOTÁ D.C - SECRETARÍA DISTRITAL DE AMBIENTE, NIT 899.999.061 -9**, con ocasión de la ejecución del contrato y de su liquidación a través de cualquiera de los mecanismos de cobertura del riesgo señalados en el artículo 2.2.1.2.3.1.2. del Decreto Nacional 1082 de 2015, que cubran los siguientes riesgos:

1. Cumplimiento

Por una cuantía equivalente al diez por ciento (10 %) del valor total del contrato, desde la suscripción del contrato y por una duración igual al plazo de ejecución del mismo y DOCE (12) meses más.

2. Pago de salarios y prestaciones sociales legales e indemnizaciones laborales

Por una cuantía igual al (5%) del valor total del contrato, desde la suscripción del contrato y por una duración igual al plazo de ejecución y TRES (3) años más.

3. Calidad y correcto funcionamiento de los bienes y equipos suministrados

Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato, desde la suscripción del contrato y con una vigencia de UN (1) año contado con posterioridad a la entrega del bien suministrado.

4. Calidad del Servicio

Por una cuantía equivalente al veinte por ciento (20%) del valor total del contrato, desde la suscripción del contrato y por una duración igual al plazo de ejecución y UN (1) año más.

NOTA 1. CONSTITUCIÓN DE LAS GARANTÍAS: EL CONTRATISTA deberá constituir la garantía dentro de los tres (3) días hábiles siguientes a la suscripción del contrato.

NOTA 2. RESTABLECIMIENTO O AMPLIACIÓN DE LAS GARANTÍAS: EL CONTRATISTA deberá restablecer el valor de las garantías antes mencionadas, cuando éste se haya visto reducido por razón de las reclamaciones efectuadas por la SECRETARIA. De igual manera, en cualquier evento en que se aumente o adicione el valor del contrato y/o se prorrogue su término, EL CONTRATISTA deberá ampliar el valor y/o la vigencia de las garantías otorgadas.

NOTA 3. VIGENCIA DE LAS GARANTÍAS: En todo caso el contratista deberá mantener vigentes las garantías hasta la liquidación del contrato.

NOTA 4: En virtud de lo establecido en el artículo 7 de la Ley 1150 de 2007, el numeral 7 del artículo 2.2.1.1.2.1.1 del Decreto Nacional 1082 de 2015 y a lo previsto en el artículo 1060 del Código de Comercio referente al mantenimiento del estado del riesgo y notificación de cambios. EL CONTRATISTA deberá notificar a la aseguradora las circunstancias no previsibles que den lugar a la modificación cobertura del riesgo. La notificación de la modificación del riesgo, así como la respuesta que otorgue la aseguradora deberá ser allegada a través de la Plataforma SECOP II, así como los documentos anexos correspondientes.

NOTA 5: Si resultare como contratista, un CONSORCIO O UNIÓN TEMPORAL, la garantía debe ser otorgada por todos sus integrantes.

NOTA 6: El contratista deberá cargar la garantía única de cumplimiento y responsabilidad extracontractual (cuando aplique), en el Sistema Electrónico para la Contratación Pública - portal SECOP II.

FORMA DE PAGO

La Secretaría Distrital de Ambiente pagará al contratista el valor del contrato en los siguientes términos:

El valor del contrato será cancelado mediante UN (1) ÚNICO PAGO EQUIVALENTE al 100% del valor total del contrato, mediante la presentación de:

i. Certificación que evidencie la entrega de las licencias adquiridas objeto del presente contrato, por una vigencia de doce (12) meses contados a partir de la activación de las mismas, así como su respectivo registro a nombre de la Secretaría Distrital de Ambiente,

ii. El comprobante de ingreso al almacén de la Entidad,

iii. El informe de actividades de la cláusula de informes del contrato y en el acápite denominado “productos finales entregables”.

El pago se realizará contra la factura y/o cuenta de cobro aprobada (según el caso), a las cuales se deberá adjuntar los siguientes documentos:

a. Informe de actividades (IAAP) debidamente firmado por el supervisor.

b. Certificado de adquisición de la totalidad de licencias establecidas, con duración de DOCE (12) MESES contados a partir de su activación.

c. Comprobante ingreso almacén.

d. Certificación suscrita por el representante legal o revisor fiscal, que acredite el cumplimiento del pago de aportes al sistema de seguridad social integral de los últimos seis (6) meses, de conformidad con el artículo 50 de la Ley 789 de 2002 o aquella que lo modifique, adicione o sustituya cuando se trate de personas jurídicas.

e. Presentar factura electrónica, conforme con las disposiciones señaladas en el Decreto Nacional No. 358 del 5 de marzo de 2020 y lo dispuesto en la Resolución expedida por la DIAN No. 000042 del 5 de mayo de 2020, la misma debe contener cada uno de los ítems, con la cantidad, unidad de medida, descripción específica y valor que permitan la identificación de los bienes vendidos o servicios prestados de acuerdo con lo estipulado en el contrato.

f. Acta de recibo final e informe de supervisión.

Condiciones generales para el pago.

El Contratista deberá tener en cuenta lo siguiente:

a. Las facturas o cuentas de cobro serán pagadas posterior al cumplimiento de todos los requisitos, aprobados y certificados por el supervisor y radicados en debida forma en concordancia con las normas tributarias vigentes, la aprobación de la Dirección Administrativa y Financiera y previa disponibilidad de PAC.

b. La factura o cuenta de cobro deberá incluir todos los impuestos, costos directos o indirectos a que haya lugar, y el detalle de los servicios efectivamente prestados y/o elementos suministrados.

c. La factura o cuenta de cobro deberá acompañarse de la copia de la planilla de pago de los aportes al régimen de seguridad social, para el periodo cobrado, en proporción al valor mensual del contrato, cuando se trate de personas naturales.

d. La factura o cuenta de cobro deberá acompañarse de la certificación suscrita por el representante legal o revisor fiscal, que acredite el cumplimiento del pago de aportes al sistema de seguridad social integral de los últimos seis (6) meses, de conformidad con el artículo 50 de la Ley 789 de 2002 o aquella que lo modifique, adicione o sustituya cuando se trate de personas jurídicas.

e. Los pagos se efectuarán dentro de los treinta (30) días calendario siguientes a la correcta radicación de la factura electrónica con los respectivos documentos soporte, en cumplimiento de lo establecido en el artículo 16 del Decreto 189 de 2020.

f. Si la(s) factura(s) no ha(n) sido correctamente elaborada(s) o no se acompañen) los documentos requeridos para el pago, el término para éste sólo empezará a contar a partir de la fecha en que se presente(n) en debida forma o que se haya aportado el último de los documentos. La(s) demora(s) en el pago originadas por la presentación incorrecta de los documentos requeridos serán responsabilidad del CONTRATISTA y no tendrá por ello derecho al pago de intereses o compensación de naturaleza alguna.

g. Las facturas deben estar diligenciadas en pesos colombianos, sin centavos.

h. Los pagos serán realizados por medio, en pesos colombianos, a través de transferencia a la cuenta corriente o de ahorros que indique el CONTRATISTA, abierta en cualquiera de las entidades financieras afiliadas al Sistema Automático de Pagos, previos los descuentos de Ley.

El contratista asume los costos establecidos para la ejecución del contrato, así como retenciones, tasas y contribuciones de orden nacional y distrital a qué hubiese lugar. Adicional a ello, se efectuarán descuentos de 3.6%, correspondientes a las estampillas distritales, así:

Concepto	Valor/ Porcentaje	Periodicidad del pago	Fuente
Rete ICA	Según corresponda a la tarifa de la actividad económica código CIIU	Mensual sobre el valor de la factura antes de IVA	Estatuto Tributario
Rete IVA	15%	Mensual sobre el valor del IVA	Artículo 462-1 Estatuto Tributario Nacional
Retención en la Fuente	2%	Mensual sobre el valor de la factura antes de A.I.U.	Artículo 462-1 Estatuto Tributario Nacional
Estampilla Pro-Adulto Mayor	2%	Mensual sobre el valor de la factura antes de A.I.U.	Acuerdo Concejo de Bogotá y Artículo 462-1 Estatuto Tributario Nacional.
Estampilla Pro-Cultura	0.5%	Mensual sobre el valor de la factura antes de A.I.U.	Acuerdo Concejo de Bogotá y Artículo 462-1 Estatuto Tributario Nacional.
Estampilla Universidad Francisco José de Caldas	1.1%	Mensual sobre el valor de la factura antes de A.I.U.	Acuerdo Concejo de Bogotá y Artículo 462-1 Estatuto Tributario Nacional.

Nota 1. Es importante tener en consideración la responsabilidad del proveedor del servicio ante las autoridades tributarias, esto es si son denominados autorretenedores y/o grandes contribuyentes y/o responsables del impuesto a las ventas.

Nota 2. Para el caso del Rete ICA, se debe tener en cuenta la territorialidad del proveedor y la actividad económica que ejerce, ya que la tarifa es diferente entre actividades.

NORMATIVIDAD QUE RIGE LAS CONDICIONES TÉCNICAS:

- Ley 1273 de 2009, "Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

- Ley 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales y las disposiciones que la reglamentan".

- Decreto 1360 de 1989, "Por el cual se reglamenta la inscripción de soporte lógico (software) en el registro nacional del derecho de autor".

- CONPES 3995 de Julio 1 de 2020. Política Nacional de Confianza y Seguridad Digital.

- MINTIC. Resolución 500 de 2021, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".

- Decreto 767 de 2022. "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

- Directiva Presidencial 2 de 2022. Reiteración de la política pública en materia de seguridad digital.

- Decreto 1078 de 2015. "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

- Norma ISO 27001 - Estándar Internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

- Norma ISO/IEC 27002 - Directrices para la gestión de la seguridad de la información en una organización.

- Norma ISO 31000 - Directrices para la gestión de riesgos en organizaciones de cualquier tipo y tamaño. Ofrece un enfoque estructurado para identificar, analizar, evaluar, tratar, monitorear y comunicar riesgos, buscando mejorar la toma de decisiones y el desempeño organizacional.

- Norma ISO/IEC 19770 - Estándar internacional para la gestión de activos de software (SAM) y Activos de tecnologías de la Información. Norma ISO 55001 – Por la cual se establece los requisitos para un sistema de gestión de activos, ayudando a las organizaciones a establecer, implementar, mantener y mejorar la gestión de sus activos para maximizar su valor.

Elaboró: Leonardo Cardenas / Victor Plazas

Historial de Cambios

VERSIÓN	FECHA	RAZÓN DEL CAMBIO
2	2 de junio de 2026	Conforme al rediseño de octubre de 2025 se ajusta plantilla, el código del procedimiento cambia de PA08-PR11 a GC-FO-009.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Jennifer Karina Vargas Moreno **Cargo:** Profesional Especializado **Nombre:** Deisy Soler Durán **Cargo:** Profesional Universitario **Fecha:** 2 de junio de 2026	**Nombre:** Andrea del Pilar Chaves Nieto **Cargo:** Contratista OAP **Nombre:** Claudia Milena Gordillo Rodríguez **Cargo:** Jefe Oficina Asesora de Planeación (E) **Fecha:** 2 de junio de 2026	**Nombre:** Karen Adriana Duarte Mayorga **Cargo:** Director (a) Contractual **Fecha:** 2 de junio de 2026