OBJETO: ADQUISICIÓN DE LICENCIAMIENTO Y SOPORTE DE ENDPOINT PROTECTION DE NUEVA GENERACIÓN CON SISTEMA XDR PARA PROTEGER LOS EQUIPOS INFORMÁTICOS (ENDPOINTS, SERVIDORES Y DISPOSITIVOS MÓVILES) DE LA SDA.

ALCANCE DEL OBJETO: El contratista se obliga a suministrar la suscripción de licencias, soporte técnico y actualización de las mismas por el término de doce (12) meses, contados a partir de su activación e implementación y a realizar la transferencia de conocimiento, de una solución de Protección de Endpoints de nueva generación (NGAV) con capacidades de detección y respuesta extendidas (XDR) bajo las especificaciones descritas en la presente ficha técnica.

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

1. 1.000 licencias endpoint NGAV (new generation antivirus) para equipos de escritorio administrados desde una única consola de gestión en nube, con sistema XDR. Incluido Soporte, Actualización y Configuración, por un término de 12 meses.
2. 160 licencias endpoint NGAV (new generation antivirus) para equipos servidores administrados desde una única consola de gestión en nube, con sistema XDR. Incluido Soporte, Actualización y Configuración, por un término de 12 meses.
3. 100 Licencias endpoint NGAV (new generation antivirus) para dispositivos móviles administrados desde una única consola de gestión en nube, con sistema XDR. Incluido Soporte, Actualización y Configuración, por un término de 12 meses.
4. Servicio de configuración, implementación, puesta en marcha y transferencia de conocimiento (mínimo 10 hr.) del licenciamiento de los ítems 1, 2 y 3.
5. Servicio de soporte especializado, actualización y configuración, mantenimientos correctivos ante fallas, servicios profesionales de configuración cuando sea requerido, sobre el licenciamiento endpoint NGAV por un término de 12 meses.

DESCRIPCIÓN GENERAL DE LA NECESIDAD

Conforme a las funciones de la OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN, esta tiene a su cargo el proyecto de inversión <<8061- Fortalecimiento de la gestión de TI en la Secretaría Distrital de Ambiente>>, cuyo objetivo general se orienta por mejorar el nivel de gestión de las tecnologías de la información en el ejercicio de su rol de autoridad y de la gestión ambiental en el Distrito y como objetivos específicos, productos y actividades, los siguientes:

Objetivo 1. Alcanzar un nivel alto en la gestión de la información y en los ciclos de vida de los sistemas de información (Producto: Documentos de lineamientos técnicos), que contempla la siguiente actividad: i). Realizar las actividades para fortalecer la gestión de la información y los ciclos de vida de los sistemas de información.
Objetivo 2. Alcanzar un nivel alto en la gestión de los servicios e infraestructura tecnológica y de la seguridad digital (Producto: Servicios tecnológicos), que contempla la siguiente actividad: ii). Fortalecer en 24 puntos porcentuales el índice de gestión de los servicios e infraestructura tecnológica y de la seguridad digital de la Secretaría Distrital de Ambiente;
Objetivo 3. Alcanzar un nivel alto de adopción de gobierno y estrategia de TI en la entidad y optimizar el uso y aprovechamiento de los servicios tecnológicos de la entidad (Producto: Documento para la planeación estratégica en TI), que contempla la siguiente actividad: iii). Fortalecer en un 100% el gobierno, estrategia y aprovechamiento de las TI en la entidad.

Que conforme a la meta Plan de Desarrollo: Implementar 3 programas de información ambiental y conocimiento ambiental establecidas para el Sector Ambiente, a la Secretaría Distrital de Ambiente - SDA le corresponde de los tres programas "Implementar un (1) programa de información ambiental y conocimiento ambiental." Por consiguiente, se formuló el proyecto de inversión 8061 "Fortalecimiento de la gestión de TI en la Secretaría Distrital de Ambiente".

Así las cosas, en aras de apuntar al cumplimiento proyecto precitado, se instituyó la actividad de inversión <<Fortalecer en 24 puntos porcentuales el índice de gestión de los servicios e infraestructura tecnológica y de la seguridad digital de la Secretaría Distrital de Ambiente>>, la cual, incluye lo siguiente:

A. Gestión de la Información: Para el cumplimiento de esta acción se deben tener en cuenta los diferentes lineamientos establecidos por el MRAE de MinTIC, referentes al dominio de gestión de información, y que se encuentran descritos en el Modelo de Gestión y Gobierno de TI (MGGTI), para esta dimensión, agrupados en los siguientes atributos: Gestión de ciclo de vida y gobierno de la información, Gestión de los tipos de datos, calidad, uso y aprovechamiento.
B. Gestión de Sistemas de Información: La meta se logrará mediante el cumplimiento de los diferentes lineamientos establecidos por el MRAE de MinTIC, referentes al dominio gestión de sistemas de información, y que se encuentran descritos en el Modelo de Gestión y Gobierno de TI (MGGTI), para esta dimensión, agrupados en los siguientes atributos: Gestión de ciclo de vida de los Sistemas de Información, Planeación y análisis y diseño, desarrollo y mantenimiento y calidad.

Así pues, la disposición de mecanismos de tecnologías de información que requiere la Entidad para el cumplimiento y adopción de la ley de transparencia y acceso a la información ambiental, permite la provisión de herramientas informáticas de seguridad para la gestión de trámites y servicios por medios electrónicos, fortaleciendo la gestión documental electrónica, fomentando y brindando la seguridad de los datos de mayor impacto o interés ambiental para la ciudadanía, mejorando tanto la divulgación proactiva de la información, así como el acceso y calidad de la información que se publica.

En ese orden de ideas, desde el componente de servicios e infraestructura tecnológica y de la seguridad digital, se requiere contar con un proceso de manejo y control de acceso de seguridad de la información para apoyar la operación normal de la entidad.

Teniendo en cuenta lo establecido en el numeral anterior, se requiere la contratación de un servicio que brinde la protección a los servidores, donde están alojados los sistemas de información de la entidad entre los cuales se encuentran Forest, Storm, Observatorio Ambiental, EVA, Portal Web, IBOCA, entre otros que soportan todos los servicios y trámites que se prestan al ciudadano del Distrito Capital y todas las funciones que desempeñan cada uno de los funcionarios de la Secretaría Distrital de Ambiente y de esta manera cumplir la misión y visión de la Entidad, garantizando los medios de protección necesarios para asegurar la confidencialidad, integridad y disponibilidad. de la información.

En la actualidad, la Secretaría Distrital de Ambiente (SDA) opera con una solución de Antivirus Endpoint Protection de nueva generación a través del contrato No SDA- 20251477 el cual tiene por objeto la "ADQUISICIÓN DEL LICENCIAMIENTO Y SOPORTE DE ENDPOINT PROTECTION DE NUEVA GENERACIÓN CON SISTEMA XDR PARA PROTEGER LOS EQUIPOS INFORMÁTICOS (ENDPOINTS, SERVIDORES Y DISPOSITIVOS MÓVILES) DE LA SDA" y el cual tiene una vigencia del licenciamiento hasta el día 5 de noviembre de 2026, que es fundamental para la seguridad de su infraestructura. Para mantener esta

protección al día y garantizar su eficacia, se requiere la adquisición, soporte y configuración de la solución de antivirus de última generación.
Así las cosas, este proceso es crucial para proteger de manera proactiva los equipos informáticos de la SDA contra las amenazas cibernéticas más recientes y sofisticadas. Con esta iniciativa, la entidad busca no solo mantener, sino también fortalecer en 24 puntos porcentuales el índice de gestión de los servicios e infraestructura tecnológica y de la seguridad digital, asegurando así una defensa robusta y alineada con los estándares de seguridad más altos.

Actualmente la entidad cuenta con los siguientes equipos instalados y en operación:

Equipos de Cómputo:

1000 equipos de cómputo y portátiles en producción, distribuido de la siguiente manera: 97 equipos portátiles en producción +253 equipos de cómputo en producción adquiridos por la entidad + 300 equipos de cómputo donados por el IDU en 2023 en reemplazo de unidades obsoletas que fueron dadas de baja, contribuyendo a la base actual de equipos en producción, más 350 equipos PC son bajo la modalidad de alquiler.

Servidores:

Se cuenta con 160 servidores en producción, que incluyen tanto máquinas virtuales como servidores físicos ubicados en el data center de la sede principal como en el datacenter de la ETB (Santa Barbara).

Cómo en la mayoría, si no todas las organizaciones hoy en día, la Secretaría Distrital de Ambiente – SDA, enfrenta un panorama de ciberamenazas en constante evolución, donde el malware tradicional basado en firmas ha sido superado por ataques de ransomware de última generación, amenazas de día cero (0-day) y ataques sin archivos (fileless). Las soluciones convencionales son insuficientes para detectar comportamientos anómalos o movimientos laterales dentro de la red. Por tal razón es necesario adquirir una herramienta de protección NGAV (Next Generation Antivirus), con capacidades de detección y respuesta extendida (XDR), que garantice la continuidad del negocio y la integridad de la información institucional mediante el despliegue de una solución de seguridad avanzada que permita:

- **Visibilidad extendida (XDR):** Correlacionar eventos de seguridad no solo en computadores y servidores, sino integrar la telemetría de dispositivos móviles para identificar ataques complejos que cruzan diferentes plataformas, visibilidad mejorada en diferentes capas del stack de seguridad, detección mejorada de ciberamenazas en múltiples dominios de seguridad, protección contra ciberataques avanzados, como ransomware.
- **Reducción del Tiempo de Respuesta (MTTR):** Automatizar la contención de amenazas (aislamiento de equipos infectados) para reducir el tiempo que transcurre entre la detección de un incidente y su neutralización.
- **Protección de Activos Críticos:** Salvaguardar los servidores que alojan las bases de datos y aplicaciones misionales, así como los dispositivos finales que manejan información sensible.
- **Cumplimiento Normativo:** Alinear a la entidad con estándares de seguridad (ISO 27001, NIST) y de protección de datos personales, mitigando riesgos legales por brechas de seguridad.

La presente contratación busca dotar a la entidad de una capacidad superior de ciberdefensa, a través de un modelo de análisis de comportamiento y respuesta automatizada, cuya capacidad requerida se encuentra basada en el inventario actualizado de activos de la infraestructura tecnológica. Esto permitirá minimizar la exposición, proteger la infraestructura tecnológica crítica y asegurar que la operación no se vea interrumpida por incidentes de seguridad digital.

Señalado lo anterior, se requiere realizar la adquisición del licenciamiento y soporte de endpoint protección de nueva generación con sistema XDR, con las siguientes cantidades:

ADQUISICIÓN de licenciamiento (a partir del 5 de noviembre del 2026):

- 1.000 licencias para equipos de escritorio
- 160 licencias para servidores
- 100 licencias para dispositivos móviles

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. Suministrar y garantizar el licenciamiento del software adquirido, por un término doce (12) meses, contados a partir del cumplimiento de los requisitos de perfeccionamiento del contrato y la activación del licenciamiento, así como registro a nombre de la Secretaría Distrital de Ambiente, de la solución ENDPOINT PROTECTION DE NUEVA GENERACION CON SISTEMA XDR.
4. Realizar la instalación, activación y puesta en marcha de la solución ENDPOINT PROTECTION DE NUEVA GENERACION CON SISTEMA XDR de acuerdo con las especificaciones técnicas mínimas de obligatorio cumplimiento relacionadas en el Anexo Técnico dentro de los primeros diez (10) días calendario siguientes a la suscripción del acta de inicio en la máquina virtual que dispone la Secretaría Distrital de Ambiente y en compañía del personal técnico designado por la supervisión, periodo dentro del cual también deben efectuarse las pruebas técnicas correspondientes.
5. Presentar un informe detallado en medio digital de la activación del licenciamiento, así como en los equipos donde se evidencie que quedaron instalados activados y actualizados el licenciamiento del ENDPOINT PROTECTION DE NUEVA GENERACION CON SISTEMA XDR, el cual deberá ser entregado a la supervisión dentro de los cinco (5) días hábiles siguientes a la aplicación o culminación de estas.
6. Proporcionar el soporte técnico sobre el correcto funcionamiento de la solución adquirida, soporte que deberá ser garantizado durante el periodo del licenciamiento, para lo cual el contratista establecerá con la SDA, los acuerdos de niveles de servicio del soporte técnico, una vez se active el licenciamiento.
7. Instalar las nuevas versiones que sean liberadas garantizando que la entidad cuente con la última versión disponible y estable del software adquirido por el término de doce (12) meses, contados a partir de la activación, así como registro a nombre de la Secretaria Distrital de Ambiente.
8. Proteger a la SDA del acceso no autorizado o cualquier modificación, divulgación o destrucción no autorizada de la información que posea el contratista.

9. Garantizar para la ejecución del presente proceso el personal idóneo y calificado para el soporte especializado del licenciamiento adquirido, la prestación oportuna y adecuada de los servicios de soporte asociados al licenciamiento, incluyendo la atención de incidentes, configuración, actualización, administración y demás actividades técnicas previstas en la Ficha Técnica.

PLAZO DE EJECUCIÓN:

El plazo de ejecución del contrato será de UN (1) MES, contado a partir de la suscripción del acta de inicio, previa expedición del registro presupuestal y de la aprobación de la garantía de cumplimiento. El plazo no podrá sobrepasar el 31 de diciembre de la vigencia presupuestal respectiva.

Nota: El contrato tiene un componente del licenciamiento por el tiempo de DOCE (12) MESES, contados a partir de su activación, durante este tiempo se contará con el soporte y actualización del licenciamiento adquirido, a partir del cumplimiento de los requisitos de ejecución, previo perfeccionamiento y legalización del contrato.

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:

Producto	Segmento	Familia	Clase
81111808	81000000	81110000	81111800
81111801	81000000	81110000	81111800
81111800	81000000	81110000	81111800
81112500	81000000	81110000	81112500
43233205	43000000	43230000	43233205
43233200	43000000	43230000	43233200

BIENES Y SERVICIOS A ADQUIRIR

No.	DESCRIPCIÓN DEL BIEN O SERVICIO	Cantidad	Unidad de medida
1	Adquisición de licenciamiento endpoint NGAV (new generation antivirus) para equipos de escritorio administrados desde una única consola de gestión en nube, con sistema XDR. Incluido Soporte, Actualización y Configuración, por un término de 12 meses.	1.000	Un.
2	Adquisición de licenciamiento endpoint NGAV (new generation antivirus) para equipos servidores administrados desde una única consola de gestión en nube, con sistema XDR. Incluido Soporte, Actualización y Configuración, por un término de 12 meses.	160	Un.
3	Adquisición de licenciamiento endpoint NGAV (new generation antivirus) para dispositivos móviles administrados desde una única consola de gestión en nube, con sistema XDR. Incluido Soporte, Actualización y Configuración, por un término de 12 meses.	100	Un.
4	Servicio de configuración, implementación, puesta en marcha y transferencia de conocimiento (mínimo 10 hr.) del licenciamiento de los ítems 1, 2 y 3.	1	Un.
5	Servicio de soporte especializado, actualización y configuración, mantenimientos correctivos ante fallas, servicios profesionales de configuración cuando sea requerido, sobre el licenciamiento endpoint NGAV por un término de 12 meses.	1	Un.

CONDICIONES TÉCNICAS

Ítem	Descripción técnica del bien, obra o servicio a contratar
1	**CARACTERÍSTICAS GENERALES**
1.1	La solución de protección de Antimalware se debe poder desplegar 100% en Nube y debe permitir como mínimo las características de Antimalware, Control de Aplicaciones y de dispositivos, protección avanzada contra Ransomware, mitigación de vulnerabilidades a través de parches virtuales o tecnologías equivalentes de mitigación y prevención de explotación de vulnerabilidades tales como exploit prevention, behavioral protection, machine learning o mecanismos avanzados EDR/XDR y, protección de fuga de información a través de expresiones regulares, diccionarios y características de los archivos.
1.2	La solución de protección Antimalware debe permitir la implementación de protección antimalware, control de aplicaciones, control de dispositivos, prevención de fuga de información, protección web, mitigación de vulnerabilidades a través de parches virtuales o tecnologías equivalentes de mitigación y prevención de explotación de vulnerabilidades tales como exploit prevention, behavioral protection, machine learning o mecanismos avanzados EDR/XDR, en un solo agente.
1.3	La solución debe permitir hacer backup y restauración automática de archivos o emplear tecnologías equivalentes ante intentos de cifrado no autorizados, como rollback automatizado, remediación automática, restauración comportamental, recuperación inteligente de archivos, protección anti-ransomware basada en comportamiento, entre otros, con el fin de generar una protección proactiva contra Ransomware, todo dentro de un agente único.
1.4	La solución debe tener la capacidad de brindar protección contra malware, virus de red, conexiones sospechosas, amenazas web, spyware, monitoreo de comportamiento, ataques combinados y ataques de día cero para equipos de punto final (Endpoint).
1.5	La solución debe contar con firewall (reglas de conexiones de aplicación, IP, puerto y protocolo), reputación de archivos y/o reputación web, que permita la creación de políticas a través de aplicaciones, aplicaciones específicas, llaves de

	registro de aplicaciones y estas se podrán aplicar a través de UDP, TCP y ICMP con puertos y direcciones IP definidas según las necesidades.
1.6	La solución debe tener la capacidad de aislar los equipos o ponerlos en cuarentena cuando se detecta algún ataque para evitar la propagación del mismo dentro de la red.
1.7	La solución debe bloquear procesos comúnmente asociados a Ransomware y debe finalizar los programas que muestren un comportamiento anormal asociado con ataques de explotación.
1.8	La solución debe incluir capacidades de Prevención de Intrusiones en el Host (HIPS), Monitoreo de Integridad (FIM) o Análisis de Comportamiento que permitan al administrador central configurar políticas granulares para monitorear, alertar y/o bloquear de manera automatizada la modificación del archivo hosts, la creación de nuevos servicios, y la alteración de archivos de sistema o políticas de seguridad.
1.9	La consola de administración debe tener un módulo de Monitoreo de comportamiento, reputación web, conexiones sospechosas, protección de vulnerabilidades, control de dispositivos y control de aplicaciones.
1.10	La solución debe tener la capacidad de analizar la reputación de archivos y recuperarlos cuando sean enviados a cuarentena. Además, debe permitir realizar escaneos de los Endpoint de forma manual, programada y en tiempo real.
1.11	La solución deberá permitir la visualización centralizada de eventos y alertas de seguridad de endpoints y servidores, clasificados según severidad, ofreciendo la posibilidad de configurar notificaciones administrativas por criticidad, producto, categoría o grupo de dispositivos involucrados. Asimismo, debe tener la capacidad de consultar eventos históricos y administrar la telemetría disponible según sea requerido.
1.12	La solución de protección de endpoints debe permitir detectar, monitorear, restringir o bloquear la fuga o transferencia no autorizada de información sensible desde endpoints y servidores, mediante políticas DLP administradas centralmente, con criterios de contenido, destino o tipo de archivo. Todo esto se debe hacer sobre el mismo agente de protección de Endpoints, device control y reputación Web.
1.13	La solución debe permitir crear identificadores de datos a través de palabras claves, atributos de archivos y expresiones regulares; además la solución debe permitir probar las expresiones regulares directamente en la plataforma.
1.14	Los templates de DLP de la solución deberán permitir definir la severidad de alto, medio, bajo como mínimo.
1.15	La solución deberá permitir tener políticas de control de aplicaciones en el mismo agente de DLP, control de dispositivos, XDR y protección de Endpoints, donde se puedan crear políticas para permitir las aplicaciones o bloquearlas y también debe permitir un modo de evaluación.
1.16	El control de aplicaciones debe permitir, bloquear o importar aplicaciones para la configuración de las políticas y deberá tener por defecto como mínimo las siguientes categorías de aplicaciones: Browsers y herramientas de browser, mensajería instantánea, productividad, P2P, cifrado, aplicaciones altamente riesgosas y en esta última como mínimo debe tener la posibilidad de bloquear key loggers, Crackers de contraseñas y proxys anónimos.
1.17	El componente de control de aplicaciones de la solución debe suministrar métricas asociadas a la legitimidad del software detectado en los endpoints. Esto debe incluir como mínimo: a) Un índice, categoría o puntaje de riesgo/reputación basado en el comportamiento histórico del ejecutable. b) Información explícita sobre el grado de adopción o presencia de la aplicación a nivel mundial (frecuencia de avistamiento o prevalencia global), permitiendo al administrador discriminar entre software comercial masivo y archivos únicos o de origen dudoso.
1.18	La solución de protección de endpoints debe permitir aplicar políticas de control y seguridad tanto a agentes internos como externos, considerando si la máquina se encuentra dentro o fuera de la red de la entidad (conciencia de ubicación). La plataforma deberá proveer, ya sea a través de sus capacidades de Control de Dispositivos, DLP integrado o de protección de contenido bajo el mismo agente unificado, las siguientes capacidades mínimas: Control, auditoría o bloqueo de medios y puertos: CD/DVD, unidades de red, unidades de almacenamiento USB, adaptadores bluetooth, dispositivos de imagen (cámaras/escáneres), dispositivos infrarrojos, módems y tarjetas de red inalámbricas (NICs Wireless).

	Protección contra captura de información visual: Capacidad de bloquear o restringir la acción de la tecla física de captura de pantalla (Print Screen / Impr Pant) y/o herramientas de recorte del sistema operativo para mitigar la fuga de datos.
1.19	El módulo de control de dispositivos debe permitir tener un listado de USB permitidas y de aplicaciones permitidas para que interactúen con dispositivos bloqueados. Además, debe tener la opción de bloquear la función AutoRun en dispositivos de almacenamiento USB.
1.20	La solución debe permitir tener reglas de prevención de intrusos de host y debe mostrar como mínimo el identificador, el nombre de la regla, el tipo de aplicación, la severidad, el tipo, el CVE al que está asociado la regla, la última actualización y estas reglas se deben poder aplicar en modo detección y prevención.
1.21	La Consola debe permitir para los servidores proporcionar monitoreo continuo para visibilidad instantánea y completa del entorno, notificaciones en tiempo real de las actividades y eventos que ocurran; permitir la generación de reportes customizables y desde el mismo dashboard de la consola de la solución poder administrar entornos físicos, virtuales y en la nube.
1.22	La solución deberá detectar automáticamente nuevos servidores en los diferentes sistemas de infraestructuras de servidores públicas y privadas en vCenter, AWS, Microsoft Azure, vCloud Air, Directorio Activo.
1.23	La solución ofrecida debe contar con capacidad de integración nativa, mediante APIs, conectores preconstruidos o webhooks, para la ingesta de telemetría, alertas y eventos de seguridad procedentes de vectores externos al endpoint. Esta capacidad de interoperabilidad debe incluir: • Integración bidireccional con ecosistemas de seguridad de terceros (como SIEM, SOAR, Firewalls NGFW, IAM o soluciones de seguridad en la nube / red). • Soporte para protocolos y formatos de integración estándar en la industria (APIs RESTful, Webhooks, o envío/recepción de eventos CEF). • Compatibilidad operativa para correlacionar datos de entornos multi-nube (como Azure, AWS, GCP) alineada a modelos de Zero Trust Architecture (ZTA). • Interoperabilidad para la apertura y gestión automatizada de tiquetes con sistemas de Gestión de Servicios de TI (ITSM) y gestión de incidentes estándar del mercado (ej. ServiceNow, Aranda, Jira, o equivalentes).
2	**ADMINISTRACIÓN**
2.1	La consola de administración debe ser 100% cloud y debe permitir la protección de Endpoints y servidores.
2.2	La solución debe permitir la creación, modificación y eliminación de roles y usuarios para la administración de la misma.
2.3	La consola de administración debe permitir administrar los agentes instalados en la red de equipos, permitiendo conocer el estado de los agentes.
2.4	La consola de administración debe estar en la Nube para garantizar la administración en todo el tiempo sin importar el lugar donde estén las máquinas administradas.
2.5	La consola de administración debe permitir agrupar los agentes en grupos para facilitar la configuración y administración de los mismos.
2.6	La consola de administración debe permitir configurar notificaciones sobre riesgos de seguridad y ver los Logs enviados por los agentes sobre los eventos de los mismos.
2.7	La consola de administración debe proporcionar un Dashboard que brinde información global sobre los agentes, eventos de reputación web, usuarios afectados, eventos de comando y control, incidentes de filtración de datos, entre otros e igualmente debe permitir que secciones o widgets sean agregados o eliminados según se requiera.
2.8	La solución propuesta debe permitir la consulta de registros (Logs) técnicos y operativos de la siguiente manera: A nivel de Endpoint: El agente local debe permitir la consulta, exportación o extracción de los logs de su proceso de instalación, actualización y comportamiento para facilitar la resolución de problemas en la estación de trabajo o servidor protegido.

	A nivel de Consola: La plataforma debe proveer acceso centralizado a los logs de auditoría, eventos del sistema y estado operativo de la administración. Se entenderá el cumplimiento de este punto mediante la disponibilidad de logs de actividad de los administradores y logs de estado de salud de la plataforma en la consola Web, sin necesidad de acceder al sistema de archivos del servidor del fabricante.
2.9	La consola de administración de la solución propuesta debe permitir consultar y visualizar de forma centralizada estadísticas, reportes históricos o estados de actualización de los diferentes motores de detección e inteligencia de amenazas instalados en los agentes (incluyendo protección contra código malicioso, análisis de comportamiento, protección de red o mitigación de exploits). La plataforma debe garantizar que el administrador pueda auditar el cumplimiento de la distribución de estas actualizaciones en todo el parque de endpoints protegidos para verificar la vigencia de la protección.
2.10	La consola de administración debe permitir la consulta, visualización y auditoría centralizada de los registros (logs) de eventos de seguridad generados por los agentes desplegados, en las siguientes condiciones: a. Cobertura de Eventos: Dichos registros deben incluir información detallada asociada a incidentes de: código malicioso (malware/spyware), reputación o protección web, conexiones sospechosas o de comando y control (C&C), detección de anomalías por análisis de comportamiento o heurística, motores de Inteligencia Artificial / Aprendizaje Automático (Machine Learning), así como eventos relacionados con el control de dispositivos y la prevención de fuga de datos (DLP). b. Capacidades de Filtrado: La plataforma debe permitir al administrador realizar búsquedas avanzadas y aplicar filtros sobre los logs mediante criterios de: periodos de tiempo preestablecidos, rangos de fechas personalizados, tipos o categorías de amenazas y módulos de protección/inspección que originaron la alerta.
2.11	La consola de administración debe permitir la visualización de los logs de registro de los eventos de la actualización del servidor de actualizaciones. Se entenderá el cumplimiento de este punto mediante la disponibilidad de logs de registro de eventos del servidor de actualizaciones a los administradores, sin necesidad de acceder al sistema de archivos del servidor del fabricante.
2.12	La consola de administración debe permitir la visualización de los logs de registro de los eventos del servidor de administración. Se entenderá el cumplimiento de este punto mediante la disponibilidad de logs de registro de eventos del servidor de administración a los administradores, sin necesidad de acceder al sistema de archivos del servidor del fabricante.
2.13	La consola de administración debe tener la capacidad de generar reportes en formato PDF,CSV y opcionalmente en DOCX y XLSX y también en formato PDF protegidos con contraseña para los reportes de los servidores.
2.14	La consola de Administración debe permitir visualizar a través de un DashBoard el riesgo corporativo donde se muestre el score de riesgo de la entidad y este debe ser calculado como mínimo con ocho ítems como las cuentas comprometidas, vulnerabilidades, actividad y comportamientos, detecciones de amenazas, configuraciones de seguridad, entre otras.
2.15	La plataforma debe mostrar listado de dispositivos descubiertos, dispositivos con agentes administrados y esto se debe poder filtrar por mes.
2.16	La solución debe tener un DashBoard donde se vea una descripción general de exposición, ataques y configuraciones de seguridad.
3	**AGENTES**
3.1	Los agentes deben ser instalados mediante instalación web, link de instalación por correo, instalación por script, y/o paquete de instalación.
3.2	Los agentes deben requerir contraseña de administración para ser desinstalados de los equipos.
3.3	Las políticas de seguridad deben aplicarse en los agentes de forma individual y/o por grupos.
3.4	El agente debe tener la capacidad de eliminar los archivos sospechosos de forma automática.

3.5	La solución debe usar solo un agente para los endpoints para realizar la protección antimalware, DLP, control de aplicaciones y EDR.
3.6	Los agentes de EPP deben poder instalarse en sistemas operativos Windows desde Windows 2012 y deben soportar las distribuciones vigentes de Linux tales como Red Hat, Ubuntu, entre otros.
3.7	El agente de protección no debe requerir reinicio en servidores para garantizar la disponibilidad de los servicios.
3.8	Los agentes deben tener la capacidad de conectarse a múltiples fuentes de actualización (patrones, firmas, url sospechosas, etc.), si alguna de estas es inaccesible para el agente.
4	**XDR (Extended detection response)**
4.1	La solución debe permitir la detección de amenazas tipo Fileless (ataques sin archivos) a través de la exploración de memoria mejorada para detectar comportamientos de procesos sospechosos. El agente debe tener la capacidad de terminar los procesos sospechosos antes de que se pueda hacer cualquier daño.
4.2	La solución debe permitir evaluar el alcance del daño causado por un ataque dirigido, proporcionar información sobre la llegada y progresión del ataque y ayudar en la planificación de una respuesta efectiva a incidentes de seguridad.
4.3	La solución deberá permitir graficar toda la cronología de los eventos generados en una investigación por medio de un gráfico que muestra el número total de puntos finales clasificados ya sea estén relacionados, o no relacionados a otros procesos, en cola o cancelados. La información debe estar siendo actualizada en tiempo real y de forma automática mientras avanza una investigación.
4.4	La solución debe permitir la búsqueda de Indicadores de Compromiso (IoC) en búsqueda de comunicaciones específicas, actividad de registro, actividad de la cuenta autenticada en el sistema y procesos en curso. Además, debe permitir la integración con información externa de IoC (Indicators Of Compromises) como reglas STIX, TAXII.
4.5	La solución debe permitir el análisis de comportamiento de un malware, actividades específicas de IoC y conexiones de comando a control.
4.6	La interfaz de la solución debe permitir integración con la consola de administración de las soluciones de seguridad perimetral o brindar la funcionalidad internamente para tener desde un solo punto el análisis, el contexto completo de los eventos y la línea de tiempo de los sucesos.
4.7	La solución debe escanear documentos en busca de códigos de exploits integrados y vulnerabilidades conocidas y controlar los programas que demuestran un comportamiento anormal asociado con ataques de exploits.
4.8	La solución debe analizar los archivos desconocidos de baja prevalencia utilizando algoritmos de aprendizaje automático para determinar si el archivo es malicioso y debe ser capaz de recopilar datos y barrido del sensor en los endpoints (IOC) y almacenarlos de forma centralizada para su posterior análisis.
4.9	La solución debe tener la capacidad de asociar los datos de registro y logs de los procesos con otros artefactos de disco y/o memoria.
4.10	La solución debe tener la capacidad de identificar amenazas aun cuando usen PowerShell codificado y debe detectar tareas programadas maliciosas además se debe mostrar todos los dispositivos en los que un proceso principal (padre) inicia otros procesos (hijos) especialmente de tipo PowerShell y cmd.
4.11	La solución debe contar con la capacidad de mostrar la línea de tiempo de incidentes y mostrar en una sola vista todo el ciclo de vida del ataque de la amenaza y debe revelar la cadena completa de procesos afectados por el malware/comportamiento malicioso.
4.12	La solución permitirá que el trabajo de investigación continúe en el dispositivo aislado sin permitir que se extienda la actividad maliciosa por medio de cuarentena y/o aislamiento de los sistemas infectados
4.13	La solución de EDR no debe requerir un agente adicional a los agentes de Endpoint Protection instalados en las máquinas de la entidad y debe permitir la correlación entre endpoints y servidores en la misma consola unificada.
4.14	XDR debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques y estos deben tener la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad.

4.15	Los modelos de correlación deben combinar múltiples reglas y filtros usando una variedad de técnicas de análisis como, pero no limitándose, a Data Stacking y Machine Learning.
4.16	XDR debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos y estos gráficos deben mostrar una representación visual de los objetos que levantaron la alerta y la relación entre ellos.
4.17	Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz (Execution Profile/Root Cause Analysis) para ver las acciones que una amenaza llevó a cabo en un servidor, Endpoint, o carga de trabajo en la nube.
4.18	Debe permitir la búsqueda proactiva a través de Endpoint y servidores (como telemetría, NetFlow, meta data, etc.) usando un simple constructor de consultas sobre una consola unificada.
4.19	La solución debe permitir hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros y filtrar los resultados añadiendo criterios adicionales de búsqueda, también debe detectar proactivamente con búsquedas automáticas de IoC publicados por el vendor.
4.20	Desde el resultado de una búsqueda se debe poder ejecutar acciones de respuesta y generar un análisis de causa raíz, además las búsquedas deben permitir construir, guardar y reutilizar búsquedas para Threat Hunting básico.
4.21	La capacidad de Threat Intelligence embebida debe ser capaz de identificar la campaña asociada, la Plataforma atacada, las Técnicas, Tácticas y Procedimientos (TTPs) alineadas a MITRE ATT&CK™ y debe proveer enlaces/links a entradas de blog relacionados si están disponibles.
4.22	En una sola ubicación debe poder ver el estado de respuestas en Endpoint y servidores y como mínimo debe mostrar la siguiente información: identificador de la tarea ejecutada, acción, objetivo, usuario que la creó, desde donde fue creada y fecha de la última actualización. Además, la solución debe permitir la creación de scripts personalizados en (power Shell script) .ps1 y (bash Script) .sh
4.23	Debe permitir ejecutar acciones de respuesta rápidamente haciendo clic derecho en el incidente y desde los resultados de búsqueda de Threat Intelligence. Las respuestas como mínimo deben ser: aislar un Endpoint, ejecutar un script personalizado, iniciar un Shell remoto, adicionar a una lista negra, entre otros.
4.24	La solución debe exponer una API pública que pueda ser usada por clientes para integrarse con SIEM y herramientas SOAR y debe permitir obtener un listado con los detalles de los Endpoints, obtener un listado de alertas con sus detalles y modificar su estado, adicionar y remover objetos sospechosos de una lista negra, eliminar entre otras.
4.25	Las alertas deben permitir ver un análisis de causa raíz para identificar el alcance del impacto y permitir tomar acciones de respuesta.
4.26	Debe priorizar las alertas y llevar registro de lo que se ha hecho y la fase de la alerta (nuevo, en progreso, finalizado/cerrado).
4.27	La solución de XDR debe mostrar un score del riesgo corporativo, en los siguientes términos: La solución de XDR propuesta debe poseer la capacidad de unificar telemetría de múltiples entornos mediante un ecosistema abierto. Para ello, deberá cumplir con: Integración Nativa con Infraestructura de Red Actual: Debe permitir la ingesta de logs y la ejecución de acciones de contención (orquestación) de forma nativa o mediante conectores oficiales con las plataformas de firewall perimetral de la entidad (tales como Fortinet, Palo Alto Networks o Check Point). Inteligencia de Amenazas Abierta: Debe soportar de forma nativa la ingesta de feeds de terceros bajo los estándares internacionales abiertos TAXII y la plataforma MISP. Ecosistema Amplio de Terceros: La solución debe contar con un Marketplace, API abierta o catálogo de conectores preconstruidos que permita la integración con soluciones líderes de la industria en los componentes de: Identidad (ej. Okta, Microsoft, OpenLDAP), Nube (ej. AWS, VMware), Gestión de Vulnerabilidades (ej. Tenable, Qualys), Gestión de Servicios (ej. ServiceNow) y Simulación de Ataques (BAS). Conector SIEM: Debe proveer un conector nativo o aplicación certificada para la exportación/integración bidireccional de eventos con la plataforma Splunk.
5	**GESTIÓN DEL RIESGO**

5.1	El proveedor debe ofrecer una solución en que la información de gestión de superficie de ataque externa (EASM) fluya hacia la misma consola de gestión del NGAV a través de una integración nativa o API y que realice un análisis continuo y en tiempo real de todos los activos de la organización, especialmente del correo electrónico, permitiendo una visión integral del riesgo de ciberseguridad. Se requiere: 5.1.1 Correlación unificada de telemetría desde múltiples fuentes. 5.1.2 Evaluación integral de riesgos. 5.1.3 Visibilidad de la superficie de ataque, incluyendo activos expuestos a Internet. 5.1.4 Calificación de riesgo contextualizada, considerando la criticidad y la exposición de los activos.
5.2	La solución debe contar con capacidades de inteligencia de amenazas en tiempo real para prevenir, detectar y priorizar vulnerabilidades críticas antes de que sean explotadas. Se requiere: 5.2.1 Priorización basada en explotación activa en el mundo real, no solo en criticidad teórica. 5.2.2 Correlación automática con intentos de explotación detectados. 5.2.3 Análisis de configuraciones incorrectas en múltiples plataformas.
5.3	El proveedor debe ofrecer una solución que permita actuar sobre los riesgos detectados sin intervención manual, asegurando una reducción proactiva de la superficie de ataque. Se requiere: 5.3.1 Recomendaciones accionables para mitigación inmediata de riesgos. 5.3.2 Playbooks de respuesta automatizados para la remediación de vulnerabilidades. 5.3.3 Integración con soluciones de control de acceso para respuesta automática ante amenazas. 5.3.4 Capacidad de personalización de reglas de riesgo. 5.3.5 Métricas de mejora de postura de seguridad en el tiempo.
5.4	La plataforma debe proporcionar una vista centralizada del riesgo organizacional con métricas claras y accionables para la toma de decisiones estratégicas. Se requiere: 5.4.1 Vista unificada de los riesgos de la organización, sin necesidad de múltiples herramientas. 5.4.2 Métricas comparativas con la industria, permitiendo evaluar el nivel de seguridad frente a otros sectores. 5.4.3 Seguimiento de tendencias de riesgo en tiempo real. 5.4.4 KPIs de reducción de riesgo, con mediciones tangibles de mejora de seguridad. 5.4.5 Visualización dinámica de la superficie de ataque, permitiendo identificar activos críticos expuestos.
5.5	El proveedor debe contar con capacidades avanzadas de análisis de riesgos en múltiples capas de seguridad. Se requiere: 5.5.1 Evaluación de riesgos en buzones de correo en la nube, detectando configuraciones inseguras o accesos sospechosos. 5.5.2 Detección de anomalías en comportamiento de usuarios, identificando accesos o actividades fuera del patrón normal.
5.6	La solución debe poder gestionar todos los activos descubiertos desde una única consola de gestión unificada.
5.7	La solución debe poder integrarse con proveedores externos para incorporar o enriquecer datos de la superficie de ataque.
5.8	La solución ofrecida debe contar con capacidades para evaluar la postura de identidad y detectar amenazas asociadas, gestionables desde su consola centralizada (ya sea de forma nativa o mediante módulos especializados totalmente integrados). Esto debe lograrse mediante la integración con el Directorio Activo (On-premises y/o Cloud) u otros proveedores de identidad corporativos. La solución debe generar un índice o nivel de riesgo que permita identificar y priorizar brechas de postura (ej. usuarios con MFA deshabilitado, contraseñas no robustas, políticas de expiración deshabilitadas) y detectar eventos de riesgo activo, tales como, pero sin limitarse a: viajes imposibles, volcado de credenciales (credential dumping), credenciales filtradas en la dark web, ataques de fuerza bruta, Golden Ticket, Pass-the-Hash, entre otros.
5.9	La solución debe contar con capacidades automatizadas de caza de amenazas que permitan realizar barridos periódicos y continuos de Indicadores de Compromiso (IoCs). Este análisis debe contrastar de forma retrospectiva la

	telemetría histórica de la entidad tanto con los reportes de inteligencia globales provistos por el fabricante (vendor), como con flujos de información de fuentes de terceros (tales como entidades gubernamentales, CSIRTs nacionales o centros de investigación de ciberseguridad), permitiendo identificar de manera precisa y oportuna el activo o endpoint afectado ante cualquier coincidencia (match) en el ambiente.
5.10	La solución debe ser capaz de identificar si la organización está por encima, por debajo o en promedio del nivel de riesgo de compañía a nivel de sector industrial, tamaño organizacional o regional.
5.11	La solución debe ser capaz de modificar la criticidad de un activo en función de la necesidad de la entidad.
5.12	La solución debe contar con la capacidad nativa de diseñar, almacenar y ejecutar flujos de trabajo u orquestaciones lógicas de respuesta automatizada (Playbooks o Runbooks). Estos componentes deben permitir la automatización de acciones de mitigación, contención y remediación de incidentes de seguridad de forma proactiva, reduciendo los tiempos de respuesta (MTTR) ante la detección de amenazas en la infraestructura de la entidad sin requerir obligatoriamente intervención manual.
5.13	La solución debe poder evaluar la situación de seguridad de Internet y otros activos externos de la organización (Gestión de la superficie de ataque externa).
5.14	La solución debe proporcionar una puntuación de riesgo para toda la organización basada en una evaluación continua de los riesgos en la organización.
5.15	La solución debe tener la funcionalidad de incorporar criticidad de los activos, las vulnerabilidades, la actividad de amenazas y la configuración de los controles de seguridad en el cálculo del puntaje de riesgo para cada tipo de activo.
5.16	La solución debe proporcionar un índice de exposición que resuma la probabilidad de que se produzca una vulnerabilidad o amenaza en el entorno.
5.17	Debe utilizar múltiples proveedores de datos de descubrimiento (la dependencia del agente existente debe complementarse con proveedores de descubrimiento adicionales).
5.18	La solución debe proporcionar capacidades analíticas para la gestión de vulnerabilidades, permitiendo visualizar el comportamiento histórico y la evolución temporal del riesgo tecnológico tanto en activos internos como en aquellos expuestos o con acceso a Internet. Asimismo, la plataforma debe cumplir con las siguientes especificaciones: a. Priorización Basada en Riesgo Real: Capacidad de identificar, contabilizar y priorizar de forma prioritaria aquellas vulnerabilidades analizadas que posean un estado de explotación activo o alta probabilidad de armamento (Weaponization / Active Exploitation) en el panorama global de amenazas. b. Benchmarking o Comparativa Sectorial: Permitir la comparación estadística y gráfica del nivel de exposición o puntuación de vulnerabilidades de la entidad frente al promedio global, regional o de su sector industrial o gubernamental.
5.19	La solución propuesta debe proporcionar capacidades analíticas para la gestión de vulnerabilidades sobre activos internos y con acceso a Internet, permitiendo el rastreo histórico y evolutivo de los riesgos a lo largo del tiempo. Asimismo, la plataforma debe incluir el siguiente indicador de gestión y funcionalidad: a. Métrica de Tiempo de Exposición o Remediación: Capacidad de calcular e informar el tiempo promedio de permanencia de las vulnerabilidades o antigüedad del riesgo sin mitigar (Mean Time to Remediate / Age of Vulnerability), permitiendo auditar la eficiencia en la aplicación de parches o controles de compensación. b. Benchmarking Global: Permitir la comparación estadística y gráfica de la puntuación de riesgo o eficiencia de la entidad frente al promedio global, regional o sectorial del fabricante.
5.20	La solución debe proporcionar la función de poder identificar aquellos riesgos de mayor prioridad para mitigar, basado en la meta que el cliente desee abordar para disminuir el número de riesgo, y así, la solución deba calcular basado en la métrica ingresada por el cliente, lograr mostrar los riesgos de mayor foco a mitigar.
5.21	Debe proporcionar información sobre la postura de seguridad de la organización mediante un panel de control de nivel ejecutivo. Debe poder mostrar la puntuación de riesgo general de la empresa, los riesgos de los activos individuales, una vista de los ataques en curso y sus factores de riesgo contribuyentes.

5.22	La solución debe permitir que los informes se puedan generar por demanda o mediante programación.
5.23	El contenido de los informes se pueda filtrar para limitar la salida según criterios seleccionados.
5.24	Debe proporcionar la capacidad de la vista de inventario y de operaciones; tener la facilidad de realizar filtros por diferentes tipos de información (Tipo de Activo, qué tecnología lo descubrió, índice de riesgo, etc).
6	**PROTECCION MOBILE**
6.1	La solución debe extender sus capacidades de detección y respuesta (XDR) hacia dispositivos móviles (sistemas operativos Android e iOS como mínimo). Para su despliegue y enrolamiento, la plataforma debe soportar métodos flexibles que incluyan el enrolamiento directo (mediante invitaciones por usuario o códigos QR) y capacidades de integración nativa o soportada con las principales plataformas de Gestión de Dispositivos Móviles / Gestión Unificada de Dispositivos (MDM/UEM) del mercado (tales como Microsoft Intune o equivalentes), facilitando la distribución masiva del agente de seguridad y la correlación de eventos móviles en la consola centralizada de la entidad.
7	**SERVICIOS PROFESIONALES**
7.1	Las licencias adquiridas deberán entregarse debidamente instaladas, configuradas y en pleno funcionamiento en la plataforma correspondiente.
7.2	El contratista deberá entregar un documento impreso en el que se especifique el número de licencias autorizadas, su vigencia, el nombre del software y la versión correspondiente. Asimismo, deberá autorizar explícitamente a la Entidad el uso de versiones posteriores que se liberen durante el período de licenciamiento establecido en el numeral 10.2.
7.3	El contratista deberá entregar un informe técnico de implementación, en el cual se documenten detalladamente las funcionalidades instaladas y configuradas en la solución, incluyendo los módulos habilitados, parámetros de configuración aplicados, componentes implementados y su estado de operación. Este informe deberá evidenciar la correcta instalación, integración y puesta en funcionamiento de la solución dentro de la infraestructura tecnológica de la Entidad.
8	**EQUIPO MÍNIMO DE TRABAJO**
8.1	Un profesional Ingeniero Electrónico, de Sistemas o Telecomunicaciones y Especialización en Seguridad de la Información o Informática, con mínimo tres (3) años de experiencia contada a partir de la expedición de la tarjeta profesional. Dentro de los tres años de experiencia se debe acreditar experiencia mínima de seis (6) meses, en configuración y mantenimiento en soluciones de seguridad informática, y debe contar con tarjeta profesional vigente. Certificaciones Mínimas: - Certificación técnica vigente por parte del fabricante ofrecido, de nivel avanzado. - CEH (Certified Ethical Hacker) vigente. - CISSP – Certified Information Systems Security Professional.
8.2	Un técnico o tecnólogo en sistemas, telecomunicaciones, electrónica o afines. Mínimo dos años de experiencia en configuración y mantenimiento en soluciones de seguridad informática. Certificaciones Mínimas: - Certificación técnica vigente por parte del fabricante ofrecido, de nivel avanzado. - ISO 27001 - Auditor Líder.
9	**TRANSFERENCIA DE CONOCIMIENTO**
9.1	El contratista llevará a cabo la transferencia de conocimiento para el manejo de la consola de gestión del software propuesto. Esta transferencia será de mínimo diez (10) horas para los colaboradores que la entidad designe, de manera virtual o de la forma que acuerden las partes. Deberá ser impartida por personal certificado por el fabricante.
10	**SERVICIOS COMPLEMENTARIOS**
10.1	**Soporte:** Se requiere soporte especializado por doce (12) meses, a partir de la fecha de activación del licenciamiento adquirido.

	La atención de incidentes debe realizarse en un máximo de cuatro (4) horas a partir del reporte del mismo, en un esquema 7x24 (7 días a la semana, 24 horas al día). **Nota:** Los acuerdos de niveles de servicio (SLA) definidos en esta ficha serán incorporados como obligaciones contractuales con las consecuencias previstas en el contrato (multas por incumplimiento, de acuerdo con el artículo 17 de la Ley 1150 de 2007). El soporte en sitio del contratista se debe realizar trimestralmente por un espacio mínimo de cuatro (4) horas, con revisión proactiva e informe sobre el comportamiento del sistema y opciones de mejora. Las fechas para realizar el soporte serán establecidas al momento de la suscripción del acta de inicio.
10.2	**Actualizaciones:** Durante doce (12) meses, a partir de la respectiva activación, así como registro a nombre de la Secretaria Distrital de Ambiente, con lo cual la SDA tiene derecho a la descarga e instalación de todas las actualizaciones, parches y mejoras tecnológicas liberadas en el mercado del software sin costo adicional.
10.3	**Configuración:** El contratista realizará la configuración de la licencia, alineado con los mejores estándares de seguridad. Se debe garantizar que todos los dispositivos finales que se encuentren operativos en la entidad queden con el agente instalado y actualizado al momento que se lleve a cabo instalaciones, actualizaciones, soportes y/o mantenimiento de las licencias. Todos los gastos que demanden la preparación y ejecución de los trabajos deben estar incluidos en el valor de la oferta.

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:

1.1. 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.

1.2. 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.

1.3. 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.

1.4. 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.

NORMATIVIDAD QUE RIGE LAS CONDICIONES TÉCNICAS:

- ISO/IEC 27001 (A.12.4.1 – registro y monitoreo de eventos).
- NIST CSF (Detect / Respond / Recover).
- MITRE ATT&CK / D3FEND Framework (detección y respuesta correlacionada).
- CIS Controls 13 y 16 (detección de anomalías, gestión de incidentes).
- Norma Técnica Colombiana NTC-ISO/IEC 27001: Esta norma define los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). El SGSI se basa en la gestión del riesgo para preservar la confidencialidad, integridad y disponibilidad de la información.
- Resolución 1519 de 2020 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y su Anexo 3, que incluye, entre otros, los requisitos:
  - Implementar sistemas antivirus en el servidor web.
  - Implementar firewalls y sistemas de detección de intrusiones.
  - Segmentar la red.
  - Utilizar protocolos de comunicación seguros (HTTPS, VPN).
- Ley 1581 de 2012 y decretos reglamentarios (Decreto 1377 de 2013, compilado en el Decreto 1081 de 2015, y el Decreto 1074 de 2015). Esta normativa establece el marco general para la protección de datos personales en Colombia y requiere la implementación de medidas técnicas y organizativas necesarias para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos personales. La implementación de soluciones como antivirus y seguridad perimetral son fundamentales para cumplir con estos requisitos de protección de datos.
- Política de Gobierno Digital (Decreto 1008 de 2018, compilado en el Decreto 1078 de 2015). Esta política promueve el máximo aprovechamiento de las TIC por parte de las entidades públicas e incluye la seguridad de la información como uno de sus habilitadores transversales fundamentales. Los lineamientos de esta política, junto con otros como la Seguridad Digital y la Gestión Documental, deben ser integrados en la implementación.
- Decreto 1074 de 2015: Este decreto reglamenta parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
- CONPES 3854 de 2016: Define la Política Nacional de Seguridad Digital, que establece directrices a nivel nacional para la seguridad en el entorno digital.

- Decreto Distrital 575 de 2023: Este decreto establece la necesidad de fortalecer los elementos que garanticen una infraestructura de datos segura y requiere que sus disposiciones se implementen interpretando de manera integral otras políticas y lineamientos como las de Gobierno Digital y Seguridad Digital.

Elaboró: Leonardo Cárdenas / Víctor Plazas / Mauricio Villegas

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