OBJETO:

ADQUISICIÓN Y RENOVACIÓN 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

ALCANCE DEL OBJETO:

Las especificaciones y requisitos técnicos mínimos se encuentran relacionados en el presente documento, en el cual se han incorporado las condiciones técnicas que deberá cumplir el contratista, con las siguientes características en el marco de la ejecución del contrato de acuerdo a las siguientes cantidades, las cuales se encuentran vigentes hasta el día 6 de Octubre del 2025:

- RENOVACIÓN
  - 1.000 licencias para equipos de escritorio
  - 100 licencias para servidores
  - 100 licencias para dispositivos móviles (se redujo 100 licencias)

- ADQUISICIÓN
  - 37 licencias para equipos de escritorio
  - 70 licencias para servidores

DESCRIPCIÓN GENERAL DE LA NECESIDAD

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

Equipos de Cómputo:

-**557 equipos de cómputo y portátiles en producción, distribuido de la siguiente manera : 97** equipos portátiles en producción **+153** equipos de cómputo en producción adquiridos por la entidad **+ 307 equipos de cómputo donados por el IDU en 2023** fueron utilizados por unidades obsoletas que fueron dadas de baja, contribuyendo a la base actual de equipos en producción

-480 equipos son bajo la modalidad de alquiler.

Servidores:

- Se cuenta con **170 servidores en producción**, que incluyen tanto máquinas virtuales como servidores físicos. Para el mantenimiento de esta infraestructura, se requiere:
  - la **renovación de 100 licencias existentes**.

- Adicionalmente, es necesario **proteger 70 nuevos servidores virtuales** que han sido recientemente adquiridos.

Dispositivos Móviles:

- La entidad dispone de **100 dispositivos móviles** que son administrados por la DPSIA (Dirección de Planificación y Seguimiento de la Información y Análisis) para la herramienta SIAMOVIL.

DESCRIPCIÓN	CANTIDAD
DONACIÓN DEL IDU EQUIPOS DE COMPUTO	307
EQUIPOS EN ALQUILER	480
ACTUALIDAD equipos de cómputo en producción adquiridos por la entidad	153
ACTUALIDAD equipos portátiles en producción	97
SERVERS (100 RENOVACIÓN Y 70 NUEVOS)	170
MÓVILES (100 RENOVACIÓN)	100
TOTAL	**1307**

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:

GRUPO	SEGMENTO	FAMILIA	CLASE
PRODUCTOS DE USO FINAL	43000000 Difusión de tecnologías de información y de las telecomunicaciones	43230000 Software	43233200 Software de seguridad y protección

F.SERVICIOS	81000000 Servicios basados en ingeniería, Investigación y Tecnología	81110000 Servicios Informáticos	81111800 Servicios de Sistemas y administración de componentes de sistemas
F.SERVICIOS	81000000 Servicios basados en ingeniería, Investigación y Tecnología	81110000 Servicios Informáticos	81112500 Servicios de alquiler o arrendamiento de licencias de software de computador
F.SERVICIOS	81000000 Servicios Basados en Ingeniería, Investigación y Tecnología	81110000 Servicios informáticos	81111808 Servicio de análisis de sistemas

A) CONDICIONES TÉCNICAS

Las especificaciones y requisitos técnicos mínimos se encuentran relacionados en el presente <<ANEXO - FICHA TÉCNICA>>, en el cual se han incorporado las características técnicas establecidas que deberá cumplir el contratista en el marco de la ejecución del contrato.

LICENCIAS END POINT DE ULTIMA GENERACIÓN			
Denominación del Bien:		Licencias	
Denominación Técnica:		Renovación, adquisición y soporte de Licencias End Point de última Generación	
Ítem	Descripción técnica del bien, obra o servicio a contratar	Cantidad	Unidad de medida
1.1.	Cantidad	RENOVAR Y ADQUISICIÓN DE MIL TRESCIENTAS SIETE (1307) LICENCIAS POR UN TERMINO DE DOCE (12) MESES Distribuidas así: ● RENOVACIÓN - 1000 licencias para equipos de escritorio - 100 licencias para servidores - 100 licencias para dispositivos móviles (se redujo 100 licencias) ● ADQUISICIÓN	UNIDAD

		- 37 licencias para equipos de escritorio - 70 licencias para servidores	
1.2.	Descripción del Bien	Renovación, adquisición y soporte para el licenciamiento de una solución de protección EndPoint de última generación, por un (1) año a partir del 6 de octubre de 2025, fecha en la cual expira el licenciamiento y soporte actual, esta solución debe ser implementada o renovada en su totalidad de acuerdo a la necesidades actuales de la SDA para salvaguardar los equipos informáticos (equipos de escritorio, servidores y dispositivos móviles) de la Secretaría Distrital de Ambiente	UNIDAD
1.3.	Generalidades	Renovación, adquisición y soporte del Licenciamiento End Point de última generación y con vigencia de un (1) año a partir del 7 de octubre de 2025, fecha en la cual expira el licenciamiento y soporte actual	UNIDAD
1.4	Características de la Renovación, adquisición y soporte	➢ Se debe garantizar que la renovación, adquisición y soporte las licencias End Point de última generación sean de la última versión liberada en el mercado tanto en la consola como en los agentes de dispositivos finales. ➢ Deben garantizar la protección de los dispositivos finales ante cualquier tipo de virus y mutaciones de los mismos, así como de cualquier software malicioso. ➢ Debe ser transparente para los usuarios que hacen uso de los dispositivos finales, como son: equipos de cómputo, equipos servidores, equipos portátiles, dispositivos móviles	UNIDAD
1.5	Tipo	Renovación, adquisición y soporte	UNIDAD
1.6	Solución	Software End Point de última Generación	UNIDAD
2.	SERVICIOS		

2.1.	Tiempo de Servicios de actualización	Vigencia de UN (1) AÑO, contado a partir de la renovación, adquisición, soporte y su respectiva activación, así como registro a nombre de la Secretaría Distrital de Ambiente MIL TRESCIENTAS (1300) LICENCIAS Distribuidas así: ● RENOVACIÓN - 1000 licencias para equipos de escritorio - 100 licencias para servidores - 100 licencias para dispositivos móviles (se redujo 100 licencias) ● ADQUISICIÓN - 37 licencias para equipos de escritorio - 70 licencias para servidores	UNIDAD
2.2.	Soporte	➢ Se requiere soporte especializado por un (1) año, 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 7*24. El soporte en sitio del contratista será trimestral por un espacio mínimo de cuatro (4) horas, con revisión proactiva e informe periódico 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.	UNIDAD
2.3.	Actualizaciones	➢ Durante UN (1) AÑO a partir de la Renovación, adquisición, soporte y su 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.	UNIDAD
2.4	Configuración	➢ La solución debe poseer la funcionalidad de protección contra el cambio de la configuración del agente	UNIDAD

		➢ Debe impedir a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección ➢ Debe tener algún mecanismo contra la desinstalación del endpoint ➢ Debe permitir la utilización de una contraseña de protección para posibilitar la reconfiguración local en el usuario o la desinstalación de los componentes de protección ➢ El Endpoint de última Generación deberá contar con detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido .	
2.5	Garantía de fábrica	Por UN (1) AÑO a partir de la Renovación, adquisición , soporte y su respectiva activación, así como registro a nombre de la SDA.	UNIDAD
2.6	Personal requerido	El contratista deberá suministrar al menos un ingeniero de Sistemas, Ingeniería Informática / Ingeniería en Tecnologías de la Información (TI), Ingeniería de Redes y Telecomunicaciones, Ciberseguridad / Seguridad Informática, Ingeniería Electrónica / Ingeniería Telemática o su equivalente; Certificado con el fabricante para garantizar el soporte y la implementación de la solución, adicional a las certificaciones técnicas que lo acrediten para el desarrollo del proyecto	UNIDAD
2.7	Transferencia de Conocimientos	El contratista llevará a cabo la transferencia de conocimiento para el manejo de la consola de gestión de la herramienta propuesta. Esta transferencia será de mínimo ocho (8) horas para los colaboradores de la entidad, de manera virtual o de común acuerdo entre las partes. Deberá ser impartida por personal certificado por el fabricante.	UNIDAD

B) CARACTERÍSTICAS DEL PRODUCTO

ITEMS SOLICITADOS		
1	Características generales. El producto debe ofrecer las siguientes capacidades	La solución debe permitir el establecimiento del ancho de banda máximo a consumir para las actualizaciones. - Debe ser capaz de comprobar el comportamiento malicioso para detectar malware desconocido - Debe poseer la funcionalidad de protección contra el cambio de la configuración del agente - Debe impedir a los usuarios, incluyendo el administrador local, configurar, deshabilitar o desinstalar componentes de la solución de protección - Debe tener algún mecanismo contra la desinstalación del endpoint, como por ejemplo, una contraseña - Debe permitir la utilización de una contraseña de protección para posibilitar la reconfiguración local en el usuario o la desinstalación de los componentes de protección - Se debe tener la capacidad de resolver características de riesgo de forma automática con un botón de acción - La administración de riesgo debe gestionar los diferentes puntos de riesgo a nivel de sistema operativo y a nivel de red - Licencias para PCs, Servidores y Dispositivos Móviles que puedan administrar los servicios de seguridad para la solución de endpoint, para servidores, desktops/laptops y dispositivos móviles. - Actualización de los componentes de la consola de administración. - El EndPoint de última generación deberá proteger computadoras portátiles, computadores de escritorio, servidores y dispositivos móviles, en tiempo real, bajo demanda o programado para detectar, bloquear y limpiar todos los virus, troyanos, gusanos y spyware. En Sistema Operativo Windows, Linux y Mac el agente también deberá detectar PUA, adware y comportamiento sospechoso - El EndPoint de última Generación deberá de contener protección integrada, es decir, en un solo agente tendrá como mínimo: control de amenazas, control de dispositivos, control de aplicaciones, control web, prevención de fuga de información (DLP), gestión del firewall de Windows, protección contra virus, spyware, troyanos, gusanos, adware y aplicaciones potencialmente no deseadas (PUA).

2	Consola de administración configuración, administración, monitoreo y manejo de la solución	1. La consola de administración centralizada , basada en web y en nube, que deberá soportar e incluir todos los componentes para la administración, monitoreo y control de la protección en estaciones de trabajo, servidores y dispositivos móviles.
		2. La consola de administración deberá utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los usuarios administrados.
		3. La consola de administración web permitirá definir grupos de usuarios con distintos niveles de acceso a las configuración, políticas y registros
		4. La consola de administración web deberá contener un Dashboard con el resumen del estado de protección en estaciones de trabajo, así como de servidores y dispositivos móviles. También tendrá que indicar de forma visible y clara las alertas de eventos críticos, altos, medios e informativos.
		5. La consola de administración web debe realizar como mínimo el envío automático de alertas críticas mediante correo electrónico a los administradores. Como mínimo problemas de licencias, alertas de brotes de ataques y amenazas, máquinas desactualizadas, entre otras.
		6. La consola de administración web deberá de mostrar información como nombre de la máquina, sistema operativo, dirección IP, versión del Endpoint de última generación instalado, versión del motor, fecha de la actualización, fecha de la última verificación, evento reciente, estado, grupo, número de virus detectados, etc.
		7. La consola de administración web debe permitir la organización en grupos de las estaciones de trabajo, así como de servidores dentro de la estructura de administración.
		8. La consola de administración web deberá tener la capacidad de aplicar políticas de protección diferentes por grupos de máquinas y equipos individuales.
		9. La consola de administración web deberá permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.
		10. La consola de administración web tendrá un mecanismo de comunicación vía API, Syslogs, para su integración con otras soluciones de seguridad, como por ejemplo análisis de comportamiento de tráfico de red con inteligencia artificial.
		11. Desde la consola de administración web se podrá descargar el o los paquetes de instalación de la solución de Endpoint de última

		generación así como las descargas de actualización del producto y de las definiciones de virus y protección contra intrusos.
		12. La consola de administración web deberá realizar la actualización remota en tiempo real, de la solución y del mecanismo de verificación (Engine) de los usuarios
		13. La consola de administración web permitirá seleccionar un grupo de dispositivos para aplicar la actualización para controlar el ancho de banda de red.
		14. La consola de administración web deberá soportar la actualización de la versión de los end point, para que esta se realice de modo transparente para los usuarios finales.
		15. La comunicación del agente hacia la consola debe permitir controlar el uso de ancho de banda para la descarga de firmas.
		16. La consola de administración deberá tener la posibilidad de implementar servidores de actualización locales para utilizar de manera eficiente el uso del ancho de banda.
		17. La consola de administración web deberá tener la posibilidad de instalar un servidor local para reenvío de eventos (message relay) en caso de que el agente no pueda comunicarse con la consola en la nube.
		18. La consola de administración web deberá permitir la programación de la exploración contra virus con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador.
		19. La consola de administración web podrá permitir exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política
		20. Los mensajes generados por el agente deben estar en el idioma castellano o permitir su edición.
		21. La consola de administración web deberá de permitir la exportación de los informes gerenciales a los formatos csv y pdf.
		22. La consola de administración deberá tener la capacidad de generar informes, estadísticas o gráficos, detallando la siguiente información: ➢ Detalle de usuarios activos, inactivos o desprotegidos, así como detalles de estos. ➢ Detalle de los equipos de escritorio, servidores y dispositivos móviles que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los equipos. ➢ Detalle de los periféricos permitidos o bloqueados, así como detalles de dónde y cuándo se utilizó cada periférico. ➢ Detalle de las principales aplicaciones bloqueadas y los equipos, usuarios que intentaron acceder a ellas.

		➢ Detalle de las aplicaciones permitidas que fueron accedidas con mayor frecuencia y los equipos, usuarios que las acceden. ➢ Detalle de los equipos y usuarios que intentaron acceder a aplicaciones bloqueadas con mayor frecuencia y las aplicaciones que ellos intentaron acceder. ➢ Detalle de todas las actividades disparadas por reglas de fuga de información.
		23. La consola de administración web deberá permitir la ejecución manual de informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF.
		24. La consola de administración web deberá tener de forma nativa los recursos de informes y monitoreo.
		25. La consola de administración web cuando identifique algún problema, deberá permitir corregir por vía remota, las siguientes acciones: ➢ Proteger el dispositivo con la opción de inicio de una exploración ➢ Forzar una actualización en ese momento ➢ Ver los detalles de los eventos ocurridos ➢ Ejecutar la comprobación completa del sistema ➢ Forzar el cumplimiento de una nueva política de seguridad ➢ Mover el dispositivo a otro grupo ➢ Borrar el dispositivo de la lista.
		26. La consola de administración web deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los equipos que necesitan atención.
		27. La consola de administración web deberá generar un registros de auditoría seguro que supervise la actividad en dicha consola para el cumplimiento de regulaciones, auditorías de seguridad, análisis y solución de problemas forenses, etc.
3	Políticas de la consola de Administración para la gestión de la seguridad de la infraestructura, el producto debe ofrecer	1. Capacidad para aplicar políticas basadas en el usuario registrado o la máquina.
		2. Capacidad para aplicar varias políticas a un único punto final o usuario, pero solo una activa a la vez.
		3. Capacidad para aplicar una política a un grupo de puntos finales o usuarios.
		4. Una plantilla única para cada servicio de seguridad.
		El sistema debe permitir la configuración granular de políticas mediante plantillas para gestionar funcionalidades como el análisis antimalware, el control de aplicaciones (incluyendo listas blancas y negras), el control de acceso web, y el control de dispositivos. Adicionalmente debe facilitar la definición de acciones automáticas ante la detección de malware o dispositivos no compatibles, incluyendo el bloqueo y desbloqueo remoto

4	Informes de la consola de administración	1. Posibilidad de crear informes customizados que incluyan por lo menos los siguientes: - Estado actual del sistema - Eventos del sistema - Informe de usuarios. - Visión General de la protección del sistema - Malware y PUA bloqueados. - Informe de periféricos - Casos generados en el mes. - informe Histórico .
		2.Filtros para informes programados para recibir por correo únicamente información relevante para cada usuario.
		3. Posibilidad de Exportar resumen a archivo .pdf, detalles a archivo .csv.
5	Usuarios	1. Administración basada en roles.
		2. Múltiples tipos predefinidos: superadminsitrador, administrador, reporte o usuario personalizado. a. superadministrador: tiene control total de la solución. b. Administrador: gestiona los servicios de seguridad. c. Reporte: monitorea y crea informes.
		3. Lista de usuarios que se puede sincronizar con Microsoft Active Directory o Azure Active Directory mediante API, crear de forma manual o importando desde un CSV.
		4. Configuración detallada de los derechos de destino administrativos, para seleccionar qué servicios y objetos puede administrar un usuario. Cierre de sesión automático para cualquier tipo de usuario para mayor seguridad con respecto a la información que se muestra en la consola de administración.
6	Logs	1. Registrar las acciones del usuario para su cumplimiento.
		2. Registros detallados para cada acción del usuario.
		3. La solución debe permitir la generación de un Informe detallado de los eventos generados en los diferentes servicios de protección realizados en los endpoints
7	Actualizaciones	1. La solución debe permitir programar las actualizaciones de versión de producto.
		2. La solución debe tener la capacidad de decidir sobre qué equipos se ejecutará la actualización de versión de producto.
		3. La solución debe permitir regresar a una versión anterior en caso de requerirse.
8	Características mínimas de carácter mandatorio	1. La solución ofertada, debe ser de un único fabricante y utilizar un único motor antimalware.
		2. Para un óptimo desempeño de la solución en los equipos, los recursos que debe requerir de los equipos son: PCs: - 8GB de Espacio en Disco - 4GB de Memoria RAM

		- Procesador de 2 Core Servidores: - 10GB de Espacio en Disco - 8GB de Memoria RAM - Procesador de 2 Core
		3. El End Point de última Generación deberá de contener protección integrada, es decir, en un solo agente tendrá como mínimo: control de amenazas, control de dispositivos, control de aplicaciones, control web, prevención de fuga de información (DLP), gestión del firewall de Windows, protección contra virus, spyware, troyanos, gusanos, adware y aplicaciones potencialmente no deseadas (PUA).
		4. El End Point de última generación deberá incluir el control web para permitir controlar el acceso a sitios inapropiados, con al menos 60 categorías de sitios inadecuados y esto se debe hacer por grupos de roles y/o usuarios. También debe permitir la creación de listas blancas y listas negras.
	Control de Aplicaciones	1. El Endpoint de última Generación con el control de aplicaciones para monitorear e impedir que los usuarios ejecuten o instalen aplicaciones que puedan afectar la productividad o el rendimiento de la red
		2. El End Point de última generación deberá tener la capacidad de reconocer y bloquear automáticamente las aplicaciones en los usuarios basándose en la huella digital (hash) del archivo.
		3. El End Point de última generación deberá actualizar de forma automática la lista de aplicaciones que se pueden controlar, permitiendo aplicaciones o las categorías específicas de aplicaciones que pueden ser liberadas o bloqueadas.
		4. El End Point de última generación deberá detectar aplicaciones controladas cuando los usuarios acceden, con las opciones de permitir y alertar o bloquear y alertar.
9	Prevención de Fuga de Información DLP	1. El End Point de última generación deberá poseer protección de fugas o pérdida de datos sensibles en el mismo agente de protección, considerando su contenido, además de la posibilidad de evaluar la extensión del archivo y múltiples destinos.
		2. El End Point de última generación deberá permitir la identificación de información confidencial, como números de pasaporte u otra información personal identificable y / o información confidencial, incluso si los documentos no se han clasificado correctamente, utilizando CCL (Lista de control de contenido).
		3. El End Point de última generación deberá permitir el bloqueo o sólo registrar el evento en la consola de administración web, o preguntar al usuario si él o ella realmente quiere transferir el archivo identificado como sensible.

		4. El End Point de última generación deberá tener listas de CCL pre configuradas con al menos los siguientes identificadores. (DLP) ➢ Números de tarjetas de crédito. ➢ Números de cuentas bancarias. ➢ Números de pasaportes. ➢ Direcciones ➢ Números de teléfono. ➢ Lista de correos electrónicos. ➢ Soportar agregar reglas propias de contenido con un asistente proporcionado para este propósito.
10	Requisitos del sistema:	1. Sistemas operativos para estaciones de trabajo: Windows 11, Windows 10, Windows 8.1 y Windows 7.
		2. El End Point de última generación deberá soportar máquinas con arquitectura de 32 bits y 64 bits.
		3. El End Point de última generación deberá ser compatible para su instalación en estaciones de trabajo con los sistemas operativos: Windows 7 en adelante, y macOS 13 en adelante.
		4. El Endpoint de última Generación ser compatible para su instalación en servidores con los sistemas operativos: Windows server 2008 R2 en adelante y Linux Amazon Linux, Amazon Linux 2, CentOS 7 y 8, Debian 10, 11 y 12, Oracle Linux 7, 8 y 9, Suse 12 y 15, Ubuntu 18 LTS, 20 LTS y 22 LTS.
		5. Sistemas operativos dispositivos móviles: smartphones y tabletas con arquitectura arm-v7a y arm64-v8a con Android 9.0 o superior, Apple iOS 15, iPadOS 15 o superior.
11	La solución de XDR deberá estar incluida en el mismo agente del End Point de última Generación deberá proveer mínimo las siguientes funcionalidades	1. La solución deberá permitir al administrador aislar de forma manual una máquina de la red para su investigación.
		2. La solución deberá permitir el aislamiento en la red de los equipos de manera automática en caso de presencia de actividad sospechosa.
		3. Analizar continuamente los riesgos utilizando cientos de factores para descubrir y priorizar los riesgos de seguridad para todos sus endpoints, lo que permite la adopción automática de acciones de endurecimiento.
		4. La solución deberá permitir que el administrador tenga la capacidad de realizar búsquedas de amenazas en los equipos, al menos por hash, IP o URL
		5. La solución deberá de ser capaz de realizar consultas basadas en lenguaje SQL para poder identificar comportamiento malicioso o hacer caza de amenazas (Threat hunting).
		6. La solución debe de contar con más de 200 consultas predefinidas para facilidad de la institución.
		7. La solución debe de poder personalizar o crear nuevas consultas para la personalización de estos indicadores de compromiso que le hagan sentido a la institución y poder detectar de forma temprana un posible evento de seguridad informática.

		8. La solución debe de poder calendarizar las consultas para que se puedan realizar en el horario que más le convenga a la institución y contar con los resultados de las consultas de forma periódica.
		9. La solución debe de poder almacenar los datos de los Indicadores de Compromiso detectados por la solución de XDR en la consola de gestión basada en nube por un periodo de 90 días para poder llevar a cabo consultas de forma histórica y sin la necesidad que el equipo y/o servidor se encuentre en línea.
		10. La solución debe de tener capacidad de iniciar procesos de investigación basados en procesos de análisis que se realicen dentro de la consola de gestión y que se encuentren mapeados al framework Mitre Attack.
		11. La solución deberá permitir la captura de un snapshot forense.
		12. Se debe poder personalizar consultas o enriquecimientos que abran sitios web de terceros para buscar información sobre posibles amenazas a partir de la selección de elementos de datos en los resultados de una consulta y utilizarlos como base para otras acciones "axiales", incluidos enriquecimientos.
		13. Debe permitir tener visibilidad de los ataques de forma previa y posterior al incidente, con el fin de que los analistas de seguridad puedan realizar análisis de causa raíz tanto en ataques bloqueados como en actividades sospechosas y riesgosas en curso.
		14. Se debe de tener la capacidad de tomar control remoto de un equipo aislado utilizando una interfaz tipo CMD y de forma segura desde la misma consola de gestión para poder ejecutar comandos de sistema operativo y poder llevar a cabo el proceso de remediación.
		15. El agente y consola para endpoint, servidores, desktops/laptops y agente y consola para usuarios Móviles deberá incorporar todas las tecnologías necesarias para proteger eficazmente los endpoints empresariales y detener todas las amenazas digitales. Eliminar la necesidad de ejecutar varios agentes y simplificar significativamente la implementación y la operativa.
		16. Cobertura multiplataforma y API de integración de terceros: Cubre todos los endpoints empresariales que ejecuten Windows, Linux o Mac, en infraestructuras físicas, virtualizadas o en la nube, y proporciona seguridad consistente en toda la infraestructura. Admite la integración con herramientas de operaciones de seguridad preexistentes (SIEMs, como por ejemplo Splunk), o Sistemas de análisis comportamentales de tráfico de red con Inteligencia Artificial y tecnologías específicas de centros de datos (los principales hipervisores del mercado).
12	Administración e instalación remota:	1. La instalación debe poder realizarse de varias formas: a. Descargando el paquete antimalware directamente a la

		estación de trabajo donde se instalará. b. Creando un paquete que se pueda impulsar desde el Directorio Activo mediante GPO. c. Enviado link de descarga al usuario para que lo ejecute de forma silenciosa.
		2. La consola de administración informará el número de estaciones de trabajo que tienen la solución instalada y el número de estaciones de trabajo que están desprotegidas.
		3. La consola de administración incluirá información detallada sobre las estaciones de trabajo / servidores: nombre, IP, sistema operativo, módulos instalados, política aplicada, información de actualización, etc.
		4. La consola de administración permitirá al administrador enviar políticas para configurar todo el producto, tanto para estaciones de trabajo, como para servidores y móviles.
		5. La consola de administración permitirá dos tipos de cuentas, administrador y usuario reporteador, que pueden asignarse a qué grupos de usuarios pueden cambiar la configuración o generar informes.
		6. La consola de administración incluirá una sección de registro donde se mencionan todas las acciones, con información detallada: iniciar sesión, editar, crear, cerrar sesión, mover, etc.
		7. La consola de administración permitirá la posibilidad de crear un paquete único, utilizado para sistemas operativos de 32 bits y de 64 bits, MAC y Linux
13	Las principales características y funcionalidades de seguridad	1. Escaneo de comportamiento y monitoreo de procesos.
		2. Tecnología anti-ransomware y anti-exploit.
		3. Capacidad para detectar ataques sin archivos, incluidos aquellos que utilizan herramientas legítimas del sistema operativo, como Powershell o intérpretes de scripts. La solución no debe bloquear globalmente los scripts para lograr esto.
		4. Escaneo bajo demanda y en acceso de cualquier medio de almacenamiento de información (CD, discos duros externos, disco compartido).
		5. La solución debe proporcionar Exclusiones incorporadas para roles de servidor de Microsoft (DNS, DHCP, AD, Exchange, Sharepoint).
		6. El producto antimalware permitirá definir la lista de exclusión del análisis, tanto para el análisis "en acceso" como para el análisis "a pedido", para ciertas carpetas, discos, archivos, extensiones o procesos.
		7. Para no sobrecargar los recursos del sistema, el producto antimalware debe contener un solo motor de análisis. Podrá ejecutar exploraciones programadas con baja prioridad y puede apagarse automáticamente después de explorar la estación de trabajo.

		8. Para una mayor protección, el antimalware debería poder escanear HTTP y SSL(TLS) también.
		9. Para una mejor administración del antimalware instalado en las estaciones de trabajo, el producto incluirá la opción de establecer una contraseña para la protección de la desinstalación.
		10. El End Point de última generación deberá contar con detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.
		11. El End Point de última generación deberá poseer la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección. Así como deberá tener algún mecanismo contra la desinstalación del end point como por ejemplo una contraseña.
		12. El End Point de última generación deberá permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el usuario o desinstalación de los componentes de protección.
		13. El End Point de última generación deberá realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque.
		14. El End Point de última generación deberá realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA)
		15. El End Point de última generación deberá proteger las funciones críticas en los navegadores de Internet (Safe Browsing).
		16. El End Point de última generación deberá permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos.
		17. El Endpoint de última generación debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.
		18. El End Point de última generación deberá ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de buffer.
		19. El End Point de última generación deberá contar con prevención de intrusión en el host (HIPS), que monitoree el código y bloques de código que pueden comportarse de forma maliciosa antes de ser ejecutados.
		20. El Endpoint de última Generación de contar con la capacidad de monitorear los cambios como creaciones o modificaciones sobre carpetas y archivos críticos del sistema basados en una lista pre definida y poder personalizar dicha lista para sistemas operativos Windows server 2008 R2 o superior debido a la criticidad de la información que manejan.

14	Detección proactiva de reconocimiento de nuevas amenazas del End Point de última Generación	1. El End Point de última generación deberá contener la funcionalidad de protección de amenazas de día 0 a través de tecnología de deep learning (signature less).
		2. El End Point de última generación deberá contener la funcionalidad de detección de amenazas desconocidas que están en memoria.
		3. El End Point de última generación deberá contener la funcionalidad de detección, y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.
		4. El End Point de última generación deberá contener la funcionalidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria.
		5. El End Point de última generación no deberá de requerir descarga de firmas de ningún tipo.
		6. El End Point de última generación deberá contener la funcionalidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.
		7. El End Point de última generación deberá contener la funcionalidad de análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro.
		8. El End Point de última generación deberá contener la funcionalidad de bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).
		9. El End Point de última generación deberá contener la funcionalidad de poder generar excepciones ante falsos positivos.
15	Firewall:	1. La solución deberá integrarse con el firewall de host para sistemas operativos Microsoft Windows.
		2. La consola de administración deberá centralizar las alertas generadas por los firewall de los host Microsoft Windows.
		3. La consola de administración deberá permitir configurar al menos dos (2) perfiles de supervisión de Firewall de Windows: únicamente supervisión y supervisión y configuración de perfiles de red.
		4. La consola de administración deberá permitir configurar perfiles de red en los firewall de Windows para redes de dominio, redes privadas y redes públicas.
		5. La consola de administración deberá permitir configurar el tipo de conexión para cada perfil de red: permitir todo, bloquear (con excepciones) o bloquear todo.
16	Control de Usuario:	1. Bloqueo del acceso a Internet para usuarios específicos o grupos de usuarios
		2. Bloqueando el acceso a ciertas aplicaciones.
		3. Bloqueando el acceso a internet por ciertos periodos de tiempo.

		5. Permitiendo el acceso a páginas web específicas especificadas por el administrador.
		6. Restringir el acceso a ciertos sitios web por algunas categorías predeterminadas (por ejemplo, citas en línea, violencia, etc.).
17	Control de dispositivos:	1. Prevención de fugas de datos confidenciales e infecciones de malware a través de dispositivos conectados.
		2. Reglas de bloqueo y exclusiones a través de políticas a nivel de tipos de dispositivo.
		3. Enviará información como el nombre del dispositivo, ID de clase, fecha y hora de conexión.
		4. Tipos de dispositivos predefinidos como: ➢ Pendrives USB ➢ Almacenables removibles seguras ➢ CD, DVD, Blu-ray, floppy drives. ➢ Interfaces de red inalámbrica ➢ Módems ➢ Bluetooth ➢ Infrarrojo ➢ MTP (Media Transfer Protocol) ➢ PTP (Picture Transfer Protocol) como cámaras digitales.
		5. Permitir configuraciones y privilegios como permitido y bloqueado.
		6. Admite el modo de solo lectura para dispositivos de almacenamiento.
		7. Capacidad para bloquear solo el USB y permitir que se utilicen todos los demás puertos.
		8. Permitir la configuración de exclusiones para diferentes tipos de dispositivos.
		9. Soporte para definir exclusiones de dispositivos: a. Por ID de producto b. Por modelo del producto
		10. Habilidad para descubrir dispositivos.
18	Análisis automático en ambiente controlado de archivos sospechosos	1. La solución debe tener la capacidad de realizar un análisis en profundidad de los archivos sospechosos.
		2. La solución debe tener la capacidad de enviar archivos de forma automática o manual a su sandbox.
		3. La solución debe bloquear el acceso al archivo mientras se determina su estado de seguridad.
		4. La solución debe bloquear el archivo si representa una amenaza.
19	Protección contra Vulnerabilidades y técnicas de explotación	1. Debe proporcionar protección en ejecución contra intentos de explotación dirigidos a vulnerabilidades conocidas y desconocidas en aplicaciones de uso común.

		2. Capacidad para agregar aplicaciones personalizadas y presentar una lista de aplicaciones predefinidas.
		3. El End Point de última Generación deberá contar como mínimo con la detección y protección de las siguientes técnicas de explotación ➢ Enforce Data Execution Prevention; ➢ Mandatory Address Space Layout Randomization; ➢ Bottom-up ASLR; ➢ Null Page (Null Deference Protection); ➢ Heap Spray Allocation; ➢ Dynamic Heap Spray; ➢ Stack Pivot; ➢ Stack Exec (MemProt); ➢ Stack-based ROP Mitigations (Caller); ➢ Branch-based ROP Mitigations (Hardware Assisted); ➢ Structured Exception Handler Overwrite (SEHOP); ➢ Import Address Table Filtering (IAF); ➢ Load Library; ➢ Reflective DLL Injection; ➢ Shellcode; ➢ VBScript God Mode; ➢ Wow64; ➢ Syscall; ➢ Hollow Process; ➢ DLL Hijacking; ➢ Squiblydoo Applocker Bypass; ➢ APC Protection (Double Pulsar / AtomBombing); ➢ Process Privilege Escalation
		4. El End Point de última generación deberá tener la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidades conocidas o de día cero.
		6. El End Point de última generación deberá contar con mitigación de inyección de códigos en procesos.
		7. El End Point de última generación deberá contar con protección contra robo de credenciales.
		8. El End Point de última generación deberá contar con protección contra malware escondido en aplicaciones legítimas (code cave).
		9. El End Point de última generación deberá evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.
		10. El End Point de última generación deberá evitar obtener escalamiento de privilegios.

		11. El End Point de última generación deberá evitar modificación de las claves de registro para la ejecución de código arbitrario.
20	Detección proactiva de protección contra ransomware	1. El End Point de última generación deberá contener la capacidad de protección contra ransomware basada en comportamiento.
		2. El End Point de última generación deberá contener la capacidad de remediación de la acción de encriptación de los ransomware.
		3. El End Point de última generación deberá contener la detección del cifrado malicioso de forma local o remoto.
		4. El End Point de última generación deberá contener la protección anti-ransomware para el sector de booteo (master boot record).
		5. El End Point de última generación deberá contener la capacidad de restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.
21	Administración del Riesgo	1. Se debe proporcionar un módulo para la administración del riesgo que proporcione indicadores de riesgo de todos los endpoints junto con la descripción de cada punto de riesgo y su correspondiente recomendación para mitigar la afectación por configuración.
		2. Se debe tener la capacidad de resolver características de riesgo de forma automática con un botón de acción.
		3. La administración de riesgo debe gestionar los diferentes puntos de riesgo a nivel de sistema operativo y a nivel de red.

C) CERTIFICACIÓN DISTRIBUIDOR AUTORIZADO El oferente debe presentar con su propuesta:

a) Certificación oficial del fabricante que acredite al oferente como Partner Autorizado para venta y soporte de servicios del producto ofertado en Colombia.
b) Certificación oficial del fabricante de la marca ofertada donde se evidencie que el oferente cuenta con una (1) persona certificada en la plataforma de endpoint de última generación ofrecida.

El documento presentado para acreditar este requisito deberá adicionalmente contener como mínimo lo siguiente:

1. La certificación directa del fabricante deberá estar dirigida a la Secretaria Distrital de Ambiente.
2. La fecha de expedición de esta no debe ser mayor a treinta (30) días calendario previos a la fecha del cierre del presente proceso de selección.
3. La certificación deberá venir expedida en papel membretado del fabricante
4. Deberá indicar expresamente el nombre del PARTNER O DISTRIBUIDOR AUTORIZADO, que en todo caso no podrá ser diferente al nombre del proponente, que está presentando la oferta al presente proceso de contratación.

NOTA 1: En el evento que se realice la oferta por medio de un proponente plural, la certificación deberá ser presentada por mínimo uno de los miembros que lo conforman.

NOTA 2: La CERTIFICACIÓN DE DISTRIBUIDOR AUTORIZADO que esté en una lengua extranjera, debe ser presentada en su lengua original junto con la traducción simple al castellano, lo anterior teniendo en cuenta que para la Entidad, la misma es un documento especializado que en el mercado es de amplia utilización y aceptación en idioma distinto al castellano.

OBLIGACIONES ESPECIFICAS DEL CONTRATISTA

1.Cumplir con las especificaciones técnicas previstas en el << ANEXO - FICHA TÉCNICA>> y demás documentos que hacen parte del contrato.

2. Suministrar y garantizar el licenciamiento del software adquirido, por un término doce (12) meses, contados a partir de la activación, así como registro a nombre de la Secretaria Distrital de Ambiente, de la solución ENDPOINT PROTECTION DE NUEVA GENERACION CON SISTEMA XDR.

3. 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.

4.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.

5. 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.

6. 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.

7. Proteger a la SDA del acceso no autorizado o cualquier modificación, divulgación o destrucción no autorizada de la información que posea el contratista.

8. El contratista deberá garantizar para la ejecución del presente proceso el personal idóneo y calificado para el soporte especializado del licenciamiento adquirido y el respectivo servicio de instalación en caso de ser requerido por la entidad

PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de hasta DOS (2) MESES, contados a partir de la suscripción del acta de inicio, previa expedición del registro presupuestal y de la aprobación de la garantía de cumplimiento.

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.

FORMA DE PAGO

El pago del contrato resultante del presente proceso de selección se efectuará de la siguiente forma:

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 y renovadas del objeto del presente contrato, por una vigencia de UN (1) AÑO contado a partir de la activación de las mismas, así como su respectivo registro a nombre de la Secretaria 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”

Nota: Debido a que las licencias requeridas por la entidad son servicio de computación en la nube (cloud computing) está excluido del IVA, Conforme El artículo 476 del Estatuto Tributario numeral 21.

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. Documento en el cual se describa cada una de las licencias adquiridas a nombre de la Secretaría Distrital de Ambiente sobre el software instalado y configurado, asi como la fecha de vigencia de la activación de las licencias por doce (12) meses.
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.

El precio incluye todos los costos y gastos directos o indirectos, derivados de la celebración, ejecución y liquidación del contrato.

Nota 1: El plazo de pago a contratistas será máximo de treinta (30) días calendario luego de recibido el bien o servicio que determine la cláusula contractual, siempre y cuando se cuente con el recibo a satisfacción por parte del supervisor o interventor y con el cumplimiento de todos los demás requisitos que correspondan a cargo del contratista. Igualmente, los contratistas deben adoptar la obligación general de efectuar el pago de sus obligaciones contractuales, en un término no mayor a treinta (30) días contados a partir de la fecha de la recepción del bien o servicio.

Nota 2: Cuando el proponente que resulte adjudicatario sea una Unión Temporal o Consorcio, una vez obtenido el RUT, debe tramitarse la resolución de autorización de facturación. La factura de venta debe discriminar el porcentaje de participación o valor del ingreso que corresponda a cada uno de los miembros de la Unión Temporal o Consorcio, indicará el nombre o razón social y el NIT de cada uno de ellos. Estas facturas deberán cumplir los requisitos señalados en las disposiciones legales y reglamentarias.

Si la Unión Temporal o el Consorcio son los adjudicatarios del proceso de selección que realice la Secretaría Distrital de Ambiente, quienes lo integran puedan abrir una cuenta corriente con pluralidad de personas en los términos del artículo 1384 del Código de Comercio o también podrá designarse a uno de los integrantes como titular para su manejo. Para tal efecto, deberán observarse las condiciones para la vinculación de clientes consagrados en el Título Primero, Capítulo Once de la Circular Básica Jurídica (Circular Básica Jurídica 007 de 1996), expedida por la Superintendencia Financiera de Colombia, para que la Entidad realice los pagos en la respectiva cuenta.

Descuentos: El proponente deberá tener en cuenta que la Secretaría efectuará los descuentos de ley del orden Nacional y Distrital vigentes y conforme a sus modificaciones de ley, de acuerdo con la información tributaria suministrada por el contratista a la Entidad y con la actividad objeto del contrato. Así mismo dará estricto cumplimiento al descuento del uno punto uno por ciento (1.1%) del valor bruto del contrato, sin tener en cuenta el valor del Impuesto a las Ventas y de la respectiva adición, si la hubiere, por concepto de Gravamen Estampilla Universidad Distrital Francisco José de Caldas, prevista en el Acuerdo 53 de 2002 del Concejo de Bogotá y el Decreto Distrital 043 del 8 de febrero de 2002 y conforme a sus modificaciones de ley.

La Entidad retendrá el valor de las Estampillas “PRO - CULTURA” y “PRO-PERSONAS MAYORES”, creadas mediante acuerdos 187 y 188 del 2005, sin tener en cuenta el valor del Impuesto a las Ventas, de conformidad con la normatividad aplicable sobre la materia y que equivale a: El 0,5% del valor del contrato por concepto de la Estampilla Pro-Cultura de conformidad con el Acuerdo 187 de 2005 reglamentado por el Decreto 479 de 2005 y el 2% del valor del contrato por concepto de la Estampilla Pro-Persona Mayor, de conformidad con el Acuerdo 645 de 2016, sin tener en cuenta el valor del Impuesto a las Ventas, de conformidad con la normatividad aplicable sobre la materia. Este contrato estará sujeto al régimen tributario vigente para la República de Colombia.

NORMATIVIDAD QUE RIGE LAS CONDICIONES TÉCNICAS.

1. Resolución 1519 de 2020 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y su Anexo 3: Esta resolución define estándares de publicación y divulgación, y su Artículo 6 establece que los sujetos obligados deben observar las condiciones mínimas técnicas y de seguridad digital definidas en su Anexo 3. Este Anexo 3 incluye 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).

- Una debilidad identificada en la implementación de estas condiciones mínimas debe generar tareas específicas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

2. Norma Técnica Colombiana NTC-ISO/IEC 27001: Esta norma especifica 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.

3. 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.

4. 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.

5. CONPES 3854 de 2016: Define la Política Nacional de Seguridad Digital, que establece directrices a nivel nacional para la seguridad en el entorno digital.

6. 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.

CUADRO DE COSTOS

ITEM	DESCRIPCION DEL BIEN O SERVICIO	PRESENTACION / UNIDAD DE MEDIDA	CANTIDAD	VALOR (UNITARIO)	% DE IVA	VALOR IVA	VALOR UNITARIO INCLUIDO IVA	VALOR TOTAL
1	Renovación de licenciamiento endpoint protection para PCs administrados desde una única consola de gestión en nube de nueva generación, con sistema XDR para proteger los equipos informaticos de la SDA. Incluido Soporte, Actualización y Configuración, por un término de 12 meses.	LICENCIAS	1000			-	-	-
2	Renovación de licenciamiento endpoint protection para Servidores administrados desde una única consola de gestión en nube de nueva generación, con sistema XDR para proteger los equipos informaticos de la SDA. Incluido Soporte, Actualización y Configuración, por un término de 12 meses.	LICENCIAS	100			-	-	-
3	Renovación de licenciamiento endpoint protection para Dispositivos Móviles administrados desde una única consola de gestión en nube de nueva generación, con sistema XDR para proteger los equipos informaticos de la SDA. Incluido Soporte, Actualización y Configuración, por un término de 12 meses.	LICENCIAS	100			-	-	-
4	Adquisición de licenciamiento endpoint protection para PCs administrados desde una única consola de gestión en nube de nueva generación, con sistema XDR para proteger los equipos informaticos de la SDA. Incluido Soporte, Actualización y Configuración, por un término de 12 meses.	LICENCIAS	37			-	-	-
5	Adquisición de licenciamiento endpoint protection para Servidores administrados desde una única consola de gestión en nube de nueva generación, con sistema XDR para proteger los equipos informaticos de la SDA. Incluido Soporte, Actualización y Configuración, por un término de 12 meses.	LICENCIAS	70			-	-	-
6	Servicio de soporte, configuración, actualización, mantenimientos correctivos ante fallas, daños de los equipos, servicios profesionales de configuraciones cuando sea requerido por el término de doce (12) meses sobre la infraestructura de antivirus de ultima genración con XDR con la que cuenta la entidad.	SERVICIOS	1			-	-	-
					TOTAL COTIZACIÓN			-

		NIT	
		IDENTIFICACION	
		TELEFONO	
		VIGENCIA COTIZACION	

CONTROL DE CAMBIOS

Versión	Descripción de la modificación	No. Acto Administrativo y fecha
1	Adopción por mejoras del proceso	Radicado 2024IE133828 del 26 de junio del 2024

RESPONSABLES DE ELABORAR O ACTUALIZAR

Elaboró	Revisó	Aprobó
Nombre: Karen Adriana Duarte Mayorga Cargo: Subdirectora Contractual Fecha: 30 de abril de 2024	Nombre: Karen Adriana Duarte Mayorga Cargo: Subdirectora Contractual Fecha: 30 de abril de 2024	Nombre: Jerónimo Juan Diego Rodríguez Rodríguez Cargo: Subsecretario General Fecha: 26 de junio del 2024

Proyecto: Wilmar Alberto González Vázquez

Carlos Mauricio Montenegro H - Apoyo Técnico DPSIA

Revisó: Jhon F Gonzalez M Apoyo Jurídico DPSIA

Adriana E Meza Santander - Apoyo Jurídico DPSIA