ANEXO 6. FICHA TÉCNICA

FICHA TÉCNICA

Proceso de Contratación: CCE-MC-007-2025

Bogotá,

Para el desarrollo del objeto contractual, el contratista debe realizar las siguientes obligaciones específicas, que delimitan el alcance de este:

1. CODIFICACIÓN DE LA NECESIDAD DENTRO DE LA CODIFICACIÓN DE BIENES Y SERVICIOS DE NACIONES UNIDAS.

SEGMENTO	FAMILIA	CLASE	PRODUCTO	NOMBRE DEL PRODUCTO
81000000	8111000	811125	81112501	Servicio de licencias del software del computador
81000000	8111000	8111220	81112200	Mantenimiento y soporte de Software
81000000	8100000	8111220	81112208	Mantenimiento de software de protección y seguridad
43000000	4323000	4313320	43233205	Software de seguridad de transacciones y de protección contra virus

2. OBJETO CONTRACTUAL.

Renovar el licenciamiento de una solución de antivirus / antimalware por un año, que incluya la implementación, configuración y puesta en marcha, que permita proteger, detectar y eliminar software malicioso contribuyendo a la implementación de herramientas de seguridad de los servicios de información para la compra pública.

3. ESPECIFICACIONES TÉCNICAS:

ANEXO 6. FICHA TÉCNICA

ITEM	ESPECIFICACIONES TECNICAS	
1	**Rendimiento Optimizado:**	• La solución de antivirus ESET debe ser eficaz en la detección y prevención de amenazas, sin comprometer significativamente el rendimiento de los servidores. • La solución de antivirus ESET debe ser compatible con la nube de Azure, la nube de Oracle y entornos on-premise y estar optimizada para funcionar eficientemente en todos estos entornos. • La solución antivirus de ESET debe contar con la capacidad de integrarse con características específicas de seguridad, especialmente en sus versiones empresariales como ESET PROTECT y ESET Server Security.
2	**Compatibilidad con Sistemas Operativos y Arquitecturas x86 y x64.**	• La solución de antivirus ESET debe ser compatible con las diferentes arquitecturas del mercado (arquitecturas x86 y x64). • La solución antivirus ESET en alguna de sus versiones disponibles debe ser compatible con los diversos sistemas operativos utilizados por la entidad en sus distintas ubicaciones implementadas: • Servidores en la nube (Azure, Oracle) que utilicen sistemas operativos basados en Windows, tales como Windows Server 2012 R2 Datacenter, Windows Server 2016, Windows Server 2016 Datacenter y versiones posteriores, incluyendo todas las ediciones recientes de Microsoft Windows para entornos de servidor. • Servidores en la nube (Azure, Oracle) que utilicen sistemas operativos Linux, tales como Oracle Linux 7.4 (2018), Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, CentOS 7.9.2009, CentOS 8.2.2004 y versiones superiores. • Servidores en On Premise que utilicen sistemas operativos basados en Windows, tales como Windows Server 2012 R2 Datacenter, Windows Server 2016, Windows Server 2016 Datacenter y versiones posteriores, incluyendo todas las ediciones recientes de Microsoft Windows para entornos de servidor.

ANEXO 6. FICHA TÉCNICA

ITEM	ESPECIFICACIONES TECNICAS	
		• Servidores en On Premise que utilicen sistemas operativos basados en Linux, tales como Oracle Linux 7.4 (2018), Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, CentOS 7.9.2009, CentOS 8.2.2004 y versiones superiores.
3	**Protección en tiempo real, detección y eliminación de malware y análisis bajo demanda.**	• La solución de antivirus ESET debe ofrecer protección en tiempo real contra nuevas amenazas emergentes. • La solución de antivirus ESET debe ofrecer protección en las nubes públicas (Oracle, Azure) • La solución de antivirus ESET debe ofrecer protección contra amenazas de día cero y permitir la recopilación de estadísticas anónima, garantizando la privacidad. • La solución de antivirus ESET debe permitir realizar análisis bajo demanda de archivos, sistemas y dispositivos conectados. • La solución de antivirus ESET debe ser capaz de detectar, eliminar o poner en cuarentena una amplia variedad de amenazas, incluyendo virus, malware, troyanos, gusanos, exploits, ransomware y spyware. • La solución de antivirus ESET debe contar con un sistema de prevención de Intrusiones Basado en Host (HIPS) para fortalecer la seguridad de los endpoints.

ANEXO 6. FICHA TÉCNICA

ITEM	ESPECIFICACIONES TECNICAS	
		• La solución de antivirus ESET debe ofrecer protección específica contra ataques basados en scripts. • La solución ESET debe contar con capacidades avanzadas de Detección y Respuesta Extendida (XDR), permitiendo identificar comportamientos anómalos, detectar ataques tipo "file-less" y realizar investigaciones detalladas. Debe integrarse con la seguridad del endpoint, instalarse localmente, y permitir la modificación de indicadores de compromiso en formato XML, combinando reputación y comportamiento. Además, debe filtrar incidentes, mostrar alertas en ambas consolas (XDR y endpoint), operar con su propia red de inteligencia y ofrecer análisis basados en MITRE ATT&CK™.
4	**Actualizaciones automáticas, programación de tareas de escaneo y/o actualizaciones.**	• La solución antivirus ESET debe realizar actualizaciones automáticas de las definiciones de virus, malware, Exploits y de los componentes críticos del motor antivirus. Además, deberá garantizar la posibilidad de revertir dichas actualizaciones en caso de que sea necesario. • La solución de antivirus ESET debe sincronizar los servidores con horas y fechas específicas para programar tareas de escaneos, actualizaciones de versiones y demás tareas planeadas que puedan surgir.
5	**Envió de informes, novedades o notificaciones.**	• La solución de antivirus ESET debe permitir seleccionar el criterio de las notificaciones para ser enviadas al administrador, cuando uno de los servidores sea puesto en cuarentena. • La solución de antivirus ESET debe realizar el envío de las notificaciones al administrador, por medio de correo electrónico, cuando existan novedades en los servidores o que sean puestos en cuarentena. • La solución de antivirus ESET debe generar informes y alertas sobre las amenazas detectadas y las acciones tomadas. • La solución de antivirus ESET debe permitir la configuración de un servidor SMTP para él envió de notificaciones vía Email.
6		

ANEXO 6. FICHA TÉCNICA

ITEM	ESPECIFICACIONES TECNICAS	
	Consola de gestión y Administración Centralizada en Nube.	• La solución de antivirus ESET debe contar con una única consola de administración centralizada, aprovisionada en la Nube (entorno web/cloud), que facilite la supervisión, el mantenimiento y la actualización de la solución ofertada. • La solución de antivirus ESET debe permitir la administración centralizada de la protección en múltiples niveles (por grupos de máquinas o endpoints), utilizando técnicas de machine learning para mejorar la detección y la respuesta ante amenazas. • La solución de antivirus ESET debe permitir, desde la consola de administración, la agrupación de los agentes instalados en diferentes dispositivos por categorías y/o subgrupos de gestión, facilitando su configuración y administración. • La solución de antivirus ESET debe permitir configurar notificaciones sobre riesgos de seguridad desde la única consola de administración. • La solución de antivirus ESET debe permitir, desde la única consola de administración, la exportación de los logs de eventos generados por los agentes instalados en los dispositivos (endpoints). • La solución de antivirus ESET debe permitir, a través de la administración centralizada desde la consola, que los agentes instalados (endpoints) soliciten contraseña para ser desinstalados o administrados. • La solución de antivirus ESET debe permitir, desde la única consola de administración centralizada aprovisionada en la Nube (entorno web/cloud), configurar el idioma de la plataforma en español o inglés. • La solución de antivirus ESET debe permitir, desde la única consola de administración centralizada aprovisionada en la Nube (entorno web/cloud), ejecutar la instalación, despliegue, implementación de exclusiones automáticas y configuración de filtros de exclusión. • La solución de antivirus ESET debe contar, desde la única consola de administración

ANEXO 6. FICHA TÉCNICA

ITEM	ESPECIFICACIONES TECNICAS	
		centralizada aprovisionada en la Nube (entorno web/cloud), con un módulo de bloqueo de exploits (navegadores web, componentes de Office, lectores de PDF y clientes de correo electrónico). • La solución de antivirus ESET debe permitir el control de acceso basado en roles (RBAC). • La solución de antivirus ESET debe proporcionar administración centralizada desde una única consola aprovisionada en la Nube (entorno web/cloud) y debe permitir la instalación de agentes en los endpoints mediante mínimo una (1) de las siguientes opciones: 1. Instalación por medio de un script apoyado en la creación e integración de una política (GPO) desde el Directorio Activo. 2. Instalación directa desde la consola de administración del antivirus mediante la ejecución de una tarea para los endpoints.

Tabla # 01 Especificaciones Técnicas – Creación SIDT

En consecuencia, se requiere de una solución antivirus/antimalware para los siguientes servidores:

1. **Antivirus servidores internos:**

Tabla # 02 antivirus que se requieren para servidores internos

DESCRIPCION	SISTEMA OPERATIVO	VERSION	CANTIDAD	VIGENCIA
Servidor	Windows	Windows Server 2012 R2 Datacenter v6.3	1	un año
Servidor	Windows	Windows Server 2019 Datacenter v1809	11	un año
Endpoint	Windows	Windows 10 v22H2	1	un año
TOTAL, SERVIDORES			13	

ANEXO 6. FICHA TÉCNICA

Resumiendo, la tabla 02, en la infraestructura interna de la entidad, se dispone de un total de trece (13) servidores con Windows.

Antivirus servidores externos:

Las tablas 3 y 4 detallan los antivirus que se requieren para los servidores externos (nube de Azure y Oracle):

Tabla # 3. Antivirus que se requieren para servidores nube Azure

DESCRIP-CION	SISTEMA OPERA-TIVO	VERSION	CANTI-DAD	VIGEN-CIA
Servidor	Linux	CentOS Linux release 7.9.2009 (Core)	1	un año
Servidor	Linux	CentOS Linux release 8.2.2004 (Core)	4	un año
Servidor	Linux	CentOS Linux release 8.5.2111	1	un año
Servidor	Linux	Ubuntu 18.04 LTS	11	un año
Servidor	Linux	Ubuntu 20.04 LTS	9	un año
Servidor	Windows	Windows Server 2012 R2 Datacenter	1	un año
Servidor	Windows	Windows Server 2016 Datacenter	68	un año
Servidor	Windows	Windows Server 2019 Datacenter	2	un año
TOTAL, SERVIDORES			97	

En total, se cuenta con noventa y siete (97) servidores en la infraestructura externa de **Azure**. De estos, veinte y seis (26) están destinados al sistema operativo Linux, mientras que setenta y uno (71) operan con Windows Server.

Tabla # 4. Antivirus que se requieren para servidores nube Oracle

DESCRIP-CION	SISTEMA OPERA-TIVO	VERSION	CANTI-DAD	VIGEN-CIA
Servidor	Linux	Ubuntu 20.04 LTS	31	un año
Servidor	Linux	Ubuntu 18.04 LTS	9	un año
Servidor	Linux	Oracle Linux-8.2	1	un año
Servidor	Linux	Oracle Linux-8.3	1	un año
Servidor	Linux	Oracle Linux-8.4	1	un año
Servidor	Linux	Oracle Linux-8.5	1	un año

ANEXO 6. FICHA TÉCNICA

Servidor	Linux	Oracle Linux-8.6	2	un año
Servidor	Linux	Oracle Linux-8.9	3	un año
Servidor	Linux	Oracle Linux-8.10	2	un año
Servidor	Linux	Oracle Linux-9.2	1	un año
Servidor	Windows	Windows Server 2012	2	un año
Servidor	Windows	Windows Server 2012 R2 Standard Edition VM	1	un año
Servidor	Windows	Windows Server 2016	1	un año
Servidor	Windows	Windows Server 2016 Standard Edition VM	1	un año
Servidor	Windows	Windows Server 2019 Standard Edition VM Gen2	1	un año
Servidor	Windows	Windows Server 2019 Standard Edition VM Gen2 (2021)	1	un año
Servidor	Windows	Windows Server 2019	1	un año
TOTAL, SERVIDORES			60	

Para el caso de los servidores de Infraestructura externa de **Oracle** se dispone de un total de sesenta (60) servidores. De estos, cincuenta y dos (52) están dedicados al sistema operativo Linux, mientras que ocho (8) operan con Windows Server.

Actualmente, la Agencia Nacional de Contratación utiliza la herramienta ESET Protection en versión Advanced, con un total de ciento ochenta y seis (186) licencias instaladas en diferentes servidores ubicados en la nube de Azure, Oracle, así como en servidores locales (on-premises). Este licenciamiento tiene una vigencia por un año comprendida entre el 17 de octubre del 2024 y el 18 de octubre del 2025. Conforme a lo anterior, la entidad actualmente cuenta con un total de servidores tanto internos como externos por:

DESCRIPCIÓN	WINDOWS	LINUX	CANTIDAD TOTAL
Servidor Internos	13	0	13
Servidores Externos	79	78	157
TOTAL	**92**	**78**	**170**

ANEXO 6. FICHA TÉCNICA

En este entendido, la entidad requiere únicamente la renovación de 170 licencias dada las actualizaciones que tuvo la infraestructura de la **solución ESET Protection en versión Enterprise o superior**, dicha solución debe permitir licenciar la totalidad de servidores conforme a las versiones detalladas en las tablas anteriores. Esto con el fin de realizar la renovación correspondiente y garantizar una cobertura completa y eficiente en ambos entornos.

3.2 OBLIGACIONES ESPECÍFICAS.

1. Suministrar la licencia de la solución antivirus/antimalware para un periodo de un año contados a partir de la entrega prevista para el 18 de octubre de 2025 y recibo a satisfacción del supervisor.
2. Acompañar en la instalación, la implementación y puesta en marcha de la solución de antivirus/antimalware en los servidores internos y externos de la ANCP-CCE acorde con el plazo establecido por el supervisor del contrato.
3. Colaborar con la ANCP-CCE en la configuración de la solución antivirus/antimalware de acuerdo con los requisitos, mejores prácticas, plazos establecidos o ventanas de ejecución que sean requeridas por la ANCP-CCE.
4. Realizar una transferencia de conocimientos de cuatro (4) horas a un máximo de 10 personas designadas por el supervisor del contrato. Estas capacitaciones cubrirán el uso de la solución antivirus/antimalware, así como la administración e implementación de excepciones o actualizaciones necesarias.
5. Proporcionar soporte técnico durante todo el período de vigencia de la licencia del antivirus, que incluya asistencia remota 5x8 y 7x24 para casos críticos, así como administración, configuración, instalación, o asesoría según lo requiera la entidad.
6. Suministrar licencias de la solución antivirus/antimalware que cumplan con la totalidad con lo exigido en la ficha técnica – especificaciones técnicas (Tabla 01).
7. Atender todos los requerimientos, peticiones o consultas que Colombia Compra Eficiente tenga al respecto sobre el uso del antivirus, las mismas deben resolverse en un plazo máximo a un (1) día hábil, dependiendo de la criticidad. En caso contrario, se espera una respuesta inmediata.
8. Garantizar la originalidad de la herramienta contratada y proporcionar protocolos para la verificación de su autenticidad.
9. Si el contratista está obligado a facturar electrónicamente, deberá presentar la factura electrónica validada previamente por la DIAN, como

ANEXO 6. FICHA TÉCNICA

requisito necesario para el pago de los bienes y/o servicios contratados, conforme con las disposiciones señaladas en el Decreto 358 del 5 de marzo de 2020, en concordancia, con lo dispuesto en la Resolución No. 000042 del 5 de mayo de 2020.

Tabla # 5. Licenciamiento Antivirus Eset

Descripción Del Producto	Cantidad
ESET PROTECT ENTERPRISE	170

La vigencia de la presente Oferta es de sesenta días (60) calendario

4. PLAZO PARA LA EJECUCIÓN DEL OBJETO.

Desde:	La firma del acta de inicio previo cumplimiento de requisitos legales de perfeccionamiento y ejecución.	**Hasta:**	15 de noviembre de 2025

Elaboró: Claudia Andrea Velásquez – Jhonatan Arango Sánchez.
Revisó: Fernando Talero Benítez – Wilson Eduardo Coronado
Aprobó: Fernando Talero Benítez

3. CONTROL DE CAMBIOS DE DOCUMENTO			**Versión vigente del documento:**		**01**
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE AJUSTES**	**ELABORÓ**	**REVISÓ**	**APROBÓ**
01	26/07/2021	Estandarización Anexo 6. Ficha Técnica	Diana Catalina Ramirez Peralta Técnico Asistencial O1 Grado 12	Natalia Ramirez Vega Analista Código T2 Grado 06 María Valeska Medellín Gestor 15	Claudia Ximena López Pareja Secretaria General