ANEXO 01

FICHA TÉCNICA
Las especificaciones técnicas se encuentran definidas en el presente Anexo Técnico, que incluye las actividades y requisitos para llevar a cabo la ejecución del futuro contrato.

1. **OBJETO:** "ADQUISICION DE LICENCIAS PARA EQUIPOS DE COMPUTO DE LA ESCUELA DE CAPACITACIÓN MUNICIPAL DE FLORIDABLANCA – ECAM CON EL FIN DE GARANTIZAR SU SEGURIDAD INFORMÁTICA Y ADECUADO FUNCIONAMIENTO".

2. **CÓDIGOS UNSPSC:**

CLASIFICACIÓN UNSPSC TERCER NIVEL	CLASE
43 23 32 00	Software de Seguridad y Protección
81 11 25 00	Servicio de alquiler o arrendamiento de licencias de software de computador

3. **LUGAR DE EJECUCIÓN:** Carrera 7 #4-35, Segundo piso, Casa Piedra del Sol, Floridablanca, Santander.

4. **PLAZO:** Quince (15) días calendario desde la suscripción del acta de inicio.

5. **ESPECIFICACIONES TÉCNICAS MINIMAS:**

5.1 Especificaciones Técnicas del bien

ITEM	DESCRIPCIÓN PRODUCTO	UNIDAD	CANT
1	Licencia Microsoft Office 365 Business. Incluye aplicaciones de escritorio instalables: Word, Excel, PowerPoint, OneNote y Outlook. Licencia por 12 meses	UND	15
2	Licencia Antivirus. Protección en múltiples niveles para Endpoints, con machine learning y una fácil administración. Licencia por 12 meses	UND	15

ESPECICIFACIONES TECNICAS MINIMAS ANTIVIRUS

Objeto técnico. Adquirir licencias de una solución de seguridad informática para la protección antimalware de equipos de usuario final y servidores de la entidad, con administración centralizada, de acuerdo con las cantidades, vigencia, sistemas operativos y demás condiciones que se establezcan en los estudios previos y en la invitación.

Alcance general. La solución deberá comprender, según las necesidades y cantidades definidas por la entidad: (i) protección de endpoints; (ii) consola de administración centralizada; y (iii) protección de

servidores. Se aceptarán productos, módulos o componentes integrados o independientes, siempre que en conjunto satisfagan los requisitos mínimos aquí establecidos.

1. Producto antimalware para equipos endpoint
La solución deberá proteger los equipos de usuario final frente a software malicioso y otras amenazas informáticas, mediante mecanismos de prevención, detección, bloqueo y, cuando la tecnología lo permita, corrección o remediación de incidentes.

1.1. Requerimientos funcionales y de protección

- Proporcionar protección en tiempo real frente a virus, troyanos, spyware, ransomware, aplicaciones potencialmente no deseadas y otras formas de código malicioso.
- Permitir la ejecución de análisis bajo demanda y análisis programados, con opciones de configuración de acuerdo con las políticas de seguridad de la entidad.
- Contar con mecanismos de detección basados en firmas, heurística, análisis de comportamiento, aprendizaje automático, reputación en la nube u otras tecnologías equivalentes.
- Permitir la actualización automática y periódica de los motores de detección, firmas, componentes y demás elementos de seguridad.
- Incluir protección de navegación o filtrado web que permita restringir el acceso a sitios o categorías de riesgo, y generar alertas o notificaciones cuando la funcionalidad esté disponible.
- Permitir aplicar políticas de protección diferenciadas por grupos de equipos o equipos individuales.
- Incluir mecanismos de protección frente a vulnerabilidades y explotación de fallos (anti-exploit), o una funcionalidad equivalente.
- Permitir identificar, bloquear, poner en cuarentena o ejecutar acciones de respuesta frente a amenazas detectadas, de acuerdo con las capacidades del producto.
- Permitir la administración de análisis y tareas de seguridad de manera centralizada.

1.2. Control de dispositivos

- Permitir controlar el uso de dispositivos extraíbles y periféricos, como mínimo los medios de almacenamiento USB, mediante políticas de autorización o restricción.
- Permitir establecer permisos de acceso a medios de almacenamiento, incluyendo, cuando la solución lo soporte, acceso completo, solo lectura y bloqueo.
- Permitir aplicar las políticas de control de dispositivos a grupos de equipos o equipos individuales.
- Ofrecer la posibilidad de analizar los medios extraíbles al conectarse o durante su utilización, de acuerdo con las opciones disponibles en la solución.

1.3. Prevención de intrusiones y protección avanzada

- Incorporar mecanismos de prevención de intrusiones en el equipo (HIPS), protección basada en comportamiento o tecnología equivalente.
- Permitir detectar comportamientos anómalos o potencialmente maliciosos de procesos, aplicaciones y archivos.
- Incluir protección contra ransomware, mediante detección y bloqueo de actividades asociadas con cifrado o modificación maliciosa de archivos.
- Permitir aislar o contener un equipo comprometido, o ejecutar una acción equivalente de respuesta, desde la consola cuando la solución disponga de dicha capacidad.
- Contar con mecanismos para detectar amenazas transmitidas mediante comunicaciones cifradas, cuando resulte técnicamente viable y conforme a la configuración de la entidad.
- Incluir protección contra ataques de fuerza bruta o intentos automatizados de acceso no autorizado, cuando corresponda al alcance funcional del producto.

1.4. Firewall

- La solución deberá incorporar firewall para endpoints o permitir su integración con el firewall del sistema operativo.
- Deberá permitir establecer reglas de comunicación para autorizar o bloquear conexiones de red, de acuerdo con las capacidades del producto.

2. Consola de administración centralizada
La solución deberá contar con una consola que permita administrar centralizadamente las licencias y los equipos protegidos, visualizar su estado de seguridad y gestionar políticas, alertas y tareas de protección. La consola podrá ser suministrada en modalidad cloud o instalada en infraestructura de la entidad.

2.1. Capacidades de administración y despliegue

- Permitir visualizar el inventario de equipos protegidos, su estado de actualización y los eventos o alertas de seguridad relevantes.

- Permitir crear y administrar grupos de equipos, así como asignarles políticas de seguridad diferenciadas.
- Permitir desplegar, instalar, actualizar, configurar y desinstalar el agente de seguridad de forma remota o mediante mecanismos de administración centralizada.
- Permitir ejecutar tareas de análisis, actualización y otras acciones de seguridad desde la consola.
- Ser compatible con los sistemas operativo Windows 11.
- Permitir la administración de usuarios y perfiles con diferentes niveles de permisos, mediante control de acceso basado en roles o mecanismo equivalente.
- Contar con mecanismos de autenticación segura para el acceso administrativo. Cuando esté disponible en la solución, deberá permitir autenticación multifactor.
- Permitir generar informes y exportar información de inventario, eventos o alertas en formatos de uso común.
- Permitir la administración remota de equipos ubicados dentro y fuera de la red institucional, siempre que cuenten con conectividad a los servicios de administración.

2.2. Integración y funcionalidades complementarias

- Permitir la integración o exportación de registros hacia herramientas de monitoreo o gestión de eventos de seguridad (SIEM), mediante formatos o mecanismos de interoperabilidad disponibles en la solución, cuando esta funcionalidad sea ofrecida por el producto.
- Permitir identificar equipos que no cuenten con el agente de seguridad o que no estén reportando a la consola, cuando la solución disponga de dicha funcionalidad.
- Permitir la gestión de actualizaciones y políticas de seguridad desde la consola.
- Las funcionalidades complementarias, tales como sandboxing, cifrado de discos, administración de dispositivos móviles (MDM/UEM), ejecución remota de scripts o integración con soluciones EDR.

3. Soporte, actualización y condiciones del proveedor

- El proveedor deberá garantizar el suministro y activación de las licencias correspondientes a la cantidad de equipos definida por la entidad, durante el término de vigencia indicado en la invitación.
- Durante la vigencia del licenciamiento, deberán estar disponibles las actualizaciones de seguridad, firmas, motores y componentes que correspondan al producto adquirido.
- El proveedor deberá ofrecer soporte técnico en idioma español, directamente o por medio del fabricante, mayorista o canal autorizado, durante la vigencia del licenciamiento.
- El proveedor deberá indicar los canales habilitados para la recepción y atención de solicitudes de soporte, así como los horarios y tiempos de respuesta ofrecidos.
- Cuando aplique, el proveedor deberá acreditar que cuenta con autorización o habilitación para comercializar y suministrar las licencias ofrecidas, mediante certificación del fabricante, mayorista o canal correspondiente. La entidad deberá aceptar medios equivalentes idóneos para verificar la legitimidad del licenciamiento.
- Las licencias deberán ser originales, legítimas, nuevas o no asignadas previamente a otro usuario, y quedar registradas o asociadas a la entidad contratante, según el modelo de licenciamiento del fabricante.

4. Equivalencia tecnológica y pluralidad de soluciones
Las especificaciones técnicas establecen las capacidades funcionales y condiciones mínimas de seguridad requeridas por la entidad. Por lo tanto, se admitirán soluciones de diferentes fabricantes y

desarrolladores que acrediten el cumplimiento de los requisitos mínimos, independientemente de la denominación comercial, arquitectura tecnológica, interfaz, metodología o mecanismo utilizado para su implementación. Se aceptarán funcionalidades equivalentes siempre que permitan alcanzar el resultado de seguridad requerido.

La acreditación del cumplimiento podrá realizarse mediante fichas técnicas, documentación oficial del fabricante, manuales, enlaces a documentación oficial o certificaciones técnicas. La entidad podrá solicitar aclaraciones o verificaciones sobre la información aportada, de conformidad con las reglas del proceso de selección.

6. RECEPCIÓN DE LOS BIENES

Los elementos serán entregados al supervisor del contrato.

OBLIGACIONES GENERALES:

1. CUMPLIR con los deberes establecidos en el artículo 5 de la Ley 80 de 1.993, en consecuencia, deberán:

a- Colaborar con la Entidad en lo que sea necesario para que el objeto contratado se cumpla y que este sea de la mejor calidad;
b- Acatar las órdenes que durante el desarrollo del contrato la Entidad le imparta;
c- Obrar con lealtad y buena fe en las distintas etapas contractuales;
d- Garantizar la calidad de los servicios contratados y responder por ellos;
e- No acceder a peticiones o amenazas de quienes actúen por fuera de la ley con el fin de obligarlos a hacer u omitir algún acto o hecho.

2. Cumplir con el objeto del contrato, en los términos y condiciones establecidos en los estudios previos, Invitación Pública, las adendas (si las hubiere) y la oferta presentada.

3. Guardar la confidencialidad de toda la información que le sea entregada y que se encuentre bajo su custodia o que por cualquier otra circunstancia deba conocer o manipular y responderá civil, penal y disciplinariamente por los perjuicios de su divulgación y/o utilización indebida que por sí o por un tercero se cause a la administración o a terceros.

4.Suscribir el contrato y cumplir con los requisitos de legalización y ejecución pertinentes, en la oportunidad establecida para el efecto.

5.Pagar los costos directos e indirectos que implique el cumplimiento del objeto contractual, tales como impuestos, retenciones, tasas, gastos de legalización, etc. En consecuencia, el precio ofertado se entiende que incluye dichos costos.

6.Otorgar las garantías requeridas, en los amparos y vigencias establecidas en el contrato y efectuar las modificaciones necesarias dentro de la etapa de ejecución o liquidación, cuando ello sea necesario.

7. Disponer por su cuenta y riesgo el personal necesario para realizar el servicio.

8. Responder por todo daño ocasionado, directa o indirectamente, en los bienes muebles o en la infraestructura de la entidad, durante la ejecución contractual para lo cual deberán ser subsanados por éste.

9. Acatar las órdenes, instrucciones e indicaciones que le imparta el supervisor del contrato;

10. Informar a la entidad por intermedio del supervisor contractual de cualquier situación que altere o pueda alterar la debida ejecución del contrato.

11. Acreditar afiliación a salud, pensión según lo establecido en el artículo 50 de la ley 789 de 2002, 797 de 2003 y Decreto 510 de 2003.

12. Presentar la factura o cuenta de cobro correspondiente al cobro de las actividades realizadas durante el respectivo periodo.

13. Cancelar los gastos administrativos que se deriven de la ejecución, estampillas e impuestos que se generen en razón del contrato.

14. Presentar informe de ejecución del contrato, según los requerimientos del supervisor asignado.

OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

Entregar los ítems plasmados en la ficha técnica y documentos, de conformidad con las especificaciones técnicas requeridas por el supervisor de contrato y ofrecidas en la propuesta.

Se deberá tener en cuenta que los bienes ofrecidos deberán cumplir con las condiciones y especificaciones establecidas en la ficha técnica.

FIRMA:
NOMBRE DEL REPRESENTANTE LEGAL:
NOMBRE O RAZON SOCIAL:
NIT O CC.:
DIRECCIÓN:
CIUDAD:
TELÉFONO:
CELULAR:
E-MAIL: