PERSONERÍA
Municipal de Villavicencio

Villavicencio, octubre 13 de 2026

Doctora
SIRLEY GUTIERREZ NAVARRO
Personera Auxiliar
Personeria Municipal de Villavicencio
Ciudad

ASUNTO: Comunicación de la necesidad de fortalecer la infraestructura tecnológica y la seguridad digital de la Personería Municipal de Villavicencio.

Cordial saludo.

En atención a los resultados consignados en el documento denominado "*Informe de Avance – Primer Corte*", correspondiente al contrato de prestación de servicios CPS No. PMV-069-2026, cuyo objeto se relaciona con la optimización y/o fortalecimiento de la gestión estratégica de tecnologías de la información y seguridad digital de la Personería Municipal de Villavicencio, me permito poner en su conocimiento la necesidad de adelantar las gestiones administrativas, técnicas y presupuestales pertinentes para fortalecer la infraestructura tecnológica de la entidad.

De acuerdo con el diagnóstico realizado, se identificaron situaciones que requieren atención prioritaria, relacionadas con la obsolescencia de los equipos de cómputo y servidores, la existencia de sistemas operativos sin soporte del fabricante, las deficiencias en la seguridad perimetral de la red institucional y la presencia de vulnerabilidades que pueden comprometer la confidencialidad, integridad y disponibilidad de la información.

El informe señala que, de los 50 equipos de usuario inventariados, se identifican 37 equipos de cómputo, debido a su estado obsolescencia y rendimiento operativo de más de 10 años de uso. Asimismo, se evidenció que los servidores institucionales tienen aproximadamente 14 años de uso y que el directorio activo depende de un único servidor, situación que incrementa el riesgo de interrupción de los servicios tecnológicos.

Adicionalmente, el análisis de vulnerabilidades registró 20.514 hallazgos, incluidos 546 asociados a vulnerabilidades explotadas activamente, y la matriz de riesgos

tecnológicos identificó diez (10) riesgos críticos y quince (15) riesgos altos. Estos resultados hacen necesario adoptar medidas que permitan reducir la exposición a incidentes de seguridad y mejorar la continuidad operativa de la entidad.

En consecuencia, y conforme a las necesidades identificadas en el informe técnico, se considera prioritario adelantar las actuaciones necesarias para evaluar y gestionar la adquisición de los siguientes bienes y licencias:

1. **Un (1) firewall de nueva generación (NGFW):** con servicios de seguridad y soporte del fabricante por doce (12) meses, que permita fortalecer la protección perimetral, controlar el tráfico de red, prevenir intrusiones y facilitar la implementación de mecanismos de acceso remoto seguro y segmentación de la red.
2. **Cuatro (4) licencias de protección de EndPoint con capacidades EPP y EDR para servidores:** con vigencia de doce (12) meses, destinadas a fortalecer la prevención, detección y respuesta ante amenazas informáticas, incluyendo ataques de ransomware.
3. **Un (1) equipo de cómputo todo en uno de tipo corporativo:** con sistema operativo de edición profesional, suite ofimática y protección de EndPoint por doce (12) meses, para atender un puesto de trabajo que sea priorizado por la Oficina de Sistemas.
4. **Siete (7) equipos de cómputo todo en uno de tipo corporativo:** con sistema operativo debidamente licenciado, destinados a iniciar la renovación prioritaria del parque tecnológico, de acuerdo con el inventario y los criterios técnicos de obsolescencia y criticidad.
5. **Dos (2) servidores de tipo empresarial:** con sistema operativo de servidor licenciado, licencias de acceso de cliente (CAL), componentes adecuados para garantizar mayor disponibilidad y garantía del fabricante por tres (3) años, con el propósito de migrar los servicios institucionales y reducir los riesgos asociados a la infraestructura actualmente instalada.

La atención de estas necesidades permitirá fortalecer los controles de seguridad digital, reducir los riesgos de pérdida de información e interrupción de los servicios institucionales, mejorar el desempeño de los puestos de trabajo y establecer una base tecnológica más confiable para el desarrollo de las funciones misionales y administrativas de la Personería Municipal de Villavicencio.

Por lo anterior, **se solicita adelantar las gestiones administrativas y precontractuales correspondientes**, de acuerdo con las competencias de cada dependencia, incluyendo la verificación de la disponibilidad presupuestal, la revisión del Plan

Anual de Adquisiciones, la elaboración del estudio de mercado y la estructuración de los estudios previos y demás documentos que resulten procedentes.

Para tal efecto, deberá verificarse la viabilidad de financiar las adquisiciones con cargo a la vigencia 2026 o, en caso de no existir disponibilidad presupuestal suficiente, evaluar su programación para la vigencia 2027, conforme a las disposiciones presupuestales y contractuales aplicables.

Las especificaciones técnicas deberán formularse con criterios de funcionalidad, desempeño, compatibilidad, seguridad, garantía y soporte, sin referencias injustificadas a marcas o fabricantes, de manera que se favorezca la pluralidad de oferentes y se atiendan las necesidades reales de la entidad.

Agradezco la atención prestada y las actuaciones que se adelanten para atender esta necesidad institucional, en procura de fortalecer la seguridad de la información, la continuidad de los servicios y la adecuada operación de la infraestructura tecnológica de la entidad.

Atentamente,

JOSE DIDIER VILLARREAL ORTIZ
Técnico Operativo Grado 04
Personeria Municipal de Villavicencio

Anexo Informe

INFORME DE AVANCE

Informe de necesidad: fortalecimiento de la seguridad perimetral, protección y renovación de servidores, y renovación de equipos de cómputo

Proyecto	Optimización y/o fortalecimiento de la gestión estratégica de tecnologías de la información y seguridad digital de la Personería Municipal de Villavicencio	**Contrato**	CPS No. PMV-069-2026

Contratista	Fecha de presentación	Periodo cubierto
Julio Eduardo Herrera Moreno C.C. 1.121.951.723	22/septiembre/2026	Primer mes de ejecución 15/09/2026 a 14/10/2026

Supervisor	José Didier Villareal Ortiz	**Cargo**	Técnico Operativo 04 – Oficina de Sistemas

Estado del proyecto en este corte

Estado general	**EN EJECUCIÓN – A TIEMPO**	**Riesgos para la Entidad**	**CRÍTICOS – REQUIEREN DECISIÓN DE INVERSIÓN**

1.Resumen

En el primer corte se ejecutó la **fase de diagnóstico** de la infraestructura tecnológica de la Personería Municipal de Villavicencio, conforme a las obligaciones específicas 1 a 5 del contrato. Como resultado se entregaron cuatro anexos técnicos: **Anexo A** (inventario de hardware), **Anexo B** (red de datos y topología) y **Anexo C** (análisis de vulnerabilidades), junto con el registro y la valoración de riesgos tecnológicos.

El diagnóstico evidencia que el **55 % del hardware** (37 de 50 equipos de usuario y 4 servidores) se encuentra en estado crítico o deficiente, el escaneo registró **20.514 hallazgos**, de los cuales **546** corresponden a vulnerabilidades explotadas activamente (catálogo KEV); y que **10 de los 37 riesgos** identificados están en nivel Crítico y 15 en nivel Alto.

En desarrollo de la obligación específica 6 (acciones correctivas para hallazgos críticos), este informe **da origen a la necesidad** de adquirir: **(i)** un firewall de nueva generación (NGFW), **(ii)** licencias de protección de EndPoint con capacidades de detección y respuesta (EDR) para los servidores, y **(iii)** ocho (8) equipos de cómputo todo en uno de tipo corporativo (uno con suite ofimática y protección de EndPoint, y siete para la renovación prioritaria del parque de cómputo), y (iv) dos (2) servidores de tipo empresarial. Estas adquisiciones atienden de forma directa cuatro riesgos de nivel Crítico y son prerrequisito de las fases siguientes del plan de mejoramiento.

2. Hitos

No.	Hito	Obligación del contrato
1	Inventario técnico y funcional de hardware (Anexo A)	Actividad 1
2	Evaluación de topología, segmentación y red de datos (Anexo B).	Actividad 2
3	Análisis de vulnerabilidades y postura de seguridad frente al MSPI e ISO/IEC 27001 (Anexo C).	Actividad 3 y 4
4	Registro, valoración y priorización de riesgos tecnológicos (probabilidad × impacto).	Actividad 5
5	Informe de necesidad y acompañamiento técnico al estudio previo de las adquisiciones críticas.	Actividad 6
6	Plan de mejoramiento con iniciativas, responsables, cronograma, presupuesto e indicadores.	Actividad 7

3. Indicadores del diagnóstico (línea base)

Por tratarse del primer corte, los valores constituyen la línea base contra la cual se medirá el avance del plan de mejoramiento.

Indicador	Valor actual	Fuente	Tendencia esperada
Activos de hardware en estado crítico o deficiente	37 de 54 (55 %)	Anexo A	↓ **Reducir**
Equipos de usuario en estado crítico o deficiente con 10 años de obsolescencia y con rendimiento de 4 GB de RAM	37 de 50	Anexo A	↓ **Reducir**
Aplicaciones fuera de soporte del fabricante	7 de 13	Anexo B	↓ **Reducir**
Hallazgos de vulnerabilidades / explotadas activamente (KEV)	20.514 / 546 en 28 equipos	Anexo C	↓ **Reducir**
Riesgos en nivel Crítico / Alto	10 / 15 de 37	Anexo D	↓ **Reducir**
Obligaciones específicas del contrato con producto entregado	5 de 7	Este informe	↑ **En avance**

4. Trabajo realizado por obligación específica

No.	Obligación específica	Actividad realizada / producto	Avance
1	Levantar un inventario técnico y funcional de los activos de hardware y software.	Inventario de 50 activos de hardware de usuario y 4 servidores, con estado, antigüedad y capacidad (Anexo A)	**Ejecutada**
2	Evaluar topología, capacidad, segmentación y cableado de la red de datos.	Levantamiento de la red de datos, equipos de conectividad y seguridad perimetral (Anexo B). Se identificó red sin segmentación, switches no administrables y firewall de software instalado sobre un computador de escritorio.	**Ejecutada**
3	Analizar la postura de seguridad frente al MSPI e ISO/IEC 27001.	Escaneo de vulnerabilidades en 28 equipos (Anexo C) y contraste con los controles del MSPI y de ISO/IEC 27001, en especial gestión de vulnerabilidades técnicas, protección contra malware y seguridad de redes.	**Ejecutada**
4	Identificar brechas (GAP) entre el estado actual y el deseado.	Brechas consolidadas por dominio: perímetro, servidores y dominio, vulnerabilidades, parque de cómputo, software sin soporte, respaldo, red interna e identidad.	**Ejecutada**
5	Valorar y priorizar los riesgos tecnológicos según probabilidad e impacto.	Registro de 37 riesgos valorados en matriz 5 × 5: 10 Críticos, 15 Altos, 11 Medios y 1 Bajo.	**Ejecutada**
6	Formular acciones correctivas para hallazgos críticos.	Presente informe de necesidad: firewall NGFW, EDR para servidores, ocho (8) equipos de cómputo y dos (2) servidores. Acompañamiento técnico a la construcción del estudio previo con especificaciones neutrales.	**En ejecución**
7	Estructurar el plan de mejoramiento.	Priorización preliminar por fases. Se consolida en los cortes 2 y 3 con responsables, cronograma, presupuesto e indicadores.	**Programada**

5. Necesidad identificada y solicitud de adquisición

Con fundamento en el diagnóstico y en la obligación específica 6 del contrato, se identifica la necesidad de adelantar las siguientes adquisiciones, que atienden de forma directa riesgos de nivel Crítico del registro de riesgos:

5.1. Firewall de nueva generación (NGFW)

Situación encontrada	La seguridad perimetral depende de un firewall de software instalado sobre un computador de escritorio de aproximadamente 15 años, sin soporte del fabricante ni redundancia (Anexos A y C). La red interna no está segmentada y la Entidad depende de un solo canal de Internet.

Riesgo asociado	R-006 Pérdida de conectividad y del perímetro – **Crítico** (probabilidad 3 × impacto 5). Una falla del equipo actual deja a la Entidad sin Internet, correo, SIP, Personería en Línea ni servicios en la nube, y sin control del tráfico entrante y saliente.
Necesidad	Contar con un firewall de nueva generación con servicios de seguridad y soporte del fabricante, que inspeccione y controle el tráfico entre la red institucional e Internet mediante prevención de intrusiones, control de aplicaciones, filtrado web y DNS, protección contra malware e inspección de tráfico cifrado, y que habilite el acceso remoto seguro (VPN), la administración de un canal de respaldo y la segmentación de la red.
Bien requerido	Un (1) firewall de nueva generación (NGFW) con suscripción de servicios de seguridad y soporte del fabricante por doce (12) meses.
Beneficio	Perímetro con soporte y actualizaciones; trazabilidad de eventos de seguridad; base técnica para la segmentación de la red (VLAN) y el doble canal de Internet.

5.2. Protección de EndPoint con detección y respuesta (EDR) para servidores

Situación encontrada	La Entidad opera cuatro (4) servidores en los que se alojan el directorio activo, los archivos y los servicios institucionales. Tienen cerca de 14 años de uso y sistema operativo sin soporte del fabricante (Anexos A y B). La protección actual es un antivirus corporativo tradicional, vigente hasta el 21/05/2027, con diferencias entre las licencias adquiridas y los equipos que reportan a la consola.
Riesgo asociado	R-001 Secuestro de información (ransomware) – **Crítico** (5 × 5), derivado de las 546 vulnerabilidades explotadas activamente (Anexo D). R-007 Paralización del dominio – **Crítico** (3 × 5).
Necesidad	Implementar en los servidores una solución de protección de EndPoint con capacidades de prevención, detección y respuesta (EDR), cacería de amenazas, aislamiento de equipos comprometidos y administración centralizada, que proteja tanto los servidores que se conservan como los dos (2) servidores nuevos del numeral 5.5.
Bien requerido	Cuatro (4) licencias de agente de protección de EndPoint (EPP + EDR) para servidores por doce (12) meses: dos (2) para los servidores que se conservan y dos (2) para los servidores nuevos.
Beneficio	Detección y contención temprana de ransomware, intrusiones y amenazas sin archivos sobre los activos más críticos; visibilidad centralizada de incidentes.

5.3. Equipo de cómputo todo en uno de tipo corporativo

Situación encontrada	De los 50 equipos de usuario están en estado crítico o deficiente; 37 tienen 10 o más años de uso y cuentan con 4 GB de RAM (Anexo A). Estas condiciones impiden ejecutar de forma adecuada las herramientas ofimáticas y de seguridad actuales.
Riesgo asociado	R-003 Obsolescencia del parque de cómputo – **Crítico**. R-015 Software sin soporte frente al MSPI – **Alto** (4 × 3).
Necesidad	Iniciar la renovación del parque de cómputo con un equipo corporativo debidamente licenciado, asignado al puesto de trabajo de mayor criticidad que defina la Oficina de Sistemas.
Bien requerido	Un (1) computador todo en uno de tipo corporativo con sistema, suite ofimática y agente de protección de EndPoint por doce (12) meses. Siete (7) computadores todo en uno corporativo debidamente licenciado.
Beneficio	Puesto de trabajo con soporte del fabricante, compatible con las herramientas institucionales y protegido desde la misma consola de los servidores.

5.4. Servidores de tipo empresarial

Situación encontrada	La Entidad opera cuatro (4) servidores con cerca de 14 años de uso y sistema operativo sin soporte del fabricante, en los que se alojan el directorio activo, los archivos y los servicios institucionales. El directorio activo depende de un único servidor, sin réplica, y los equipos no cuentan con repuestos ni garantía (Anexos A y B).
Riesgo asociado	R-007 Paralización del dominio – **Crítico**. R-008 y R-009 Falla de servidores sin soporte ni repuestos – **Alto**.
Necesidad	Renovar dos (2) servidores con equipos de tipo empresarial, con soporte y garantía del fabricante, componentes redundantes y capacidad para alojar el directorio activo y los servicios críticos, con virtualización y mecanismos de respaldo, y migrar a ellos los servicios de los servidores que se retiran.
Bien requerido	Dos (2) servidores de tipo empresarial con sistema operativo de servidor licenciado, licencias de acceso de cliente (CAL) y garantía del fabricante de tres (3) años.

Beneficio	Directorio activo y servicios institucionales sobre plataforma con soporte, mayor disponibilidad de los aplicativos y base para el retiro de los servidores sin soporte.

5.5. Resumen de la solicitud

Ítem	Bien o licencia	Cant.	Vigencia	Riesgos que atiende
1	Firewall de nueva generación (NGFW) con servicios de seguridad y soporte	1	12 meses	R-006 Crítico
2	Licencia de protección de EndPoint EPP + EDR para servidores	4	12 meses	R-001 Crítico · R-007 Crítico
3	Computador todo en uno corporativo con sistema operativo, ofimática y protección de EndPoint	1	Garantía 1 año 12 meses (licencias)	R-003 Crítico · R-015 Alto
4	Computador todo en uno corporativo con sistema operativo licenciado	7	Garantía 1 año	R-003 Crítico · R-015 Alto
5	Servidor de tipo empresarial con sistema operativo de servidor y licencias de acceso (CAL)	2	Garantía 3 años	R-007 Crítico · R-008 · R-009 Alto

En consecuencia, se solicita a la Personera Auxiliar – Delegada Contractual y a la Oficina de Sistemas **iniciar las gestiones precontractuales** (Certificado de Disponibilidad Presupuestal, verificación del Plan Anual de Adquisiciones, estudio de mercado y estudio previo) para la adquisición de los bienes relacionados. El contratista acompañará técnicamente la elaboración del estudio previo, cuyas especificaciones se definen en términos de funcionalidad y desempeño, sin referencia a marcas ni fabricantes, para garantizar la pluralidad de oferentes.

6. Riesgos y obstáculos

Riesgo	Descripción	Responsable	Tratamiento propuesto
R-006	Firewall de software sobre equipo de escritorio sin soporte; único canal de Internet.	Oficina de Sistemas	Adquisición de NGFW (ítem 1); respaldo de la configuración actual antes del cambio.
R-001	Ransomware por vulnerabilidades explotadas activamente sin corregir.	Oficina de Sistemas	EDR en servidores (ítem 2); parcheo prioritario de los equipos con más hallazgos.
R-007	Único controlador de dominio en servidor sin soporte.	Oficina de Sistemas	Adquisición de dos (2) servidores (ítem 5) y EDR en servidores (ítem 2).
R-003	Parque de cómputo obsoleto.	Oficina de Sistemas	Ocho (8) equipos todo en uno (ítems 3 y 4) y renovación por fases del resto del parque en el plan de mejoramiento.
Obstáculo	Disponibilidad presupuestal en la vigencia 2026 para las cinco adquisiciones.	Oficina Administrativa y Financiera	Expedición del CDP o programación en la vigencia 2027.

Puntuación de riesgos (probabilidad × impacto, escala 1–5)

Riesgo	Probabilidad	Impacto	Puntaje y nivel
R-001 Ransomware	5	5	**Crítico · 25**
R-006 Perímetro y conectividad	3	5	**Crítico · 15**
R-007 Paralización del dominio	3	5	**Crítico · 15**
R-015 Software sin soporte	4	3	**Alto · 12**

7. Aspectos destacados

- Se completó la fase de diagnóstico dentro del primer mes, con cuatro anexos técnicos y el registro de riesgos como soporte.

- Los riesgos críticos se concentran en ransomware, pérdida del perímetro, caída del dominio y obsolescencia del parque de cómputo.
- Las cinco adquisiciones solicitadas atienden cuatro de los diez riesgos críticos y habilitan las fases siguientes del plan de mejoramiento (segmentación de red, doble canal y migración de los servicios a servidores con soporte).
- Se recomiendan, en paralelo y sin costo, acciones de contención: respaldo verificado de servidores y configuraciones, parcheo prioritario y revisión de accesos remotos.

8. Cronograma del contrato

Mes	Estado	Actividades
Mes 1	**Ejecutado**	Inventario (Anexo A), red de datos (Anexo B), vulnerabilidades (Anexo C), registro de riesgos e informe de necesidad.
Mes 2	**Programado**	Análisis de brechas frente al MSPI, acciones correctivas para hallazgos críticos y acompañamiento técnico del proceso de adquisición.
Mes 3	**Programado**	Plan de mejoramiento con iniciativas, responsables, cronograma, presupuesto estimado e indicadores de seguimiento; informe final.