

Versión: 2

Fecha de vigencia: 12 de junio de 2025

FECHA: 2 DE FEBRERO DE 2026.

SECRETARÍA ENCARGADA: TIC

NOMBRE Y NÚMERO DEL PROCESO: SMTIC-SASIE-001-2026

OBJETO DEL PROCESO: ADQUIRIR LICENCIAS DE SOFTWARE ANTIMALWARE DE ÚLTIMA GENERACIÓN PARA LOS EQUIPOS DE CÓMPUTO DE LA ALCALDÍA DE PEREIRA INCLUYENDO LA SECRETARÍA DE EDUCACIÓN, Y LICENCIA DE PLATAFORMA CLOUD PARA EL MONITOREO DE ALERTAS Y OPERACIONES DE CIBERSEGURIDAD.

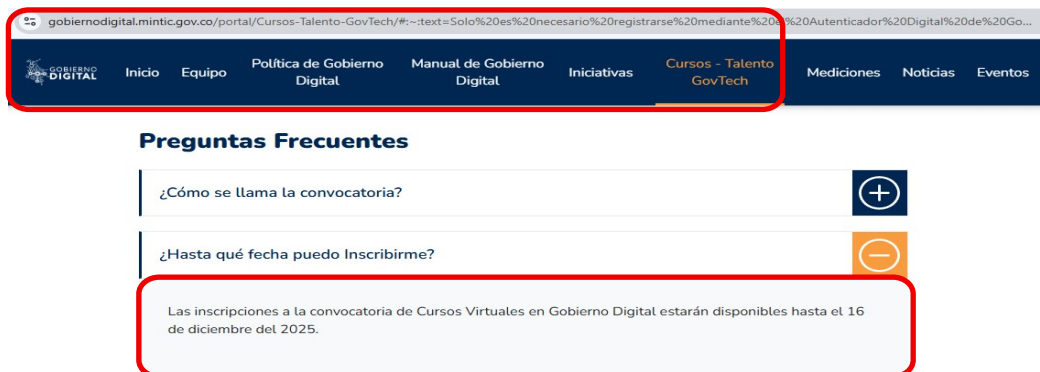
RESPUESTA DE OBSERVACIONES

OBSERVACIÓN 1		
1	NOMBRE DEL INTERESADO:	GRUPO LUMA SAS
2	REPRESENTANTE LEGAL:	CIELO MORENO
3	CORREO ELECTRÓNICO:	info@lumacloud.co
4	FECHA Y HORA DE LLEGADA:	29-01-2026 8:42 a.m.
5	OBSERVACIÓN:	
Por medio de la presente nos comunicamos con Ustedes con el fin de hacer observaciones al pliego de condiciones en los siguientes puntos:		
OBSERVACION 1:		
Solicitud de eliminación del certificado de MinTic		
De manera respetuosa, presentamos contraobservación a la respuesta de la Entidad frente al requisito del Numeral 9.1 – Perfiles y Capacidad de Respuesta, en el cual se mantiene la exigencia de “Certificación en Seguridad y Privacidad de la Información – Gobierno Digital (MinTIC) y certificación en el Modelo de Seguridad y Privacidad de la Información (MSPI)”, bajo el argumento de que (i) se requiere conocimiento del marco nacional para evitar riesgos de incumplimiento normativo y (ii) se trata de un requisito “objetivo, verificable” y de “libre acceso y a cero costo” al ser ofertado por MinTIC.		
Si bien la Entidad afirma que las certificaciones MinTIC se obtienen mediante plataformas gratuitas y abiertas a cualquier ciudadano, lo cierto es que la exigencia se torna actualmente de imposible cumplimiento para nuevos integrantes del equipo, porque el acceso depende de que el MinTIC habilite (o reabra) convocatoria/cupos.		
En efecto, la evidencia disponible indica que las inscripciones a la convocatoria de cursos virtuales estuvieron disponibles “hasta el 16 de diciembre de 2025”. y que a la fecha de la		

Versión: 2

Fecha de vigencia: 12 de junio de 2025

observación no existe una ruta cierta e inmediata para obtener la certificación, al no estar visible oferta activa “Cursos 2026”. Dejamos evidencia:



Adicionalmente en la plataforma apti, necesaria para la realización de la certificación, al día de hoy NO tienen ningún programa habilitado para el 2026



Por tanto, mantenerlo como requisito habilitante restringe el universo de proponentes solo a quienes ya estaban certificados antes del cierre, afectando de manera objetiva la pluralidad de oferentes y la libre concurrencia, al imponer una condición que no depende del proponente sino de un tercero (MinTIC).

Debido a lo anterior, solicitamos a la Entidad eliminar dicho requisito, por las siguientes razones:

Esta situación implica que el requisito no permite una competencia real, pues restringe la participación únicamente a quienes, por circunstancias previas (y ajenas al proceso), hayan obtenido el curso en convocatorias anteriores. Por ello, mantenerlo como habilitante atenta contra los principios de la contratación estatal, en particular:

Versión: 2

Fecha de vigencia: 12 de junio de 2025

- Selección objetiva (Ley 80 de 1993, art. 29; Ley 1150 de 2007, art. 5), dado que los requisitos deben permitir comparar ofertas en condiciones reales de competencia y deben recaer sobre factores verificables y accesibles para todos los potenciales oferentes en el marco del proceso, evitando exigencias imposibles o no disponibles que distorsionen la escogencia.
- Transparencia y economía (Ley 80 de 1993, arts. 24 y 25), en la medida en que los requisitos habilitantes deben ser razonables, pertinentes y proporcionales al objeto contractual y no pueden imponer cargas que, sin aportar un valor técnico adicional, restrinjan la concurrencia e induzcan a controversias.
- Igualdad y libre competencia (Constitución Política, arts. 13 y 333), pues un requisito que actualmente no se puede obtener en el mercado, por depender exclusivamente de la apertura de oferta estatal, genera una barrera de acceso injustificada que afecta la pluralidad de oferentes.

En contratación estatal, los requisitos deben ser conexos, razonables y proporcionales al objeto, evitando barreras que limiten injustificadamente la competencia y la posibilidad de obtener la oferta más favorable, en desarrollo del principio de transparencia (Ley 80) y la selección objetiva (Ley 1150).

En la misma línea, la jurisprudencia ha explicado que la libertad de concurrencia se relaciona con la igualdad de oportunidades y favorece la selección de la oferta más favorable. Adicionalmente, la Guía/Manual de Colombia Compra Eficiente sobre requisitos habilitantes insiste en que estos son mínimos para participar y, por ello, deben estructurarse sin imponer cargas innecesarias o desalineadas con la finalidad real del proceso.

En este caso, incluso aceptando que la Entidad requiere conocimiento del marco nacional la forma en que se exige (únicamente certificación MinTIC habilitante y vigente) resulta desproporcionada cuando no hay oferta disponible para que el mercado la obtenga en igualdad de condiciones.

Observación 2:

Solicitud de eliminar requisito del Establecimiento de Comercio en Pereira:

De manera respetuosa, nos permitimos presentar contraobservación frente a la respuesta de la Entidad mediante la cual no accede a eliminar o modificar el requisito de contar con establecimiento de comercio o punto de atención en el Área Metropolitana, manteniéndolo “tal cual” en el Pliego y el Anexo Técnico.

La Entidad sustenta su negativa en que el objeto contractual consistiría en la operación y soporte de un SOC 24x7, y que ante incidentes críticos existirían escenarios donde la intervención física sería “insustituible”, con un ANS presencial de una (1) hora (pérdida de conectividad, contención de malware/ransomware, análisis forense/cadena de custodia), además de la cobertura sobre instituciones educativas con conectividad variable, incluso rurales.

Versión: 2

Fecha de vigencia: 12 de junio de 2025

No obstante, con todo respeto, consideramos que la exigencia de “establecimiento de comercio” no es el medio idóneo, necesario ni proporcional para cumplir la finalidad que la Entidad pretende (respuesta presencial en 1 hora), y además restringe la pluralidad de oferentes sin aportar una mitigación real del riesgo.

1) El requisito no guarda relación directa con el objeto y la naturaleza del servicio

El proceso corresponde a la adquisición/implementación de licencias antimalware y plataforma cloud para monitoreo y operación de alertas de ciberseguridad, servicios cuya administración, operación y soporte se realizan principalmente de forma remota mediante herramientas tecnológicas, canales de soporte y plataformas en la nube. Por ello, la existencia de un establecimiento de comercio en un territorio específico no constituye un elemento esencial para la correcta ejecución del contrato.

2) “Establecimiento” no garantiza el ANS de 1 hora

El punto central que pretende asegurar la Entidad es la capacidad de respuesta en un tiempo máximo de una (1) hora cuando la situación requiera presencia física. Sin embargo, un establecimiento de comercio, por sí mismo, no acredita:

- disponibilidad de personal 24/7,
- esquema de turnos o guardias,
- capacidad logística de desplazamiento inmediato,
- ni la ejecución efectiva de la atención dentro del tiempo requerido.

En consecuencia, el requisito confunde el medio con el fin: exige una figura formal (establecimiento) que no garantiza el resultado buscado (respuesta presencial ≤ 1 hora).

3) Restricción de la concurrencia sin aporte técnico equivalente

Mantener la exigencia de un establecimiento de comercio en un área determinada limita la participación a quienes ya cuentan con presencia física previa en la zona, aun cuando existan oferentes idóneos con operación nacional y capacidad real de atención in situ. Esto afecta la pluralidad de oferentes y la posibilidad de selección objetiva de la propuesta más favorable, sin que se demuestre que el requisito sea el único mecanismo idóneo para mitigar el riesgo operativo.

De manera respetuosa, nos permitimos precisar que el numeral que establece “implementar una plataforma Cloud que funcione como Centro de Operaciones de Seguridad (SOC) para el monitoreo, correlación y gestión de alertas de ciberseguridad, garantizando la administración centralizada de todas las licencias...” debe entenderse, desde un punto de vista técnico, como la provisión de una herramienta tecnológica en la nube (consola centralizada) para la gestión y administración de la solución, y no como la prestación de un SOC integral.

En ciberseguridad, un SOC no es únicamente una plataforma; corresponde a un modelo operativo compuesto por personas, procesos y tecnología, incluyendo operación 24/7 con

Versión: 2

Fecha de vigencia: 12 de junio de 2025

analistas, procedimientos de escalamiento, respuesta a incidentes, contención y actividades forenses, entre otros. En contraste, el alcance descrito en el pliego se concentra en la capa tecnológica: monitoreo, correlación y gestión de alertas, y administración centralizada de licencias, lo cual corresponde a una plataforma cloud de administración y monitoreo (por ejemplo, consola tipo EDR/XDR/SIEM según la solución) y no implica, por sí mismo, la exigencia de infraestructura física permanente en el territorio.

Ahora bien, el pliego adicionalmente establece que el contratista debe “prestar el servicio de asistencia técnica, mantenimiento y soporte posventa, a través de mesa de ayuda telefónica, electrónica y presencial, durante los diez (10) meses de vigencia contractual, con tiempos máximos de respuesta de una (1) hora y de solución de ocho (8) horas, conforme al Acuerdo de Niveles de Servicio (ANS) que se establezca con la Entidad”.

Sobre este punto, es importante precisar que:

A. El “tiempo máximo de respuesta” de 1 hora en el marco de una mesa de ayuda se entiende técnicamente como el tiempo de atención inicial y activación del soporte (registro, diagnóstico preliminar, priorización, asignación y escalamiento), lo cual se cumple de forma telefónica o electrónica en la gran mayoría de eventos, especialmente tratándose de una plataforma cloud y licenciamiento administrado centralmente.

B. La inclusión del canal “presencial” no significa que todos los casos deban atenderse físicamente, sino que existirá disponibilidad de atención en sitio cuando sea estrictamente necesario y bajo solicitud; por tanto, no resulta técnico ni proporcional asumir que el ANS de 1 hora corresponde automáticamente a presencia física o desplazamiento, pues ello dependerá de la naturaleza del incidente, el lugar, la sede y el diagnóstico inicial.

C. En servicios basados en plataforma cloud y administración centralizada, el cumplimiento del ANS se acredita por la capacidad operativa de respuesta (procedimientos, canales 24/7, escalamiento, disponibilidad de recursos), no por la existencia de un “establecimiento de comercio” en una ubicación específica. Un establecimiento, por sí solo, no garantiza turnos, disponibilidad, ni respuesta efectiva; en cambio, el ANS se garantiza mediante compromisos de atención y soporte.

En ese sentido, el establecimiento de comercio no es idóneo ni proporcional para garantizar el ANS.

Aun en los casos excepcionales en los que se requiera intervención en sitio, la exigencia de un establecimiento de comercio no garantiza por sí misma:

- disponibilidad de personal 24/7,

Versión: 2

Fecha de vigencia: 12 de junio de 2025

- turnos o guardias,
- logística para desplazamiento,
- ni capacidad real de respuesta efectiva.

Por tanto, el requisito confunde el medio con el fin: se exige una figura formal registral que no acredita cumplimiento del ANS, mientras que lo verdaderamente verificable es el compromiso operativo de atención y escalamiento.

Adicionalmente, mantener este requisito restringe la participación únicamente a proponentes con presencia comercial previa en el área, limitando la pluralidad de oferentes y la posibilidad de selección objetiva de la oferta más favorable, sin aportar una mitigación real y medible del riesgo operativo.

En mérito de lo anterior, solicitamos respetuosamente a la Entidad:

1. **Eliminar** del numeral 15.5 el requisito de contar con establecimiento de comercio o punto de atención en el Área Metropolitana.
2. **Sustituirlo** por un requisito funcional y verificable, consistente en que el proponente aporte una Carta de Compromiso, suscrita por el representante legal, mediante la cual se obligue expresamente a:

- Brindar atención inicial y activación del soporte (mesa de ayuda telefónica y electrónica) con tiempo máximo de respuesta de una (1) hora, conforme al ANS.
- En caso de que, por la naturaleza del incidente, sea estrictamente necesaria una intervención en sitio, disponer los recursos para atender presencialmente bajo las condiciones del ANS que se acuerde con la Entidad.

Con esta modificación se protege el interés de la Entidad (garantía del ANS), se exige lo realmente relevante (capacidad y compromiso operativo), y se evita restringir la competencia mediante un requisito formal que no garantiza el cumplimiento del nivel de servicio.

6	NUMERAL Y/O LITERAL OBSERVADO:	Numeral 15.5 requisitos especiales técnicos del pliego de condiciones
7	DOCUMENTO Y PÁGINA:	
8	SE ACCEDE A LA OBSERVACIÓN	SI ☐ NO ☒
9	RESPUESTA:	

RESPUESTA A OBSERVACION 1

La Entidad NO ACCEDE a la solicitud de eliminar o modificar el requisito relativo a la Certificación en Seguridad y Privacidad de la Información – Gobierno Digital (MinTIC) y Certificación en el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se

Versión: 2

Fecha de vigencia: 12 de junio de 2025

mantiene inalterado en los términos establecidos en el Pliego y el Anexo Técnico, con fundamento en las siguientes consideraciones:

1. Conexidad directa con el objeto contractual y el marco normativo aplicable

El objeto del proceso contractual involucra la protección de activos de información institucionales, la operación de un SOC, la gestión de incidentes de ciberseguridad y el cumplimiento de obligaciones normativas en materia de seguridad y privacidad de la información.

En este contexto, la Entidad no solo requiere competencias técnicas en ciberseguridad, sino también conocimiento específico y demostrado del marco normativo nacional aplicable al sector público, en particular:

- Política de Gobierno Digital,
- Modelo de Seguridad y Privacidad de la Información (MSPI),
- Lineamientos y obligaciones expedidas por el Ministerio TIC.

La certificación exigida es un mecanismo objetivo de verificación de que el personal clave comprende y aplica correctamente dicho marco, lo cual resulta esencial para mitigar riesgos de incumplimiento normativo, responsabilidad que recae directamente sobre la Entidad.

2. Objetividad, verificabilidad y razonabilidad del requisito

El requisito cuestionado cumple plenamente con los criterios definidos por la Estrategia Nacional de Seguridad Digital 2025-2027 y la lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) para entidades del estado para los requisitos habilitantes, toda vez que:

- Es objetivo, al tratarse de una certificación emitida por la autoridad nacional competente en la materia.
- Es verificable, mediante constancia oficial expedida por MinTIC.
- Es pertinente y proporcional, dado que se exige exclusivamente para los perfiles críticos definidos en el Numeral 9.1, y no de manera indiscriminada para todo el personal.

Contrario a lo señalado por el observante, la Entidad no está exigiendo una certificación de carácter exclusivo, oneroso o reservado, sino una acreditación gratuita, pública y abierta, diseñada precisamente para estandarizar capacidades en el sector público.

3. Sobre la supuesta “imposibilidad actual” de obtener la certificación

La Entidad no comparte la interpretación según la cual el requisito sea de imposible cumplimiento, por las siguientes razones:

- La exigencia no se limita a certificaciones que se hayan obtenido dentro de un período o vigencia específica.

Versión: 2

Fecha de vigencia: 12 de junio de 2025

- La contratación estatal no se estructura en función de la disponibilidad coyuntural de cupos o convocatorias, sino sobre la base de competencias previas demostrables en los perfiles clave.
- Es legítimo y razonable que la Entidad exija que los proponentes cuenten desde la presentación de la oferta con personal que ya tenga experiencia y certificación en el marco MSPI, dada la criticidad del servicio y los riesgos asociados a su ejecución de acuerdo a la Estrategia de Seguridad Nacional, las políticas que rigen la entidad y al Modelo Integrado de Planeación y Gestión (MIPG).

Aceptar la eliminación del requisito bajo este argumento implicaría trasladar a la Entidad el riesgo de capacitación y curva de aprendizaje, lo cual es contrario a los principios de planeación, eficiencia y responsabilidad.

4. No vulneración de la libre concurrencia ni de la igualdad

La Entidad aclara que:

- Existen en el mercado múltiples profesionales que ya cuentan con la certificación exigida, lo que descarta la configuración de una barrera artificial.
- La libre concurrencia no implica la eliminación de requisitos técnicos o normativos, sino la posibilidad de que todos los interesados compitan bajo reglas claras, objetivas y previamente definidas.

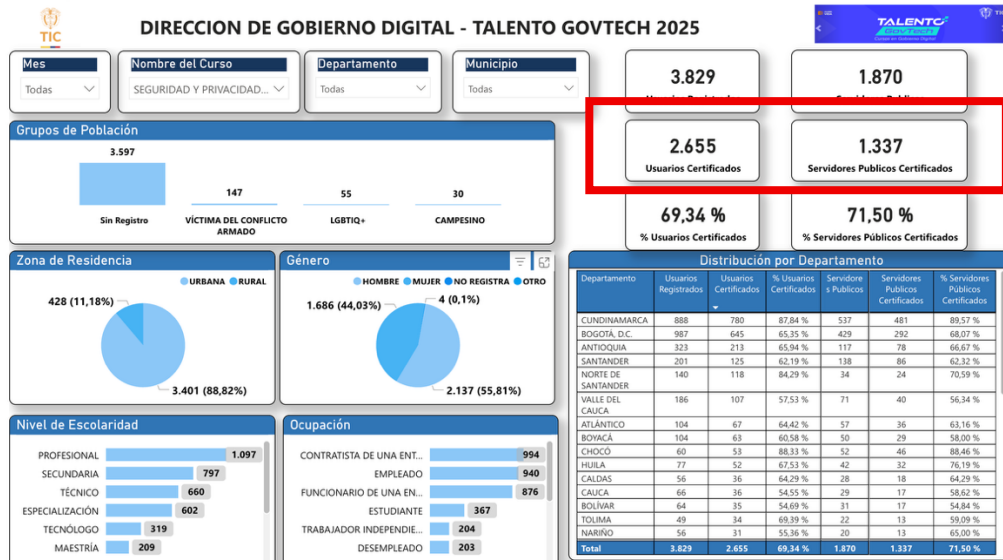
Anexamos evidencia que en el mercado nacional existe pluralidad de profesionales que ya se encuentran certificados en la necesidad de conocimiento de la Alcaldía de Pereira, donde hasta diciembre de 2025 se han certificado 4.179 colombianos, lo que evidencia una alta oferta de talento humano que cuenta con las certificaciones requeridas en este proceso.

Versión: 2

Fecha de vigencia: 12 de junio de 2025

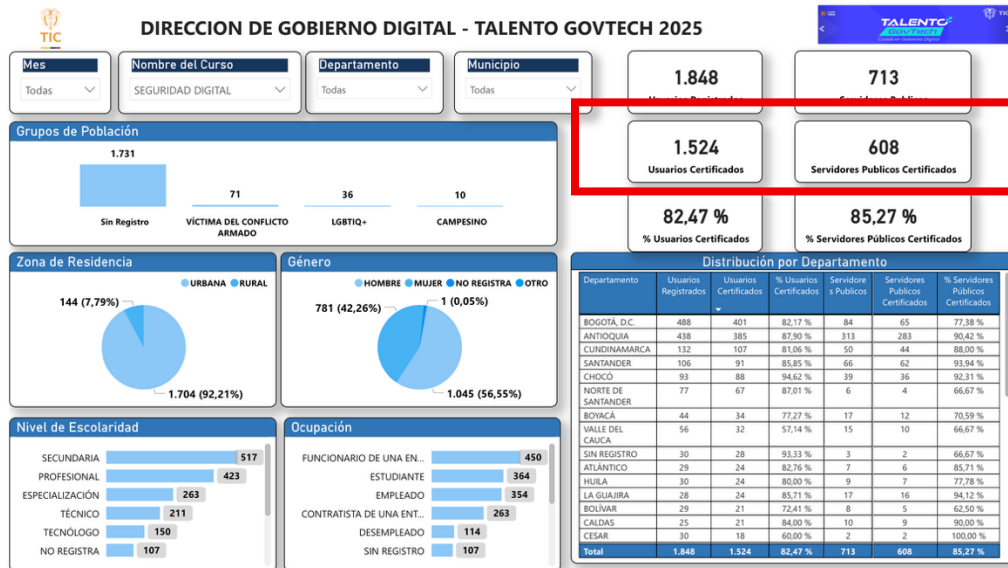
Cursos Talento GovTech

Si el visor no carga, utilice el [link alternativo](#)



Cursos Talento GovTech

Si el visor no carga, utilice el [link alternativo](#)



Fuente: <https://gobiernodigital.mintic.gov.co/> (2026)

La jurisprudencia y las guías de Colombia Compra Eficiente han sido consistentes en señalar que la pluralidad de oferentes no obliga a la Entidad a rebajar estándares técnicos o de

Versión: 2

Fecha de vigencia: 12 de junio de 2025

cumplimiento, especialmente cuando estos están directamente relacionados con la protección de intereses públicos.

5. Principio de selección objetiva y gestión del riesgo

Desde la perspectiva de la matriz de riesgos del proceso, el riesgo de incumplimiento normativo en materia de seguridad y privacidad de la información ha sido calificado como alto/extremo y este se encuentra inmerso en la matriz de riesgo (ítem 33,34 y 40).

RESPUESTA A OBSERVACION 2

La Entidad NO ACCEDE a la solicitud de eliminar o sustituir el requisito de contar con establecimiento de comercio o punto de atención en el Área Metropolitana, el cual se mantiene inalterado en los términos establecidos en el Pliego de Condiciones y en el Anexo Técnico, con fundamento en las siguientes consideraciones:

1. Conexidad directa con el objeto contractual y la gestión del riesgo

Si bien el proceso contractual incorpora componentes tecnológicos basados en plataformas Cloud para el monitoreo, correlación y gestión de alertas de ciberseguridad, el objeto contractual no se limita a la provisión de licencias o herramientas tecnológicas, sino que comprende de manera integral:

- La instalación de las **1.400 licencias** de software antimalware para los equipos de cómputo de la Alcaldía de Pereira y sus sedes externas, y las **6.542 licencias** para los equipos de cómputo de las 178 instituciones educativas oficiales adscritas a la Secretaría de Educación Municipal ubicadas en la zona urbana y rural del municipio de Pereira; es importante señalar que la disponibilidad de la sede y el personal requerido al proveedor deben estar disponibles desde la suscripción del acta de inicio para iniciar de manera inmediata con el proceso de instalación y activación de las licencias en todas las sedes tanto urbanas como rurales, con el fin de cumplir con el requisito de contar con la operación del 100% del servicio y las licencias instaladas a mas tardar el 01 de marzo del 2026, como se define en el pliego de condiciones. Por ende, es pertinente que el proveedor o partner tenga establecimiento local que permita coordinar las respectivas cuadrillas para ejecutar en el tiempo establecido.
- La operación continua de la solución de ciberseguridad,
- La gestión de incidentes críticos,
- La atención de eventos de alto impacto que pueden requerir intervención física inmediata,
- Y la prestación de soporte técnico presencial, cuando la criticidad del evento así lo exija, conforme a los Acuerdos de Niveles de Servicio (ANS).

En este contexto, el requisito de establecimiento de comercio es un mecanismo de mitigación del riesgo operativo, de acuerdo con las necesidades y criticidad de la disponibilidad de la

Versión: 2

Fecha de vigencia: 12 de junio de 2025

infraestructura tecnológica y sus sistemas de información asociados, esto orientado a garantizar la capacidad real de respuesta presencial oportuna, especialmente frente a:

- Incidentes de ransomware.
- Activos críticos comprometidos, afectados o vulnerados.
- Eventos de ciberseguridad que involucren pérdida de conectividad.
- Actividades de contención, análisis forense, trazabilidad de incidentes y preservación de cadena de custodia, tanto para atención, mitigación y solución como para reporte a entidades de orden nacional.
- Atención y soporte en instituciones educativas y demás sedes de la alcaldía, con condiciones de conectividad limitadas, incluso en zonas rurales.

2. Idoneidad y razonabilidad del requisito frente al ANS presencial

La Entidad aclara que el ANS de una (1) hora, previsto en el Pliego y el Anexo Técnico, no se circunscribe únicamente a la activación telefónica o electrónica; se aclara que si bien la mesa de ayuda se determina como canal centralizado de comunicación, la presencia física resulta insustituible, conforme a la realidad operativa de la infraestructura institucional como se desglosa a continuación con la explicación de los ANS expuestos:

Asistencia técnica

- Tiempos máximos de respuesta de una (1) hora
- Tiempo de solución de ocho (8) horas

Mantenimiento

- Tiempos máximos de respuesta de una (1) hora
- Tiempo de solución de ocho (8) horas,

Soporte posventa

- Tiempos máximos de respuesta de una (1) hora
- Tiempo de solución de ocho (8) horas.

Igualmente, como se manifiesta en el anexo técnico “El proveedor debe realizar el acompañamiento en la atención, mitigación y contención de los eventos e incidentes que se presenten, apoyando de manera remota y de no solucionarse, se requerirá la asistencia de manera presencial en un tiempo máximo de 1 hora”.

En dichos escenarios, la exigencia de un establecimiento de comercio o punto de atención en el Área Metropolitana y su personal técnico exigido en el pliego de condiciones, constituye un indicador objetivo y verificable de capacidad logística, que permite a la Entidad:

- Reducir la incertidumbre sobre tiempos reales de desplazamiento.

Versión: 2

Fecha de vigencia: 12 de junio de 2025

- Minimizar dependencias de traslados intermunicipales o interdepartamentales, por riesgos fortuitos o contingencias, que impidan el desplazamiento efectivo a las sedes y la Alcaldía de Pereira.
- Mitigar el riesgo de incumplimiento del ANS en eventos críticos.

Contrario a lo afirmado por el observante, la Entidad no confunde el medio con el fin, sino que adopta un criterio preventivo, coherente con el principio de planeación, para garantizar que el fin (respuesta oportuna presencial), sea materialmente alcanzable.

3. Sobre la suficiencia de cartas de compromiso u obligaciones declarativas

En el pliego de condiciones- Requisitos especiales y técnicos, se define la manera de acreditar el establecimiento de comercio con *“Certificado de Cámara de comercio en donde conste la existencia del establecimiento, sucursal o agencia o contrato o promesa de contrato, en donde se acredite el punto de atención en el área metropolitana centro occidente, para ello deberá aportar la respectiva constancia del mismo, la cual será verificada por la entidad y/o promesa de contrato mínimo por diez (10) meses”*.

En la observación del GRUPO LUMA SAS manifiestan que se está solicitando “presencia comercial previa en el área”, frente a esto queremos informar que esta interpretación es errónea, ya que en los pliegos de condiciones se establece que el requerimiento puede ser cumplido con la figura de promesa de contrato, en donde garanticen punto de atención físico a partir del inicio de la ejecución de este proceso de contratación, sin exigir presencia previa.

4. No vulneración de la libre concurrencia ni de la selección objetiva

La Entidad reitera que el requisito cuestionado:

- Se aplica de manera general, abstracta y no discriminatoria a todos los potenciales oferentes.
- No exige una marca, proveedor o modelo específico.
- Permite la participación de oferentes con operación nacional, que cuenten con presencia o punto de atención en el Área Metropolitana a partir de la fecha de inicio de contrato.

En este sentido, la exigencia de establecimiento de comercio no constituye una barrera injustificada, sino una condición razonable y proporcional frente a los riesgos identificados en la matriz del proceso. A continuación, evidenciamos un riesgo crítico:

Versión: 2

Fecha de vigencia: 12 de junio de 2025

Vulnerabilidades y Riesgos Críticos de la Plataforma AIRE Pereira

Una caíd

a de la Plataforma AIRE Gestión, particularmente si es motivada por incidentes de ciberseguridad, tendría consecuencias devastadoras para el Municipio de Pereira, ya que se trata de una herramienta de misión crítica que soporta el ciclo completo de los ingresos públicos.

A continuación, se describen los impactos detallados identificados:

1. Impactos Específicos por Ciberseguridad

Ataques de ransomware, como una de las amenazas más relevantes, es un incidente o una vulneración de seguridad que provocaría:

- Pérdida de atributos de la información: Se vería comprometida la disponibilidad, integridad, confidencialidad y trazabilidad de los datos tributarios y financieros.
- Parálisis de servicios digitales: Se interrumpiría la prestación de servicios virtuales a los contribuyentes, impidiendo trámites y pagos en línea.
- Compromiso de información sensible: Al concentrar grandes volúmenes de datos estratégicos, personales y empresariales sensibles, una caída por ciberataque expondría al municipio a prácticas extorsivas y a la divulgación no autorizada de datos.

2. Impactos Operativos y Administrativos

- Colapso de la gestión tributaria: La falta de acceso a la plataforma conllevaría un colapso en el manejo de la información de impuestos y contribuciones.
- Interrupción de procesos misionales: Se verían afectados los procesos internos de liquidación, facturación, fiscalización y cobranzas, generando retrasos y errores críticos.
- Pérdida de control institucional: La alcaldía dejaría de conocer y controlar los ingresos pagados por los contribuyentes, perdiendo la trazabilidad de la cartera.
- Mano de obra y equipos cesantes debido a la pérdida de acceso al sistema financiero

3. Impactos Financieros y Económicos

Versión: 2

Fecha de vigencia: 12 de junio de 2025

- Riesgo sobre el recaudo masivo: La plataforma administra operaciones superiores al billón de pesos anuales (registrando más de \$1.2 billones en 2025). Cualquier caída afecta directamente el flujo de caja del municipio, lo cual se hace más grave en los momentos de cierre en cualquiera de las vigencias de pago.
- Elevación de costos: Las fallas operativas generan sobrecostos institucionales y posibles detrimentos patrimoniales debido a la ineficacia en el recaudo y la necesidad de acciones de contingencia.

4. Impactos Legales y Reputacionales

- Incumplimiento normativo: Una caída impediría la rendición oportuna de informes ante entes de control y la rama judicial.
- Pérdida de confianza ciudadana: La inoperatividad del servicio daña la confianza de los contribuyentes en la administración municipal y genera riesgos jurídicos por el incumplimiento en la prestación de servicios públicos digitales.
- Inestabilidad fiscal: Se pone en riesgo la sostenibilidad fiscal del municipio al no poder asegurar una operación estable de sus rentas propias.

En resumen, una falla prolongada ocasionada por un incidente de ciberseguridad sin atención prioritaria, no es solo un problema técnico, sino una crisis que afectaría la estabilidad y continuidad operativa y financiera de la alcaldía de Pereira y sus instituciones educativas.

Si bien lo expuesto es uno de los posibles escenarios de materialización de riesgos, existen más activos de información críticos y sensibles que requieren contar con estas capacidades de protección en ciberseguridad y respuesta oportuna de acuerdo a los ANS, para que la Alcaldía de Pereira asegure la continuidad en todos sus procesos.

La Entidad tiene la responsabilidad de proteger activos críticos (como la Plataforma AIRE que recauda más de 1.2 billones de pesos de manera anual), así como todos los demás activos de la información que administra la alcaldía, los cuales contienen información de ciudadanos, programas y proyectos sociales, información contable y financiera, información de activos como bienes inmuebles, procesos jurídicos y judiciales y sistema de información para la gestión documental, entre otros; no exigir el establecimiento local, sabiendo que existen riesgos que solo se mitigan con presencia física (como fallas de conectividad total o remediación de ransomware en sitio), significa que la Entidad está contratando un servicio con un "vacío o

Versión: 2

Fecha de vigencia: 12 de junio de 2025

deficiencia de cobertura'. Es importante precisar que, en procesos contractuales adelantados en vigencias anteriores de la adquisición de este tipo de licencias y servicios, la entidad incorporó la exigencia de este mismo requisito, el cual ha demostrado ser una medida técnica eficaz para asegurar la cobertura técnica de los servicios complementarios requeridos. Si las amenazas son hoy más críticas que en el pasado, la calidad de la respuesta debe ser, como mínimo, igual o superior a la exigida anteriormente. Por esto, eliminar este requisito cuando en procesos previos (con amenazas menos complejas) sí se pedía, representa una contradicción técnica que deja a la Entidad en una posición de mayor vulnerabilidad frente a incidentes como el ransomware.

Coherencia con el Anexo Técnico y las respuestas previas a observaciones

La Entidad resalta que este requisito:

- Guarda concordancia con la exigencia de atención presencial ante eventos críticos, definida y ratificada con su propia observación por el GRUPO LUMA SAS, en el numeral 3.A donde manifiestan "en la gran mayoría de eventos", confirmando con esto que no todos los eventos y contingencias de ciberseguridad pueden ser solucionados de manera remota y requieren una atención presencial, que por su naturaleza imprevista no pueden ser planeados en un cronograma de atención, y es en estos eventos que se requiere presencialidad oportuna, para garantizarle a la alcaldía de Pereira el restablecimiento de los servicios que garanticen la continuidad en la operación en el menor tiempo posible.
- Hace parte integral de la estrategia de protección reforzada de activos críticos, junto con los demás requisitos técnicos y operativos del proceso.

Modificar o eliminar este requisito implicaría desnaturalizar el alcance del servicio esperado y debilitar los controles definidos por la Entidad.

El Principio de eficiencia y eficacia

Según el Manual de Contratación de la ANCP-CCE, en la aplicación de estos principios surge el concepto de Valor por Dinero que insta a la Entidad a obtener el "máximo beneficio posible en términos de calidad, precio, oportunidad, eficiencia, sostenibilidad y resultados".

Versión: 2

Fecha de vigencia: 12 de junio de 2025

De acuerdo al análisis del sector se demuestra que el mercado de ciberseguridad actual no ofrece solo una "licencia", sino una "canasta de componentes" que incluyen soporte en sitio y capacidad de respuesta ante incidentes, el hecho de no exigir la presencia física significa que la Entidad está renunciando a la oportunidad y a los resultados que el mercado ya tiene integrados en sus ofertas; pagar el mismo valor por un servicio con soporte remoto, cuando el mercado ofrece soporte presencial por ese valor, constituye una ineficiencia en el uso de los recursos públicos.

En consecuencia, la contra observación es rechazada y el requisito se mantiene sin modificación en el Pliego de Condiciones y el Anexo Técnico.

10	MODIFICA EL DOCUMENTO:	SI ☐ NO ☒ X
11	NUMERAL Y/O LITERAL ACTUALIZADO:	N/A



CARLOS ANDRÉS VASQUEZ R
Secretario de Tecnologías de la
Información y la Comunicación



CARLOS FERNANDO GARCÍA C
Director de Infraestructura tecnológica

CARLOS JAIRÓ BEDOYA NARANJO
Secretario de Educación

CESAR AUGUSTO CASATAÑO
Dir. Administrativo de Bienes y Servicios
Educativos

Componente financiero: Luz Geraldine Hernández Ospina, Contratista Secretaria de las TIC

Revisión legal: Laura García G, Abogada contratista, TIC. *Laura García G*

Apoyo técnico: Gustavo Adolfo Rivera, contratista Secretaria de las TIC *Gustavo Adolfo Rivera*

Apoyo técnico Yohan Sebastián Betancur Aricapa, contratista Secretaria de las TIC *Yohan Sebastián Betancur Aricapa*