Emitir resolución de recursos

1. Generar resolución de recursos

Digitador	Adriana Artavia		
Fecha/hora gestión	04/09/2026 08:13	**Fecha/hora resolución**	04/09/2026 08:38
* **Procesos asociados**	Recursos	**Número documento**	8072026000001647
* **Tipo de resolución**	Fondo		
Número de procedimiento	2026LY-000003-0009100001	**Nombre Institución**	MINISTERIO DE HACIENDA
Descripción del procedimiento	Servicios de nube pública, suscripción a licenciamiento, monitoreo y respuesta de ciberseguridad		

2. Listado de recursos

Número	Fecha presentación	Recurrente	Empresa/Interesado	Resultado	Causa resultado
8002026000001826	13/08/2026 20:45	MARCELO MEZA VALVERDE	SMART CITY CENTRO AMERICA HOLDING SOCIEDAD ANONIMA	Parcialmente con lugar	Por el fondo

Emitir el por tanto de la resolución	☐

3. *Resultando

I. Que mediante auto No. 8052026000001190, del 14 de agosto de 2026, de las 13:25 horas, esta División otorgó audiencia especial a la Administración licitante.

II. Que la presente resolución se emite dentro del plazo de ley, y en su trámite se han observado las prescripciones legales y reglamentarias correspondientes.

4. *Considerando

Recurso 8002026000001826 - SMART CITY CENTRO AMERICA HOLDING SOCIEDAD ANONIMA

I. SOBRE EL FONDO DEL RECURSO PRESENTADO. 1) RECURSO DE SMART CITY CENTROAMÉRICA SOCIEDAD ANONIMA. 1) Sobre certificaciones de seguridad. Criterio de la División: El pliego de condiciones solicita lo siguiente: *"2. La plataforma utilizada para brindar el servicio debe cumplir, como mínimo, con las certificaciones de seguridad ISO 27001, ISO 27017, ISO 27018 y las certificaciones de seguridad y procesos SOC 1, SOC 2 Y SOC 3, EU Safe Harbor y GDPR".*

Como aspecto de primer orden el gestionante señala que no se cuestiona la legitimidad de que la Administración exija un marco robusto de seguridad de la información, controles específicos para nube, protección de datos, aseguramiento independiente y evidencia vigente.

No obstante objeta que la cláusula convierta ocho referencias de distinta naturaleza y fuerza probatoria en un bloque acumulativo de supuestas certificaciones de seguridad y procesos, sin delimitar su alcance, versión, periodo, sujeto aplicable, equivalencia o riesgo específico cubierto.

Ante ello señala que la formulación actual no permite distinguir cuáles documentos son indispensables, cuáles dependen de un supuesto particular de tratamiento, cuáles acreditan materias distintas y cuáles se superponen.

Indica que adjunta a su escrito de objeción el documento titulado "Anexo 1. Prueba técnica", el cual concluye que la cláusula mezcla una norma certificable de sistema de gestión, guías de controles especializados, informes de aseguramiento con finalidades diferentes, un régimen de transferencias invalidado desde 2015 y una regulación de protección de datos y la acumulación literal no demuestra por sí sola una capa adicional y proporcional de seguridad.

Referente a la solicitud de: *"ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018*", afirma que según el dictamen o prueba técnica aportada, ISO/IEC 27001:2022, acredita la existencia de un sistema de gestión de seguridad de la información dentro de un alcance determinado.

La ISO/IEC 27017:2026 desarrolla controles y orientación especializados para servicios de nube y la ISO/IEC 27018:2025 se ocupa de la protección de información de identificación personal en nube pública cuando el proveedor actúa en el rol correspondiente.

Sobre el "*SOC 1*", señala que tiene una finalidad distinta, ya que el dictamen que adjunta explica que SOC 1, se refiere a controles de una organización de servicios relevantes para el control interno de las entidades usuarias sobre información financiera, por ello, no acredita por sí solo una capa general adicional de ciberseguridad para una plataforma de nube o un servicio SOC/MDR y su exigencia sólo sería técnicamente pertinente si la Administración identifica una dependencia concreta con controles relevantes para información financiera y justifica por qué ese examen resulta indispensable para el servicio contratado.

En relación a *"SOC 2 y SOC 3*", presentan solapamiento directo, ya que agrega el SOC 2 y SOC 3, se relacionan con las mismas categorías generales de servicios de confianza y la diferencia relevante es que SOC 2 ofrece un informe restringido con mayor detalle, mientras SOC 3 es de uso general y no contiene el mismo nivel de información.

Sobre la solicitud del pliego de "*EU Safe Harbor"* añade que dejó de ser un mecanismo vigente y la prueba técnica establece que fue un marco relativo a determinadas transferencias de datos entre la Unión Europea y los Estados Unidos, sustentado en la Decisión 2000/520/CE, declarada inválida el 6 de octubre de 2015, e indica que su eliminación no rebaja el nivel de protección.

Por último afirma que la solicitud del "*GDPR"* es una regulación, no una certificación universal de plataforma, indica que es una regulación de protección de datos personales cuyo ámbito debe determinarse según el tratamiento concreto.

Alude al artículo 8 y 40 de la LGCP y el artículo 84 y 90 del Reglamento e indica que la potestad de exigir seguridad no habilita una acumulación inconexa, redundante u obsoleta, cita precedentes de esta División y afirma que de mantenerse la redacción actual, su representa se ve afectada porque la cláusula limita desde la fase de preparación de la oferta las plataformas, proveedores y esquemas de aseguramiento que podría integrar adyacente a que refiere la acumulación reduce el universo competitivo y obliga a trasladar al precio costos documentales sin valor incremental acreditado y puede favorecer estructuras cerradas que reúnen por razones históricas documentos heterogéneos.

En virtud de lo expuesto solicita eliminar la referencia a EU Safe Harbor; eliminar el tratamiento de GDPR como una certificación de plataforma; eliminar SOC 1 como requisito general e incondicionado, conservando únicamente si la Administración identifica y motiva una necesidad vinculada con controles relevantes para información financiera; eliminar la exigencia acumulativa de SOC 2 y SOC 3 sobre el mismo sistema y periodo, dejando SOC 3 como evidencia complementaria; y reformular las referencias ISO conforme a sus versiones, alcance, aplicabilidad y equivalencias técnicamente controladas.

Solicita sustituir íntegramente la redacción actual por la siguiente redacción, o por otra que produzca el mismo efecto competitivo y técnico: "*La plataforma utilizada para brindar el servicio deberá demostrar un marco vigente de seguridad de la información, seguridad de nube, privacidad y aseguramiento independiente aplicable al alcance del servicio. Como evidencia mínima se aceptará: (a) certificación vigente ISO/IEC 27001:2022 o equivalente, con alcance aplicable a la plataforma o servicio; (b) para servicios de nube, evidencia de aplicación de controles de ISO/IEC 27017:2026 y, cuando el proveedor actúe como procesador de PII en nube pública, de ISO/IEC 27018:2025, o controles equivalentes; (c) informe SOC 2 Type 2 vigente o atestación independiente equivalente, que cubra al menos Security y, según el alcance, Availability, Confidentiality, Processing Integrity y/o Privacy; y (d) cumplimiento de la normativa de protección de datos y de los mecanismos de transferencia internacional que resulten aplicables. No se exigirá EU Safe Harbor. SOC 1 únicamente será requerido cuando se identifique una necesidad vinculada con controles relevantes para información financiera. SOC 3 podrá aportarse como evidencia complementaria de uso general, pero no será obligatorio de forma acumulativa cuando se aporte SOC 2 Type 2 sobre el mismo sistema y periodo*."

La Administración mediante respuesta a audiencia especial señala que la referencia a "*EU Safe Harbor*" será eliminada por corresponder a un mecanismo de transferencia internacional de datos declarado inválido desde 2015 y que no constituye una certificación vigente ni una acreditación que pueda ser demostrada por los actuales proveedores de servicios en la nube. Por lo anterior, se acepta su eliminación como certificación requerida dentro del pliego.

Ratifica que las certificaciones "*ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018*", constituyen referencias internacionales ampliamente aceptadas para acreditar controles de seguridad de la información, servicios en la nube y protección de datos, no obstante, indica el ministerio que acepta la solicitud de actualizar y reformular dichas referencias conforme a sus versiones vigentes, alcance y aplicabilidad.

Señala que en cuanto a las restantes pretensiones formuladas, relacionadas con las referencias a los System and Organization Controls "*SOC 1, SOC 2 y SOC 3"* y la eliminación del requisito relativo al cumplimiento de "*GDPR*", se rechazan y aclara que tales requerimientos no están dirigidos al contratista intermediario, sino a la plataforma de nube que soportará los servicios objeto de la contratación.

En relación con el "*GDPR*", precisa que este no corresponde a una certificación, sino a una regulación en materia de protección de datos personales, por ello, no se exige que el oferente cuente con una certificación GDPR, sino que la infraestructura tecnológica propuesta disponga de mecanismos, controles y capacidades que permitan demostrar su alineamiento y cumplimiento con dicha normativa y de igual forma agrega que, las referencias a SOC 1, SOC 2 y SOC 3 recaen sobre la plataforma tecnológica que brindará el servicio.

De acuerdo con el criterio técnico rendido, reitera que se allana parcialmente al primer motivo de objeción en cuanto a la eliminación de la referencia a EU Safe Harbor y a la actualización de las referencias ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018 conforme a sus versiones vigentes, alcance y aplicabilidad.

En cuanto a SOC 1, SOC 2, SOC 3 y GDPR, no comparte la pretensión de la recurrente, por las razones apuntadas por el departamento técnico, por último afirma que el pliego de condiciones goza de una presunción de validez.

Señala que la prueba técnica aportada con el recurso fue analizada por las unidades competentes y producto de esa valoración se aceptaron los cuestionamientos relativos a EU Safe Harbor y a la actualización de las referencias ISO, sin embargo, no ocurrió lo mismo respecto de SOC 1, SOC 2, SOC 3 y GDPR. En consecuencia afirma, se acoge parcialmente este motivo de objeción.

Ante el cuadro fáctico expuesto, procede esta División a indicar lo siguiente:

Sobre el EU Safe Harbor y actualización de normas ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018: En virtud de las posiciones vertidas, resulta procedente acoger la objeción del gestionante en cuanto al requerimiento de *EU Safe Harbor*.
Lo anterior tomando en consideración que como bien lo reconoció la Administración licitante a partir de la prueba técnica del recurrente, dicho marco fue declarado nulo e inválido por el Tribunal de Justicia de la Unión Europea desde el 6 de octubre de 2015.
Ante ello resulta cierto que de mantener en el pliego de condiciones actual, el requerir una acreditación legalmente inexistente constituye una transgresión directa al principio de razonabilidad y se convierte en un requisito de imposible cumplimiento.
Asimismo considerando el argumento del recurrente, la prueba aportada y la respuesta de la Administración licitante, en apego a al principio de eficiencia es procedente la actualización de las normas *ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018,* conforme a sus versiones vigentes, alcance y aplicabilidad.
En cuanto a SOC 1, SOC 2, SOC 3 y GDPR: Es criterio indicar que se toma en consideración que tal como lo aclaró la Administración en su respuesta, estos requerimientos no fueron formulados para ser cumplidos por la empresa oferente, sino sobre la plataforma tecnológica de nube que sustentará la infraestructura y los servicios contratados, así mismo se entiende que la Administración como conocedora de su necesidad ha decidido mantener los requerimientos en el tanto favorece la plataforma y se alinean a su funcionalidad y se contará con un marco holístico e integral de control interno, ciberseguridad, integridad y gobernanza.

La parte recurrente cuestiona la conveniencia y la necesidad funcional de adquirirlos de forma conjunta, pero la objeción al pliego no constituye un mecanismo para sustituir el criterio de oportunidad y conveniencia técnica de la Administración licitante, adyacente a que el objetante no logró demostrar que el requerimiento carezca de vínculo con los riesgos que la Administración busca mitigar o que constituya una cláusula que direccione el concurso hacia un único proveedor.

Sobre el GDPR, habiendo puntualizado el Ministerio que la exigencia no consiste en aportar una certificación formal inexistente, sino en comprobar que la plataforma disponga de capacidades, controles técnicos y mecanismos efectivos para asegurar el cumplimiento y alineamiento con los principios de dicha regulación de protección de datos personales, el requerimiento resulta plenamente válido y razonable dentro del marco de protección de información institucional sensible. Únicamente se instruye a la Administración a fin de que ajuste la redacción de la cláusula en el pliego para que refleje textualmente esta precisión, eliminando la ambigüedad que genera calificar al GDPR como una certificación.

Debe indicarse que de conformidad con los artículos 88 y 95 de la LGCP y 246 y 254 del RLGCP, los actos de la Administración, -incluido la confección del pliego de condiciones-, gozan de presunción de legalidad y acierto técnico y la carga de la prueba recae en la parte objetante, quien debe desvirtuar dicha presunción mediante elementos técnicos y jurídicos concluyentes que evidencien una arbitrariedad, un vicio sustancia o una transgresión directa al ordenamiento jurídico.

Por otra parte, resulta válido indicar que la prueba técnica adjunta señala; "*...Quien suscribe, Esteban Alonso Jiménez Cabezas, cédula de identidad 1-1394-0838, emite el presente dictamen técnico a solicitud de un potencial oferente del procedimiento descrito. Soy fundador y Chief Technology and Information Officer (CTIO) de ATTICYBER y mantengo una relación profesional directa con la parte interesada. Esta circunstancia se declara expresamente para que el documento sea valorado con transparencia como criterio técnico de parte…*".

Ante ello debe advertirse que se evidencia el vínculo profesional y comercial directo del Sr. Esteban Alonso Jiménez Cabezas, con la empresa objetante, lo que origina que el dictamen carece de la imparcialidad y objetividad propia de una pericia independiente.

Así mismo debe advertirse que las condiciones del pliego de condiciones responden a la necesidad pública, no siendo procedente que este se adapte al modelo comercial, estructura operativa o catálogo de acreditaciones con que cuente una empresa interesada en particular.

Ante ello el hecho de que un requisito límite una oferta o le demande mayor esfuerzo de cumplimiento, no lo convierte en una barrera ilegítima, siempre que la exigencia guarde relación con el objeto y se encuentre dentro de la disponibilidad objetiva del mercado tecnológico.

En consecuencia, al haberse allanado la Administración a suprimir un requisito inexistente y actualizar las normas internacionales vigentes, pero manteniéndose incólume la potestad institucional para exigir un marco robusto de control (SOC) y privacidad (GDPR) sobre la plataforma de nube, lo procedente es declarar **parcialmente con lugar,** el extremo, debe proceder la Administración con los ajustes pertinentes y brindarles la debida publicidad.

2) Sobre la exigencia de que los analistas Soc Nivel 2., estén destacados en Costa Rica. Criterio de la División: El pliego de condiciones indica lo siguiente: "*Analista de seguridad de SOC nivel 2. Al menos 2 años de experiencia en telecomunicaciones, redes, ciberseguridad o administración de TI. • Al menos 3 proyectos o servicios de TI o ciberseguridad en los últimos 6 años. • Estos especialistas deben estar destacados en Costa Rica para la atención y contención de incidentes de seguridad …"*

Ante ello señala la gestionante que su objeción se dirige a la frase en la cual los dos analistas de Seguridad SOC Nivel 2, deben estar destacados en Costa Rica para la atención y contención de incidentes.

Afirma que no objeta la cantidad de dos analistas, la formación de Nivel 2 o equivalente, la experiencia, los proyectos previos, las certificaciones, la obligación de confidencialidad, la cobertura ni el cumplimiento de los SLA y cuestiona únicamente que la ubicación territorial se convierta en condición general y permanente, sin análisis de las funciones que realmente exigen presencia física.

Adjunta prueba técnica en la cual se analiza las tareas ordinarias de un analista SOC Nivel e indica que esas actividades se realizan sobre consolas, registros, SIEM, herramientas de respuesta y canales digitales. Su ejecución depende de credenciales, privilegios controlados, conectividad segura, procedimientos, turnos, supervisión y trazabilidad, no de la presencia física en un país determinado. Cita precedentes de esta División, solicita la eliminación de la frase "*Estos especialistas deben estar destacados en Costa Rica para la atención y contención de incidentes de seguridad"* y sugiere una nueva redacción en pro de los principios que rigen la materia.

Propone el siguiente texto: *"Los Analistas de Seguridad SOC Nivel 2 deberán formar parte del equipo operativo que brinde cobertura efectiva 24x7x365 y cumplir íntegramente los requisitos de experiencia, formación y certificación establecidos en el pliego. Podrán prestar sus funciones desde Costa Rica o desde centros de operaciones de seguridad autorizados del contratista ubicados en otras jurisdicciones, siempre que el contratista garantice: (i) cumplimiento de los SLA de atención, investigación y contención; (ii) atención y escalamiento en idioma español; (iii) acceso remoto seguro mediante MFA, mínimo privilegio y controles PAM/JIT cuando corresponda; (iv) cifrado y trazabilidad de sesiones y acciones; (v) continuidad y redundancia operativa; (vi) confidencialidad y tratamiento de información conforme al contrato y la normativa aplicable; (vii) las certificaciones y experiencia exigidas; y (viii) disponibilidad de atención presencial en Costa Rica únicamente cuando una actividad específica no pueda ejecutarse remotamente y sea previamente coordinada con la Administración"*.
La Administración mediante respuesta a audiencia señala que, analizada la justificación técnica aportada y la revisión al documento Anexo 1. Prueba técnica.pdf aportada por el oferente, respecto de la naturaleza remota de las actividades desarrolladas por los Analistas de Seguridad SOC Nivel 2, considera procedente eliminar la obligación de que dichos especialistas se encuentren permanentemente destacados en Costa Rica.
Asimismo afirma, se valoraron los controles y mecanismos técnicos propuestos, tales como el acceso remoto seguro mediante autenticación multifactor (MFA), el cumplimiento de los niveles de servicio (SLA) requeridos, así como las medidas de confidencialidad, trazabilidad y cumplimiento aplicables al personal que presta el servicio. Con base en lo anterior, se concluye que estos elementos permiten garantizar la adecuada prestación del servicio, en concordancia con el razonamiento técnico expuesto en el recurso presentado.
En consecuencia indica, el requisito será reformulado para permitir que los Analistas SOC Nivel 2 desempeñen sus funciones, aunque no se encuentren en el territorio nacional, independientemente de su ubicación geográfica, siempre que se garantice el cumplimiento de los niveles de servicio, seguridad, confidencialidad y continuidad operativa establecidos en el pliego de condiciones.
Por lo anterior manifiesta, se acepta la solicitud relacionada con la ubicación territorial de los Analistas SOC Nivel 2 y se procederá a realizar la modificación correspondiente en el pliego de condiciones.
En virtud de lo anterior es criterio señalar que la Administración acogió la pretensión sustantiva de suprimir la obligatoriedad de que dichos analistas se encuentren permanentemente destacados en Costa Rica.
No obstante es criterio indicar que a pesar de allanarse la Administración sobre la procedencia del reclamo en su aspecto medular, no resulta procedente aceptar la redacción alternativa que de manera específica propone la empresa objetante en su recurso, se reitera en cuanto a que el pliego de condiciones goza de una presunción de validez y legalidad y emana del ejercicio de la discrecionalidad técnica y administrativa que el ordenamiento jurídico le confiere en exclusiva a la entidad licitante.
Es así que corresponde declarar **parcialmente con lugar** en extremo en general y deberá proceder la Administración a realizar el ajuste correspondiente y brindarle la debida publicidad.

5. Aprobaciones

Encargado	ADRIANA ARTAVIA GUZMAN	**Estado firma**	La firma es válida
Fecha aprobación(Firma)	04/09/2026 08:14	**Vigencia certificado**	07/05/2024 14:28 - 06/05/2028 14:28
DN Certificado	CN=ADRIANA ARTAVIA GUZMAN (FIRMA), OU=CIUDADANO, O=PERSONA FISICA, C=CR, GIVENNAME=ADRIANA, SURNAME=ARTAVIA GUZMAN, SERIALNUMBER=CPF-01-1137-0068		
CA Emisora	CN=CA SINPE - PERSONA FISICA v2, OU=DIVISION SISTEMAS DE PAGO, O=BANCO CENTRAL DE COSTA RICA, C=CR, SERIALNUMBER=CPJ-4-000-004017		

Encargado	KAREN MARIA CASTRO MONTERO	**Estado firma**	La firma es válida
Fecha aprobación(Firma)	04/09/2026 08:37	**Vigencia certificado**	05/02/2026 13:12 - 04/02/2030 13:12
DN Certificado	CN=KAREN MARIA CASTRO MONTERO (FIRMA), OU=CIUDADANO, O=PERSONA FISICA, C=CR, GIVENNAME=KAREN MARIA, SURNAME=CASTRO MONTERO, SERIALNUMBER=CPF-04-0181-0227		
CA Emisora	CN=CA SINPE - PERSONA FISICA v2, OU=DIVISION SISTEMAS DE PAGO, O=BANCO CENTRAL DE COSTA RICA, C=CR, SERIALNUMBER=CPJ-4-000-004017		

6. Notificación resolución

Fecha/hora máxima adición aclaración	09/09/2026 23:59		
Número resolución	R-DCP-SICOP-01583-2026	**Fecha notificación**	04/09/2026 09:01