Emitir resolución de recursos

1. Generar resolución de recursos

Digitador	CELINA MEJIA CHAVARRIA		
Fecha/hora gestión	23/11/2026 08:06	**Fecha/hora resolución**	23/11/2026 09:21
* **Procesos asociados**	Recursos	**Número documento**	8072026000002220
* **Tipo de resolución**	Fondo		
Número de procedimiento	2026LY-000029-0015700001	**Nombre Institución**	BANCO DE COSTA RICA
Descripción del procedimiento	Contratación de una solución SAAS personalizada en la nube para la emisión, recepción y aceptación de comprobantes electrónicos para el conglomerado BCR		

2. Listado de recursos

Número	Fecha presentación	Recurrente	Empresa/Interesado	Resultado	Causa resultado
8002026000002525	30/10/2026 18:45	ANISIA YENORY VEGA VILLALOBOS	TECNOWARE SOLUCIONES INFORMÁTICAS SOCIEDAD ANÓNIMA	Parcialmente con lugar	Por el fondo
8002026000002508	30/10/2026 10:27	CARLOS FRANCISCO MORENO HERNANDEZ	CYBERFUEL SOCIEDAD ANONIMA	Parcialmente con lugar	Por el fondo

Emitir el por tanto de la resolución	☐

3. *Resultando

I. Que mediante auto número 8052026000001665 del 02 de noviembre del 2026, esta División otorgó audiencia especial a la Administración licitante para que se refiera a los argumentos expuestos por los objetantes.
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 8002026000002525 - TECNOWARE SOLUCIONES INFORMÁTICAS SOCIEDAD ANÓNIMA

I. FONDO

1) Cláusula 17.10. Certificaciones Obligatorias.

En el documento denominado "Condiciones Generales" del pliego de condiciones, se indica lo siguiente: *"**17.10 Certificaciones Obligatorias** / 17.10.1 El oferente deberá acreditar contar con las siguientes certificaciones vigentes emitidas por organismos acreditados: / 17.10.1.1 ISO 22301: Sistema de Gestión de Continuidad del Negocio. / 17.10.1.2 ISO 27017: Controles de Seguridad para Servicios de Computación en la Nube. / **17.10.2 Verificación:** / 17.10.2.1 Copia de las certificaciones vigentes emitidas por organismos acreditados. / 17.10.2.2 Documentación que permita verificar su vigencia y autenticidad. / 17.10.2.3 La no presentación de cualquiera de estas certificaciones o la presentación de certificaciones vencidas dará lugar a la declaratoria de inadmisibilidad de la oferta."* (el destacado es del original).

La **empresa objetante** cuestiona la cláusula 17.10.1 porque en ella se exige que el oferente sea titular de certificaciones cuyo núcleo de riesgo corresponde a la capa de infraestructura, ya certificada por el proveedor de nube. Considera que con ello se obliga a duplicar controles existentes, sin que el pliego justifique técnicamente esa duplicidad como requisito mínimo de admisibilidad. Solicita lo siguiente:

A) Como pretensión principal solicita que se modifique la redacción de la cláusula 17.10.1 y se incorporen las cláusulas 17.10.2.4 y 17.10.2.5, de la siguiente manera: *"17.10.1 El oferente deberá acreditar que la solución ofertada opera dentro del alcance de las siguientes certificaciones vigentes, emitidas por organismos acreditados, las cuales podrán estar a nombre del oferente o del proveedor de infraestructura de nube en que se aloja la solución, siempre que su alcance comprenda los servicios utilizados por esta: / 17.10.1.1 ISO 22301: Sistema de Gestión de Continuidad del Negocio / 17.10.1.2 ISO/IEC 27017: Controles de Seguridad para Servicios de Computación en la Nube." / "17.10.2.4 Cuando las certificaciones indicadas en el numeral 17.10.1 correspondan al proveedor de infraestructura de nube sobre el que opera la solución, el oferente deberá aportar, junto con su oferta: / (a) Documento emitido por el proveedor de nube o por el organismo de certificación que acredite el alcance de las certificaciones, en el que consten los servicios y la infraestructura utilizados por la solución ofertada, o bien los certificados y, de ser necesario, la declaración de aplicabilidad (SoA), de los que ese alcance pueda verificarse; y (b) Declaración jurada del representante legal de que la solución se aloja en dicha infraestructura y dentro del alcance de las certificaciones. / Los informes de auditoría que el proveedor de nube mantenga bajo confidencialidad podrán ofrecerse a la Administración para su verificación en los términos que ella establezca. No se tendrán por acreditadas las certificaciones cuyo alcance no comprenda los servicios de nube utilizados por la solución ofertada." / "17.10.2.5 Durante la ejecución contractual, el contratista deberá mantener la solución dentro del alcance de certificaciones vigentes. La Administración podrá verificar esa vigencia en cualquier momento, para lo cual el contratista pondrá a su disposición, dentro de los diez días hábiles siguientes a su solicitud, la certificación vigente o la evidencia de su renovación. Cualquier cambio de proveedor de infraestructura requerirá aviso previo al Banco, y el nuevo proveedor deberá contar con certificaciones equivalentes a las exigidas en el numeral 17.10.1."*

B) Como pretensión subsidiaria, y en caso de mantenerse las certificaciones como requisito de admisibilidad, solicita que se admita que el oferente las acredite mediante las certificaciones vigentes del proveedor de infraestructura de nube sobre el que opera la solución, siempre que aporte junto con su oferta la documentación de alcance y la declaración jurada descritas en el numeral 17.10.2.4, y que el mantenimiento de esas certificaciones se verifique durante la ejecución contractual conforme al numeral 17.10.2.5.

C) Como pretensión subsidiaria de la anterior, solicita que la titularidad de las certificaciones se incorpore como factor de evaluación y no como requisito de admisibilidad, conforme al criterio reiterado de la Contraloría General.

Al contestar la audiencia especial, la **Administración** aceptó modificar el pliego de condiciones y en este sentido manifiesta lo siguiente: *"Se acoge el extremo de la objeción relacionado con la necesidad de revisar el tratamiento otorgado a las certificaciones ISO 22301 e ISO/IEC 27017, así como la necesidad de admitir mecanismos de acreditación acordes con modelos de prestación de servicios bajo modalidad SaaS soportados sobre infraestructura de computación en la nube. / La Administración reconoce que, tratándose de soluciones SaaS, determinados controles asociados a continuidad operativa, resiliencia tecnológica, seguridad física y seguridad de infraestructura pueden encontrarse bajo responsabilidad del fabricante de la solución o del proveedor de infraestructura utilizado para la prestación del servicio. / Como resultado del análisis realizado, las certificaciones ISO 22301 e ISO/IEC 27017 dejarán de formar parte de los requisitos de admisibilidad y pasarán a formar parte de los criterios de evaluación del procedimiento, reconociendo el valor agregado que dichas certificaciones aportan en materia de continuidad del negocio y seguridad en servicios de computación en la nube. / En consecuencia, la no presentación de dichas certificaciones no constituirá causal de inadmisibilidad de la oferta. No obstante, los oferentes que cuenten con ellas podrán acreditarlas para efectos de la evaluación correspondiente. / Asimismo, la Administración aceptará que dichas certificaciones sean acreditadas por el oferente, por el fabricante de la solución o por el proveedor de infraestructura utilizado para la prestación del servicio, siempre que el alcance de las certificaciones cubra efectivamente los componentes y servicios sobre los cuales operará la solución ofertada. / Cuando las certificaciones correspondan al proveedor de infraestructura o al fabricante de la solución, el oferente deberá aportar documentación que permita verificar su vigencia, alcance y relación con la solución propuesta. / Para tales efectos podrá aportarse, entre otros: / a) Copia del certificado vigente correspondiente. / b) Información oficial emitida por el organismo certificador, el fabricante de la solución o el proveedor de infraestructura que permita verificar la vigencia y alcance de la certificación. / c) Declaración del oferente que identifique la infraestructura, los servicios utilizados y su relación con la solución ofertada. / d) Cuando resulte pertinente, documentación o matriz de responsabilidad compartida que permita identificar los controles gestionados por el proveedor de infraestructura y aquellos que se encuentran bajo responsabilidad del oferente. / No se acoge el extremo de la objeción que pretende que la acreditación de las certificaciones mediante el proveedor de infraestructura implique la sustitución de los mecanismos de verificación definidos por la Administración o la aceptación automática de certificaciones cuyo alcance no cubra efectivamente los componentes y servicios utilizados por la solución ofertada. / La Administración considera indispensable mantener mecanismos objetivos que permitan verificar la vigencia, alcance y aplicabilidad de las certificaciones aportadas, así como la efectiva cobertura de los controles asociados a continuidad operativa, seguridad y protección de la información requeridos para la prestación del servicio. / En consecuencia, la atención de la presente objeción no implica la eliminación de dichos controles, sino el ajuste de los mecanismos mediante los cuales serán acreditados y valorados dentro del procedimiento de contratación."*

Criterio de la División: como punto de partida debemos indicar que este órgano contralor ha sostenido en forma reiterada que las normas de aseguramiento de la calidad establecidas por la Organización Internacional para la Normalización ISO son acreditaciones a las que se someten las empresas de manera voluntaria, por lo que no es aceptable que se soliciten como un requisito de admisibilidad, y en este sentido se pueden consultar, entre otras, las resoluciones R-DCA-0641-2017, R-DCA-00657-2021, R-DCA-SICOP-0244-2022, R-DCA-SICOP-01134-2023, R-DCP-SICOP-01209-2025 y R-DCP-SICOP-01602-2025, entre otras. Concretamente en la resolución R-DCP-SICOP-01209-2025 del 03 de julio del 2025 se indicó sobre este tema lo siguiente: *"En primer lugar, con respecto a la cláusula 3.1.7 del pliego de condiciones que refiere: "(...) El equipo de medición contará necesariamente con certificado de calibración de fábrica, bajo norma internacional INTE ISO IEC 17025 (El alcance del requisito es asegurar que el fabricante posee o subcontrata un laboratorio ISO 17025. La certificación tiene que ser de un laboratorio homologado en el ECA. (...)"; esta División determina que dicha cláusula se encuentra en el apartado "3.1.1 Requisitos de admisibilidad del oferente" del pliego de condiciones y a partir de allí, se debe indicar que la certificación ISO no puede ser un requisito de admisibilidad, sino más bien, un factor ponderable en metodología de evaluación, al respecto ha sido criterio reiterado de esta División mediante resolución n.° R-DCA-SICOP-00255-2023 de las 09:41 horas del 14 de febrero de 2023 la cual refiere en lo conducente: "(…) Por otra parte ha de indicarse que, ciertamente lleva razón el gestionante cuando señala que, la certificación ISO no puede ser un requisito de admisibilidad, sino más bien un factor ponderable en metodología de evaluación, al respecto ha sido criterio de esta División mediante resolución No. R-DCA-0464-2019, de las siete horas con cincuenta y dos minutos del veintiuno de mayo de dos mil diecinueve, lo siguiente:"...Así mismo, respecto de la solicitud del objetante respecto de la incorporación de la certificación ISO 14001 como requisito de admisibilidad, esta División ya se ha referido ampliamente al respecto, indicando lo siguiente: "De igual manera, ha sido el criterio de este Despacho, que en razón de que las normas de aseguramiento de la calidad establecidas por la Organización Internacional para la Normalización ISO, es una acreditación a la que se someten las empresa de manera voluntaria, que de acuerdo con nuestro ordenamiento jurídico, no sería dable constituir su requerimiento como una condición de admisibilidad, como ha sido establecido en este cartel (…) Posteriormente, en la resolución No. R-DCA-285-2013 (...), este Despacho indicó:*

"(...), tener presente que con relación a las certificaciones ISO, este órgano contralor, de manera reiterada(entre otras las resoluciones No. RC-257-2001, RC-239-2001) ha indicado que aquellas no pueden establecerse como requisito de admisibilidad como en el caso concreto, por lo que se puede valorar su incorporación pero como factor de evaluación (...)" (resolución R-DCA-0641-2017 del dieciséis de agosto del dos mil diecisiete).(...)". Ahora bien, de la referencia hecha a los antecedentes de esta misma División, se logra extraer que no resulta jurídicamente viable establecer en las bases del concurso las normas de aseguramiento de la calidad establecidas por la Organización Internacional para la Normalización ISO como requerimiento "invariable o de admisibilidad.",...". En el caso bajo análisis se observa que la Administración aceptó modificar el pliego de condiciones de forma tal que las certificaciones ISO 22301 e ISO/IEC 27017 dejarán de formar parte de los requisitos de admisibilidad y pasarán a formar parte de los criterios de evaluación, lo cual resulta acorde con la petición subsidiaria de la empresa objetante y con el criterio reiterado de este órgano contralor. Por lo tanto, se declara **parcialmente con lugar** el recurso en este aspecto.

2) Certificaciones de los bloques 5 y 6.

En el documento denominado "Especificaciones Técnicas" del pliego de condiciones se indica lo siguiente: *"**Bloque 5: Solución en la Nube** / […] **Mitigación de Amenazas y Cumplimiento Nube** / Realización de pruebas de penetración periódicas con entrega de resultados al BCR si se solicitan. / Controles antimalware y detección de amenazas avanzadas. / Cumplimiento verificado con estándares internacionales: ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3, GDPR y PCI-DSS."* (el destacado es del original).

*"**Bloque 6: Apego a las Normas de Seguridad del Conglomerado Financiero del Banco de Costa Rica** / […] **Certificaciones de Seguridad Requeridas** / Tenencia de certificaciones internacionales vigentes: / ISO/IEC 27001. / ISO/IEC 27017. / ISO/IEC 27018. / SSAE-16 / SOC 1 / SOC 2 Tipo II. / SOC 3 / GDPR / PCI-DSS. / ISO 22301."* (el destacado es del original).

La **empresa objetante** cuestiona dichas cláusulas porque no indican a nombre de quién deben estar las certificaciones y los informes requeridos. Considera que la única lectura que la Administración podría aplicar al evaluar las ofertas es que el oferente sea titular de todas las certificaciones e informes listados, y ello produce una restricción efectiva a la participación. Solicita lo siguiente:

A) Como pretensión principal, solicita que se modifique la redacción de los bloques 5 y 6 de la siguiente manera: *"**Bloque 6, "Certificaciones de Seguridad Requeridas**": / "Tenencia de certificaciones e informes internacionales vigentes, emitidos a nombre del proveedor de infraestructura de nube en que se aloja la solución, con alcance sobre los servicios utilizados por esta: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 22301, SOC 1 Tipo II (emitido bajo la norma SSAE-18 del AICPA o la norma ISAE 3402, o las que las sustituyan), SOC 2 Tipo II, SOC 3 y PCI DSS. El cumplimiento de la Ley N.° 8968 y el alineamiento con los principios del Reglamento (UE) 2016/679 (GDPR) se acreditarán mediante los compromisos contractuales de protección de datos del proveedor de infraestructura de nube y del oferente, complementados con declaración jurada del oferente. / Para efectos de este requisito, se entenderá vigente el informe SOC más reciente emitido, cuyo periodo auditado haya concluido dentro de los doce meses anteriores a la fecha de apertura de ofertas. / Estas certificaciones e informes se acreditarán conforme a lo dispuesto en los numerales 17.10.2.4 y 17.10.2.5 de las Condiciones Generales." / **Bloque 5, "Mitigación de Amenazas y Cumplimiento Nube":** / "Cumplimiento verificado con estándares internacionales: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1, SOC 2, SOC 3, protección de datos personales y PCI-DSS, el cual podrá acreditarse mediante certificaciones e informes emitidos a nombre del proveedor de infraestructura de nube en que se aloja la solución, y mediante compromisos contractuales de protección de datos del proveedor o del oferente, en los términos del Bloque 6."*

B) Como pretensión subsidiaria, solicita que se disponga expresamente en el pliego que las certificaciones y los informes de los bloques 5 y 6 pueden acreditarse mediante el proveedor de infraestructura de nube, con alcance sobre los servicios utilizados por la solución.

C) Como pretensión subsidiaria de la anterior, solicita que la titularidad de dichas certificaciones e informes se incorpore como factor de evaluación y no como requisito de admisibilidad, conforme el criterio reiterado de la Contraloría General.

Al contestar la audiencia especial, la **Administración** aceptó modificar el pliego de condiciones y en este sentido manifiesta lo siguiente: *"Se acoge el extremo de la objeción relacionado con la necesidad de aclarar la titularidad de las certificaciones e informes requeridos en los Bloques 5 y 6 de las Especificaciones Técnicas, así como la necesidad de evitar ambigüedades respecto a los mecanismos mediante los cuales podrá acreditarse su cumplimiento. / La Administración reconoce que, tratándose de soluciones bajo modalidad SaaS soportadas sobre infraestructura de computación en la nube, determinados controles asociados a disponibilidad, continuidad operativa, seguridad de infraestructura, protección de la información y resiliencia tecnológica pueden corresponder al oferente, al fabricante de la solución o al proveedor de infraestructura utilizado para la prestación del servicio. / En consecuencia, se procederá a ajustar el pliego de condiciones con el fin de establecer expresamente que las certificaciones, informes de auditoría y demás mecanismos de acreditación requeridos podrán ser acreditados mediante documentos emitidos a nombre del oferente, del fabricante de la solución o del proveedor de infraestructura que soporte el servicio, según corresponda al componente o control objeto de acreditación, siempre que su alcance cubra efectivamente los componentes y servicios utilizados por la solución ofertada. / Asimismo, cuando las certificaciones o informes correspondan al proveedor de infraestructura o al fabricante de la solución, el oferente deberá aportar documentación que permita verificar su vigencia, alcance y relación con la solución propuesta. / Para tales efectos podrá aportarse, entre otros: / a) Copia del certificado o informe vigente correspondiente. / b) Información oficial emitida por el organismo certificador, auditor independiente, fabricante de la solución o proveedor de infraestructura que permita verificar su vigencia y alcance. / c) Declaración del oferente que identifique la infraestructura, los servicios utilizados y su relación con la solución ofertada. / d) Cuando resulte pertinente, documentación o matriz de responsabilidad compartida que permita identificar los controles gestionados por el proveedor de infraestructura y aquellos que se encuentran bajo responsabilidad del oferente. / Los documentos indicados anteriormente constituirán medios válidos de acreditación para los requisitos correspondientes, debiendo permitir verificar objetivamente la vigencia, alcance y aplicabilidad de la certificación o informe aportado respecto de la solución ofertada. / Asimismo, se procederá a ajustar los requisitos asociados a certificaciones y mecanismos de cumplimiento contenidos en los Bloques 5 y 6, incluyendo: / 1. La eliminación de la referencia a GDPR como certificación técnica. / 2. La eliminación de SOC 3 como requisito acumulativo de cumplimiento. / 3. La actualización de la referencia a SSAE-16, sustituyéndola por la exigencia de informes SOC 1 Tipo II y SOC 2 Tipo II vigentes, emitidos por un auditor independiente bajo los estándares de atestiguamiento aplicables de AICPA, o informes equivalentes emitidos bajo estándares internacionalmente reconocidos, siempre que proporcionen un nivel de aseguramiento y alcance equivalente. / 4. El traslado de ISO 22301 e ISO 27017 desde los requisitos de admisibilidad hacia los criterios de evaluación. / 5. La revisión de los mecanismos de acreditación asociados a infraestructura y servicios en la nube. / No se acoge la pretensión de establecer que las certificaciones e informes requeridos deban acreditarse exclusivamente mediante documentos emitidos a nombre del proveedor de infraestructura de nube, ni que la sola presentación de dichos documentos implique su aceptación automática sin la verificación de su alcance, vigencia, aplicabilidad y relación con la solución ofertada. / La Administración considera indispensable mantener mecanismos objetivos de validación que permitan verificar que las certificaciones, informes y demás evidencias aportadas cubren efectivamente los componentes, servicios e infraestructura utilizados para la prestación de la solución, así como el cumplimiento de los controles asociados a seguridad, continuidad operativa, disponibilidad, protección de la información y gestión de riesgos requeridos para la presente contratación. / En consecuencia, la atención de la presente objeción no implica la eliminación de los mecanismos de aseguramiento requeridos, sino la redefinición y clarificación de los mecanismos mediante los cuales podrá acreditarse su cumplimiento, así como la eliminación de requisitos redundantes o susceptibles de generar interpretaciones restrictivas."*

Criterio de la División: se observa que la Administración aceptó ajustar el pliego de condiciones con el fin de establecer expresamente que las certificaciones, informes de auditoría y demás mecanismos de acreditación requeridos podrán ser acreditados mediante documentos emitidos a nombre del oferente, del fabricante de la solución o del proveedor de infraestructura que soporte el servicio, según corresponda al componente o control objeto de acreditación, siempre que su alcance cubra efectivamente los componentes y servicios utilizados por la solución ofertada, lo cual resulta acorde con la pretensión subsidiaria de la empresa objetante. Por lo tanto, se declara **parcialmente con lugar** el recurso en este aspecto. Sin embargo, las cláusulas cuestionadas incluyen las certificaciones ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018,

ISO/IEC 22301 y en su respuesta, la Administración solamente aceptó trasladar las certificaciones ISO 22301 e ISO 27017 de los requisitos de admisibilidad hacia los criterios de evaluación, por lo tanto **de oficio** se advierte a la Administración que todas las certificaciones ISO deberán eliminarse como requisitos de admisibilidad, según lo explicado anteriormente, y si es de su interés, podrá incorporarlas como aspectos de evaluación.

3) Norma SSAE-16.

En el documento denominado "Especificaciones Técnicas" del pliego de condiciones se indica lo siguiente: *"**Bloque 6: Apego a las Normas de Seguridad del Conglomerado Financiero del Banco de Costa Rica** / […] **Certificaciones de Seguridad Requeridas** / Tenencia de certificaciones internacionales vigentes: / ISO/IEC 27001. / ISO/IEC 27017. / ISO/IEC 27018. / SSAE-16 / SOC 1 / SOC 2 Tipo II. / SOC 3 / GDPR / PCI-DSS. / ISO 22301."* (el destacado es del original).

La **empresa objetante** explica que el AICPA sustituyó la norma SSAE-16 por la SSAE-18, aplicable a los informes fechados a partir del 1 de mayo de 2017, y desde entonces no se emiten informes bajo la SSAE-16, de modo que ningún oferente puede aportar un informe vigente emitido bajo esa norma. Por ello considera que la aplicación literal del requisito conduce a la inadmisión de todas las ofertas. Solicita lo siguiente:

A) Como pretensión principal, solicita que se sustituyan los requisitos "SSAE-16" y "SOC 1" del Bloque 6 por el siguiente texto: "SOC 1 Tipo II, emitido bajo la norma SSAE-18 del AICPA o la norma ISAE 3402, o las que las sustituyan."

B) Como pretensión subsidiaria, solicita que se sustituya la referencia a "SSAE-16" por "SSAE-18 o ISAE 3402, o las que las sustituyan".

Al contestar la audiencia especial, la **Administración** aceptó modificar el pliego de condiciones y en este sentido manifiesta lo siguiente: *"La Administración reconoce que la referencia a SSAE-16 corresponde a un estándar que fue sustituido por normas posteriores actualmente vigentes y utilizadas para la emisión de informes de aseguramiento independientes aplicables a proveedores de servicios tecnológicos y servicios de computación en la nube. / Asimismo, se considera procedente ajustar la redacción del requisito con el fin de diferenciar claramente entre los estándares de atestiguamiento utilizados para la emisión de los informes y los propios informes de aseguramiento requeridos como evidencia de cumplimiento. / En virtud de lo anterior, y con el fin de mantener la vigencia técnica, actualidad y razonabilidad de los requisitos establecidos en el procedimiento, la Administración procederá a eliminar la referencia a SSAE-16 contenida en las Especificaciones Técnicas y establecer que el oferente deberá presentar informes SOC 1 Tipo II y SOC 2 Tipo II vigentes, emitidos por un auditor independiente bajo los estándares de atestiguamiento aplicables de AICPA, o informes equivalentes emitidos bajo estándares internacionalmente reconocidos, siempre que proporcionen un nivel de aseguramiento y alcance equivalente respecto de los controles asociados al servicio ofertado. / Asimismo, la Administración considera procedente revisar la consistencia de los mecanismos de aseguramiento contemplados en el pliego, con el propósito de garantizar una definición clara de las evidencias requeridas, sus alcances, vigencias y mecanismos de acreditación aceptados. / La Administración considera necesario mantener evidencia objetiva e independiente que permita verificar la existencia y efectividad de controles asociados a la prestación del servicio objeto de contratación, incluyendo aspectos relacionados con seguridad, disponibilidad, continuidad operativa, integridad del procesamiento y protección de la información. En ese sentido, la actualización de la referencia normativa no tiene como finalidad reducir los niveles de aseguramiento requeridos, sino adecuarlos a los estándares vigentes de la industria y a los mecanismos de acreditación actualmente reconocidos. / Por consiguiente, la actualización del requisito tiene como finalidad corregir una referencia normativa desactualizada y precisar los mecanismos de acreditación aceptables, sin disminuir el nivel de aseguramiento requerido por la Administración ni eliminar los controles cuya verificación resulta necesaria para garantizar la adecuada prestación del servicio contratado. / En consecuencia, se elimina la referencia a SSAE-16 y se actualizan los mecanismos de aseguramiento exigidos mediante informes vigentes y reconocidos por la industria que permitan demostrar controles equivalentes a los originalmente requeridos, manteniendo el alcance de control que la Administración considera necesario para la presente contratación."*

Criterio de la División: se observa que la Administración aceptó eliminar la referencia a SSAE-16, y además indica que va a actualizar los mecanismos de aseguramiento exigidos mediante informes vigentes y reconocidos por la industria que permitan demostrar controles equivalentes a los originalmente requeridos, pero sin aceptar la redacción propuesta por el recurrente y sin que la recurrente haya explicado por qué debe aceptarse su redacción propuesta y no otra. Por lo tanto, se declara **parcialmente con lugar** el recurso en este aspecto.

4) Certificación GDPR.

En el documento denominado "Especificaciones Técnicas" del pliego de condiciones se indica lo siguiente: *"**Bloque 5: Solución en la Nube** / […] **Mitigación de Amenazas y Cumplimiento Nube** / Realización de pruebas de penetración periódicas con entrega de resultados al BCR si se solicitan. / Controles antimalware y detección de amenazas avanzadas. / Cumplimiento verificado con estándares internacionales: ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3, GDPR y PCI-DSS."* (el destacado es del original).

*"**Bloque 6: Apego a las Normas de Seguridad del Conglomerado Financiero del Banco de Costa Rica** / […] **Certificaciones de Seguridad Requeridas** / Tenencia de certificaciones internacionales vigentes: / ISO/IEC 27001. / ISO/IEC 27017. / ISO/IEC 27018. / SSAE-16 / SOC 1 / SOC 2 Tipo II. / SOC 3 / GDPR / PCI-DSS. / ISO 22301."* (el destacado es del original).

La **empresa objetante** explica que el GDPR es una norma jurídica, no un esquema de certificación técnica equiparable a los demás de la lista; sin embargo el pliego condiciones enumera "GDPR" como si fuera una certificación más, sin indicar qué instrumento debe aportarse para acreditarlo. Considera que el requisito es indeterminado y no permite una evaluación objetiva. El pliego no precisa si se exige un sello de certificación del artículo 42 del GDPR, compromisos contractuales de protección de datos u otro medio. Tampoco indica sobre qué tratamientos debe recaer. Deja a la discrecionalidad de la evaluación la determinación de qué se tiene por cumplido, en perjuicio de la seguridad jurídica y de la igualdad de trato entre oferentes. Solicita lo siguiente:

A) Como pretensión principal, solicita que se sustituya la referencia a "GDPR" en los Bloques 5 y 6 por el siguiente texto: *"Cumplimiento de la Ley N.° 8968, de Protección de la Persona frente al Tratamiento de sus Datos Personales, y alineamiento con los principios del Reglamento (UE) 2016/679 (GDPR), acreditados mediante los compromisos contractuales de protección de datos del oferente o del proveedor de infraestructura de nube en que se aloja la solución (por ejemplo, Data Protection Addendum), complementados con declaración jurada del oferente."*

B) Como pretensión subsidiaria, solicita que se precise en el pliego el medio concreto por el cual debe acreditarse el cumplimiento del GDPR y se admitan como medio suficiente los compromisos contractuales de protección de datos del oferente o del proveedor de infraestructura de nube.

C) Como pretensión subsidiaria de la anterior, solicita que si el Banco considera necesaria una certificación conforme al artículo 42 del GDPR, esta no sea un requisito de admisibilidad.

Al contestar la audiencia especial, la **Administración** aceptó modificar el pliego de condiciones y en este sentido manifiesta lo siguiente: *"La Administración acoge la pretensión principal del objetante relacionada con la eliminación de la referencia a GDPR como certificación dentro de los Bloques 5 y 6 de las Especificaciones Técnicas, por cuanto dicho reglamento constituye un marco normativo de protección de datos personales y no una certificación técnica susceptible de acreditación en los términos planteados en el pliego. / La Administración reconoce que el Reglamento General de Protección de Datos de la Unión Europea (GDPR) constituye un marco normativo de protección de datos personales y no una certificación técnica equiparable a las certificaciones ISO o a los informes de aseguramiento contemplados dentro de la presente contratación. / Asimismo, la Administración comparte el criterio de que la referencia al GDPR como certificación puede generar ambigüedades respecto a la naturaleza del requisito y a los mecanismos mediante los cuales debe acreditarse su cumplimiento. / En consecuencia, se procederá a eliminar la referencia a GDPR como certificación o requisito de acreditación dentro de los Bloques 5 y 6 de las Especificaciones Técnicas. / No obstante, la Administración mantiene la necesidad de verificar que la solución propuesta incorpore controles adecuados para la protección, confidencialidad, integridad y tratamiento de la información, así como mecanismos alineados con las mejores prácticas en materia de*

protección de datos personales y con la normativa aplicable. / Asimismo, los oferentes deberán garantizar el cumplimiento de la Ley N.° 8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, su Reglamento y demás normativa aplicable en materia de protección de datos personales, así como los controles y medidas de seguridad requeridos para la protección de la información administrada por la solución. / La Administración incorporará una redacción distinta a la propuesta por el recurrente, por considerarla técnicamente más adecuada para satisfacer la necesidad institucional y mantener los controles de protección de datos requeridos para la presente contratación. / La presente modificación no implica la eliminación de los controles de protección de datos requeridos por la Administración, sino la eliminación de la referencia al GDPR como certificación y la adecuación del requisito a la naturaleza regulatoria de dicho marco normativo."

Criterio de la División: se observa que la Administración aceptó eliminar la referencia a GDPR como certificación o requisito de acreditación dentro de los Bloques 5 y 6 de las Especificaciones Técnicas, pero indica que incorporará una redacción distinta a la propuesta por el recurrente, sin que la recurrente haya explicado por qué lo más conveniente es aceptar su redacción exacta y no otra. Por lo tanto, se declara **parcialmente con lugar** el recurso en este aspecto.

5) Ubicación geográfica del alojamiento de datos.

En el documento denominado "Especificaciones Técnicas" del pliego de condiciones se indica lo siguiente: *"**Bloque 5: Solución en la Nube** / **Modelo de Servicio y Operación** / […] Ubicación geográfica del alojamiento de datos garantizando la permanencia en jurisdicción costarricense o equivalente."* (el destacado es del original).

La **empresa objetante** considera que el requisito es indeterminado y contradice otras cláusulas del pliego, ya que el pliego no define qué se entiende por "jurisdicción equivalente" ni tampoco establece criterios para determinar qué país o región cumple esa condición ni qué garantías debe ofrecer el alojamiento. Solicita lo siguiente:

A) Como pretensión principal, solicita que se sustituya el requisito de ubicación de los datos por el siguiente texto: *"Ubicación geográfica del alojamiento de datos en Costa Rica o en una jurisdicción cuyo marco de protección de datos personales ofrezca un nivel de protección igual o superior al de la Ley N.° 8968. El oferente deberá declarar dicha jurisdicción conforme al Bloque 8 e indicar la normativa de protección de datos aplicable en ella. La jurisdicción declarada no deberá figurar en la lista de jurisdicciones no admitidas que, en su caso, la Administración incorpore al pliego antes de la apertura de ofertas. En todo caso, el alojamiento deberá cumplir las siguientes condiciones: / (a) El oferente indicará en su oferta la región o regiones de alojamiento principal y de respaldo; / (b) Los datos se cifrarán en reposo y en tránsito, con llaves criptográficas custodiadas en módulos HSM con validación FIPS 140-2 o superior, y con trazabilidad de su uso; / (c) El Banco conservará en todo momento la titularidad de sus datos, así como el derecho de acceso, auditoría, recuperación y portabilidad sobre ellos durante la vigencia del contrato y el período de transición de salida que se establezca; y / (d) Los datos no se trasladarán a regiones distintas de las indicadas en la oferta sin autorización previa y por escrito del Banco."*

B) Como pretensión subsidiaria, solicita que se definan en el pliego criterios objetivos para determinar qué se entiende por "jurisdicción equivalente" y se admita la región declarada por el oferente conforme al Bloque 8, siempre que cumpla las condiciones (a) a (d) del texto propuesto.

Al contestar la audiencia especial, la **Administración** aceptó modificar el pliego de condiciones y en este sentido manifiesta lo siguiente: *"Se acoge el extremo de la objeción relacionado con la necesidad de precisar el concepto de "jurisdicción costarricense o equivalente", así como la necesidad de armonizar las disposiciones contenidas en el pliego relacionadas con la ubicación geográfica, almacenamiento, procesamiento, respaldo y privacidad de la información. / La Administración reconoce que la referencia a una "jurisdicción costarricense o equivalente" requiere mayor precisión para facilitar su correcta interpretación y aplicación, así como para garantizar una evaluación objetiva de las ofertas. / En consecuencia, la Administración procederá a efectuar las siguientes modificaciones: / Se incorporará una definición más precisa del concepto de "jurisdicción equivalente", estableciendo los criterios que deberán considerarse para determinar su aceptabilidad dentro del procedimiento considerando aspectos relacionados con protección de datos personales, cumplimiento normativo, seguridad de la información, continuidad operativa y gestión de riesgos. / Se corregirán los errores de numeración existentes en las Especificaciones Técnicas, particularmente aquellos relacionados con la duplicidad de los Bloques 7 y 8, con el fin de evitar ambigüedades en la referencia de los requisitos. / Se revisarán y ajustarán los apartados relacionados con la privacidad, almacenamiento, procesamiento y respaldo de la información contenidos en los Bloques 4, 7 y 8 de las Especificaciones Técnicas, con el propósito de garantizar consistencia en las disposiciones aplicables a la ubicación de los datos y a los países donde estos podrán almacenarse, procesarse o respaldarse. / No se acoge el extremo de la objeción que pretende que la jurisdicción declarada por el oferente sea considerada automáticamente admisible por el solo cumplimiento de las condiciones propuestas en su recurso o que limite la facultad de la Administración para determinar las condiciones de aceptabilidad de las jurisdicciones donde se almacene, procese o respalde la información institucional. / La Administración considera indispensable mantener la capacidad de valorar las jurisdicciones propuestas desde la perspectiva de protección de la información, cumplimiento normativo, continuidad operativa, recuperación ante desastres, seguridad y demás elementos asociados a la gestión de riesgos institucionales. / Asimismo, la Administración mantiene la necesidad de conocer y controlar las ubicaciones geográficas utilizadas para el almacenamiento, procesamiento y respaldo de la información institucional, así como de verificar que dichas ubicaciones ofrezcan condiciones adecuadas de seguridad, continuidad operativa, protección de la información y cumplimiento normativo acordes con los requerimientos de la presente contratación. / En consecuencia, la atención de la presente objeción no implica la eliminación de los controles asociados a la ubicación de los datos, sino la aclaración de los criterios aplicables y la armonización de las disposiciones contenidas en el pliego de condiciones."*

Criterio de la División: el artículo 88 del Reglamento a la Ley General de Contratación Pública establece que el pliego de condiciones deberá constituir un cuerpo de especificaciones técnicas, claras y objetivas, sin embargo en este caso la frase "equivalente" resulta imprecisa y puede generar distintas interpretaciones al momento del estudio de las ofertas. Por lo tanto, lleva razón la recurrente al solicitar que se definan criterios objetivos para determinar qué se entiende por jurisdicción equivalente. Ahora bien, se observa que la Administración aceptó modificar el pliego de condiciones para incorporar una definición más precisa del concepto de "jurisdicción equivalente", pero no aceptó la redacción propuesta por el recurrente. En consecuencia, se declara **parcialmente con lugar** el recurso en este aspecto.

6) Centro de datos.

En el documento denominado "Especificaciones Técnicas" del pliego de condiciones se indica lo siguiente: *"**Bloque 5: Solución en la Nube** / […] **Mitigación de Amenazas y Cumplimiento Nube** / […] El centro de datos y específicamente los gabinetes en donde se almacena o procesa la información del Conglomerado Financiero BCR, debe contar con un sistema de video vigilancia que almacene al menos los últimos (12) doce meses de grabación."* (el destacado es del original).

La **empresa objetante** indica que el requisito no puede cumplirse ni verificarse en una solución SaaS alojada en infraestructura de nube de hiper escala. Explica que conforme al modelo de responsabilidad compartida, la seguridad física de los centros de datos, incluidos el control de acceso y la video vigilancia, la opera el proveedor de infraestructura para todos sus clientes, bajo un programa único de controles. Ni el oferente ni el Banco disponen de gabinetes dedicados ni administran las cámaras o el periodo de conservación de las grabaciones, de modo que ninguno puede comprometer, por sí mismo, un plazo de doce meses. Considera que el requisito es incompatible con el objeto contractual y con el propio pliego. Solicita lo siguiente:

A) Como pretensión principal, solicita que se sustituya el requisito de videovigilancia con doce meses de grabación por el siguiente texto: *"El centro de datos en que se aloja la solución deberá contar con un sistema de videovigilancia permanente, y con conservación de las grabaciones conforme a la política documentada del proveedor de infraestructura. Este requisito se acreditará con las certificaciones e informes de auditoría independientes del proveedor (ISO/IEC 27001 y SOC 2 Tipo II o SOC 3) cuyo alcance comprenda los controles de seguridad física del centro de datos, y con la declaración jurada prevista en el numeral 17.10.2.4. Los informes de carácter confidencial se pondrán a disposición del Banco bajo acuerdo de confidencialidad."*

B) Como pretensión subsidiaria, solicita que se admita expresamente como medio suficiente la acreditación de la seguridad física mediante las certificaciones e informes del proveedor de infraestructura, sin exigir un plazo específico de conservación de las grabaciones.
C) Como pretensión subsidiaria de la anterior, solicita que si el Banco mantiene el plazo de doce meses, este no sea un requisito de admisibilidad sino una obligación verificable en la ejecución contractual, a cargo del proveedor de infraestructura.
Al contestar la audiencia especial, la **Administración** aceptó modificar el pliego de condiciones y en este sentido manifiesta lo siguiente: *"Se acoge el extremo de la objeción relacionado con la necesidad de adecuar el requisito de conservación de grabaciones de videovigilancia a las condiciones propias de los servicios prestados sobre infraestructura de computación en la nube. / La Administración reconoce que, tratándose de soluciones bajo modalidad SaaS soportadas sobre infraestructura de terceros, los controles asociados a videovigilancia, seguridad física, control de acceso y conservación de grabaciones son administrados directamente por el proveedor de infraestructura utilizado para la prestación del servicio, de conformidad con sus políticas y controles de seguridad. / En consecuencia, se procederá a modificar el requisito relacionado con la conservación de las grabaciones de videovigilancia, estableciendo que dicho período corresponderá a las políticas y controles de seguridad definidos por el proveedor de infraestructura utilizado para la prestación del servicio. / Asimismo, se aceptará la acreditación de estos controles mediante certificaciones e informes de auditoría que permitan verificar la existencia de controles adecuados de seguridad física sobre la infraestructura utilizada para la prestación del servicio, tales como ISO/IEC 27001, SOC 2 Tipo II, informes equivalentes emitidos bajo estándares internacionalmente reconocidos que proporcionen un nivel de aseguramiento y alcance equivalente, informes de auditoría independientes o documentación oficial emitida por el proveedor de infraestructura que permita verificar la vigencia, alcance y aplicación de dichos controles. Los documentos aportados deberán permitir la verificación objetiva de los controles de seguridad física implementados sobre la infraestructura que soportará la solución ofertada. / No se acoge el extremo de la objeción que pretende que la acreditación mediante certificaciones o informes del proveedor de infraestructura sustituya por sí sola la verificación de los controles de seguridad física requeridos por la Administración para la protección de la información institucional. / La Administración mantiene la necesidad de verificar que la infraestructura propuesta disponga de controles adecuados de seguridad física que permitan proteger la información institucional y soportar la atención, investigación y análisis de eventuales incidentes de seguridad que involucren los componentes utilizados para la prestación del servicio. / Asimismo, la Administración considera indispensable mantener mecanismos que permitan evidenciar la existencia de controles de acceso físico, monitoreo y protección de la infraestructura empleada para el alojamiento, procesamiento o respaldo de la información asociada a la presente contratación. / En consecuencia, la atención de la presente objeción no implica la eliminación de los controles de seguridad física requeridos por la Administración, sino la adecuación del requisito de conservación de grabaciones a las condiciones propias de la infraestructura que soportará la solución ofertada, manteniendo los niveles de seguridad necesarios para la protección de la información institucional."*
Criterio de la División: se observa que la Administración aceptó modificar el requisito relacionado con la conservación de las grabaciones de videovigilancia, estableciendo que dicho período corresponderá a las políticas y controles de seguridad definidos por el proveedor de infraestructura utilizado para la prestación del servicio, y también aceptó la acreditación de estos controles mediante certificaciones e informes de auditoría que permitan verificar la existencia de controles adecuados de seguridad física sobre la infraestructura utilizada para la prestación del servicio, sin embargo la Administración no aceptó la redacción propuesta por la recurrente. Por lo tanto, se declara **parcialmente con lugar** el recurso en este aspecto.

Recurso 8002026000002508 - CYBERFUEL SOCIEDAD ANONIMA

I. FONDO

1) Cláusula 17.10. Certificaciones Obligatorias.

En el documento denominado "Condiciones Generales" del pliego de condiciones, se indica lo siguiente: *"**17.10 Certificaciones Obligatorias** / 17.10.1 El oferente deberá acreditar contar con las siguientes certificaciones vigentes emitidas por organismos acreditados: / 17.10.1.1 ISO 22301: Sistema de Gestión de Continuidad del Negocio. / 17.10.1.2 ISO 27017: Controles de Seguridad para Servicios de Computación en la Nube. / **17.10.2 Verificación:** / 17.10.2.1 Copia de las certificaciones vigentes emitidas por organismos acreditados. / 17.10.2.2 Documentación que permita verificar su vigencia y autenticidad. / 17.10.2.3 La no presentación de cualquiera de estas certificaciones o la presentación de certificaciones vencidas dará lugar a la declaratoria de inadmisibilidad de la oferta."* (el destacado es del original).

La **empresa objetante** menciona que el pliego contiene al menos cuatro regulaciones distintas e incompatibles sobre la misma materia: en la cláusula 17.10 exige al oferente solo dos certificaciones: ISO 22301 e ISO 27017; en el bloque 6 exige diez certificaciones, sin indicar si deben pertenecer al oferente, al fabricante del software o al proveedor de infraestructura, en el bloque 5 exige una lista distinta de ocho, que omite SSAE-16 e ISO 22301, en el Bloque 4, "Seguridad de Datos y Cumplimiento Local", pide demostrar cumplimiento con "ISO 27001, NIST, PCI-DSS, GDPR o Ley 8968 de Costa Rica", en forma alternativa. Considera que el pliego de condiciones también es inconsistente en su trato a las equivalencias. Para el centro de datos acepta "Tier II o superior o alguna certificación similar" (Bloque 5), pero para las certificaciones de seguridad no admite equivalente alguno. Además, la numeración del anexo repite los Bloques 7 y 8, lo que dificulta identificar con certeza qué requisito se evalúa. Solicita unificar en una sola cláusula el régimen de certificaciones, indicar expresamente si cada certificación es acumulativa o alternativa y precisar a quién se exige (oferente, fabricante o proveedor de infraestructura).

Al contestar la audiencia especial, la **Administración** aceptó modificar el pliego de condiciones y en este sentido manifiesta lo siguiente: *"Se acoge el extremo relacionado con la necesidad de clarificar, armonizar y ordenar los requisitos asociados a certificaciones, informes de aseguramiento y mecanismos de cumplimiento contenidos en el pliego de condiciones y en las Especificaciones Técnicas. / La Administración reconoce que actualmente existen referencias a certificaciones e instrumentos de acreditación distribuidas en distintos apartados del pliego, lo que puede generar interpretaciones diferentes respecto de su alcance, forma de acreditación, naturaleza de los requisitos y sujeto legitimado para aportar las evidencias correspondientes. / Asimismo, se ha determinado que determinados mecanismos de aseguramiento y certificaciones requeridos para la contratación pueden corresponder al oferente, al fabricante de la solución o al proveedor de infraestructura que soporte la prestación del servicio, según la naturaleza del control acreditado y el componente tecnológico sobre el cual recaiga la certificación o informe respectivo. / Por lo anterior, la Administración procederá a: / 1. Consolidar y armonizar los requisitos asociados a certificaciones, informes de aseguramiento y mecanismos de cumplimiento dentro de un único apartado del pliego de condiciones. / 2. Precisar expresamente para cada certificación, informe o mecanismo de aseguramiento requerido su carácter de admisibilidad o evaluación, la forma de acreditación aceptada, las equivalencias expresamente definidas por la Administración para cada requisito y el sujeto facultado para aportar la evidencia correspondiente, sea el oferente, el fabricante de la solución o el proveedor de infraestructura que soporte el servicio. / 3. Actualizar las referencias normativas y mecanismos de aseguramiento correspondientes, incluyendo la sustitución de la referencia a SSAE-16 por los requisitos de SOC 1 Tipo II y SOC 2 Tipo II vigentes, emitidos por un auditor independiente bajo los estándares de atestiguamiento aplicables de AICPA, o informes equivalentes emitidos bajo estándares internacionalmente reconocidos que proporcionen un nivel de aseguramiento y alcance equivalente. / 4. Eliminar o ajustar aquellos requisitos que, conforme al análisis técnico realizado por la Administración, resulten redundantes, desactualizados o susceptibles de generar interpretaciones restrictivas respecto del objeto contractual. / 5. Corregir los errores de numeración identificados en las Especificaciones Técnicas, incluyendo la numeración repetida de los Bloques 7 y 8. / No se acoge el extremo de la objeción en cuanto pretende que la clarificación del régimen de certificaciones implique la eliminación de los mecanismos de acreditación, validación de alcance y verificación de las certificaciones, informes y demás evidencias requeridas por la Administración. / La Administración considera indispensable mantener mecanismos objetivos que permitan verificar que las certificaciones, informes y demás evidencias aportadas cubran efectivamente los componentes, servicios e infraestructura utilizados para la prestación de la solución ofertada, así como validar el cumplimiento de los controles asociados a seguridad, continuidad operativa, disponibilidad, protección de la información y gestión de riesgos requeridos para la presente contratación. / En consecuencia, aunque se procederá a reorganizar, actualizar y aclarar el régimen de certificaciones y mecanismos de cumplimiento, la Administración mantendrá la facultad de verificar la vigencia, alcance, aplicabilidad y suficiencia de las certificaciones, informes y demás evidencias aportadas por los oferentes."*

Criterio de la División: se observa que la Administración aceptó consolidar y armonizar los requisitos asociados a certificaciones, informes de aseguramiento y mecanismos de cumplimiento dentro de un único apartado del pliego de condiciones; y también aceptó precisar expresamente para cada certificación, informe o mecanismo de aseguramiento requerido su carácter de admisibilidad o evaluación, la forma de acreditación aceptada, las equivalencias expresamente definidas por la Administración para cada requisito y el sujeto facultado para aportar la evidencia correspondiente, sea el oferente, el fabricante de la solución o el proveedor de infraestructura que soporte el servicio. Por lo tanto, se declara **parcialmente con lugar** el recurso en este aspecto.

2) Norma SSAE-16.

En el documento denominado "Especificaciones Técnicas" del pliego de condiciones se indica lo siguiente: *"**Bloque 6: Apego a las Normas de Seguridad del Conglomerado Financiero del Banco de Costa Rica** / […] **Certificaciones de Seguridad Requeridas** / Tenencia de certificaciones internacionales vigentes: / ISO/IEC 27001. / ISO/IEC 27018. / SSAE-16 / SOC 1 / SOC 2 Tipo II. / SOC 3 / GDPR / PCI-DSS. / ISO 22301."* (el destacado es del original).

La **empresa objetante** explica que la norma SSAE-16 era la norma del AICPA de Estados Unidos bajo la cual se emitían los informes SOC 1, pero fue sustituida por SSAE-18 para los informes fechados a partir del 1 de mayo de 2017. Por tanto, ningún auditor puede emitir hoy un informe SSAE-16, y ningún oferente puede presentar uno "vigente". Además, SSAE-16 no es una certificación sino la norma que regula el informe SOC 1, que el mismo Bloque 6 exige por separado. El requisito es, a la vez, imposible y redundante. Solicita que se elimine la norma SSAE-16 del pliego.

Al contestar la audiencia especial, la **Administración** aceptó modificar el pliego de condiciones y en este sentido manifiesta lo siguiente: *"La Administración reconoce que la referencia a SSAE-16 corresponde a un estándar que fue sustituido por normas posteriores actualmente vigentes y utilizadas para la emisión de informes de aseguramiento independientes aplicables a proveedores de servicios tecnológicos y servicios de computación en la nube. / Asimismo, se considera procedente ajustar la redacción del requisito con el fin de diferenciar claramente entre los estándares de atestiguamiento utilizados para la emisión de los informes y los propios informes de aseguramiento requeridos como evidencia de cumplimiento. / En virtud de lo anterior, y con el fin de mantener la vigencia técnica, actualidad y razonabilidad de los requisitos establecidos en el procedimiento, la Administración procederá a eliminar la referencia a SSAE-16 contenida en las Especificaciones Técnicas y establecer que el oferente deberá presentar informes SOC 1 Tipo II y SOC 2 Tipo II vigentes, emitidos por un auditor independiente bajo los estándares de atestiguamiento aplicables de AICPA, o informes equivalentes emitidos bajo estándares internacionalmente reconocidos, siempre que proporcionen un nivel de aseguramiento y alcance equivalente respecto de los controles asociados al servicio ofertado. / Asimismo, la Administración considera procedente revisar la consistencia de los mecanismos de aseguramiento contemplados en el pliego, con el propósito de garantizar una definición clara de las evidencias requeridas, sus alcances, vigencias y mecanismos de acreditación aceptados. / La presente modificación tiene como finalidad eliminar una referencia normativa desactualizada y precisar los mecanismos de acreditación aceptables, manteniendo el nivel de aseguramiento requerido por la Administración para verificar la existencia y efectividad de controles asociados a seguridad, disponibilidad, continuidad operativa, integridad del procesamiento y protección de la información. / En consecuencia, se elimina la referencia a SSAE-16 y se actualizan los mecanismos de aseguramiento exigidos mediante informes vigentes y reconocidos por la industria que permitan demostrar controles equivalentes a los originalmente requeridos."*

Criterio de la División: se observa que la Administración aceptó eliminar la referencia a SSAE-16, tal y como lo solicitó la recurrente. Por lo tanto, se declara **con lugar** el recurso en este aspecto.

3) Certificación GDPR.

En el documento denominado "Especificaciones Técnicas" del pliego de condiciones se indica lo siguiente: *"**Bloque 5: Solución en la Nube** / […] **Mitigación de Amenazas y Cumplimiento Nube** / Realización de pruebas de penetración periódicas con entrega de resultados al BCR si se solicitan. / Controles antimalware y detección de amenazas avanzadas. / Cumplimiento verificado con estándares internacionales: ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3, GDPR y PCI-DSS."* (el destacado es del original).

*"**Bloque 6: Apego a las Normas de Seguridad del Conglomerado Financiero del Banco de Costa Rica** / […] **Certificaciones de Seguridad Requeridas** / Tenencia de certificaciones internacionales vigentes: / ISO/IEC 27001. / ISO/IEC 27017. / ISO/IEC 27018. / SSAE-16 / SOC 1 / SOC 2 Tipo II. / SOC 3 / GDPR / PCI-DSS. / ISO 22301."* (el destacado es del original).

La **empresa objetante** explica que el Reglamento (UE) 2016/679 (GDPR) es una norma jurídica de la Unión Europea, no una certificación. Según su artículo 3, aplica al tratamiento de datos de personas que se encuentran en la Unión Europea o a responsables establecidos allí. Los comprobantes electrónicos del Conglomerado BCR se rigen por la normativa tributaria costarricense, y los datos personales que contienen están sujetos a la Ley N.° 8968 y a la PRODHAB. El artículo 42 del GDPR prevé mecanismos voluntarios de certificación, pero son escasos y no existe una "certificación GDPR" general que un proveedor costarricense pueda obtener para este objeto. El propio pliego reconoce la norma correcta: la cláusula 23.4 de las Condiciones Generales exige cumplir la Ley 8968, y el Bloque 4 admite la Ley 8968 como alternativa al GDPR. Por ello, considera que exigir el GDPR como certificación carece de relación con el objeto y de sustento técnico. Solicita que se elimine el GDPR como certificación y sustituirlo por una declaración de cumplimiento de la Ley N.° 8968 y su reglamento, con los compromisos contractuales que la Administración estime necesarios.

Al contestar la audiencia especial, la **Administración** aceptó modificar el pliego de condiciones y en este sentido manifiesta lo siguiente: *"La Administración reconoce que el Reglamento General de Protección de Datos de la Unión Europea (GDPR) constituye un marco normativo de protección de datos personales y no una certificación técnica equiparable a las certificaciones internacionales ni a los informes de aseguramiento contemplados en el pliego de condiciones. / Asimismo, se considera atendible el señalamiento realizado por el objetante respecto a la necesidad de eliminar cualquier ambigüedad sobre la naturaleza del requisito y los mecanismos mediante los cuales deberá acreditarse el cumplimiento de las obligaciones asociadas a la protección de datos personales. / En consecuencia, la Administración procederá a eliminar la referencia a GDPR como certificación o requisito de acreditación dentro de los Bloques 5 y 6 de las Especificaciones Técnicas. / No obstante, la Administración mantiene la necesidad de verificar que la solución propuesta incorpore controles adecuados para la protección, confidencialidad, integridad, disponibilidad y tratamiento de la información administrada por la solución, así como mecanismos acordes con las mejores prácticas aplicables en materia de protección de datos personales. / Asimismo, los oferentes deberán garantizar el cumplimiento de la Ley N.° 8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, su Reglamento y demás normativa aplicable en materia de protección de datos personales. / La Administración incorporará una redacción distinta a la propuesta por el recurrente, por considerarla técnicamente más adecuada para satisfacer la necesidad institucional y mantener los controles de protección de datos requeridos para la presente contratación. / La atención de la presente objeción no implica la eliminación de los controles asociados a la protección de datos personales, sino la eliminación de la referencia al GDPR como certificación y la adecuación del requisito a la naturaleza regulatoria de dicho marco normativo."*

Criterio de la División: se observa que la Administración aceptó eliminar la referencia a GDPR como requisito de acreditación dentro de los bloques 5 y 6, tal y como lo solicitó la recurrente. También indicó que los oferentes deberán garantizar el cumplimiento de la Ley N.° 8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, su Reglamento y demás normativa aplicable en materia de protección de datos personales. Por lo tanto, se declara **con lugar** el recurso en este aspecto.

4) Certificación PCI-DSS.

En el documento denominado "Especificaciones Técnicas" del pliego de condiciones se indica lo siguiente: *"**Bloque 5: Solución en la Nube** / […] **Mitigación de Amenazas y Cumplimiento Nube** / Realización de pruebas de penetración periódicas con entrega de resultados al BCR si se solicitan. / Controles antimalware y detección de amenazas avanzadas. / Cumplimiento verificado con estándares internacionales: ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3, GDPR y PCI-DSS."* (el destacado es del original).

*"**Bloque 6: Apego a las Normas de Seguridad del Conglomerado Financiero del Banco de Costa Rica** / […] **Certificaciones de Seguridad Requeridas** / Tenencia de certificaciones internacionales vigentes: / ISO/IEC 27001. / ISO/IEC 27017. / ISO/IEC 27018. / SSAE-16 / SOC 1 / SOC 2 Tipo II. / SOC 3 / GDPR / PCI-DSS. / ISO 22301."* (el destacado es del original).

La **empresa objetante** explica que PCI-DSS (Payment Card Industry Data Security Standard) aplica a las entidades que almacenan, procesan o transmiten datos de titulares de tarjetas de pago. El objeto licitado es la emisión, recepción, aceptación y almacenamiento de comprobantes electrónicos (Condiciones Generales 1.2.1 y 2.1.1). Un comprobante electrónico conforme a la normativa de Hacienda no contiene números de tarjeta ni datos de autenticación de tarjetas. Indica que el propio pliego lo reconoce implícitamente, ya que en el Bloque 8, "Seguridad y Privacidad", solo pide "consideración y alineación con la regulación PCI-DSS", y en el Bloque 4 lo incluye como una alternativa entre otras. Considera que exigirlo como una certificación de admisibilidad es desproporcionado. El expediente no muestra que la solución vaya a tratar datos de tarjetas. Solicita que se elimine PCI-DSS como certificación de admisibilidad. Subsidiariamente, solicita que la Administración acredite en el expediente qué flujo de datos de tarjetas procesaría la solución que justifique su exigencia.

Al contestar la audiencia especial, la **Administración** aceptó modificar el pliego de condiciones y en este sentido manifiesta lo siguiente: *"Se acoge el extremo de la objeción relacionado con la necesidad de delimitar la aplicabilidad del estándar PCI-DSS, por cuanto la Administración reconoce que dicho estándar resulta pertinente únicamente cuando la solución propuesta almacene, procese o transmita datos de tarjetas de pago. En consecuencia, se considera procedente ajustar la redacción del requisito para precisar los casos en los cuales resulta exigible. / Por lo anterior, la Administración aclara que el requisito relacionado con PCI-DSS será exigible únicamente cuando la solución propuesta, debido a su arquitectura, funcionalidades o componentes asociados, almacene, procese o transmita datos de tarjetas de pago. / Cuando la solución ofertada no contemple el almacenamiento, procesamiento o transmisión de información de tarjetas de pago, el requisito podrá considerarse como "No aplica", debiendo el oferente justificar técnicamente dicha condición dentro de su propuesta. / No se acoge el extremo de la objeción que pretende eliminar completamente el requisito asociado a PCI-DSS del pliego de condiciones, por cuanto la Administración considera necesario mantener mecanismos que permitan verificar el cumplimiento de controles de seguridad cuando la solución propuesta almacene, procese o transmita información relacionada con tarjetas de pago. / La Administración mantiene la necesidad de verificar el cumplimiento de los controles de seguridad y protección de información aplicables cuando la solución o alguno de sus componentes procese información relacionada con tarjetas de pago, por tratarse de un estándar ampliamente reconocido para la protección de este tipo de información sensible. / En consecuencia, la atención de la presente objeción no implica la eliminación del requisito, sino la definición objetiva de los escenarios en los cuales resulta aplicable, manteniendo los controles de seguridad que la Administración considera necesarios para la protección de la información."*

Criterio de la División: se observa que la Administración aceptó modificar la redacción de la cláusula para precisar los casos en los cuales resulta exigible la certificación PCI-DSS, de forma tal que la certificación PCI-DSS será exigible únicamente cuando la solución propuesta, debido a su arquitectura, funcionalidades o componentes asociados, almacene, procese o transmita datos de tarjetas de pago, mientras que si la solución ofertada no contempla el almacenamiento, procesamiento o transmisión de información de tarjetas de pago, el requisito podrá considerarse como "No aplica", debiendo el oferente justificar técnicamente dicha condición dentro de su propuesta. Como puede observarse, la

Administración deja a cada oferente la decisión de incluir o no en la solución propuesta, el almacenamiento, procesamiento o transmisión de información de tarjetas de pago, y solamente en caso de que la solución propuesta por el oferente incluya dichas funciones, deberá cumplir con la certificación PCI-DSS.
Así las cosas, la modificación propuesta por la Administración no coincide con lo solicitado por la recurrente. Por lo tanto, se declara **parcialmente con lugar** el recurso en este aspecto. No obstante lo anterior, este órgano contralor considera que en la respuesta dada por la Administración no queda claro cómo analizará la Administración la justificación que brinde el oferente, si solamente verificará que en la oferta esté la respectiva justificación, o la Administración realizará algún análisis o valoración de la justificación dada por el oferente, por lo que dicho aspecto deberá definirse expresamente en el pliego de condiciones.

5) Informes SOC 1, SOC 2, SOC 3.
En el documento denominado "Especificaciones Técnicas" del pliego de condiciones se indica lo siguiente: *"**Bloque 5: Solución en la Nube** / […] **Mitigación de Amenazas y Cumplimiento Nube** / Realización de pruebas de penetración periódicas con entrega de resultados al BCR si se solicitan. / Controles antimalware y detección de amenazas avanzadas. / Cumplimiento verificado con estándares internacionales: ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3, GDPR y PCI-DSS."* (el destacado es del original).
*"**Bloque 6: Apego a las Normas de Seguridad del Conglomerado Financiero del Banco de Costa Rica** / […] **Certificaciones de Seguridad Requeridas** / Tenencia de certificaciones internacionales vigentes: / ISO/IEC 27001. / ISO/IEC 27017. / ISO/IEC 27018. / SSAE-16 / SOC 1 / SOC 2 Tipo II. / SOC 3 / GDPR / PCI-DSS. / ISO 22301."* (el destacado es del original).
La **empresa objetante** explica que los informes SOC 1, SOC 2 y SOC 3 no son certificaciones, sino que son informes de atestación emitidos por contadores públicos de Estados Unidos bajo normas del AICPA, la SOC 1 evalúa controles relevantes para la información financiera del cliente, la SOC 2 Tipo II evalúa la eficacia operativa de controles de seguridad, disponibilidad, integridad, confidencialidad y privacidad; la SOC 3 es la versión resumida y de uso general del SOC 2, sin sus detalles. Solicita que se elimine la SOC 3 por redundante; admitir ISO/IEC 27001 vigente como equivalente de SOC 2 Tipo II; y admitir SOC 1 o ISO/IEC 27001 de forma alternativa, o trasladar los informes SOC a factor de evaluación.
Al contestar la audiencia especial, la **Administración** aceptó modificar el pliego de condiciones y en este sentido manifiesta lo siguiente: *"Se acoge el extremo de la objeción relacionado con la necesidad de revisar la estructura de los mecanismos de aseguramiento requeridos en el pliego, con el fin de evitar duplicidades y garantizar que las evidencias solicitadas resulten proporcionales y consistentes con los controles que la Administración busca verificar. / En consecuencia, la Administración procederá a ajustar el contenido de las Especificaciones Técnicas para eliminar el requisito de SOC 3 como requisito acumulativo de cumplimiento cuando ya se exija SOC 1 Tipo II, SOC 2 Tipo II u otros mecanismos de aseguramiento que permitan verificar los mismos controles requeridos para la prestación del servicio. / Asimismo, se procederá a revisar los mecanismos de aseguramiento requeridos con el fin de garantizar una definición clara de las evidencias exigidas, sus alcances, vigencias y mecanismos de acreditación aceptados, evitando solicitar mecanismos redundantes para acreditar un mismo objetivo de control. / No se acoge el extremo de la objeción que pretende considerar ISO/IEC 27001 como equivalente automático o sustituto de los informes SOC 1 Tipo II o SOC 2 Tipo II, ni la pretensión de admitir dichos mecanismos de forma alternativa cuando tengan finalidades, alcances y objetivos de control distintos. Asimismo, no se acoge la pretensión de trasladar los informes SOC a factores de evaluación, por cuanto la Administración considera que dichos mecanismos de aseguramiento constituyen requisitos mínimos necesarios para verificar la capacidad de la solución propuesta respecto de los controles requeridos para la prestación del servicio. / La Administración considera que la certificación ISO/IEC 27001 y los informes SOC constituyen mecanismos de aseguramiento de naturaleza distinta y complementaria. Mientras la certificación ISO/IEC 27001 acredita la implementación y operación de un sistema de gestión de seguridad de la información, los informes SOC permiten obtener una evaluación independiente sobre la existencia y efectividad de controles específicos asociados a la prestación de los servicios, incluyendo aspectos relacionados con seguridad, disponibilidad, integridad del procesamiento, confidencialidad y protección de la información. / En consecuencia, la sola presentación de una certificación ISO/IEC 27001 no resulta suficiente para acreditar aquellos controles cuya verificación requiere los mecanismos de aseguramiento establecidos mediante los informes SOC 1 Tipo II, SOC 2 Tipo II o informes equivalentes emitidos bajo estándares internacionalmente reconocidos que proporcionen un nivel de aseguramiento y alcance equivalente, según corresponda. / No obstante, la Administración podrá considerar certificaciones, informes y demás evidencias complementarias que permitan fortalecer la acreditación de los controles requeridos, siempre que su alcance cubra efectivamente los servicios utilizados para la prestación de la solución ofertada y que dicha documentación permita verificar objetivamente los controles cuya validación se exige en el procedimiento. / La atención de la presente objeción no implica la eliminación de los mecanismos de aseguramiento requeridos por la Administración, sino la eliminación de requisitos redundantes y la clarificación de los mecanismos de acreditación aplicables, manteniendo aquellos controles que se consideran necesarios para verificar la seguridad, disponibilidad, continuidad operativa, integridad del procesamiento y protección de la información asociados a los servicios objeto de contratación."*
Criterio de la División:
a) se observa que la Administración aceptó eliminar el requisito de SOC 3 como requisito acumulativo de cumplimiento cuando ya se exija SOC 1 Tipo II, SOC 2 Tipo II u otros mecanismos de aseguramiento que permitan verificar los mismos controles requeridos para la prestación del servicio, lo cual resulta coincidente con parte de la petitoria de la recurrente. Por lo tanto, se declara **parcialmente con lugar** el recurso en este aspecto.
b) con respecto a la solicitud de la recurrente para que se admita la certificación ISO/IEC 27001 vigente como equivalente de SOC 1 y SOC 2, es criterio de este órgano contralor que dicha propuesta resulta improcedente, ya que al resolver el recurso interpuesto por la empresa Tecnoware Soluciones Informáticas se explicó que este órgano contralor ha sostenido en forma reiterada que las normas de aseguramiento de la calidad establecidas por la Organización Internacional para la Normalización ISO son acreditaciones a las que se someten las empresas de manera voluntaria, por lo que no es aceptable que se soliciten como un requisito de admisibilidad. Por lo tanto, se declara **sin lugar** el recurso en este aspecto.
c) con respecto a la solicitud de la recurrente para que se trasladen los informes SOC como factores de evaluación, se observa que la Administración no acoge la pretensión ya que considera que dichos mecanismos de aseguramiento constituyen requisitos mínimos necesarios para verificar la capacidad de la solución propuesta respecto de los controles requeridos para la prestación del servicio. Sin embargo, el artículo 90 del Reglamento a la Ley General de Contratación Pública establece que "*El pliego de condiciones no podrá imponer restricciones, ni exigir el cumplimiento de requisitos que no sean indispensables o resulten inconvenientes al interés público, si con ello limita las posibilidades de concurrencia a eventuales participantes."*, y en el caso bajo análisis la recurrente menciona que los informes SOC son informes emitidos por contadores públicos de Estados Unidos bajo normas del AICPA y que favorece a proveedores con operación en Estados Unidos sin una justificación vinculada al objeto, aspecto que no fue rebatido ni desvirtuado por la Administración. La Administración tampoco explicó ni acreditó si la obtención de esos informes por parte de las empresas es un requisito de cumplimiento obligatorio o es voluntario, lo cual resulta importante a fin de determinar si los informes SOC se pueden pedir a los oferentes como un requisito de admisibilidad o no. Por lo tanto, se declara **parcialmente con lugar** el recurso en este aspecto para que la Administración emita un criterio técnico mediante el cual explique y justifique si hay una normativa que obligue a las empresas a solicitar y obtener los informes SOC como un requisito obligatorio, o si por el contrario la obtención de los informes SOC es voluntario. Dicho criterio deberá ser incorporado al expediente del concurso, concretamente en el apartado 2 denominado "Información de Pliego de condiciones", ello de conformidad con lo dispuesto en el artículo 29 del Reglamento a la Ley General de Contratación Pública.

6) Certificaciones de seguridad requeridas en el bloque 6.

En el documento denominado “Especificaciones Técnicas” del pliego de condiciones se indica lo siguiente: *“**Bloque 6: Apego a las Normas de Seguridad del Conglomerado Financiero del Banco de Costa Rica** / […] **Certificaciones de Seguridad Requeridas** / Tenencia de certificaciones internacionales vigentes: / ISO/IEC 27001. / ISO/IEC 27017. / ISO/IEC 27018. / SSAE-16 / SOC 1 / SOC 2 Tipo II. / SOC 3 / GDPR / PCI-DSS. / ISO 22301.”* (el destacado es del original).

La **empresa objetante** explica que la lista acumulativa del Bloque 6 coincide con el portafolio de certificaciones de los grandes proveedores globales de nube pública. Sin embargo, el pliego no aclara si basta que la infraestructura las tenga. Considera que esto genera un dilema que la Administración no resuelve, ya que si el Banco acepta las certificaciones de la infraestructura de un tercero, entonces lo relevante es la seguridad de la infraestructura; y en ese caso, debe aceptar también una infraestructura nacional que acredite un nivel equivalente, como un centro de datos ANSI/TIA-942 Rated-3 con ISO/IEC 27001 vigente. Pero si el Banco exige que el oferente mismo tenga todas las certificaciones, prácticamente ningún proveedor nacional de facturación electrónica puede participar. El concurso quedaría reservado a muy pocas empresas, sin una justificación proporcional al objeto, que es un servicio de comprobantes electrónicos de alrededor de 300.000 documentos anuales. Solicita que se precise a qué capa aplica cada certificación; admitir que las certificaciones de infraestructura se acrediten por el proveedor del centro de datos o nube que se utilice; y admitir como equivalentes, para la infraestructura, un centro de datos certificado ANSI/TIA-942 o Uptime Tier en nivel III o superior, con ISO/IEC 27001 vigente.

Al contestar la audiencia especial, la **Administración** aceptó modificar el pliego de condiciones y en este sentido manifiesta lo siguiente: *“Se acoge el extremo de la objeción relacionado con la necesidad de reconocer que, tratándose de soluciones bajo modalidad SaaS soportadas sobre infraestructura de computación en la nube, determinados controles asociados a la infraestructura pueden ser implementados y administrados por el proveedor de infraestructura utilizado para la prestación del servicio. / Asimismo, se acoge el extremo relacionado con la posibilidad de acreditar los requisitos asociados a infraestructura mediante mecanismos que permitan demostrar niveles adecuados de seguridad, disponibilidad, continuidad operativa y resiliencia tecnológica. / En consecuencia, para efectos de la presente contratación, se considerarán aceptables infraestructuras que cuenten con certificaciones vigentes tales como ANSI/TIA-942 Rated-3, Uptime Tier III o superior e ISO/IEC 27001, siempre que el alcance de dichas certificaciones cubra efectivamente la infraestructura que soportará los servicios ofrecidos al Conglomerado Financiero BCR. / Adicionalmente, se aceptará que las certificaciones e informes asociados a infraestructura sean acreditados por el proveedor de infraestructura utilizado para la prestación del servicio, siempre que permitan verificar los controles requeridos por la Administración y su alcance cubra efectivamente los componentes y servicios utilizados por la solución ofertada. / Para tales efectos podrán presentarse, entre otros: / **a) Certificaciones vigentes emitidas por organismos acreditados, tales como ANSI/TIA-942 Rated-3, Uptime Tier III o superior e ISO/IEC 27001. / b) Informes de auditoría y aseguramiento independientes aplicables a la infraestructura utilizada para la prestación del servicio. / c) Documentación emitida por el proveedor de infraestructura que permita verificar la vigencia, alcance y aplicabilidad de las certificaciones o informes presentados. / La acreditación podrá realizarse mediante informes SOC vigentes, certificaciones ISO aplicables, documentación emitida por organismos certificadores o informes de auditoría independientes cuya cobertura permita verificar los controles requeridos. / No se acoge el extremo de la objeción que pretende que la sola acreditación de certificaciones de infraestructura nacional equivalga al cumplimiento integral de los requisitos de seguridad, disponibilidad, continuidad operativa y protección de la información exigidos para la presente contratación. / La Administración considera indispensable mantener la totalidad de los controles definidos en el procedimiento, independientemente de que la infraestructura utilizada corresponda a nube pública, nube privada o infraestructura nacional certificada, por cuanto dichos controles resultan necesarios para garantizar la adecuada protección de la información institucional, la continuidad operativa de los servicios y la gestión de los riesgos asociados a la presente contratación. / En consecuencia, la atención de la presente objeción no implica la eliminación de los requisitos de infraestructura definidos por la Administración, sino la admisión de alternativas técnicamente equivalentes para acreditar su cumplimiento, manteniendo los niveles de control y seguridad requeridos para la prestación del servicio.”***

Criterio de la División: se observa que la Administración aceptó modificar el pliego de condiciones para aceptar que las certificaciones e informes asociados a infraestructura sean acreditados por el proveedor de infraestructura utilizado para la prestación del servicio, siempre que permitan verificar los controles requeridos por la Administración y su alcance cubra efectivamente los componentes y servicios utilizados por la solución ofertada. La Administración también considerará aceptables infraestructuras que cuenten con certificaciones vigentes tales como ANSI/TIA-942 Rated-3, Uptime Tier III o superior e ISO/IEC 27001, siempre que el alcance de dichas certificaciones cubra efectivamente la infraestructura que soportará los servicios ofrecidos al Conglomerado Financiero BCR. Sin embargo, se reitera lo indicado anteriormente en el sentido de que las normas de aseguramiento de la calidad establecidas por la Organización Internacional para la Normalización ISO son acreditaciones a las que se someten las empresas de manera voluntaria, por lo que no es aceptable que se soliciten como un requisito de admisibilidad. Por lo tanto, se declara **parcialmente con lugar** el recurso en este aspecto. Finalmente, se observa que en la redacción propuesta por la Administración se incluye el término “entre otros”, lo cual resulta inaceptable ya que genera inseguridad jurídica y deja abierta la posibilidad a los oferentes de presentar otros documentos para cumplir con el requisito, lo cual puede generar problemas en la etapa de estudio de las ofertas. Por lo tanto, de oficio se advierte a la Administración que debe indicar de forma taxativa los documentos que aceptará a los oferentes para cumplir con el requisito.

7) Certificaciones ISO 22301, ISO 27017, ISO 27018.

En el documento denominado “Especificaciones Técnicas” del pliego de condiciones se indica lo siguiente: *“**Bloque 5: Solución en la Nube** / […] **Mitigación de Amenazas y Cumplimiento Nube** / Realización de pruebas de penetración periódicas con entrega de resultados al BCR si se solicitan. / Controles antimalware y detección de amenazas avanzadas. / Cumplimiento verificado con estándares internacionales: ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3, GDPR y PCI-DSS.”* (el destacado es del original).

*“**Bloque 6: Apego a las Normas de Seguridad del Conglomerado Financiero del Banco de Costa Rica** / […] **Certificaciones de Seguridad Requeridas** / Tenencia de certificaciones internacionales vigentes: / ISO/IEC 27001. / ISO/IEC 27017. / ISO/IEC 27018. / SSAE-16 / SOC 1 / SOC 2 Tipo II. / SOC 3 / GDPR / PCI-DSS. / ISO 22301.”* (el destacado es del original).

La **empresa objetante** explica que el Reglamento General de Gobierno y Gestión de la Tecnología de Información, Acuerdo CONASSIF 5-24 (Alcance 130 a La Gaceta 134 del 22 de julio de 2024), dispone en su artículo 23, inciso c), que la entidad supervisada debe verificar que el proveedor de servicios en la nube tenga vigente, al menos, la certificación ISO 27001. Respecto de ISO 27017 e ISO 27018, la norma solo exige verificar el cumplimiento de estándares o buenas prácticas tales como esas normas o las del Cloud Security Alliance, según el servicio externalizado. El pliego convierte en certificaciones obligatorias lo que el regulador trata como buenas prácticas, y lo hace sin justificación en el expediente. Solicita ajustar el pliego al artículo 23, inciso c), del Acuerdo CONASSIF 5-24, exigiendo ISO/IEC 27001 vigente como certificación y admitiendo, para ISO 27017 e ISO 27018, la acreditación del cumplimiento de sus controles o de las buenas prácticas del Cloud Security Alliance; admitir para ISO 22301 un plan de continuidad documentado y probado con sitio alterno. Subsidiariamente, solicita exigir estas certificaciones como condición de ejecución antes de la puesta en producción, o trasladarlas a factor de evaluación.

Al contestar la audiencia especial, la **Administración** aceptó modificar el pliego de condiciones y en este sentido manifiesta lo siguiente: *“Se acoge el extremo de la objeción relacionado con la necesidad de revisar el tratamiento otorgado a las certificaciones ISO 22301, ISO/IEC 27017 e ISO/IEC 27018, considerando la naturaleza de la contratación, el modelo de prestación de servicios bajo modalidad SaaS y las disposiciones regulatorias aplicables a servicios soportados sobre infraestructura de computación en la nube. / Como resultado del análisis realizado, la Administración procederá a ajustar el pliego de condiciones de la siguiente forma: / Las certificaciones ISO 22301 e ISO/IEC 27017 dejarán de formar parte de los requisitos de admisibilidad establecidos en las Condiciones Generales. / Las certificaciones ISO 22301 e ISO/IEC 27017 se incorporarán como parte de los criterios de evaluación del procedimiento, reconociendo el valor agregado que aportan en materia de continuidad*

del negocio y seguridad de servicios en la nube. / En consecuencia, la no presentación de las certificaciones ISO 22301 e ISO/IEC 27017 no constituirá incumplimiento técnico ni causal de inadmisibilidad de la oferta. / La certificación ISO/IEC 27018 se mantendrá dentro de las Especificaciones Técnicas. / Asimismo, para efectos de ISO/IEC 27018, la Administración aceptará tanto la certificación correspondiente como evidencia que permita demostrar el cumplimiento de controles y buenas prácticas para la protección de información en servicios de computación en la nube. / Para tales efectos podrán aportarse, entre otros: / a) Certificaciones vigentes emitidas por organismos acreditados cuyo alcance cubra los servicios utilizados por la solución ofertada. / b) Documentación técnica o informes emitidos por el proveedor de infraestructura o por el fabricante de la solución que permitan demostrar la implementación de controles de protección de información y privacidad aplicables al servicio. / c) Evidencia asociada a marcos de referencia reconocidos por la industria, tales como Cloud Security Alliance (CSA). / d) Informes de cumplimiento, reportes de auditoría independientes o documentación que permita verificar la aplicación de controles de protección de información, privacidad y tratamiento de datos aplicables a servicios de computación en la nube. / Para efectos de la acreditación de estos requisitos, podrán aceptarse certificados vigentes emitidos por organismos acreditados, documentación técnica emitida por el proveedor de infraestructura o fabricante de la solución, informes de cumplimiento, reportes de auditoría independientes, declaraciones de alcance y demás evidencias que permitan verificar la implementación de los controles requeridos. Los documentos antes indicados constituirán medios válidos de acreditación para demostrar el cumplimiento de los controles de protección de información y privacidad requeridos para la presente contratación, según el alcance aplicable a la solución ofertada. / No se acoge el extremo de la objeción que pretende sustituir íntegramente los mecanismos de acreditación definidos por la Administración por las alternativas propuestas por el recurrente o reemplazar la verificación de dichos controles únicamente mediante los mecanismos sugeridos en el recurso. / La Administración considera indispensable mantener mecanismos objetivos que permitan verificar que la solución propuesta dispone de controles adecuados de continuidad operativa, seguridad y protección de la información acordes con la criticidad de los servicios requeridos para el Conglomerado Financiero BCR. / En consecuencia, la atención de la presente objeción no implica la eliminación de dichos controles, sino el ajuste de los mecanismos mediante los cuales serán acreditados y valorados dentro del procedimiento de contratación, manteniendo los niveles de seguridad, continuidad operativa y protección de la información requeridos por la Administración."

Criterio de la División:

a) se observa que la Administración aceptó eliminar las certificaciones ISO 22301 e ISO/IEC 27017 de los requisitos de admisibilidad e incorporarlas como parte de los criterios de evaluación, pero decidió mantener a certificación ISO/IEC 27018 dentro de las especificaciones técnicas como un requisito de admisibilidad. Al respecto, resulta necesario reiterar lo indicado anteriormente en el sentido de que las normas de aseguramiento de la calidad establecidas por la Organización Internacional para la Normalización ISO son acreditaciones a las que se someten las empresas de manera voluntaria, por lo que no es aceptable que se soliciten como un requisito de admisibilidad. Por lo tanto, no resulta aceptable que la Administración mantenga la certificación ISO/IEC 27018 como un requisito de admisibilidad. En consecuencia, se declara **parcialmente con lugar** el recurso en este aspecto.

b) se observa que la empresa recurrente solicita que se ajuste el pliego de condiciones para que se exija a los oferentes la certificación ISO/IEC 27001, ello con fundamento en el artículo 23, inciso c) del "Reglamento General de Gobierno y Gestión de la Tecnología de Información" Acuerdo CONASSIF 5-24, publicado en el Alcance 130 a la Gaceta 134 del 22 de julio del 2024. Dicha norma dispone lo siguiente: *"Artículo 23. Obligaciones generales para el uso de la computación en la nube / Las entidades y empresas supervisadas que utilicen servicios de computación en la nube deben: / […] c) Verificar que el proveedor de servicios de computación en la nube tenga y conserve vigente, al menos, la certificación ISO 27001. Además, de conformidad con el servicio externalizado, verificar que cumpla con estándares o buenas prácticas, tales como las ISO 27017, 27018 o las mejores prácticas del Cloud Security Alliance."* Como puede observarse, el artículo mencionado por la recurrente establece la obligación de la certificación ISO 27001 al proveedor de los servicios de computación, lo cual implica que la Administración debe verificar el cumplimiento de dicho requisito al contratista, y no necesariamente al oferente. Por lo tanto, al no acreditar que el requisito se deba solicitar a los oferentes, se declara **sin lugar** el recurso en este aspecto.

5. Aprobaciones

Encargado	CELINA MEJIA CHAVARRIA	**Estado firma**	La firma es válida
Fecha aprobación(Firma)	23/11/2026 08:21	**Vigencia certificado**	20/04/2026 13:52 - 19/04/2030 13:52
DN Certificado	CN=CELINA MEJIA CHAVARRIA (FIRMA), OU=CIUDADANO, O=PERSONA FISICA, C=CR, GIVENNAME=CELINA, SURNAME=MEJIA CHAVARRIA, SERIALNUMBER=CPF-01-0789-0549		
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	MARCO ANTONIO LOAICIGA VARGAS	**Estado firma**	La firma es válida
Fecha aprobación(Firma)	23/11/2026 09:20	**Vigencia certificado**	16/02/2026 13:52 - 15/02/2030 13:52
DN Certificado	CN=MARCO ANTONIO LOAICIGA VARGAS (FIRMA), OU=CIUDADANO, O=PERSONA FISICA, C=CR, GIVENNAME=MARCO ANTONIO, SURNAME=LOAICIGA VARGAS, SERIALNUMBER=CPF-03-0425-0430		
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	26/11/2026 23:59		
Número resolución	R-DCP-SICOP-02138-2026	**Fecha notificación**	23/11/2026 09:21