Emitir resolución de recursos

1. Generar resolución de recursos

Encargado	Kathia Volio Cordero		
Fecha/hora gestión	29/09/2025 11:32	**Fecha/hora resolución**	02/10/2025 08:14
* **Procesos asociados**	Recursos	**Número documento**	8072025000001902
* **Tipo de resolución**	Fondo		
Número de procedimiento	2025XE-000492-0000400001	**Nombre Institución**	INSTITUTO COSTARRICENSE DE ELECTRICIDAD
Descripción del procedimiento	S.T- Licitación Pública Adquisición de bienes y servicios para la implementación de redes móviles de última generación, entrega según demanda		

2. Listado de recursos

Número	Fecha presentación	Recurrente	Empresa/Interesado	Resultado	Causa resultado
8002025000001806	12/09/2025 14:29	MARIA CLARET ARAYA MATAMOROS	SISAP INFOSEC SOCIEDAD ANONIMA	Rechazo de plano	Falta de fundamentació
8002025000001796	10/09/2025 23:27	JOHAN FRANCISCO MONTERO GRANADOS	ERICSSON DE COSTA RICA SOCIEDAD ANONIMA	Rechazo de plano	Falta de fundamentació
8002025000001795	10/09/2025 21:26	FERNANDO ENRIQUE BERROCAL VALVERDE	COASIN COSTA RICA SOCIEDAD ANONIMA	Rechazo de plano	Falta de fundamentació
8002025000001794	10/09/2025 20:20	MANUEL ANDRES QUIROS ZUÑIGA	ONE WAY TECHNOLOGIES SOCIEDAD ANONIMA	Parcialmente con lugar	No aplica
8002025000001793	10/09/2025 18:25	MARCEL ALONSO AGUILAR SANDOVAL	HUAWEI TECHNOLOGIES COSTA RICA SOCIEDAD ANONIMA	Parcialmente con lugar	No aplica

8002025000001791	10/09/2025 16:19	ARIEL FERNANDO NUÑEZ CAMACHO	AFN GLOBAL SOCIEDAD DE RESPONSABILIDAD LIMITADA	Parcialmente con lugar	No aplica

Emitir el por tanto de la resolución	☑

3. *Resultando

I.Que mediante auto Nro. 8052025000001915 del 11/09/2025 14:54 esta División otorgó audiencia especial a la Administración licitante.
II. Que mediante auto Nro. 8052025000001929 del 16/09/2025 13:12 esta División otorgó audiencia de acumulación a la Administración licitante.
III. Que mediante auto Nro 8052025000001959 DEL 19/09/2025 11:20 esta División otorgó audiencia a la Administración licitante.
IV. Que mediante auto Nro. 8052025000002012 15:37 horas del 29/09/2025 se comunicó el POR TANTO de la resolución de los recursos de objeción interpuestos.
V. 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 8002025000001806 - SISAP INFOSEC SOCIEDAD ANONIMA

SOBRE EL FONDO DEL RECURSO DE SISAP INFOSEC SOCIEDAD ANONIMA. Punto 9.7 Anexo 8. Protección y mitigación de DDoS en el dominio de Backhaul. Criterio de la División: La objetante alega que se ha incluido en el pliego este requisito contrario a lo que el propio ICE dispuso cuando atendió una aclaración en etapa previa, en concreto la extemporánea de CIBERC y que se trata ahora de un requerimiento que solo beneficia al fabricante CISCO y al potencial oferente CIBERC S.A. Que el licitante al atender consulta de DATASYS GROUP S.A. (Nro.7002025000000837) se había pronunciado categóricamente indicando que no era necesario dicho requerimiento, pero ahora lo impone. La recurrente transcribió lo que el ICE en ese entonces respondió, fundamentó y justificó técnicamente para que no fuese necesario. Añade que lo exigido en el pliego -que beneficia a Cisco con un DDoS-, presenta limitaciones técnicas, operativas y económicas que generan dudas sobre su idoneidad para un despliegue nacional de 5G multivendor, multi-tecnología e IPv4/IPv6. Expuso en su recurso las debilidades y limitaciones técnicas, los aspectos económicos, presentando tabla comparativa que en su criterio evidencia que el requerimiento es coincidente con la funcionalidad que cumple CISCO y se lesiona la neutralidad tecnológica. Añade que no existe sustento ni evidencia técnica en el expediente del porqué de la condición, considerando que hay falta de motivación que provoca la nulidad del requisito al no justificarse técnicamente la razón por la cual cambió el criterio. **Solicita se ordene eliminar el punto 9.7** Protección y mitigación de DDoS en el dominio de Backhaul por cuanto el mismo licitante indicó: "*No existe una norma universal que haga obligatoria la función anti-DDoS en los routers de backhaul 5G (…) Debido a lo anterior, la interpretación de que la funcionalidad de protección contra ataques DDoS en backhaul sea obligatoria es errónea, para los enrutadores destinados al Backhaul en la partida 4".*

La Administración por su parte expuso que el requisito no fuerza a usar una solución específica de un solo fabricante, sino que solicita ciertas funciones que se pueden lograr con varias tecnologías y de distintos proveedores. Que lo requerido es razonable y necesario, está directamente relacionado con la naturaleza del proyecto. Su propósito es garantizar que solo participen proveedores que realmente puedan cumplir con el contrato, lo que se considera un requisito válido y urgente para proteger el interés público. Refirió a la licitación pública 2021LN000009-000010000, del Banco Nacional de Costa Rica, para indicar que este órgano contralor avaló requerimientos técnicos específicos que la Administración justificó como necesarios para garantizar la seguridad operativa y prevenir vulnerabilidades, en ese caso relacionadas con la manipulación de efectivo y la trazabilidad de dispositivos. El ICE, no indicó el número de resolución, pero añade en su respuesta: "*...Lo más destacable es que la CGR reafirma que: "La Administración conserva la potestad de definir técnicamente sus necesidades, siempre que lo haga de forma motivada y proporcional, especialmente cuando se trata de proteger la integridad operativa o prevenir riesgos que puedan comprometer la seguridad institucional." Este criterio valida los requerimientos de la infraestructura tecnológica, redes críticas o ciberseguridad, como en el caso de mitigación DDoS en redes 5G. La resolución valida que, cuando la Administración demuestra que un requerimiento técnico está vinculado a la protección de activos sensibles o continuidad operativa, ese requerimiento no debe considerarse restrictivo, sino proporcional al interés público…".* Exponiendo sobre la exigencia de capacidades de detección y mitigación DDoS en el backhaul, el ICE enuncia que lo pedido es estratégicamente necesario, no restrictivo a un solo fabricante y coherente con redes 5G y amenazas actuales. En su respuesta de audiencia especial, la licitante expuso varios puntos en los cuales desarrolló el requerimiento del pliego, lo que argumentó la objetante, y ante ello el ICE brinda una justificación técnica y cumplimiento en la industria de cada uno, todo lo cual puede ser revisado en la respuesta de audiencia especial, a lo cual remite esta División. Añadió además la Administración que esta Contraloría General ha indicado la potestad que ostenta quien contrata para definir técnicamente sus necesidades.

Ante todo lo expuesto es importante indicar primero que todo, que quien recurre, debe aportar la prueba idónea en que apoye las argumentaciones que efectúa. La carga de la prueba le compete al tenor de lo regulado en el artículo 148 del Reglamento al Título II de la Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones y además, se destaca que el recurso de objeción está diseñado para modificar aquellas cláusulas cartelarias que impliquen una limitante en la participación de los potenciales oferentes todo lo cual debe ser debidamente fundamentado y probado por quien impugna el pliego.

En este caso, se puede destacar que la recurrente entre otros, hizo referencia al hecho de que en su criterio, el requisito del pliego que señala beneficia a Cisco con un DDoS presenta limitaciones técnicas, operativas y económicas que generan dudas sobre su idoneidad para un despliegue nacional de 5G multivendor, multi-tecnología e IPv4/IPv6. También a aspectos económicos. No obstante se observa que se trata de manifestaciones que las realiza a partir de sus propias apreciaciones, y para ellas no aporta la prueba fehaciente que las ausente. No están apoyadas en algún criterio técnico formal que lo sustente. A esto se puede adicionar que argumentaciones pensadas en el hecho de que CISCO cumpla, no acredita que nadie más pueda cumplir.

Quien recurre, no acredita con documentación propia del fabricante en cuestión, que logre demostrar que efectivamente solo ese puede cumplir y no haya algún otro que pueda cumplir lo pedido por el ICE, licitante éste que goza de la discrecionalidad para establecer los requisitos del concurso que le permiten satisfacer el interés público. Ante esto se tiene que ha sido la Administración la que ante esa discrecionalidad ha

definido cómo y de qué manera pretende tecnológicamente hacer frente a los riesgos que se le puedan presentar. En adición, se expone que la tabla comparativa que aporta la objetante en su su recurso, a efectos de señalar sus apreciaciones sobre funcionalidades que solo el equipo CISCO cumple, hace referencia por ejemplo pero no limitado a: a*rchivo: secure-edge-protection-tech-wp.pdf– página 3.* Ha de indicarse sobre el particular que documentación aportada en idioma distinto al español, sin su debida traducción al español -propia u oficial-, impiden que sean admitidos por esta División como sustento válido de los argumentos, aún y cuando pretenda ligar el argumento con un folio en particular del archivo. Los anexos aportados al recurso vienen en idioma distinto al español (ver expediente digital, consultando el apartado Recursos de objeción tramitados por la CGR/número de recurso 8002025000001806/Enviado/2. Detalle del recurso número 8002025000001806/Consulta/4. Documentos adjuntos y pruebas Número del 2 al 5). Sobre este mismo tema y lo resuelto por esta División se puede ver la resolución R-DCA-SICOP-00215-2025, en lo que resulta de interés.

En adición, referencia a pruebas que correspondan a un enlace o a una página web como por ejemplo el indicado, pero no limitado y que corresponde a https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5xx/applicationhosting/711x/b-app-hosting-config-guide-ncs540/m-install-and-configure-ddos-on-ncs540l.html, tampoco resultan prueba idónea debido al hecho de que están sujetos a modificaciones, resultan manipulables, o pueden incluso ser eliminados, impidiendo brindar certeza para tener el caracter de prueba idónea. Sobre este otro aspecto, se puede observar la resolución R-DCP-SICOP-00103-2025 en lo que interesa cuando expuso: "...*Este despacho contralor debe señalar al objetante que los enlaces de páginas web no constituyen un medio idóneo de prueba, conforme a lo exigido por los numerales 88 de la LGCP y 246 y 254 del RLGCP, dado que no existe garantía de contenido en el tiempo, ya que la información es fácilmente manipulable y sujeta a modificaciones periódicas, lo cual no brinda suficiente certeza para otorgarle el carácter de plena prueba, lo anterior en los términos ya señalados por esta Contraloría General al indicar lo siguiente: "Como se indicó, un link o dirección electrónica no puede considerarse como prueba idónea por la facilidad con la que puede alterarse su contenido, siendo además que el recurrente no realiza un ejercicio para vincular el argumento que se expone con la información a la que remite, lo que lleva a concluir que hay una falta de fundamentación". De igual manera, extraer información de una página web para ser tomada como prueba, no se considera como idónea por las mismas razones esbozadas líneas atrás, esto es, por la facilidad de modificación de la información, lo cual quedó ya expuesto en la resolución No. R-DCA-00864-2020 de las siete horas con treinta y tres minutos del veinte de agosto de dos mil veinte,..."*. En otro orden de ideas, la recurrente no demuestra tampoco que no exista una solución equivalente a la que puede ofrecer quien represente al fabricante CISCO, y que se pueda ofertar en el caso concreto. En consecuencia, **se rechaza de plano** el recurso por falta de fundamentación. No omite manifestar esta División que no se refiere a la licitación del Banco Nacional que cita la contratante, en tanto no se ha advertido con precisión cuál número de resolución quiso identificar.

Recurso 8002025000001796 - ERICSSON DE COSTA RICA SOCIEDAD ANONIMA

SOBRE EL FONDO DEL RECURSO DE ERICSSON DE COSTA RICA S.A. Punto 9.7. del Anexo 8. Criterio de la División: La objetante menciona que se extrae del requisito que los equipos de backhaul de borde (tipo compacto) soporten las funcionalidades de control y mitigación de ataques DDoS descritas. Adiciona que esa condición impone limitaciones a la participación, primero, según lo estipulado en la tabla incorporada en el numeral 9.6.1 del mismo Anexo, es obligatorio que el tráfico entre RAN y CORE esté cifrado mediante el protocolo IPSEC (protocolo de seguridad de internet). Esto quiere decir que el tráfico que pasa por todos los equipos de backhaul estará encriptado y no será posible su monitoreo para identificar posibles ataques DDoS. Solo los extremos donde se encripta/desencripta el tráfico (Baseband y SecGW ubicado en el CORE) tendrán posibilidad de hacer este monitoreo. Por ello el numeral 9.7 no tiene aplicabilidad (porque carece de lógica o sentido técnico) cuando se considera el requerimiento completo de ciberseguridad de la red. Añade que al crearse un túnel IPSEC entre RAN y CORE, los equipos de backhaul en el medio quedan automáticamente protegidos ante ataques ya que el tráfico dentro del túnel solo puede terminar en alguno de estos dos extremos. Como segundo punto menciona que los requerimientos de ciberseguridad relacionados con DDoS para otros componentes de la red, se limitan *a "el oferente debe presentar soluciones orientadas a proteger posibles amenazas…*" como lo son los casos numeral 9.6.1 para interfaz UE, numeral 9.5.6 para RAN y numeral 9.4.8 para CORE 5G. No obstante, en este caso para el backhaul el requerimiento se encamina a una serie de funcionalidades y protocolos específicos, que no son implementables cuando se considera la red completa (como un todo) RAN-Backhaul-CORE. Alega que hay inconsistencia -técnica-, en el tanto, si se pide bajo el primer requerimiento que la información esté cifrada extremo a extremo, limita la posibilidad para que pueda ser monitoreada en el Backhaul. Expuso además la objetante que funcionalidades como DDoS no están consideradas como obligatorias por 3GPP/ETSI/GSMA para equipos de backhaul en redes 5G y que el ICE lo reconoció en la respuesta dada a la solicitud de aclaración número 7002025000000837. **Las petitorias de la recurrente son:** Considerando la contradicción técnica, limitación a participar, que no corresponde a los diseños y protecciones que comúnmente se implementan en este tipo de redes, sino que además es ajeno al objeto originario del pliego solicitó se ordene eliminar el numeral 9.7 del Anexo 8 y mantener la condición originaria. Subsidiariamente, solicita se ordene al ICE modificar el pliego permitiendo la discrecionalidad del oferente y la posibilidad de dimensionar en su solución cualquiera de las dos opciones: IPSEC o protección DDoS. Del mismo modo, sea indicada la cantidad de los equipos que apliquen para estos casos.

La Administración sobre la petitoria específica, en lo conducente expuso que el requisito responde a necesidades del objeto contractual garantizando que el adjudicatario cuente con la capacidad técnica suficiente. Lo cataloga de necesidad razonable, vinculados e intrínsecos con la naturaleza misma de la solución pedida. Añadió que diversos fabricantes y referentes de la industria reconocen la importancia de la mitigación de DDoS, todo los cual cita en su respuesta y añade que ello evidencia que pluralidad de oferentes reconocen la necesidad de mitigación de DDoS en el borde y que no se trata de una función "propietaria" o de un solo fabricante. Que no se excluye potenciales oferentes, sino busca asegurar la participación de participantes que puedan cumplir con las condiciones del pliego. El ICE menciona que debe basar su estrategia de ciberseguridad en la premisa de que, al no ser obligatoria en las normas internacionales, la implementación de defensas avanzadas pueda omitirse. Los ciberataques son una realidad, se busca una postura proactiva de seguridad institucional y no hacerlo más bien generaría riesgos e incluso responsabilidades. La Administración explica que el cifrado extremo a extremo garantiza la confidencialidad e integridad de la información transmitida y no elimina completamente la visibilidad del flujo de datos, por lo que gestionando los metadatos, patrones de tráfico o comportamiento del flujo, se pueden implementar medidas de defensa para la detección y mitigación de DDoS.

Además, como se expuso supra, el ICE hizo referencia a recursos de objeción interpuestos en la licitación pública 2021LN-000009-0000100001, del Banco Nacional de Costa Rica, (sin citar la resolución precisa). También expuso la licitante las razones por las cuales mantiene como obligatoria la cláusula del pliego, a lo cual se remite a su respuesta de audiencia especial. Sobre la petitoria 2, indica que ante lo descrito se rechaza.

De conformidad con lo resumido supra, es menester reiterar como se expuso para el recurso de la empresa SISAP INFOSEC S.A. que la licitante goza de la discrecionalidad para establecer los requisitos del concurso que le permiten satisfacer el interés público y ha definido cómo y de qué manera pretende tecnológicamente hacer frente a los riesgos que se le puedan presentar. A lo anterior se suma que la objetante no ha demostrado con la prueba fehaciente que sustente el hecho de que la forma en que ella propone dimensionar en su solución IPsec resulte ser similar y aplicable a lo que el ICE pretende obtener con el requerimiento impugnado, sobre todo porque la forma en que la recurrente desarrolla sus argumentaciones reflejan ser una solución distinta a la protección y mitigación de DDoS que es lo pedido en el pliego.

La licitante al atender audiencia precisó que: "...• *El cifrado extremo a extremo (E2E) aplicado al tráfico del backhaul en redes 5G garantiza la confidencialidad y la integridad de la información transmitida; sin embargo, la protección ante ataques de DDoS es un tema de disponibilidad de los servicios y comunicaciones. Aunque el cifrado E2E protege el contenido, no elimina la visibilidad completa del flujo de datos, y por ende, no evita que este pueda ser protegido contra ataques de DDoS. • La protección contra ataques de denegación de servicio distribuido (DDoS) en*

dicho dominio no depende exclusivamente del análisis de contenido (el cual vendría cifrado), sino de la observación y gestión de metadatos, volúmenes de tráfico, tasas de paquetes y comportamiento de flujos. Por tanto, aun en escenarios con tráfico cifrado, los oferentes pueden ofrecer soluciones que se integren a los sistemas del ICE (EDR, SIEM, entre otros) que permitan implementar medidas de defensa basadas en técnicas de detección y mitigación en capa de red y transporte (por ejemplo: NetFlow/sFlow, rate-limiting, RTBH, BGP FlowSpec, scrubbing externo, entre otros). • En consecuencia, el cifrado E2E no elimina la capacidad de prevención ni de respuesta ante ataques DDoS en el backhaul, sino que redefine el enfoque hacia mecanismos de protección basados en patrones de tráfico y control de flujo, en concordancia con las mejores prácticas internacionales de seguridad en redes móviles y segmentos empresarial a través de soluciones fijas….".

Aunado a que la recurrente no debe proponer al ICE la forma en que ella podría cumplir, pues la discrecionalidad de la contratante ha definido una forma que al no demostrarse que haga del todo nugatoria la participación de oferentes, o que resulte ser una limitación injustificada a la participación, no tiene que adaptarse a determinada necesidad de un participante, que podría no cumplir con lo que actualmente regula el pliego. En consecuencia, las argumentaciones de quien objeta, se exponen en la forma en que ella pretende sea propuesta su solución, sin acreditar que ella proteja de la misma manera en que el ICE enfocó su requerimiento, por lo que no sustenta que puede cumplir en la forma en que la licitante lo pide. En cuanto a las cantidades que pide la recurrente se le precisen, esta División menciona que no ha sustentado o fundamentado por qué es que las requiere, sobre todo de frente a un procedimiento de licitación en modalidad según demanda. En consecuencia, **se rechaza** el recurso por falta de fundamentación.

Recurso 8002025000001795 - COASIN COSTA RICA SOCIEDAD ANONIMA

SOBRE EL FONDO DEL RECURSO DE COASIN COSTA RICA S.A. PUNTO 9.7 Anexo 8. Criterio de la División: La objetante considera que el numeral 9.7 adolece de respaldo técnico y lesiona igualdad, libre concurrencia y neutralidad tecnológica. Que es una contradicción de la Administración Técnica, pues había desechado esa misma solicitud, según consta en el expediente del propio proceso - respuesta del ICE 0132025711700031 del 19 de Agosto a la empresa Datasys Group. Que se agregó un nuevo requerimiento funcional a los equipos originalmente solicitados, sin justificación técnica, ni estudio de mercado que permita dimensionar el nuevo costo de estos elementos y la especificación técnica para la detección y protección/mitigación de ataques DDoS en el dominio de backhaul obliga a que esta función se realice de una única manera específica, exigiendo sea realizada por el mismo router de backhaul, como si fuese la única manera de lograr el objetivo funcional perseguido. Que el modelo de protección que el ICE ahora exige, no es eficiente, genera falsos positivos que bloquean tráfico legítimo de los clientes y falsos negativos que dejan pasar tráfico malicioso. Además impacta negativamente el desempeño de los routers de backhaul al tener que instalar y ejecutar procesos/mecanismos que consumen recursos importantes de CPU, memoria, etc, en un equipo que no debe tener ese rol en la capa de acceso, ocasionando una degradación significativa en los servicios de los usuarios. Alega que la administración técnica del ICE debe considerar que el mayor impacto, frecuencia, cantidad y tipos de ataques DDoS (volumétricos) provienen de forma masiva de dispositivos/usuarios infectados conectados al Internet (botnets). **Solicita** que cada oferente y/o fabricante pueda presentar la solución que implemente las mejores prácticas en la industria orientadas a detectar y mitigar dicho tráfico malicioso tan pronto ingresa a la red del operador (ICE) en la capa de Peering y/o Edge y no esperar a que el tráfico malicioso llegue hasta la capa de backhaul para poder ser detectado y mitigado, lo cual consumiría recursos costosos de capacidad (ancho de banda de los enlaces y procesamiento en los routers) en la red de transporte del ICE. Alega la recurrente que la solución debe permitir arquitecturas donde la detección se realice en controladores inteligentes y la mitigación en el punto más eficaz de la red (edge, peering, scrubbing center), evitando que el tráfico malicioso consuma recursos de la red de transporte. Esta práctica, adoptada por múltiples operadores a nivel global —como K2 Telecom (Brasil), Telecentro (Argentina) y NL-ix (Europa), ha demostrado mitigar ataques en menos de 30 segundos usando Sampled Port Mirror, frente a los 3–4 minutos que tardan soluciones tradicionales, ineficaces ante ataques de ráfagas cortas. Que en relación al cifrado, lo típico, recomendado y estándar (3GPP TS 33.501) en redes móviles es que el túnel GTP sea cifrado (IPSec) desde el gNodeB hasta los equipos centrales (Security Gateway) co-localizados con el core 5G. Que el nuevo requerimiento del pliego implicaría no cifrar el tráfico GTP desde el gNodeB/UE para poder realizar la detección y mitigación de ataques DDoS en el router de backhaul, dejando expuesta la red del ICE a vulnerabilidades de seguridad y privacidad de los datos de los usuarios en esos tramos no cifrados de la red. Que la solución que ahora se solicita para los routers de backhual, presenta peligros y desventajas evidentes, ya que al obligar que estas funcionalidades estén dentro del propio equipo, los procesadores (chips) destinados a realizar el routing de acceso de la red móvil tienen que sacrificar su propio desempeño para correr un número significativo de listas de control de acceso como lo exige una solución de mitigación DDoS eficiente/inteligente. Paliativos que buscan habilitar esa funcionalidad usando memorias TCAM tienen también el inconveniente que degradan el performance del chip/router significativamente y por lo tanto existen otros modelos de protección que otros fabricantes han desarrollado de manera más eficiente. Para la objetante el requerimiento se debe modificar para que al menos la solución propuesta por los oferentes para la detección y protección/mitigación de ataques DDoS dirigida a los routers de backhaul se pueda realizar utilizando otros componentes distribuidos en la red (a criterio de diseño del oferente) como parte de la solución anti-DDoS a proponer. Ello brindaría al ICE una solución más eficiente e inteligente (visibilidad y control/filtrado quirúrgico del tráfico malicioso) sin el riesgo de degradación del desempeño de los routers de backhaul. Solicita que el Inciso 9.7 sea eliminado del pliego al no responder a ninguna normativa internacional tal y como la propia Administración lo aceptó y evidenció, y en caso de que no se elimine, se permita que cada oferente/fabricante presente su propio modelo de protección modificando la cláusula objetada y permitiendo una participación abierta y no sólo la de un único fabricante.
La Administración al atender la audiencia expuso primero sobre la petitoria 1 desarrollo similar a lo que ya se expuso en el recurso de Ericsson Costa Rica S.A. por lo que este órgano contralor remite a lo resumido en él. Ante lo que manifestó el ICE en esos temas, rechaza ambas petitorias.

Ante esto, se observa de lo argumentado por la recurrente, que ha propuesto el poder cotizar una solución distinta a la que detalla el ICE en el requisito impugnado, contratante éste que basó sus requerimientos a partir de la discrecionalidad de la que goza y que se viene mencionando en esta resolución, tal y como lo que fue detallado al resolver el recurso de ERICSSON DE COSTA RICA SOCIEDAD ANONIMA y a lo cual se remite. No acredita quien recurre que no se pueda ofertar con lo que la contratante ha dispuesto en el pliego, sino que la objetante propone algo diferente. La limitante no se acredita, distinto puede ser que no pueda cotizar lo requerido por el pliego, y que proponga maneras distintas de presentar la solución. Se recuerda que un pliego no tiene que adaptarse a la propuesta de una eventual participante y que por ello deba ser

eliminada, sobre todo si la contratante ha explicado el por qué de mantener la solución en los términos que defendió. Tampoco se acredita que ningún otro oferente no pueda cumplir con lo pedido. En consecuencia, hay una falta de fundamentación de quien recurre, para que sea eliminado el requerimiento, y por eso se **rechaza de plano** el recurso. Y en cuanto a la segunda petitoria, por lo que se ha emitido en este criterio, deviene improcedente acoger lo pedido.

Recurso 8002025000001794 - ONE WAY TECHNOLOGIES SOCIEDAD ANONIMA

SOBRE EL FONDO DEL RECURSO DE ONE WAY COSTA RICA: Criterio de la División: Remitiendo a los argumentos de la empresa objetante establecidos en su acción recursiva y a la respuesta de la licitante al atender audiencia especial, este órgano se permite precisar lo siguiente: En fecha 9 de setiembre de 2025, la licitante publicó la versión del pliego que fue impugnada por la aquí recurrente. Para ese entonces, la fecha de presentación de plicas era 19 de setiembre de 2025 con apertura para el día 22 del mismo mes y año (ver expediente digital, ingresando a la versión del pliego publicada 09/09/2025/Ingreso del pliego de condiciones/1. Información general). Ante este escenario, el plazo de presentación de ofertas era de 7 días hábiles. En adición, el día 18 de setiembre de 2025, el ICE comunica nueva fecha de cierre de presentación de ofertas para el día 2 de octubre de 2025, con apertura de ofertas para el 3 del mismo mes y año, generando que ahora el plazo total para presentación de ofertas, sea de 17 días hábiles, sin considerar para este cómputo el día 15 de setiembre que fue feriado de ley (ver expediente digital, ingresando a las versiones del pliego publicadas 18/09/2025 / Ingreso del pliego de condiciones/1. Información general). Hay que tomar en cuenta que la licitante para atender este recurso expuso en lo que interesa: *"...Se aclara que de los 30 documentos que refiere el recurrente, solamente fueron objeto de actualización 4, que obedecen a las modificaciones del cartel publicadas, por lo que no es correcto asegurar que toda la información es nueva. Inclusive en el anexo Modificación 1, 2025XE-000432-0000400001 de la documentación subida al expediente de la licitación, se refiere a un resumen de las cláusulas y documentos que fueron objeto de una modificación con el fin de facilitar el análisis de los interesados y específicamente en lo que refiere a los anexos técnicos, se muestra un extracto de los 4 anexos que fueron objeto de variación con respecto al cartel inicial, los 26 documentos restantes, se mantienen sin variación, información disponible en el expediente de la licitación, lo cuál en la modificación se indicaron cuales tenían variación. (...) Los siguientes documentos que fueron modificados en SICOP se enlistan a continuación: Anexo 6 modificación 1 Anexo 8 modificación 1 Anexo 9 modificación 1 Con respecto a los anexos técnicos modificación 1, se aclara que solamente se modificaron los siguientes: Anexo X Norte Core y NOC, Anexo X Norte baterías. Anexo Y San Pedro, Anexo Y San Pedro piso 4). Se aclara que los demás anexos que no se indican con el nombre "modificación 1", se mantienen invariables" Como se puede observar y como queda demostrado, las modificaciones no son sustanciales como lo hace ver el recurrente. Por otro lado, de conformidad con el artículo 149 del Reglamento al Título II de la Ley 8660, en caso de modificaciones al pliego de condiciones, se debe dar ¼ (un cuarto) del plazo restante para recibir ofertas, contados a partir del momento de publicación de las modificaciones al cartel…",* (ver expediente digital, consultando apartado Recursos de objeción tramitados por la CGR número de recurso 8002025000001791/Enviado/4.Listado de autos número 8052025000001915 /Consulta/5. Detalle de respuesta/Contenido). Sin embargo el indicar que no se trata de modificaciones sustanciales puede incluso resultar contrario a manifestaciones que hizo el mismo licitante al atender el recurso de AFN GLOBAL SRL. relacionado con el numeral 9.7 del Anexo 8 del pliego cuando el ICE indicó"*...En respuesta a la petitoria "1", Se considera razonable conceder un plazo adicional a la fecha establecida para cierre de recepción de ofertas del 19/09/2025. Se acoge parcialmente el punto y se realizará una prórroga a la fecha de apertura de ofertas*….", esto resaltando que esa respuesta es ante la petitoria que hizo AFN GLOBAL SRL en el siguiente sentido: "...*Que se declare que la inclusión de la cláusula 9.7 Protección y mitigación de DDoS en el dominio de Backhaul constituye una* ***modificación trascendente al cartel de concurso,*** *de modo tal que se ordene a partir de su debida publicidad, otorgar el plazo correspondiente adicional de ley para que los oferentes ajusten sus ofertas…",* -resaltado no es del original-, (ver expediente digital consultando apartado Recursos de objeción tramitados por la CGR número de recurso 8002025000001791/Enviado/4.Listado de autos número 8052025000001915 /Consulta/5. Detalle de respuesta/Contenido). Incluso se permite acotar esta División que también para el recurso interpuesto por Huawei Technologies Costa Rica S.A. en lo que interesa señaló el ICE: "...*Se considera razonable conceder un plazo adicional a la fecha establecida para cierre de recepción de ofertas del 19/09/2025.* ***Se acoge parcialmente el punto y se realizará una prórroga a la fecha de apertura de ofertas…",*** respuesta dada por la contratante de frente a estas petitorias en el recurso: "...*Se disponga al ICE que conforme al artículo 49 del Reglamento al Título II de la Ley 8660, se cambie la fecha de recepción de ofertas, ampliándose en 17 días por corresponder a un plazo igual a la mitad del plazo original previsto en el pliego de condiciones para esos efectos. b. Se le disponga al ICE que mientras se tramita este recurso de objeción, se suspenda el plazo de recepción de ofertas para que el concurso en trámite no se vea impactado por recibir ofertas y que luego el órgano contralor resuelva algo no considerado en las condiciones del cartel que se impugna"*, (ver expediente digital consultando apartado Recursos de objeción tramitados por la CGR número de recurso 8002025000001791/Enviado/4.Listado de autos número 8052025000001915 /Consulta/5. Detalle de respuesta/Contenido). Si bien, no cataloga si los cambios son esenciales o no, el ICE aceptó modificar el plazo de apertura.

En consecuencia, para esta División hay meridiana claridad en el hecho de que, con las manifestaciones del ICE, cuando un recurrente solicitó la modificación del plazo de presentación de plicas por considerar la modificación al pliego trascendente, el licitante lo acogió parcialmente y mencionó que lo modificaría. Bajo esta tesitura, opina esta División que **con solo que haya una modificación esencial al pliego** y no

necesariamente se presenten en la totalidad de anexos o documentos que puedan conformar el mismo, el plazo de presentación de ofertas, debe ser el que la ley o reglamentos que aplican para la contratante, dispongan para ese tipo de cambios cartelarios.
Ahora bien, ante la anuencia de la contratante de modificar el plazo, y lo ha trasladado para el 2 de octubre del año en curso conforme lo expuesto, se **declara parcialmente con lugar** el recurso de objeción.

Recurso 8002025000001793 - HUAWEI TECHNOLOGIES COSTA RICA SOCIEDAD ANONIMA

SOBRE EL FONDO DEL RECURSO DE HUAWEI TECHNOLOGIES COSTA RICA S.A. 1) Sobre la normativa vigente en materia de ciberseguridad. Criterio de la División: La objetante impugna lo incorporado por el ICE en la cláusula 9.1 del Anexo 8. Añadió que en la resolución R-DCP-SICOP-01621-2025 se le ordena incorporar en esa cláusula 9.1 las normas en materia de ciberseguridad que se tenían que declarar bajo juramento al participar. Refirió la recurrente acciones de inconstitucionalidad sobre varios de los artículos del Reglamento sobre Medidas de Ciberseguridad Aplicables a los Servicios de Telecomunicaciones Basados en la Tecnología de Quinta Generación Móvil (5g) y Superiores, Decreto Ejecutivo Nro. 44196-MSP-MICITT del 25 de agosto de 2023. Expuso ser de relevancia porque de acuerdo a la Sala Constitucional al admitir la acción de inconstitucionalidad dispuso conforme al artículo 81 de la Ley de la Jurisdicción Constitucional No. 7135 que los tribunales y los órganos que agotan la vía administrativa en los procesos o procedimientos en que se discuta la aplicación de la norma de ese Reglamento, se abstengan de dictar resolución final mientras la Sala no haya hecho el pronunciamiento final. Alega que no le es claro si la declaración jurada que se emita debe considerar que se hace con la salvedad de que esa normativa que ahora determina el ICE en la cláusula 9.1 debe considerar lo dispuesto por la Sala en la resolución Nro. 2025-005950 para que en este caso el ICE y este órgano contralor tomen las acciones que correspondan para que se cumpla con el artículo 81 de comentario y lo que dispone en su párrafo segundo. Añade que en cuanto a redes 4G, el ICE no hizo ningún señalamiento sobre la normativa que se debe aplicar en materia de ciberseguridad con lo que ordenó esta Contraloría General en la R-DCP-SICOP-01621-2025, lo que la objetante considera necesario para que los oferentes puedan declarar lo pedido. Manifiesta que solo parece vincularse como normativa a declarar bajo juramento el Decreto Ejecutivo Nro. 44196-MSP-MICITT, el cual enuncia no aplicar en redes 4G como lo indica el Transitorio 1, de manera que el ICE no ha señalado cuál es la normativa en ciberseguridad que debe ser declarada para este tipo de redes. **Su petitoria**: **a)** Se modifique la cláusula 9.1 del anexo 8 y se indique expresamente las normas de ciberseguridad que se deben declarar bajo juramento para que las ofertas sean admisibles. **b)** Se le disponga al ICE que de aplicarse artículos adicionales al primero del Decreto en mención, indique con claridad cuáles serían. Adicionalmente que si alguno de ellos está siendo analizada su inconstitucionalidad por la Sala Constitucional, bajo el expediente 24-024405-0007-CO, se incluya en el pliego que se cumplirá con lo dispuesto en el artículo 81 de la Ley de la Jurisdicción Constitucional y la resolución de la Sala que se publicó en el Boletín Judicial nro. 234 del 12 de diciembre de 2024.

La Administración indicó que desde el inicio, el pliego estableció expresamente que los oferentes debían cumplir con la normativa sectorial vigente en materia de ciberseguridad aplicable al desarrollo de redes 5G y para verificar dicho cumplimiento, se solicitó la declaración jurada. Que entonces no es correcto afirmar que el pliego omite indicar cuál normativa debe ser declarada bajo juramento. Que de acuerdo con lo solicitado por la recurrente, respuesta del ICE y lo ordenado por esta División, incorporaron un enlace en la cláusula 9.1 que visualiza la normativa aplicada. Para la licitante la cláusula es clara en cuanto a la obligación de presentar una declaración jurada, la referencia específica a la normativa sectorial aplicable, la incorporación de un enlace directo para consulta de dicha normativa. Añadió que la inclusión del enlace no constituye una modificación sustantiva del contenido, sino una medida adicional para evitar confusiones y facilitar el acceso a la norma correspondiente.

El ICE acota en su respuesta que la recurrente vuelve a traer a discusión la siguiente petitoria: “a- 1- Solicita la recurrente que se modifique el apartado 9 del anexo 8 de ciberseguridad para que se determine la obligación de los oferentes para acreditar normas NESAS/SCAS y TS33.” Refiere la licitante que para ese efecto modificó la cláusula 9.2 del pliego para incorporar los protocolos de SCAS los cuales forman parte de NESAS (no significa que sean diferentes) y su complemento con las especificaciones de seguridad del Working Group 11 de la O-RAN Alliance (requisitos y pruebas), ambas en su versión vigente a la fecha de presentación de la oferta.

Ante lo anteriormente expuesto, considera esta Contraloría General que la recurrente lo que está solicitando son aclaraciones, lo cual no es materia de recurso de objeción, sino que ello debe ser interpuesto ante la Administración licitante. El artículo 49 del Reglamento al Título II de la Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones. Cuando pide que se le indiquen expresamente las normas de ciberseguridad que se deben declarar bajo juramento, es una precisión que necesita, de frente a una cláusula que expuso lo que aplica, y que el ICE reconoce que es clara. Además, pide la objetante que de aplicarse artículos adicionales al primero del Decreto en mención, indique con claridad cuáles serían. por lo que se precisa una aclaración también. Razones estas suficientes para **rechazar de plano** el recurso en este punto por improcedencia. No omite manifestar esta División, que aún y cuando un pliego de condiciones no haga referencia a una ley o norma en particular, es sabido que todo contratante y partes del proceso, deben respeto al ordenamiento jurídico en general, en cuyo caso todo lo que pueda disponer la Ley de la Jurisdicción Constitucional o cualquier otra ley, reglamentos, decretos, etc. aplica conforme en derecho corresponda. Asimismo, resulta de aplicación y respeto todo aquello que sea dispuesto por las instancias judiciales, con mayor razón si llegasen a aplicar al caso concreto. Todo lo anterior se indica sin perjuicio de que la recurrente tome en cuenta lo que aclaró el ICE al atender la audiencia especial.

2) Sobre la Antijuricidad de la cláusula 9.1 Anexo 8. Criterio de la División: La objetante expuso que la cláusula incorpora un enlace que remite al Decreto Ejecutivo Nro. 44196-MSP-MICITT. Considera que al incorporarla como requisito habilitante, el ICE la convierte en una cláusula de acatamiento obligatorio para todos los oferentes. Añade que al ser el Decreto parte del pliego, debe entenderse incorporado y aplicable en su totalidad, y el licitante no puede escoger qué artículos aplicar y cuáles no y está obligado a hacer valer la norma en su conjunto. Que por ello, cualquier vicio de nulidad absoluta, ilegalidad, inconstitucionalidad o inconvencionalidad que afecte al Decreto, se transmite de forma directa a la cláusula 9.1, viciándola en su totalidad, tornándose en antijurídica. Expone que esta Contraloría General en su condición de órgano de control de la Hacienda Pública y jerarca impropio de los procedimientos de contratación administrativa, tiene la potestad y el deber de velar por la legalidad de las actuaciones de la Administración. Manifestó la objetante razones y argumentaciones por las cuales considera antijurídica la norma y añadió a su vez normativa que en su criterio apoya sus argumentos, incluidos en ello lo que considera habilita a este órgano contralor para declararla antijurídica. A todo ello, esta División remite al recurso. **Solicita** se declare tal antijuridicidad y nulidad absoluta de la cláusula 9.1 ordenando al ICE desaplicar en este procedimiento el Decreto citado por ser su contenido contrario al bloque de legalidad y disponer la eliminación de las bases del pliego. Para la Administración la cláusula del pliego refiere a una normativa vigente, por lo tanto no comparte el alegato de que es contraria al bloque de legalidad.

Ante lo expuesto, revisando la cláusula impugnada, se precisa primeramente que indica lo siguiente: *El oferente deberá presentar declaración jurada que indique que cumple con la normativa sectorial vigente en materia de ciberseguridad aplicable para el desarrollo de redes 5G.* Sobre este primer detalle, no observa esta División que se haya estipulado algo que resulte ser antijurídico. Adicionalmente, el punto cartelario impugnado establece también: *La normativa sectorial puede ser consultada en el siguiente enlace:---------- https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_articulo.aspx?param1=NRA&nValor1=1&nValor2=100155&nValor3=137277&nValor5=2.*

El enlace redirecciona al artículo 1 del REGLAMENTO SOBRE MEDIDAS DE CIBERSEGURIDAD APLICABLES A LOS SERVICIOS DE TELECOMUNICACIONES BASADOS EN LA TECNOLOGÍA DE QUINTA GENERACIÓN MÓVIL (5G) Y SUPERIORES.

Se trata de un reglamento vigente al momento de emisión de esta resolución, por lo que ante esa condición, este otro aspecto de la norma cartelaria impugnada, no puede ser declarado antijurídico como lo pide la recurrente, siendo incluso que no es competencia de este órgano contralor declarar la antijuridicidad del reglamento referenciado. En consecuencia, se declara **sin lugar** el recurso en este punto.

3) Sobre la regulación de los estándares de ciberseguridad requeridos que sean declarados bajo juramento por los oferentes cláusula 9.2 del Anexo 8. Criterio de la División: La objetante considera que la redacción del ICE para indicarle a los oferentes los estándares de ciberseguridad que deben declarar bajo juramento que cumplen para las capas de BACKHAUL, CORE y RAN de las redes por desarrollar, no son claras y al ser de admisibilidad se incumple el principio de seguridad jurídica y afecta la participación de los oferentes. Añade que la forma del ICE para explicar qué estándares de seguridad debe cumplir el oferente y por consiguiente declarar bajo juramento, se sustenta en 3 posibilidades: Que el estándar aplica directo, que el estándar aplica de forma condicionada/indirecta y que el estándar no aplica, indicando los símbolos con los que se representa cada posibilidad según pliego. Para la recurrente, la forma no es acorde a la resolución R-DCP-SICOP-016212025 de esta Contraloría General. Que ello se materializa puntualmente cuando "*se incorpora el símbolo ◐ para determinar el estándar pedido es aplicado de forma condicionada o indirectamente sin explicar a cuáles son las partes del estándar son entonces las que se debe declarar bajo juramento que se cumple "* (sic). Que aún y cuando existe una "Nota de alcance", no especifica con la claridad requerida, qué parte del estándar es el que se debe considerar y declarar. Expuso por qué en su criterio los insumos son imprecisos y por qué no queda claro las declaraciones por hacer, todo a lo cual esta División remite al recurso. Opina la objetante que el ICE debe precisar qué aplica y qué no para hacer una declaración informada. **Solicita: a)** Se ordene al ICE determinar claramente y sin confundir, qué estándar se debe cumplir o no en temas de ciberseguridad para cada capa de la red (BACKHAUL, CORE y RAN), indicando en los casos de aplicación alternativa, indirecta o condicionada, lo que debe ser cumplido. **b)** Se exija al ICE indicar de manera clara, precisa y en concordancia con la práctica, cómo se debe demostrar el cumplimiento de estándares, normas, mejores prácticas u otros requisitos, así como el mecanismo de evaluación que utilizará la Administración para evaluar cada requisito. **c)** Se exija al ICE demostrar cómo se va a comprobar que lo declarado bajo juramento es veraz, para garantizar transparencia y se establezcan mecanismos objetivos de calificación y evaluación de los oferentes.

La Administración sobre la petitoria a) expuso no incurrir en inseguridad jurídica con la metodología de símbolos indicada, que es una herramienta clara, objetiva y suficiente, permitiendo participar en igualdad de condiciones. Que no es jurídicamente posible ni técnicamente viable que el pliego reproduzca el contenido completo de cada marco/estándar internacional. Que los marcos/estándares citados en el pliego no se limitan a un solo dominio técnico, sino que establecen lineamientos técnicos que deben aplicarse según el diseño de red ofertado. Sobre la petitoria b) el licitante expone que la verificación de lo declarado se realizará en las fases correspondientes del proceso de contratación en

apego a las leyes costarricenses vigentes, mediante diferentes mecanismos técnicos y documentales que el ICE considere suficientes. Añade que la verificación del ICE al cumplimiento se hará en verificación de las declaraciones juradas presentadas con la oferta, y en complemento con la documentación técnica de los equipos y licencias que debe presentar en la plica. Por último, sobre la petitoria c), la licitante menciona que la obligación de presentar declaraciones juradas -donde corresponda- tiene como fin asegurar jurídicamente que los oferentes se comprometan al cumplimiento de dichos marcos/estándares, en la medida que correspondan a su solución técnica, conforme la aplicación directa, condicionada o no aplicable definida en la tabla y sus notas de alcance.

Considerado lo argumentado por la recurrente y sus peticiones específicas, esta División es del criterio que lo pretendido es que se le aclaren una serie de aspectos relacionados con la cláusula impugnada. Sus petitorias en lo de interés precisan se determine claramente qué estándar se debe cumplir o no en temas de ciberseguridad para cada capa de la red (BACKHAUL, CORE y RAN), indicando en los casos de aplicación alternativa, indirecta o condicionada, lo que debe ser cumplido, se indique de manera clara, precisa cómo se debe demostrar el cumplimiento de estándares, normas, mejores prácticas u otros requisitos, así como el mecanismo de evaluación que utilizará la Administración para evaluar cada requisito, y por último indica que se exija al ICE demostrar cómo se va a comprobar que lo declarado bajo juramento es veraz, para garantizar transparencia y se establezcan mecanismos objetivos de calificación y evaluación de los oferentes, que si bien lo plantea como exigencia lo que pide realmente es que se le determine cómo la licitante va a comprobar las declaraciones. Se reitera como se indicó anteriormente que las aclaraciones no son objeto de recurso de objeción y por lo tanto, las mismas deben ser interpuestas ante la Administración licitante, conforme en derecho corresponda, Por tanto, procede el **rechazo de plano** de este extremo del recurso por improcedente. Puede ver en todo caso la objetante las respuestas que sobre los temas expuso el ICE.

4) Sobre la indebida modificación del apartado de Ciberseguridad (NESAS / SCAS). Cláusula 9.2 del anexo 8. Criterio de la División: La objetante considera que la modificación efectuada no corrige las omisiones que había apuntado en la ronda de objeciones anterior, sino que agrava más el vicio al mezclar indebidamente un estándar internacional consolidado, (SCAS de 3GPP/GSMA) con lineamientos no concluidos ni normativamente obligatorios (WG11 de la O-RAN Alliance), generando requisitos de imposible cumplimiento. Alega que la referencia a O-RAN WG11 no corresponde a una normativa obligatoria reconocida por SUTEL ni a un estándar consolidado, lo que favorece indirectamente a proveedores que participan en dicha alianza, en detrimento de otros. Que el pliego incorpora como requisito técnico el WG11 (Working Group 11 por sus siglas en inglés), que es un grupo de trabajo interno de la misma O-RAN ALLIANCE, que elabora componentes de un sistema de seguridad, pero no equivale, por sí mismo, a una norma obligatoria o vinculante emitida por entes reconocidos por la industria global, como sí lo es la GSMA. Informa que la descripción dada fue tomada del sitio web: https://map.o-ran.org/ donde se presenta la descripción del WG11 (lo cual está certificado por el Notario Público Carlos Alberto Riba Gutiérrez No. de carné 13739), como consta en la Prueba número 1(se entiende adjunta al recurso). Expuso la objetante por qué no comparte lo requerido, la diferenciación entre SCAS Y WG11 y por qué en su criterio imposibilita el cumplimiento, a todo lo cual esta División remite al recurso. Añade la recurrente que se obliga a los oferentes a declarar bajo juramento el cumplimiento de una norma que ninguna arquitectura O-RAN puede acreditar. Para la recurrente se afecta el interés público en materia de ciberseguridad, al pretender homologar como equivalentes lineamientos en desarrollo (WG11) con normas internacionales vigentes (SCAS/3GPP) y le impide participar. **Su petitoria: a)** Se ordene al ICE eliminar la referencia al WG11 de la O-RAN Alliance en el punto 9.2 de comentario, por no constituir un estándar internacional vigente ni verificable. **b)**. Precisar que la declaración jurada de los oferentes debe referirse únicamente al cumplimiento de SCAS/3GPP y TS33 de la serie NESAS, conforme a lo requerido por la SUTEL. **c)** Exigir al ICE que de mantener otros requisitos, aporte justificación técnica documentada que respalde la equiparación entre SCAS y WG11, bajo apercibimiento de nulidad por falta de motivación. **d)** Declarar que la redacción actual vulnera los principios de legalidad, seguridad jurídica, igualdad de oferentes, equidad y protección del interés público en materia de ciberseguridad, y ordenar su corrección inmediata. **e)** Que por cuanto las soluciones OPEN RAN no cumplen con los requisitos de ciberseguridad establecidos en la normativa internacional ni nacional vigente, solicita que el ICE elimine el requisito de admisibilidad de OPEN RAN.

La Administración consideró aclarar que hay error conceptual en las afirmaciones de quien recurre. Que hay imprecisión al indicar que SCAS constituye una certificación. El licitante enuncia que SCAS (Security Assurance Specifications) corresponde a un conjunto de especificaciones técnicas desarrolladas por el 3GPP que establecen requisitos de seguridad para el equipamiento de red, y no a un esquema de certificación en sí mismo. Que confundirlo es un error y debilita la fundamentación. Añadió que es incorrecto afirmar que: "*...las soluciones basadas en O-RAN no cuentan con certificaciones SCAS, lo cual las coloca en una situación de imposibilidad de cumplir con los estándares de seguridad requeridos por la Superintendencia de Telecomunicaciones SUTEL…*", y carece de sustento porque SCAS no es una certificación, sino que se *"... basa en las especificaciones definidas por el 3GPP (serie TS 33.XXX), lo cual permite que cualquier tipo de solución (Open RAN y no Open RAN) cumpla eventualmente con dichas especificaciones. Se debe recordar, tal y como se indicó en la respuesta de la Administración a las objeciones*

anteriores, que el modelo de la O-RAN Alliance se basa en las especificaciones del 3GPP y las complementa, particularmente en lo referente a interfaces abiertas, gestión y seguridad. Open RAN no sustituye los marcos de 3GPP, sino que se articula sobre ellos, a lo cual se incorporan, además, los lineamientos de seguridad definidos por el Working Group 11 (WG11)". Que el Anexo 8 exige la adopción tanto de SCAS, como de los requisitos de seguridad de O-RAN WG11, lo cual asegura un marco de seguridad integral. Añade el ICE que D-RAN es un modelo de arquitectura de despliegue, mientras que Open RAN es un marco de estándares abiertos que puede aplicarse sobre D-RAN, C-RAN o Cloud-RAN, no siendo conceptos opuestos, sino que pueden coexistir e integrarse en un mismo despliegue. No comparte la imposibilidad de cumplimiento alegados, manifestado el ICE que los requerimientos son viables, están respaldados por los estándares internacionales (3GPP, GSMA y O-RAN Alliance) y garantizan un nivel de seguridad adecuado, sin excluir a ningún oferente que efectivamente cumpla con las normas aplicables. En otro orden de ideas la contratante menciona que la SUTEL, conforme a lo dispuesto en la Ley General de Telecomunicaciones (Ley 8642) y sus reglamentos, tiene la facultad de incluir requisitos técnicos y de seguridad en los pliegos de licitación (como en la última subasta 5G), así como dictar normas técnicas en materia de instalaciones comunes de telecomunicaciones, calidad del servicio, interconexión, entre otros. Pero que esos requisitos no constituyen una normativa de aplicación automática y general a todos los operadores en cualquier circunstancia, sino que dependen del marco particular de cada concurso, licitación o regulación específica. En el caso de la subasta de espectro (N°2024LY-000001-SUTEL), las obligaciones derivadas del pliego aplicaban únicamente a quienes decidieron participar bajo ese procedimiento. Que el ICE, al no haber participado en dicho proceso no está vinculado por las condiciones específicas de ese concurso en aquellos aspectos que sólo resultan exigibles para los oferentes adjudicatarios. Que el ICE incluyó requerimientos de seguridad de SCAS/NESAS y ORAN WG11 en el Anexo 8 no por obligación directa de la licitación de la SUTEL, sino porque la institución considera que estas medidas son necesarias para garantizar la seguridad de su red. El contratante menciona que estas medidas responden al interés público y a la necesidad de tener una red segura y resistente. Que el requisito impugnado establece el presentar una declaración jurada de cumplimiento con estándares internacionales de ciberseguridad, incluyendo las SCAS aplicables adoptadas bajo el marco GSMA NESAS, y su complemento con las especificaciones de seguridad del Working Group 11 (WG11) de la O-RAN Alliance, ambos en su versión vigente a la fecha de presentación de la oferta. Que la recurrente desconoce el rol de O-RAN WG11, el cual establece lineamientos de seguridad que no sustituyen las especificaciones SCAS ni las "equipara", sino que las complementa en lo relativo a interfaces abiertas, interoperabilidad y pruebas de seguridad específicas para arquitecturas O-RAN.

Sobre la petitoria a) reitera que el WG11 de la O-RAN Alliance es el grupo técnico especializado en especificaciones de seguridad y pruebas de conformidad en arquitecturas abiertas, reconocido como parte de los trabajos de estandarización colaborativa global. Sus especificaciones también son aceptadas por diferentes operadores y fabricantes a nivel mundial y utilizadas en procesos de aseguramiento (SCAS, test suites de interoperabilidad y seguridad). La incorporación del WG11 en el pliego de condiciones agrega requisitos y especificaciones de seguridad para interfaces abiertas no cubiertas por SCAS, que pueden ser consultadas en el documento oficial: https://www.etsi.org/deliver/etsi_ts/104100_104199/104107/09.00.00_60/ts_104107v090000p.pdf y tanto SCAS como WG11 parten de principios de evaluación basados en amenazas y controles de seguridad. La equiparación técnica puede justificarse en términos de alcance funcional. En cuanto a petitoria b). menciona que la normativa vigente (Decreto Ejecutivo 44196- MSP-MICITT y lineamientos de SUTEL) reconoce la necesidad de aplicar un conjunto transversal de normas, que incluye marcos ISO/IEC 27000, NIST, SCAS/NESAS, y especificaciones técnicas de 3GPP. El interés público exige un enfoque multi normativo y multicapa, dado que la seguridad en redes 5G no depende solo del plano RAN/Core, sino también de backhaul, gestión, cadena de suministro y entornos cloud. Restringir la declaración jurada únicamente a SCAS/3GPP equivaldría a debilitar el aseguramiento integral de ciberseguridad, lo cual contraviene los principios de protección del usuario final y de gestión de riesgo establecidos en la NIST CSF. En respuesta a la petitoria c) reitera que el ICE ya reconoce que SCAS (GSMA/3GPP) y WG11 (O-RAN Alliance) no son idénticos, pero su equiparación en el pliego de condiciones se justifica en términos de alcance funcional. En respuesta a la petitoria d) enuncia quedar demostrado que la redacción no vulnera los principios de legalidad, seguridad jurídica, entre otros. Y respondiendo la petitoria e) añade que O-RAN es impulsado por operadores globales y respaldado por iniciativas de estandarización abierta. Excluirlo sería contrario a la competencia efectiva.

Sobre el particular y ante lo argumentado esta División se permite indicar que ante los argumentos de la recurrente no ha demostrado con la respectiva prueba de referencia que sustente los mismos. Se añade que la objetante no demuestra que los requerimientos no sean complementarios o no puedan coexistir. Ha desarrollado quien recurre sus apreciaciones sobre el tema, pero sin el criterio técnico que lo respalde, y en su acción recursiva fue clara para indicar que la documentación aportada en el anexo, fue para "*...La descripción anterior fue tomada del sitio web: https://map.o-ran.org/ donde se presenta la descripción del WG11 (lo cual está certificado por el Notario Público Carlos Alberto Riba Gutiérrez No. de carné 13739)...*".

Se reitera la discrecionalidad de la licitante para determinar los requerimientos del pliego, y ante eso esta División no encuentra obstáculo para que quien licite pueda pedir algunos requerimientos adicionales a los que pueda pedir el ente regulador. Aunado a lo anterior, el ICE expuso en lo que interesa: "*...SCAS, se basa en las especificaciones definidas por el 3GPP (serie TS 33.XXX), lo cual permite que cualquier tipo de solución (Open RAN y no Open RAN) cumpla eventualmente con dichas especificaciones. Se debe recordar, tal y como se indicó en la respuesta de la Administración a las objeciones anteriores, que el modelo de la O-RAN Alliance se basa en las especificaciones del 3GPP y las complementa, particularmente en lo referente a interfaces abiertas, gestión y seguridad. Open RAN no sustituye los marcos de 3GPP, sino que se articula sobre ellos, a lo cual se incorporan, además, los lineamientos de seguridad definidos por el Working Group 11 (WG11)".*
Se adiciona a lo anterior que lo relacionado con el OPEN RAN, ya fue abordado en la resolución de esta División R-DCA-SICOP-01621-2025, por lo que los requerimientos asociados al mismo estarían precluidos. En consecuencia, se rechaza de plano el recurso en este punto por falta de fundamentación.

5) Sobre los requisitos de seguridad pedidos en el requisito 9.3 del Anexo 8. Criterio de la División: La recurrente alega que la forma del ICE para explicar qué estándares de seguridad debe cumplir el oferente y por consiguiente, declararlo bajo juramento, se sustenta en 3 posibilidades: 1.Que el estándar aplica directo, que el estándar aplica de forma condicionada/indirecta y que el estándar no aplica, todos representados con el respectivo símbolo según posibilidad. Alega que se ha requerido declarar bajo juramento el cumplimiento de una serie de requisitos de seguridad obligatorios pero en varios componentes se indica que los requisitos para las capas de las de backhaul Core y RAN de las redes no indica ninguna referencia que explique cuándo los requisitos deben ser cumplidos incondicionados ni de forma indirecta. Para la objetante en tratándose de la capa BACKHAUL no queda claro lo que se debe considerar que aplica condicionado respecto a los requisitos de OpenID Connect (OIDC), CMPv2, Benchmarks CIS para plataformas de contenedores (p. ej., Kubernetes), Benchmarks CIS para contenedores, Detección avanzada de APT y Hoja de ruta con EDR nativo. Y en el caso de la capa CORE no queda claro lo que se debe considerar que aplica condicionado respecto al requisito de Detección de estación base falsa (FBS). **Solicita** se ordene al ICE que determine claramente qué parte de los requisitos obligatorios de seguridad se deben cumplir o no para las capas de BACKHAUL y CORE indicando qué debe ser expresamente lo que debe considerar en la declaración jurada.
La Administración indica que el requerimiento obliga a los oferentes a presentar una declaración jurada en la que confirmen que cumplen con una serie de requisitos de seguridad. Entre ellos se incluyen el uso de algoritmos de cifrado aprobados por NIST, la deshabilitación de algoritmos obsoletos como MD5 y SHA-1, la implementación de TLS 1.2/1.3 y mTLS, y el cumplimiento de las interfaces de la O-RAN Alliance (CUS-Plane, M-Plane, O1, O2, R1 y SMO). Estos requerimientos no se consideran arbitrarios, sino que se basan en estándares internacionales como NIST, ISO, 3GPP, GSMA NESAS/SCAS y O-RAN WG11, con el objetivo de aumentar la seguridad, asegurar la interoperabilidad y reducir riesgos en las redes 5G. Que el alegato se centra en que algunos de estos requisitos se aplican de manera general a todas las capas de la red (RAN, Core y Backhaul), cuando deberían ser específicos para cada una. Que sobre este punto esta Contraloría General declaró parcialmente con lugar el recurso anterior y ordena al ICE segregar los protocolos según la capa, sin que implique eliminar los requisitos de seguridad. Por lo tanto, la pretensión del oferente de anular el requisito 9.3 no procede. Que la resolución de este órgano contralor no cuestiona la validez de los requisitos, sino que era precisar su aplicación diferenciada en cada capa de la red, lo que garantiza que el requisito 9.3 sigue siendo válido y exigible para proteger la infraestructura de telecomunicaciones. Reiteró el ICE aspectos mencionado en el punto 3) anterior, sobre la metodología de símbolos, añadiendo que no modificó el pliego en los requisitos de protocolos de seguridad solicitados, sino que hizo cambio para detallar su aplicación diferenciada por capas de red, y que en la objeción anterior, no se impugnaron los requisitos, simplemente solicitó que se diferenciaran, por lo que no es de recibo el alegato y para el ICE podría estar precluido.
Al igual que como viene indicado este órgano contralor en los anteriores puntos se considera que lo requerido es una aclaración, su petitoria indica determinar con claridad en cuanto a qué parte de los requisitos obligatorios de seguridad se deben cumplir o no para las capas de BACKHAUL y CORE indicando qué debe ser expresamente lo que debe considerar en la declaración jurada, y por ello no compete ser tramitada por recurso de objeción, por lo que se **rechaza de plano** el recurso en este punto.Puede considerar la recurrente , lo expresado por el ICE en su respuesta.

6) Sobre la reafirmación de independencia de capas de red. Objeta lo incorporado por el ICE en la cláusula 9.3 respecto a lo previsto en la cláusula 1 del Anexo 8. Criterio de la División: La recurrente expuso que la propia tabla del punto 9.3 confirma lo que señaló en su anterior recurso de objeción: los requisitos específicos de O-RAN solo aplican a la capa RAN, no así a CORE ni a Backhaul. Que la licitante intenta la inclusión de los requerimientos con argumentos genéricos sobre interoperabilidad o compatibilidad que no guardan relación directa con las capas mencionadas y generan restricción innecesaria. Alega reafirmar la solicitud de separar las partidas CORE y RAN, ya que la unión en un solo bloque no obedece a razones técnicas objetivas, sino a decisiones administrativas que lejos de

perjudicar la concurrencia, la beneficia, trasladando así los beneficios a la Administración. Expuso la recurrente las razones por las cuales no comparte la argumentación que hizo el ICE para no permitir la separación de partidas, refiriendo a temas de incompatibilidades, dispersión de responsabilidades, sobrecargos de mantenimiento entre otros, a todo lo cual esta División remite al recurso actual. También alegó que se pudo por ello, haber confundido a este órgano contralor sobre los temas. Que en el oficio SUTEL Nro. 01765-SUTEL-OTC-2025 del 27 de febrero de 2025 se advirtió al ICE una serie de condiciones a tomar en cuenta en los recursos tendientes a potenciar la máxima participación. Que no es acorde que se ponga una limitación de participación por el hecho de vincular las capas de RAN con la del CORE, lo cual no se fundamenta ni técnicamente como lo exige el artículo 16 de la Ley General de la Administración Pública, ni por las disposiciones del regulador de comunicaciones, ni por los principios de libre concurrencia, libre participación. **Solicita**: **a)** Se ordene al ICE a separar las capas de RAN y CORE en partidas distintas, para no limitar la participación y se puedan presentar ofertas independientes para las capas de red según sus ventajas competitivas. **b)** Que se le ordene al ICE aportar al expediente los estudios técnicos que demuestren la supuesta complejidad o problemas de interoperabilidad indicados para oponerse a la división de la capa de RAN y de CORE en partidas distintas que puedan ser adjudicadas a distintos oferentes. **c)** Que se separen las partidas de CORE y RAN, donde las partidas 1, 2 y 3 se refieren a la RAN, las 4, 5 y 6 se refieren al BACKHAUL y se creen partidas 7, 8 y 9 para la capa de CORE. **d)** Ordenar al ICE fundamentar sus decisiones en la ciencia y la técnica, con información verificable y de fuentes referentes en la industria como la 3GPP, para cada uno de los requerimientos. La Administración considera precluidos los argumentos. Remite a la resolución anterior emitida por esta División en cuanto a este tema.
Ante lo anteriormente expuesto, este órgano contralor señala que al tema de la separación de partidas ya fue resuelto en la anterior resolución emitida por esta División, por lo que se comparte que el tema está precluido, en consecuencia se rechaza de plano, y se remite a lo resuelto sobre el tema en la resolución R-DCP-SICOP-01621-2025.
7) Sobre los escenarios LTE, LTE + NR y NR objetando lo incorporado por el ICE en los ÍTEMS 6 y 7 de la cláusula 18 del Anexo 8. Criterio de la División: La recurrente transcribe los requerimientos impugnados alegando además que en la resolución R-DCP-SICOP-01621-2025 se declaró parcialmente con lugar su anterior recurso relacionado con la inadecuada homologación de requerimientos entre escenarios LTE, LTE+NR Y NR. Transcribió las petitorias que había planteado en ese otro momento, para alegar que el ICE no cumple con lo requerido por este órgano contralor al emitir la versión modificada. La recurrente añade observar un cumplimiento parcial de los cambios no cumpliendo a cabalidad con las petitorias y enuncia que se mantiene el mismo problema por el que objetaron anteriormente. Expuso los argumentos que en su criterio evidencian aún más el problema, todo a lo cual remite esta División al recurso. Ahí realiza una descripción de escenarios por cada uno de los ítems. Apunta que la Administración solicita y reconoce que se tienen 3 diferentes escenarios de implementación en este cartel, los cuales enumera entre otros, la recurrente para una mejor comprensión: •Escenario 1: Es una solución solo 4G (LTE), para los sitios donde la Administración solamente instalará equipos y soluciones 4G. • Escenario 2: Es una solución solo 5G (NR), para los sitios donde la Administración solamente instalará equipos y soluciones 5G.• Escenario 3: Es una solución 4G+5G (LTE+NR), para los sitios donde la Administración instalará equipos y soluciones 4G+5G (LTE+NR). Considera que los cambios efectuados no son suficientes y el pliego debe ser modificado. También menciona que la modificación del pliego omite incluir el escenario 2 como un escenario de instalación de un sitio 5G el cual es la configuración más relevante de la licitación donde se instalarán soluciones 5G, lo que provoca que no haya certeza de lo que se está solicitando en ese escenario, no permitiendo garantizar a los oferentes tener información correcta para estructurar oferta. También refirió inconsistencias sobre las potencias, relacionando el punto 18.6 con los ítems 6 y 7 para afirmar que a pesar de que se menciona que solo debe soportar por hardware la configuración de portadoras las cuales serán adquiridas por los ítems 32 al 34 sí están solicitando que se incluya la licencia de la potencia y configuraciones MIMO para lo requerido en ambos ítems. Manifiesta que al no ponderar lo pedido en el pliego, el ICE va a tener que pagar por licencias que no va a aprovechar necesariamente para todos los sitios donde desarrolle la red, salvo que todos esos sitios sean para 4G y 5G simultáneamente, pero no es consistente con los 3 escenarios que el pliego pide. Que la ausencia de esta diferenciación genera un efecto anti económico: se obliga a licenciar funcionalidades completas en escenarios donde no resultan necesarias, produciendo un uso ineficiente de recursos públicos y afectando la proporcionalidad de la contratación. Advirtió escenarios o ejemplos de implementación o uso del ítem 6, lo mismo para el ítem 7, a lo cual esta División remite al recurso. Refirió la objetante la afectación del valor por el dinero. **Su petitoria es: a)** Que el pliego se adecúe para definir claramente los escenarios específicos de despliegue (LTE, LTE+NR y NR), y que los requerimientos funcionales y de licenciamiento de cada ítem se ajusten de forma proporcional y coherente a la demanda real de cada configuración. **b)** Que se incluyan líneas para cada uno de los sitios según su tipo de configuración, permitiendo una oferta técnica más precisa, eficiente y ajustada a la realidad del despliegue.
La Administración considera haber efectuado las modificaciones que correspondían. Que los ítems 6 y 7, y el Anexo 8 especifican claramente las capacidades y tecnologías que debe tener el nuevo equipo. Estas especificaciones cubren los escenarios de despliegue LTE y 5G, y se hicieron

para modernizar la red, lo que el ICE considera necesario. Que la objetante ha vuelto a insistir en este punto, a pesar de que se cumplió con lo ordenado por esta Contraloría General. Que la recurrente busca que se cambien los términos de la licitación para que se ajusten a su forma de comercializar su producto, lo que no justifica un nuevo cambio en las bases del concurso, pero no se limita que pueda cumplir con el pliego.
De lo que viene dicho, esta División se permite precisar que la recurrente no ha demostrado que el escenario que ha considerado omitido, le impida participar, distinto pueda ser que en su criterio considere que podía haber aspectos sin utilizar, o el tema de costos que en su criterio expuso en la acción recursiva, pero no sustenta que obligatoriamente tenga que existir. Hay que recordar la discrecionalidad del ICE para confeccionar el pliego de condiciones, y en este caso decidió que para cumplir con 5G lo hará de la forma en que lo previó en el pliego de condiciones y consideró cuáles escenarios son necesarios para la modernización y expansión de la red. En consecuencia, se **rechaza de plano** el recurso en este punto por falta de fundamentación.

8) Sobre los Servicios de Instalación de Radio Base (GAM vs. No GAM) 115 y 116 del Anexo 8. Criterio de la División: La recurrente estima que el cartel no diferencia los precios de instalación entre la zona GAM y No GAM, a pesar de que el costo es distinto (viáticos, transporte). Esto induce a sobrecostos. Solicita que se ordene al ICE la separación de las líneas de servicio de instalación de radio base en GAM y No GAM. **La Administración** señala que para el ítem 45, no se dieron modificaciones, que por el contrario el recurrente intenta utilizar las modificaciones a los ítemes 115 y 116 para esa objeción. Apunta además, que esto no fue objetado por el recurrente en ronda anterior. Según se desprende del cartel original y la modificación efectuada por la Administración el ítem 45 no fue objeto de modificación, por otro lado, se denota que tampoco fue planteada una objeción en la primera ronda para este ítem, de tal manera que este aspecto se tiene por precluído, por lo que se procede al **rechazo de plano** de este aspecto.

9) Sobre la Sobreestimación de Capacidad y falta de progresividad. (Punto 18 del anexo 8 ítemes 6 y 7). Criterio de la División: La recurrente considera que el cartel es rígido al establecer una capacidad de hardware superior a la activación mínima inicial de usuarios, sin prever un mecanismo de ampliación progresiva para utilizar el hardware adquirido a medida que crezca la demanda. Solicita que se ordene al ICE incluir un mecanismo objetivo para la ampliación progresiva de usuarios (RRC y DRB). **La Administración** expone que procedió a realizar modificaciones, las cuales considera son claras a los requerimientos. Considera que el objetante pretende que se ajuste el pliego a su estructura comercial, lo cual no es de recibo, y que cumplió con lo ordenado por la CGR en la ronda anterior. Considera que lo objetado no contiene sustento técnico. Como punto de partida se tiene que este aspecto fue conocido por este órgano contralor en la primera ronda de objeciones, ordenando la modificación, ya que la Administración accedió a realizar ajustes.
Tal cómo lo manifiesta la empresa recurrente, sobre este punto, interesa destacar lo resuelto en la primera ronda de objeciones. Así, se consideró que no llevaba lugar lo solicitado por el recurrente sobre la separación de líneas, siendo rechazado. Por lo que sería improcedente pretender reabrir la discusión sobre esto, sobre lo cual se remite al punto 6 de esta resolución.
Ahora, sobre la cantidad de usuarios que requiere cada tecnología, se rechazó, pues no se acreditó cómo esto resultaba esencial para su cotización.
Finalmente, la Administración aceptó modificar en lo que se refiere a la cantidad mínima de RRC y DRB a activar por unidad de banda base. Siendo este el único punto que podría entrarse a conocer.
Sobre esto, se extrae del texto del recurso manifestaciones en las que se señala que la actual redacción mantiene un licenciamiento rígido y estático, pues no prevé mecanismos de ampliación. Manifestaciones que no se observa mayor acreditación.
Vale destacar que la empresa considera que es rígido, y que la forma en qué se plantea no permite la progresividad. Pero no acredita que no es técnicamente correcto.
Debe tenerse en cuenta que la necesidad que debe satisfacerse es la de la Administración, quien conocedora de lo que requiere y cómo atender el fin público lo plantea. De ahí que es relevante que el recurrente acredite que esto no es así. Lo que en este caso no ocurre. Si bien la empresa pretende desarrollar un fundamento de afectación al interés público no acredita que se vayan a dar saturaciones y malas experiencia, que se afecte a la prestación continua, cómo se afecta el derecho de usuarios finales, pues son meras manifestaciones, siendo relevante en este caso, que es una empresa participante del mercado de telecomunicaciones.
Sobre el apartado de petitoria, llama la atención que solicita se ordene a la Administración que documenten y justifiquen las razones técnicas, olvida el recurrente que en este estadio, es él quien debe aportar los documentos y pruebas técnicas que evidencian la carencia, pues los actos administrativos se presumen válidos. Los demás aspectos de esa petitoria se han abordado en este criterio.
Bajo esa lógica, se **rechaza de plano** este aspecto del recurso. Sobre este aspecto, se debe estar adicionalmente a lo expuesto en el punto 6 de este recurso.

10) Sobre la Adquisición de Gestores (Ítems 30 y 103). Criterio de la División: La objetante considera que se mantiene una mezcla improcedente de bienes y servicios, generando desorden e incertidumbre. La verificación de bienes se condiciona a la finalización de la instalación (servicios), lo cual es contradictorio. Solicita que se ordene al ICE a separar e incluir líneas de servicios para los ítems 30 y 103, y prohibir la mezcla arbitraria de actividades.
La Administración apunta que la intención del recurrente es separar líneas de servicios para esos ítemes; señala que los servicios de instalación de equipos del ítem 30 está en el ítem 53, según lo que ordenó la CGR. Y en el caso del ítem 103, corre por cuenta del ICE, siendo que no se indica que el contratista lo debe hacer. Además, considera que el recurrente no especifica cómo afecta la presentación de su oferta. Por otro lado considera que el recurrente intenta nuevamente que se separen partidas, a pesar del rechazo de la CGR en la anterior ronda.
En esa oportunidad el ICE señaló que en el caso de los servicios del ítem 30 debían ser cotizados en el ítem 53; en el caso del ítem 103, el servicio correría por cuenta del ICE. Ahora, en cuanto al ítem 30 considera el recurrente que la modificación es artificiosa, porque mezcla líneas de servicios con naturalezas distintas. En el caso del 103 considera que el ICE no tiene experiencia ni recursos para instalar un software de gestión nuevo.
De la lectura que hace el recurrente, considera que aún subsiste la confusión pues en el caso del ítem 30, la verificación se hace incluyendo el servicio. De esto, no se observa que exista una mezcla si no una condición propia que por un lado el ítem 30 incluye bienes y el 53 los servicios, por lo que no se comprende el problema que plantea el recurrente, y por qué no se puede solicitar de esa manera.
De esto último, se extraña que el recurrente considere improcedente hacer esto, pues señala que son de diferente naturaleza, pero no se aporta prueba que así lo afirme con contundencia, de ahí que este aspecto carece de fundamentación.
En cuanto al ítem 103, no se comprende la afectación, pues el alegato conforme se desarrolla gira en relación al ítem 30. Más allá de considerar que no se incluyen los servicios, lo cual ya fue aclarado y modificado por la Administración.
Por otro lado, apunta que no se atendió lo ordenado por la CGR de separar líneas; sin embargo, esto no fue ordenado por la Contraloría.
Sobre el señalamiento que no se aplicó modificación en relación con especificaciones técnicas diferenciadas, no se comprende, puesto según lo ya expuesto si se realizaron modificaciones, pero sobre todo, porque el recurrente no hace mayor detalle de qué sería lo que faltaría por detallar, recordando que tiene el deber de fundamentar y demostrar que lo realizado por la Administración no es suficiente para asegurar el cumplimiento del fin público.
De frente a lo que se ha expuesto, se procede a declarar **sin lugar** este aspecto del recurso.
11) Sobre la Verificación de Licencias (Cláusula 6.4.1). Criterio de la División: La recurrente expone que la frase "previa verificación de las cantidades entregadas" mantiene la incertidumbre jurídica al supeditar el pago a una verificación no delimitada en tiempo. Solicita que se ordene eliminar la frase "previa verificación de las cantidades entregadas".
Sobre esto, **la Administración** explica que el recurrente interpreta erróneamente la cláusula. Señala que se eliminó que las licencias se aceptarían hasta que se verifique, posterior a su carga en el sistema, y se amplió la cláusula a que en caso que el ICE demore más tiempo en la carga, se realizaría la aceptación de las mismas previa verificación de cantidades.
Apunta que la verificación no depende de la carga en sistemas.
Sobre este punto, llama la atención lo pretendido por el recurrente en cuanto a eliminar la previa verificación, lo cual coincide este órgano contralor que es una obligación de la Administración, quien debe constatar que el objeto que licita y recibe es acorde con lo requerido, por lo que lo procedente es declarar sin lugar.
Ahora bien, siendo que la Administración explica la cláusula, se entiende que esto corresponde a una aclaración, por lo que el recurrente debe estar a lo aquí expuesto. De tal manera, se procede a **rechazar de plano** este aspecto del recurso.
12) Sobre Pruebas Técnicas Adicionales (Cláusula 6.5.8.13). Criterio de la División: La recurrente considera que la cláusula le otorga al ICE discrecionalidad absoluta para realizar "cualquier prueba adicional que considere conveniente", lo que atenta contra la seguridad jurídica y el deber de delimitación objetiva del alcance contractual. Solicita que se ordene ajustar la redacción para indicar expresamente los objetivos y criterios de aceptación específicos (SMART).
La Administración señala que no se modificó pues esas pruebas adicionales son por su cuenta, y no tienen costo en la oferta, pero considera que modificará este punto. De frente a lo expuesto por la Administración, y de la verificación realizada, se denota que la cláusula objetada, no fue modificada por lo que este aspecto se encuentra precluido. Así las cosas, lo que corresponde es **rechazar de plano** este aspecto del recurso.
13) Sobre el Servicio de Instalación de Core (Ítem 53, punto 68.2.4). Criterio de la División: El inciso l) solicita una declaración sobre "Cualquier otro componente o elemento requerido" de lo cual señala la recurrente que no especifica su alcance, imponiendo

una exigencia ambigua. Solicita que se ordene definir de manera clara y objetiva el alcance del inciso l, y proveer especificaciones técnicas mínimas.
Sobre este aspecto, **la Administración** considera que lo objetado se encuentra precluído, señala que estas cláusulas no fueron modificadas y que utiliza una aclaración para señalar que puede presentar una objeción.
Indica que por aclaración se eliminó el inciso k), y que respecto al l) se aclaró que se debían incorporar todos los elementos de puesta a tierra que requieran los equipos ofertados, siendo su dimensionamiento de conocimiento exclusivo de la empresa.
Sobre el particular denota este órgano contralor que en efecto, el contenido del inciso l), se encontraba descrito en el pliego, sin que fuese objeto de modificación por parte de la Administración, por otro lado, se denota que no fue objeto de recurso en la primera ronde da objeciones, de manera que este aspecto se encuentra precluído, de tal manera, se procede al **rechazo de plano** de este aspecto.
14) Sobre las Omisiones Comprometidas (O&M CORE). Criterio de la División: La objetante señala que el ICE omitió incorporar modificaciones que se comprometió a realizar en el SICOP, como excluir los sistemas de climatización de las obligaciones de O&M, y precisar que la disponibilidad 24/7 es en modalidad remota (de guardia). Solicita que se ordene al ICE la incorporación inmediata de las modificaciones comprometidas en el cartel.
La Administración señala que es correcto lo manifestado en cuanto a las aclaraciones 52 y 53 sobre el sistema de climatización y el personal, pero que al momento de realizar modificaciones se estimó que el numeral 73.11.5 era claro pues señalaba que siempre y cuando sean suministrados por el contratista.
Por otro lado, considera que es un aspecto precluído pues no fue modificado.
Sobre el punto 73.11.5, se destaca que no fue recurrido en la primera ronda de objeciones. Ahora bien, se denota que si bien esta cláusula fue modificada, se indica que los elementos o componentes son mínimos en el tanto estén dentro de la solución del contratista, e incluso, en el punto i) sistemas de climatización, se detalla que será según sea aplicable, lo cual coincide con lo que la Administración expone, de ahí que no se encuentra cómo limita la participación esta condición, máxime que el argumento del recurrente se encamina al compromiso de la Administración, por lo que se procede a declarar **sin lugar**, este aspecto del recurso.
Ahora, en cuanto al punto 73.11.9 (sobre el personal), considera la Administración que lleva razón el recurrente y se debe aplicar una modificación. Ahora bien, se denota que el punto en cuestión si bien sufrió modificaciones, no en cuanto a la obligación de disponer el personal, que es su punto de objeción. Por lo que debió recurrir esto en la primera ronda de objeciones. Así las cosas, se **rechaza de plano** este aspecto del recurso.
Debe considerar el recurrente que las aclaraciones no tiene por objeto modificar el pliego, y que en caso que la Administración considere que modificará un aspecto lo hará de oficio, siendo su responsabilidad y potestad hacerlas.
15) Sobre la Confidencialidad de Documentos y las Diligencias de Adición y Aclaración. Criterio de la División: La recurrente señala que el ICE no ha incorporado al expediente los documentos declarados confidenciales (como el "Programa 5G" del 2022) que la CGR ordenó incluir para su fiscalización. Solicita que se ordene al ICE incorporar al expediente todos los documentos declarados confidenciales.
La Administración considera que no lleva razón el recurrente, pues cumplió con lo ordenado. Señala que la Adición y aclaración ya fue resuelta.
Sobre este aspecto debe considerarse que ya fue abordado por este órgano contralor por medio de la resolución No. R-DCP-SICOP-1621-2025, así como en la resolución No. R-DCP-SICOP-1712-2025. De tal manera, se declara **sin lugar** este aspecto del recurso.
16) Sobre el Plazo de Presentación de Ofertas. Criterio de la División: La recurrente considera que las grandes modificaciones del cartel impactan elementos esenciales de la oferta, lo que justifica una ampliación del plazo. La resolución del recurso podría darse después de la fecha de recepción de ofertas. Así, solicita: 1. Ordenar al ICE que amplíe la fecha de recepción de ofertas en 17 días. 2. Disponer al ICE que suspenda el plazo de recepción mientras se tramita este recurso de objeción. La Administración considera razonable conceder un plazo adicional, por lo que se acoge **parcialmente con lugar**. Sobre el particular se denota que la Administración ha modificado el plazo para presentar ofertas, por lo que se ha cumplido con una de las pretensiones del recurrente. Sobre la suspensión del plazo, debe considerarse que de acuerdo con el artículo 150 del Reglamento al Título II de la Ley 8660, dicha posibilidad no está establecida. Así las cosas, se declara **sin lugar** este aspecto.

SOBRE EL FONDO DEL RECURSO DE AFN GLOBAL SRL. **Criterio de la División:** La objetante refirió a la aclaración que solicitó la empresa Nokia sustentada en consultas previas de DATASYS GROUP S.A. en donde se advirtió sobre la inconsistencia del ICE al rechazar inicialmente la pretensión de DATASYS y, en fecha posterior, acoger la misma solicitud presentada extemporáneamente por CIBERC, en beneficio de un fabricante particular (CISCO). Que en la respuesta brindada a Datasys, el ICE indica: *"No existe una norma universal (p. ej. 3GPP/GSMA/ETSI) que haga obligatoria la función anti-DDoS en los routers de backhaul 5G. (…) La interpretación de que la funcionalidad de protección contra ataques DDoS en backhaul sea obligatoria es errónea, para los enrutadores destinados al Backhaul en la partida 4."* Pero, se incluyó la cláusula 9.7 imponiendo un conjunto de exigencias técnicas que implican funcionalidades avanzadas de seguridad directamente en los routers compactos de cada sitio. Alega que el ICE modificó su propio criterio pasando de declarar improcedente la obligatoriedad de la funcionalidad DDoS en routers de backhaul con fundamento en un criterio técnico claramente expuesto, a imponerla como requisito sin fundamento, sin motivación técnica. La recurrente lo cataloga de cambio trascendente, que se debió publicar adecuadamente y darle plazo adicional a todos los potenciales oferentes. Para la objetante la funcionalidad requerida no corresponde a un estándar universal ni a una práctica obligatoria en el diseño de arquitecturas de backhaul, sino capacidades propias de appliances especializados que únicamente ciertos fabricantes -entre ellos CISCO- han integrado a sus routers compactos. En su opinión se limita la participación de otros oferentes incluida -ella incluida- y añade que lo pedido es técnicamente impertinente, infundado. Que en otros apartados el ICE sostiene la necesidad de adoptar estándares abiertos y universales (v.gr. Open RAN) para ampliar la participación, pero ahora incorpora una exigencia técnica propietaria y restrictiva, evidenciando favorecimiento hacia un oferente específico. Sus petitorias: 1-Que se declare que la inclusión de la cláusula 9.7 es una modificación trascendente de modo tal que se ordene a partir de su debida publicidad otorgar el plazo correspondiente adicional de ley para que los oferentes ajusten sus ofertas. 2. Que se disponga la eliminación de la obligatoriedad de mitigación de DDoS en las partidas 4, 5 y 6, limitando el requerimiento únicamente a las capas de red en que resulta técnicamente pertinente (partidas 1, 2 y 3). 3. Que, en caso de considerarse procedente por parte de la Administración la inclusión de nuevas funcionalidades de seguridad: 1.Se le ordene emitir una motivación técnica y jurídica pertinente que justifique el cambio de criterio en relación con la obligatoriedad de la mitigación DDoS en routers de backhaul, explicando por qué razón técnica se pasó de rechazarla a imponerla como requisito. 2.La Administración se vea obligada a fundamentar su exigencia en un estudio de mercado debidamente actualizado y objetivo, que respalde que tales funcionalidades no restringen la competencia ni favorecen a un único fabricante.

La Administración expuso sobre la petitoria 1 que es razonable conceder un plazo adicional a la fecha establecida para cierre de recepción de ofertas del 19/09/2025. Acoge parcialmente el punto y refiere que realizará una prórroga a la fecha de apertura de ofertas. Sobre la petitoria 2, brindó respuesta el ICE de manera similar a los aspectos que ya esta División expuso en el recurso de Ericsson Costa Rica S.A., a lo cual se remite. La licitante rechaza la petición por considerar que quien recurre no lleva razón. En cuanto a la petitoria 3, el ICE acotó: a) que el cifrado extremo a extremo (E2E) aplicado al tráfico del backhaul en redes 5G garantiza la confidencialidad y la integridad de la información transmitida; sin embargo, la protección ante ataques de DDoS es un tema de disponibilidad de los servicios y comunicaciones. Aunque el cifrado E2E protege el contenido, no elimina la visibilidad completa del flujo de datos, y por ende, no evita que este pueda ser protegido contra ataques de DDoS. b) La protección contra ataques de denegación de servicio distribuido (DDoS) en dicho dominio no depende exclusivamente del análisis de contenido (el cual vendría cifrado), sino de la observación y gestión de metadatos, volúmenes de tráfico, tasas de paquetes y comportamiento de flujos. Por tanto, aun en escenarios con tráfico cifrado, los oferentes pueden ofrecer soluciones que se integren a los sistemas del ICE (EDR, SIEM, entre otros) que permitan implementar medidas de defensa basadas en técnicas de detección y mitigación en capa de red y transporte (por ejemplo: NetFlow/sFlow, rate-limiting, RTBH, BGP FlowSpec, scrubbing externo, entre otros). c) En consecuencia, el cifrado E2E no elimina la capacidad de prevención ni de respuesta ante ataques DDoS en el backhaul, sino que redefine el enfoque hacia mecanismos de protección basados en patrones de tráfico y control de flujo, en concordancia con las mejores prácticas internacionales de seguridad en redes móviles y segmentos empresarial a través de soluciones fijas. Considera entonces el licitante que no lleva razón la objetante y rechaza la petición.

Reseñado lo anterior, primeramente sobre la petitoria relacionada con que se declare que la inclusión de la cláusula 9.7 como una modificación trascendente de modo tal que se ordene a partir de su debida publicidad, otorgar el plazo correspondiente adicional de ley para que los oferentes ajusten sus ofertas, se **declara con lugar** el recurso en este punto, y se remite al Criterio de División que con ocasión de este tema similar, se desarrolla en el recurso de objeción de la empresa ONE WAY COSTA RICA S.A., por resultar de aplicación.

Sobre la petición de la recurrente en cuanto a que se disponga la eliminación de la obligatoriedad de mitigación de DDoS en las partidas 4, 5 y 6, limitando el requerimiento únicamente a las capas de red en que resulta técnicamente pertinente (partidas 1, 2 y 3), es importante indicar que en criterio de esta División, ante lo desarrollado por la objetante en su acción recursiva, no ha comprobado la viabilidad técnica de la eliminación que propone para unas partidas y el mantenerlas solo en otras. Su petición, adolece de la debida fundamentación, recordando que la carga de la

prueba le compete a quien recurre. En este orden de ideas, debió la recurrente haber presentado prueba pertinente e idónea para haber acreditado que efectivamente lo solicitado por el ICE es improcedente técnicamente o de imposible cumplimiento, que no solo podría afectar su participación sino a otras ofertas, tratándose de una limitación injustificada a la participación, y que por el contrario lo procedente era la modificación que estaba solicitando, ejercicio de argumentación que no realizó la objetante y que era su deber. Aunado a lo anterior, no se trata tampoco de que quien recurre pida que la contratante le brinde un estudio de mercado que respalde que tales funcionalidades no restringen la competencia ni favorecen a un único fabricante, pues ante la carga de la prueba en mención, la acción recursiva es la que debe demostrar que realmente se restringe la participación, y bien pudo la recurrente demostrar con sus propios estudios que efectivamente se favorece a un único fabricante y que ninguno que pueda cumplir, siendo incluso que es un conocedor del mercado de telecomunicaciones y cuenta con la experiencia y el conocimiento para haber aportado la prueba idónea que demostrara que lo solicitado por ICE es improcedente técnicamente. Asimismo, se tiene que el ICE al contestar la audiencia especial ha externado las razones técnicas por las cuales se debe mantener el requisito en el pliego de condiciones respecto a la protección contra ataques de denegación de servicio. En consecuencia, **se rechaza de plano** el recurso en este punto por falta de fundamentación.

5. Aprobaciones del por tanto

Encargado	KATHIA GABRIELA VOLIO CORDERO	**Estado firma**	La firma es válida
Fecha aprobación(Firma)	29/09/2025 11:34	**Vigencia certificado**	15/05/2024 10:32 - 14/05/2028 10:32
DN Certificado	CN=KATHIA GABRIELA VOLIO CORDERO (FIRMA), OU=CIUDADANO, O=PERSONA FISICA, C=CR, GIVENNAME=KATHIA GABRIELA, SURNAME=VOLIO CORDERO, SERIALNUMBER=CPF-01-0774-0693		
CA Emisora	CN=CA SINPE - PERSONA FISICA v2, OU=DIVISION SISTEMAS DE PAGO, O=BANCO CENTRAL DE COSTA RICA, C=CR, SERIALNUMBER=CPJ-4-000-004017		

Encargado	KAREN MARIA CASTRO MONTERO	**Estado firma**	La firma es válida
Fecha aprobación(Firma)	29/09/2025 12:03	**Vigencia certificado**	08/03/2022 10:05 - 07/03/2026 10:05
DN Certificado	CN=KAREN MARIA CASTRO MONTERO (FIRMA), OU=CIUDADANO, O=PERSONA FISICA, C=CR, GIVENNAME=KAREN MARIA, SURNAME=CASTRO MONTERO, SERIALNUMBER=CPF-04-0181-0227		
CA Emisora	CN=CA SINPE - PERSONA FISICA v2, OU=DIVISION SISTEMAS DE PAGO, O=BANCO CENTRAL DE COSTA RICA, C=CR, SERIALNUMBER=CPJ-4-000-004017		

Encargado	FERNANDO MADRIGAL MORERA	**Estado firma**	La firma es válida
Fecha aprobación(Firma)	29/09/2025 12:52	**Vigencia certificado**	17/05/2024 15:22 - 16/05/2028 15:22
DN Certificado	CN=FERNANDO MADRIGAL MORERA (FIRMA), OU=CIUDADANO, O=PERSONA FISICA, C=CR, GIVENNAME=FERNANDO, SURNAME=MADRIGAL MORERA, SERIALNUMBER=CPF-02-0652-0911		
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 del por tanto de la resolución

Número resolución	R-DCP-SICOP-01809-2025	**Fecha notificación**	29/09/2025 12:53

De conformidad con la Ley General de Contratación Pública, se comunica a las partes lo resuelto por este órgano contralor sobre el/los recurso (s) interpuesto (s). Así las cosas, el contenido integral de la resolución será comunicada dentro del plazo de los tres días hábiles siguientes.

7. Aprobaciones

Encargado	KATHIA GABRIELA VOLIO CORDERO	**Estado firma**	La firma es válida
Fecha aprobación(Firma)	02/10/2025 08:02	**Vigencia certificado**	15/05/2024 10:32 - 14/05/2028 10:32
DN Certificado	CN=KATHIA GABRIELA VOLIO CORDERO (FIRMA), OU=CIUDADANO, O=PERSONA FISICA, C=CR, GIVENNAME=KATHIA GABRIELA, SURNAME=VOLIO CORDERO, SERIALNUMBER=CPF-01-0774-0693		
CA Emisora	CN=CA SINPE - PERSONA FISICA v2, OU=DIVISION SISTEMAS DE PAGO, O=BANCO CENTRAL DE COSTA RICA, C=CR, SERIALNUMBER=CPJ-4-000-004017		

Encargado	KAREN MARIA CASTRO MONTERO	**Estado firma**	La firma es válida
Fecha aprobación(Firma)	02/10/2025 08:12	**Vigencia certificado**	08/03/2022 10:05 - 07/03/2026 10:05
DN Certificado	CN=KAREN MARIA CASTRO MONTERO (FIRMA), OU=CIUDADANO, O=PERSONA FISICA, C=CR, GIVENNAME=KAREN MARIA, SURNAME=CASTRO MONTERO, SERIALNUMBER=CPF-04-0181-0227		
CA Emisora	CN=CA SINPE - PERSONA FISICA v2, OU=DIVISION SISTEMAS DE PAGO, O=BANCO CENTRAL DE COSTA RICA, C=CR, SERIALNUMBER=CPJ-4-000-004017		

Encargado	FERNANDO MADRIGAL MORERA	**Estado firma**	La firma es válida
Fecha aprobación(Firma)	02/10/2025 08:13	**Vigencia certificado**	17/05/2024 15:22 - 16/05/2028 15:22
DN Certificado	CN=FERNANDO MADRIGAL MORERA (FIRMA), OU=CIUDADANO, O=PERSONA FISICA, C=CR, GIVENNAME=FERNANDO, SURNAME=MADRIGAL MORERA, SERIALNUMBER=CPF-02-0652-0911		
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		

8. Notificación resolución

Fecha/hora máxima adición aclaración	07/10/2025 23:59		
Número resolución	R-DCP-SICOP-01809-2025	**Fecha notificación**	02/10/2025 08:14