

RESUMEN EJECUTIVO DE LAS ACTUACIONES PREPARATORIAS (BIENES)									
1. DATOS GENERALES									
1.1 FECHA DE EMISIÓN DEL FORMATO		21/02/2025							
1.2 ÁREA USUARIA		Área de Redes, Comunicaciones y Soporte Técnico							
1.3 DENOMINACIÓN DE LA CONTRATACIÓN		RENOVACIÓN DE LA RED LAN SEDE CENTRAL							
1.4 ACTIVIDAD DEL POI VINCULADA A LA CONTRATACIÓN		Implementar el Gobierno y la Transformación Digital de la empresa..							
1.5 N° DE REFERENCIA DEL PAC		23							
1.6 PROYECTO DE INVERSIÓN PÚBLICA		Código							
		Documento que declaró la viabilidad							
2. INFORMACIÓN SOBRE EL REQUERIMIENTO									
2.1 DATOS DEL REQUERIMIENTO		Documento de requerimiento	MEMORANDO GCAF.GTIC.2.382.2022			Fecha de recepción		17.10.2022	
2.2 MODIFICACIONES EFECTUADAS AL REQUERIMIENTO POR PARTE DEL ÁREA USUARIA		Fecha de la segunda versión	20.09.2023	De oficio		Con motivo de observaciones		X	
		Fecha de la tercera versión	06.11.2023	De oficio		Con motivo de observaciones		X	
		Fecha de la cuarta versión	01.12.2023	De oficio		Con motivo de observaciones		X	
		Fecha de la quinta versión	20.03.2024	De oficio		Con motivo de observaciones		X	
		Fecha de la sexta versión	10.06.2024	De oficio		Con motivo de observaciones		X	
		Fecha de la setima versión	12.07.2024	De oficio		Con motivo de observaciones		X	
		Fecha de la octava versión	31.07.2024	De oficio		Con motivo de observaciones		X	
		Fecha de la novena versión	26.08.2024	De oficio		Con motivo de observaciones		X	
		Fecha de la décima versión	16.09.2024	De oficio		Con motivo de observaciones		X	
		Fecha de la undécima versión	20.12.2024	De oficio		Con motivo de observaciones		X	
		Fecha de la decimosegunda versión	13.02.2025	De oficio		Con motivo de observaciones		X	
		Fecha de la decimotercera versión	18.02.2025	De oficio		Con motivo de observaciones		X	
		2.3 SEÑALAR SI LA CONTRATACIÓN INCLUIRÁ PAQUETE(S)		SI	-			NO	X
De ser afirmativa la respuesta, detallar el sustento técnico del área usuaria o el órgano encargado de las contrataciones, según el caso.				-					
2.4 SEÑALAR SI LA CONTRATACIÓN SE EFECTUARÁ POR ITEMS		SI			NO		X		
2.5 SEÑALAR SI SE HA LLEVADO A CABO UN PROCESO DE ESTANDARIZACIÓN		SI			NO		X		
		Documento de aprobación de la estandarización					Fecha de aprobación		
2.6 SEÑALAR SI EL BIEN OBJETO DE LA CONTRATACIÓN HA SIDO HOMOLOGADO		SI			NO		X		
		N° de Resolución que aprobó la Ficha de Homologación					Fecha de inicio de vigencia		
2.7 REQUERIMIENTO		Lo indicado se visualiza en el Capítulo III de la Sección Especifica de las Bases.							
2.8 OBSERVACIONES AL REQUERIMIENTO									
N° Item	Cantidad total de observaciones	Cantidad de observaciones formuladas por el OEC	Comunicación con la cual se remitió al área usuaria las observaciones al requerimiento	Fecha de remisión de la comunicación	Cantidad de observaciones formuladas por los proveedores	Comunicación con la cual se remitió al área usuaria las observaciones al requerimiento	Fecha de remisión de la comunicación		
1	17	17	INFORME GCAF.GL.4.074.2023	24.03.2023					

RESUMEN EJECUTIVO DE LAS ACTUACIONES PREPARATORIAS (BIENES)

Observaciones realizadas por el OEC

- 1) Se hace referencias a marcas; se solicita al área usuaria remitir la Resolución de Estandarización
- 2) Se solicita al área usuaria confirmar que el requerimiento se enmarca dentro del principio de vigencia tecnológica.
- 3) Respecto al sistema de cableado estructurado, se solicita compatibilizar tiempo de horizonte y garantía del sistema de cableado estructurado.
- 4) Se solicita corregir la palabra ondoso a nodos.
- 5) Se solicita incluir el lugar exacto para entrega de los bienes.
- 6) En conformidad con los plazos señalados en el requerimiento, la prestación principal sería de 120 días.
- 7) Referente a la experiencia: a fin de promover la libertad de concurrencia y competencia, el texto debe ser "() ... para organizaciones públicas y/o privadas....()
- 8) Perfil del Personal, deberá tener en cuenta que la colegiatura y habilitación será exigida para el inicio efectivo del servicio; por otro lado deberá indicar su despacho, desde cuando se contabiliza la experiencia laboral si desde la colegiatura o partir desde la obtención del título o bachiller según corresponda para cada perfil.
- 9) Sobre la TRANSFERENCIA TECNOLÓGICA, se solicita al área usuaria indicar en las especificaciones técnicas si la capacitación será de forma virtual o presencial
- 10) A fin de facilitar la supervisión de la ejecución del requerimiento, se solicita al área usuaria resumir en un cuadro todas las actividades, entregables y plazos previstos en las especificaciones técnicas.
- 11) Se advierte que la estructura de costos se deberá presentar para la suscripción de contrato; en la etapa de presentación de ofertas, el postor sólo presenta el monto total desagregando la prestación principal y prestación accesoria; por lo tanto se debe eliminar el párrafo.
- 12) Se solicita actualizar a la Directiva Administrativa N° 339-MINSA/DGIESP-2023. Asimismo, precisar los Protocolos Sanitarios vigentes establecidos por CORPAC S.A.
- 13) Se solicita agregar lo siguiente: "().....equivalente al 10% del monto contratado de la prestación principal..."; asimismo se debe especificar en lo sucesivo PAGO POR ENTREGA INFRAESTRUCTURA PASIVA Y OTROS, PAGO POR IMPLEMENTACIÓN, PAGO POR ADQUISICION Y OPERACIÓN.
- 14) Adecuar Otras Penalidades según las bases estándar.
- 15) Subcontratación: Indicar si procede la subcontratación en el presente requerimiento.
- 16) SERVICIOS COMPLEMENTARIOS: Se solicita indicar la forma de realizar la prestación accesoria, será remota o presencia
- 17) Se debe adecuar formato de requisitos de calificación conforme a bases estándar de licitación pública.

2	15	7	INFORME GCAF.GL.4.395.2023	11.10.2023	8	INFORME GCAF.GL.4.395.2023	11.10.2023
---	----	---	-------------------------------	------------	---	-------------------------------	------------

Observaciones realizadas por los proveedores

- 1) Respecto al numeral 2.1 de los TDR: Se solicita confirmar si se considerará una carta de fabricante que indique que los equipos propuestos no cuenten con anuncio de fin de venta (End-of-sale) al momento de la presentación de la oferta.
 - 2) Respecto al numeral 2.2 de los TDR: Se solicita confirmar que para poder sustentar este punto se considerará una carta de fabricante que indique que los equipos propuestos no cuenten con anuncio de fin de venta (End-of-sale) al momento de la presentación de la oferta.
 - 3) Respecto al numeral 2.3 de los TDR: Se solicita confirmar si se considerará una carta de fabricante que indique que los equipos propuestos no cuenten con anuncio de fin de venta (End-of-sale) al momento de la presentación de la oferta.
 - 4) Respecto al numeral 3.1 de los TDR: Se solicita confirmar que el periodo de tres (03) años se considerará a partir de la fecha en la que el cliente aceptará el acta de conformidad luego de la culminación de la implementación.
 - 5) Respecto al numeral 3.1 de los TDR: Se solicita confirmar que el mantenimiento preventivo tendría una frecuencia de una (01) vez al año.
 - 6) Respecto al numeral 5.2.2.1.1.6 de los TDR: Se solicita indicar el flujo de aire para estos equipos (entrada de aire por los puertos o por los ventiladores).
 - 7) Respecto al numeral 5.2.2.1.5 de los TDR: Se solicita indicar si el periodo de soporte solicitado será de tres (03) ó cinco (05) años.
 - 8) Respecto al numeral 5.2.2.1.5 de los TDR: Se solicita confirmar que será admitido un esquema de licenciamiento en el cual se cuente con un componente de licenciamiento que sea de carácter perpetuo.
- Observaciones realizadas por el OEC**
- 9) Se solicita verificar las cantidades de los bienes listados (números y letras) en el numeral 5.2.2.1.1 EQUIPOS DE COMUNICACIONES TIPO CORE, DISTRIBUCION, ACCESO, DATACENTER; en adelante.
 - 10) Se debe indicar que el postor ganador de la buena pro, para la firma de contrato presentará ser distribuidor o partner autorizado del fabricante.
 - 11) En requisitos de calificación, se debe adecuar a bienes similares.
 - 12) Suprimir el párrafo de la página 114.
 - 13) Adecuar el momento de presentación de la documentación del perfil del personal clave (para firma de contrato), salvo lo relacionado a la experiencia del personal clave que será al momento de la presentación de ofertas como lo estipula los requisitos de calificación.
 - 14) Se solicita al área usuaria resumir en un cuadro todas las actividades, entregables y plazos previstos en las especificaciones técnicas.
 - 15) Subcontratación: Indicar en las EETT, si procede la subcontratación en el presente requerimiento.

3	122				122	INFORME GCAF.GL.4.399.2023.I	16.10.2023
---	-----	--	--	--	-----	---------------------------------	------------

Se recepcionó 122 observaciones por parte de los proveedores, las cuales se encuentran detallados en el Anexo A del Resumen Ejecutivo.

4	12				12	INFORME GCAF.GL.4.467.2023.	28.11.2023
---	----	--	--	--	----	--------------------------------	------------

Observaciones realizadas por los proveedores:

- 1) Respecto al numeral 5.2.2.1.1.3 del requerimiento: Se solicita indicar que el switch tenga una capacidad RAM no menor a 4 GB.
- 2) Respecto al numeral 5.2.2.1.1.4 del requerimiento: Se solicita indicar que el switch tenga una capacidad RAM no menor a 4 GB.
- 3) Respecto al numeral 5.2.2.1.1.5 del requerimiento: Se solicita indicar que el switch tenga una capacidad RAM no menor a 4 GB.
- 4) Respecto al numeral 5.2.2.1.1.5 del requerimiento: se solicita incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS
- 5) Respecto al numeral 5.2.2.1.1.6 del requerimiento: Se solicita indicar que el switch tenga una capacidad RAM no menor a 4 GB
- 6) Respecto al numeral 5.2.2.1.1.6 del requerimiento: Se solicita confirmar se aceptará MC-LAG o M-LAG.. sírvase a confirmar se aceptará MC-LAG o CSS.
- 7) Respecto al numeral 5.2.2.1.2.1 del requerimiento: Se solicita confirmar que: "Debe de incluir la capacidad de identificar los dispositivos inalámbricos y crear políticas de acuerdo con la identidad del dispositivo (Android, iPhone, Etc.) o también será válido si esta función será soportada por la plataforma de gestión de forma centralizada."
- 8) Respecto al numeral 5.2.2.1.2.2 del requerimiento: Sírvase confirmar que se acepta Consola Bluetooth.
- 9) Respecto al numeral 5.2.2.1.1.6 del requerimiento: se solicita incluir en su requerimiento el término "TACACS+ o equivalentes".
- 10) Respecto al numeral 5.2.2.1.1.1 del requerimiento: se solicita confirmar que aceptará capacidades entre 1 (RU) o 8 (RU) y 10 (RU).
- 11) Respecto al numeral 5.2.2.1.1.2 del requerimiento: se solicita confirmar que aceptará capacidades entre 1 (RU) o 8 (RU) y 10 (RU).
- 12) Respecto al numeral 7.4 del requerimiento Sírvase precisar la forma de pago de la prestación principal y accesoria.

5	4				4	Correo Electrónico	18.12.2023
---	---	--	--	--	---	--------------------	------------

Observaciones realizadas por los proveedores:

- 1) Respecto al numeral 5.2.2.1.1.3 del requerimiento: Se solicita indicar que el switch tenga una capacidad RAM no menor a 4 GB.
- 2) Respecto al numeral 5.2.2.1.1.4 del requerimiento: Se solicita indicar que el switch tenga una capacidad RAM no menor a 4 GB.
- 3) Respecto al numeral 5.2.2.1.1.5 del requerimiento: Se solicita indicar que el switch tenga una capacidad RAM no menor a 4 GB.
- 4) Respecto al numeral 5.2.2.1.1.6 del requerimiento: Se solicita indicar que el switch tenga una capacidad RAM no menor a 4 GB.

RESUMEN EJECUTIVO DE LAS ACTUACIONES PREPARATORIAS (BIENES)

6	1	1	INFORME GCAF.GL.4.160.2024	02.04.2024			
El OEC realiza observaciones respecto a la cantidad de folios de las Especificaciones Técnicas, toda vez que el área usuaria señaló que no habían realizado cambios en el requerimiento.							
7	13	13	INFORME GCAF.GL.4.0301.2024	20.06.2024			
Observaciones realizadas por el OEC 1) En el numeral 6. REQUISITOS Y RECURSOS DEL PROVEEDOR se solicita adecuar. 2) Se solicita precisar con que documento se deberá acreditar dicha certificación PMP (copia simple u original) 3) En el numeral 6. REQUISITOS Y RECURSOS DEL PROVEEDOR se solicita suprimir lo resaltado. 4) Adecuar respecto a la habilitación, asimismo indicar el momento de la presentación de las certificaciones solicitadas y si corresponde copia simple u original. 5) Indicar el momento de la presentación de las certificaciones solicitadas y si corresponde copia simple u original. 6) Respecto al perfil del personal clave: Se solicita adicionar entre las carreras profesionales el "o" a fin de que el postor tenga alternativas de carreras a presentar en su oferta. 7) Respecto a la experiencia Se solicita precisar la experiencia detallada en ciertas actividades. 8) En el numeral 7.1.4 TRANSFERENCIA TECNOLÓGICA: Se solicita precisar cuál será el perfil profesional del personal y en qué momento presentará dicha acreditación 9) En el numeral 7.4 FORMA DE PAGO: Se solicita revisar los porcentajes indicados por la prestación principal y prestación accesoria (preventivo, correctivo y soporte técnico) 10) En el numeral 7.5 PENALIDADES APLICABLES 7.5.2 OTRAS PENALIDADES De la revisión integral a las EETT no se encuentra el Anexo 8 y el Anexo 11, por lo cual se solicita adicionar dicho anexo a la EETT. 11) En el numeral 7. OTRAS OBLIGACIONES Y RESPONSABILIDADES DEL NUMERAL 8, se solicita suprimir lo resaltado y adicionar la normativa que se encuentra vigente.. 12) REFERENTE A LA FOLIACION: Se solicita realizar la verificación correspondiente, toda vez que se observa que de la página 120 pasa a la página 145 13) REFERENTE A LA NUMERACIÓN: Se solicita realizar la verificación en las Especificaciones Técnicas, a fin de no generar confusión.							
8	18	18	INFORME GCAF.GL.4.0367.2024	22.07.2024			
Observaciones realizadas por el OEC 1) En el numeral 5.1: se solicita aclarar si la cantidad de nodos es 16 o 18. 2) Se solicita mayor precisión en el numeral 6. 3) Respecto al numeral 8 se solicita ceñirse a las bases estándar. 4) JEFE DE PROYECTO: Se observa que no se ha indicado la "o" en la acreditación 5) Se solicita aclarar si la CERTIFICACION PMP generaría un valor agregado sobre otros tipos de capacitaciones y/o cursos que no tendrían la misma consideración. En ese sentido, se recomienda como área usuaria especialista del presente requerimiento revisar dicho apartado. 6) En el LÍDER DE NETWORKING LAN.: Se observa que indican en letras "cinco" y en números "(04)", se solicita aclarar cuál es la cantidad correcta. 7) Se solicita aclarar si solicitan experiencia en "tecnología SDN" o "tecnología SDN o fabric" 8) Se solicita uniformizar las carreras profesionales solicitada en el perfil profesional con la forma de acreditación. 9) En el numeral 9.1.4 TRANSFERENCIA TECNOLÓGICA Capacitación: Se solicita indicar que toda la documentación requerida para la acreditación del perfil del capacitador deberá ser presentada para la suscripción del contrato. 10) Se solicita aclarar si corresponde a "certificaciones", de ser el caso se solicitar eliminar "especializaciones" e incorporar "certificaciones". 11) Se solicita suprimir del numeral 9.4 FORMA DE PAGO. Asimismo, se solicita eliminar el anexo 4. 12) En ese sentido, se solicita adicionar un numeral para SISTEMAS DE CONTRATACION y otro numeral para indicar la MODALIDAD DE CONTRATACION * MODALIDAD DE CONTRATACIÓN Llave en Mano * SISTEMAS DE CONTRATACION Suma Alzada 13) Adecuar la FORMA DE PAGO 14) se solicita suprimir el supuesto N° 8 de OTRAS PENALIDADES 15) se solicita uniformizar el perfil de los RESIDENTES. Por otro lado, respecto a la experiencia indican tres (03) años como, sin embargo, en la página 97 de las EETT se indica que ambos RESIDENTES deberán tener experiencia mínima de dos (02) años 16) Indican una resolución COVID no vigente, por lo cual se solicita indicar la directiva vigente COVID, 17) En requisitos de calificación: UN (01) IMPLEMENTADOR DE NETWORKING LAN UN (01) IMPLEMENTADOR DE NETWORKING WLAN ,Se solicita añadir por ser parte del personal clave. 18) Se solicita realizar la verificación correspondiente si los bienes y/o servicios en los portales de Perú Compras.							
9	32				32	INFORME GCAF.GL.4.395.2024	07.08.2024
Observaciones realizadas por los proveedores Se recepción 32 observaciones respecto a las Especificaciones Técnicas, las cuales se encuentran detallados en el Anexo B del Resumen Ejecutivo. (1era Parte)							
10	153				153	INFORME GCAF.GL.4.412.2024	13.08.2024
Observaciones realizadas por los proveedores Se recepción 153 observaciones respecto a las Especificaciones Técnicas, las cuales se encuentran detallados en el Anexo C del Resumen Ejecutivo.(2da Parte)							
11	53				53	INFORME GCAF.GL.4.416.2024	19.08.2024
Observaciones realizadas por los proveedores Se recepción 53 observaciones respecto a las Especificaciones Técnicas, las cuales se encuentran detallados en el Anexo D del Resumen Ejecutivo.(3era Parte)							
12	103				103	INFORME N° GCAF.GL.4.466.2024	10.09.2024
Observaciones realizadas por los proveedores Se recepción 103 observaciones respecto a las Especificaciones Técnicas, las cuales se encuentran detallados en el Anexo E del Resumen Ejecutivo.							
13	14	14	Informe N° 001-2024-CS LP.010.2024.CORPAC S.A.-1 - PML	18.12.2024			
Observaciones realizadas por el Comité de Selección: Se remite al área usuaria las nueve observaciones formuladas por el Comité de Selección.							

RESUMEN EJECUTIVO DE LAS ACTUACIONES PREPARATORIAS (BIENES)

14	4	4	Acta de Comité de Selección	21.01.2025			
Observaciones realizadas por el Comité de Selección: Se remite al área usuaria observaciones formuladas por el Comité de Selección.							

2.9 RESPUESTA DEL ÁREA USUARIA							
Nº Item	Cantidad total de respuestas a las observaciones	Cantidad de respuestas a las observaciones formuladas por el OEC	Comunicación de respuesta del área usuaria	Fecha de remisión de la comunicación	Cantidad de respuestas a las observaciones formuladas por los proveedores	Comunicación de respuesta del área usuaria	Fecha de remisión de la comunicación
1	17	17	MEMORANDO GCAF.GTIC.2.404.2023.M	20.09.2023			
Respuestas por el área usuaria: 1) Se precisa que lo puede realizar cualquier proveedor y no necesariamente por el fabricante de la marca. 2) Se acoge 3) No absuelve 4) Se acoge y se modifica. 5) Se acoge y se modifica. 6) No absuelve. 7) Se acoge y se modifica. 8) Se acoge y se modifica. 9) Se acoge y se modifica. 10) No absuelve. 11) Se acoge y se modifica. 12) Se acoge. 13) Se acoge y se modifica. 14) Se acoge y se modifica. 15) No absuelve 16) Se precisa. 17) No absuelve. En virtud a las absoluciones, el área usuaria remite la Segunda Versión de las Especificaciones Técnicas de fecha 20.09.2023							
2	15	8	MEMORANDO GCAF.GTIC.2.471.2023.M	06.11.2023	7	MEMORANDO GCAF.GTIC.2.471.2023. M	06.11.2023
Respuestas por el área usuaria: 1) Se precisa lo señalado. 2) Se precisa lo señalado. 3) Se aclara. 4) Se confirma lo indicado. 5) Se aclara. 6) Se confirma lo indicado. 7) Se acoge y se modifica. 8) Se confirma lo indicado. 9) Se confirma lo indicado. 10) Se acoge y se modifica. 11) Se acoge y se suprime. 12) Se acoge y se modifica. 13) Se acoge y se modifica. 14) Se aclara lo indicado. 15) Se aclara En virtud a las absoluciones, el área usuaria remite la Tercera Versión de las Especificaciones Técnicas de fecha 06.11.2023							
3	122				122	MEMORANDO GCAF.GTIC.2.471.2023. M	06.11.2023
Respuestas del área usuaria: El área usuaria remite el pliego absolutorio de las 122 consultas y/u observaciones realizadas por los proveedores, las cuales fueron trasladadas al área usuaria las cuales se encuentran detallados en el Anexo A.1 del Resumen Ejecutivo. En virtud a las absoluciones, el área usuaria remite la Tercera Versión de las Especificaciones Técnicas de fecha 06.11.2023							
4	12				12	MEMORANDO GCAF.GTIC.2.510.2023. M	01.12.2023
Respuestas del área usuaria: El área usuaria remite el pliego absolutorio y en virtud a ello, el área usuaria remite la Cuarta Versión de las Especificaciones Técnicas de fecha 01.12.2023							
5	4				4	MEMORANDO GCAF.GTIC.2.133.2024.M	22.03.2024
Respuestas del área usuaria: El área usuaria remite el pliego absolutorio de las 4 consultas por los proveedores, el área usuaria remite la Quinta Versión de las Especificaciones Técnicas de fecha 20.04.2023							
6	1	1	MEMORANDO GCAF.GTIC.2.231.2024. M	11.06.2024			
Respuestas del área usuaria: A raíz de las observaciones realizadas por parte del OEC, el área usuaria remite la Sexta Versión de las Especificaciones Técnicas de fecha 10.06.2024							
7	13	13	MEMORANDO GCAF.GTIC.2.280.2024. M	15.07.2024			

RESUMEN EJECUTIVO DE LAS ACTUACIONES PREPARATORIAS (BIENES)							
	Respuestas del área usuaria: El área usuaria remite el pliego absolutorio de las 13 observaciones por los proveedores, por lo cual el área usuaria remite la Séptima Versión de las Especificaciones Técnicas de fecha 12.07.2024						
	8	18	18	MEMORANDO GCAF.GTIC.2.294.2024.M	31.07.2024		
	Respuestas del área usuaria: El área usuaria remite el pliego absolutorio de las 18 observaciones por el OEC, el área usuaria remite la Octava Versión de las Especificaciones Técnicas de fecha 31.07.2024						
	9	32				32	INFORME GCAF.GL.4.395.2024 07.08.2024
	Respuestas del área usuaria: El área usuaria remite el pliego absolutorio, las cuales fueron trasladadas al área usuaria las cuales se encuentran detallados en el Anexo B.1 del Resumen Ejecutivo. el área usuaria remite la Novena Versión de las Especificaciones Técnicas de fecha 26.08.2024						
	10	153				153	MEMORANDO GCAF.GTIC.2.341.2024.M 27.08.2024
	Respuestas del área usuaria: El área usuaria remite el pliego absolutorio, las cuales fueron trasladadas al área usuaria las cuales se encuentran detallados en el Anexo C.1 del Resumen Ejecutivo. el área usuaria remite la Novena Versión de las Especificaciones Técnicas de fecha 26.08.2024						
	11	53				53	MEMORANDO GCAF.GTIC.2.341.2024.M 27.08.2024
	Respuestas del área usuaria: El área usuaria remite el pliego absolutorio, las cuales fueron trasladadas al área usuaria las cuales se encuentran detallados en el Anexo D.1 del Resumen Ejecutivo. el área usuaria remite la Novena Versión de las Especificaciones Técnicas de fecha 26.08.2024						
	12	103				103	MEMORANDO GCAF.GTIC.2.377.2024.M 17.09.2024
	Respuestas del área usuaria: El área usuaria remite el pliego absolutorio, las cuales se encuentran detallados en el Anexo E.1 del Resumen Ejecutivo. A raíz de las observaciones realizadas por los proveedores, el área usuaria remite la Décima versión de las Especificaciones Técnicas de fecha 16.09.2024						
	13	14	14	correo electrónico	20.12.2024		
	El Área Usuaria absuelve las observaciones realizadas por el comité de selección remitiendo la Undécima versión de las Especificaciones Técnicas de fecha 20.12.2024						
	14	4	4	correo electrónico	19.02.2025		
El Área Usuaria absuelve las observaciones realizadas por el comité de selección remitiendo la DecimaSegunda versión de las Especificaciones Técnicas de fecha 13.02.2025 y DecimaTercera versión de las Especificaciones Técnicas de fecha 18.02.2025							
2.10	AJUSTES QUE SE REALIZARON AL REQUERIMIENTO						
	Nº Item	Ajustes realizados al requerimiento					
	1	Se realizaron ajustes a las Especificaciones Técnicas a partir de las observaciones formuladas por el OEC, quedando definido en la Segunda Versión de las Especificaciones Técnicas de fecha 20.09.2023					
	2	Se realizaron ajustes a las Especificaciones Técnicas a partir de las observaciones formuladas por el OEC, y por los proveedores quedando definido en la Tercera Versión de las Especificaciones Técnicas de fecha 06.11.2023					
	3	Se realizaron ajustes a las Especificaciones Técnicas a partir de las observaciones formuladas por los proveedores, quedando definido en la Cuarta Versión de las Especificaciones Técnicas de fecha 01.12.2023					
	4	Se realizaron ajustes a las Especificaciones Técnicas a partir de las observaciones formuladas por los proveedores, quedando definido en la Quinta Versión de las Especificaciones Técnicas de fecha 20.03.2024					
	5	Se realizaron ajustes a las Especificaciones Técnicas a partir de las observaciones formuladas por el OEC, quedando definido en la Sexta Versión de las Especificaciones Técnicas de fecha 10.06.2024					
	6	Se realizaron ajustes a las Especificaciones Técnicas a partir de las observaciones formuladas por los proveedores, quedando definido en la Séptima Versión de las Especificaciones Técnicas de fecha 12.07.2024					
	7	Se realizaron ajustes a las Especificaciones Técnicas a partir de las observaciones formuladas por el OEC, quedando definido en la Octava Versión de las Especificaciones Técnicas de fecha 31.07.2024					
	8	Se realizaron ajustes a las Especificaciones Técnicas a partir de las observaciones formuladas por los proveedores, quedando definido en la Novena Versión de las Especificaciones Técnicas de fecha 26.08.2024					
	9	Se realizaron ajustes a las Especificaciones Técnicas a partir de las observaciones formuladas por los proveedores, quedando definido en la Décima Versión de las Especificaciones Técnicas de fecha 16.09.2024					
	10	Se realizaron ajustes a las Especificaciones Técnicas a partir de las observaciones formuladas por el comité de selección quedando definido en la Undécima Versión de las Especificaciones Técnicas de fecha 20.12.2024					
	11	Se realizaron ajustes a las Especificaciones Técnicas a partir de las observaciones formuladas por el comité de selección, quedando definido en la DecimaSegunda versión de las Especificaciones Técnicas de fecha 13.02.2025 y DecimaTercera versión de las Especificaciones Técnicas de fecha 18.02.2025					
3 INFORMACIÓN RELEVANTE ADICIONAL COMO RESULTADO DE LAS INDAGACIONES EN EL MERCADO							
3.1	FECHA DE INICIO DE LAS INDAGACIONES EN EL MERCADO		25.09.2023		FECHA DE CULMINACIÓN DE LAS INDAGACIONES EN EL MERCADO		03.12.2024
3.2	PLURALIDAD DE PROVEEDORES QUE CUMPLEN CON EL REQUERIMIENTO			SI	X	NO	
De ser negativa la respuesta, indicar la evaluación de la Entidad respecto de la falta de pluralidad de proveedores que cumplen con el requerimiento.							
3.3	PLURALIDAD DE MARCAS QUE CUMPLEN CON EL REQUERIMIENTO			SI	X	NO	
En caso de no existir pluralidad de marcas que cumplen a cabalidad con el requerimiento, indicar aquí la evaluación de la Entidad al respecto.							

RESUMEN EJECUTIVO DE LAS ACTUACIONES PREPARATORIAS (BIENES)					
3.4	POSIBILIDAD DE DISTRIBUIR LA BUENA PRO	SI		NO	X
	En caso de existir la posibilidad de distribuir la buena pro, sustentar.				
3.5	SOBRE LA INFORMACIÓN QUE PUEDA UTILIZARSE PARA LA DETERMINACIÓN DE LOS FACTORES DE EVALUACIÓN	SI		NO	X
	En caso de obtenerse información que se puede utilizar para determinar los factores de evaluación, detallarla.				
3.6	SOBRE OTROS ASPECTOS NECESARIOS QUE TENGAN INCIDENCIA EN LA EFICIENCIA DE LA CONTRATACIÓN	SI		NO	X
	En caso de obtenerse información de otros aspectos que tengan incidencia en la eficiencia de la contratación, detallarla.				
4	Lic. José Antonio Espinal Rodríguez Jefe del Área de Programación y Control de Adquisiciones CORPAC S.A				
	NOMBRE, FIRMA Y SELLO DEL FUNCIONARIO COMPETENTE DEL ÓRGANO ENCARGADO DE LAS CONTRATACIONES				

ANEXO A

ITEM 3 DEL NUMERAL 2.8 OBSERVACIONES AL REQUERIMIENTO

N° de orden	Términos de Referencia		Consulta u Observación	Indicar si corresponde a consulta u observación de las empresas invitadas en la indagación de mercado
	Nu	P		
	me	ág		
	ral	.		
1	2.1	04	<p>Se menciona: Adquisición de Equipos TIC (Switches Core – Distribución y Acceso), Equipamiento TIC para Datacenter, así como el sistema Control de Acceso a la Red, Sistema de automatización, administración y gestión de la Infraestructura de Red, SISTEMAS DE WLAN; con un horizonte de proyección de correcto funcionamiento y operación de Cinco (05) años; contemplando la tecnología actual y emergente.</p> <p>Consulta: Sírvasse confirmar que para poder sustentar este punto se considerará una carta de fabricante que indique que los equipos propuestos no cuenten con anuncio de fin de venta (End-of-sale) al momento de la presentación de la oferta</p>	Consulta ITALTEL
2	2.2	04	<p>Se menciona: Implementación de todo el sistema de Networking, considerando para ellos una configuración detallada de cada uno de los componentes de la red; de WLAN, así como sistema de gestión de la Infraestructura de red. Con un horizonte de proyección de correcto funcionamiento y operación de cinco (05) años; contemplando la tecnología actual y emergente.</p> <p>Consulta: Sírvasse confirmar que para poder sustentar este punto se considerará una carta de fabricante que indique que los equipos propuestos no cuenten con anuncio de fin de venta (End-of-sale) al momento de la presentación de la oferta</p>	Consulta ITALTEL
3	2.3	04	<p>Se menciona: Implementación de Enlaces de Comunicaciones Inalámbricos, con un horizonte de proyección de correcto funcionamiento y operación de cinco (05) años; contemplando la tecnología actual y emergente.</p> <p>Consulta: Sírvasse confirmar que para poder sustentar este punto se considerará una carta de fabricante que indique que los equipos propuestos no cuenten con anuncio de fin de venta (End-of-sale) al momento de la presentación de la oferta</p>	Consulta ITALTEL

4	3.1	04	<p>Se menciona: Renovar el mantenimiento preventivo y correctivo de todo el equipamiento de la presente contratación tanto nuevo y el que se encuentra operando. Este mantenimiento preventivo y correctivo será por un periodo no menor de tres (03) años.</p> <p>Consulta: Sírvasse confirmar que el periodo de tres (03) años se considerará a partir de la fecha en la que el cliente aceptará el acta de conformidad luego de la culminación de la implementación</p>	Consulta ITALTEL
5	3.1	04	<p>Se menciona: Renovar el mantenimiento preventivo y correctivo de todo el equipamiento de la presente contratación tanto nuevo y el que se encuentra operando. Este mantenimiento preventivo y correctivo será por un periodo no menor de tres (03) años.</p> <p>Consulta: Sírvasse confirmar que el mantenimiento preventivo tendría una frecuencia de una (01) vez al año, siendo el alcance del mantenimiento de tipo lógico (revisión de logs, actualización de sistema operativo, y similares)</p>	Consulta ITALTEL
6	5.2 .2. 1.1 .6	32	<p>Se menciona: Debe incluir fuentes de poder redundantes e intercambiables en caliente (Hotswappable)</p> <p>Consulta: Sírvasse indicar el flujo de aire para estos equipos (entrada de aire por los puertos o por los ventiladores)</p>	Consulta ITALTEL
7	5.2 .2. 1.5	37	<p>Se menciona: Debe incluir soporte directo del fabricante en la modalidad 24X7X365. La entidad debe poder abrir casos directamente en el TAC del fabricante. El soporte debe incluir la capacidad de poder descargar nuevos sistemas operativos y upgrade al sistema en su totalidad.</p> <p>Consulta: Sírvasse indicar si el periodo de soporte solicitado será de tres (03) ó cinco (05) años</p>	Consulta ITALTEL
8	5.2 .2. 1.5	37	<p>Se menciona: El licenciamiento debe ser perpetuo desde la aceptación por la puesta en funcionamiento de la solución.</p> <p>Consulta: Con el fin de permitir una mayor pluralidad de postores, sírvase confirmar que será admitido un esquema de licenciamiento en el cual se cuente con un componente de licenciamiento que sea de carácter perpetuo</p>	Consulta ITALTEL
9			Verificar las cantidades de los bienes listados (números y letras) en el numeral 5.2.2.1.1 EQUIPOS DE COMUNICACIONES TIPO CORE, DISTRIBUCION, ACCESO, DATACENTER; en adelante.	Observación OEC
10	6. RE QU ISI TO S Y RE CU RS OS DE L PR OV EE	11 4	<p>Se debe adecuar lo siguiente:</p> <p>El postor deberá acreditar ser distribuidor o Partner autorizado del fabricante de los equipos ofertados, para tal fin debe presentar carta original del fabricante con referencia o dirigida al proceso en mención o en su defecto la impresión del link público del fabricante donde se evidencie que es distribuidor o Partner autorizado.</p> <p>Se debe indicar que el postor ganador de la buena pro, para la firma de contrato presentará ser distribuidor o partner autorizado del fabricante...</p>	Observación OEC

	DO R			
11	6. RE QU ISI TO S Y RE CU RS OS DE L PR OV EE DO R	11 4	<p>El párrafo siguiente:</p> <p>El postor deberá acreditar un monto facturado acumulado equivalente a una vez el valor estimado de la presente contratación, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran servicios similares a: Servicios de Implementación y/o Renovación de Redes de Voz y/o Datos, Servicios de Telecomunicaciones o Redes Corporativas (Enlaces), Implementación de Centros de Datos, Servicios de Cableado Estructurado, Gestión de Redes Corporativas, Implementación de Cableado estructurado, Implementación de Red de Datos o Switches e Implementación de Red de Voz, Telefonía IP o Comunicaciones Unificadas, Servicio de Mesa de Ayuda o Mesa de Ayuda, Soporte de Comunicaciones, Gestión de Activos de TI, Servicios de Red LAN (Instalación e Implementación de: Cableado Estructurado o Equipos de Networking), Servicio de Arrendamiento de Equipos de Comunicaciones de Networking, alquiler y/o arrendamiento y/o renting de equipamiento informático, instalación y/o configuración de redes de fibra óptica, acondicionamiento de cuarto de telecomunicaciones, instalación y/o configuración de gabinetes, Servicio de Centro de Datos y Comunicaciones, Servicios de Gestión de Servicios de TI, Servicios de Mesa de Administración de Servicios TI.</p> <p>Se debe retirar de las EETT, e insertar en requisitos de calificación. Por otro lado en requisitos de calificación, se debe adecuar a bienes similares.</p>	Observación OEC
12	6. RE QU ISI TO S Y RE CU RS OS DE L PR OV EE DO R	11 5	<p>Eliminar lo siguiente:</p> <p>La experiencia exigida deberá acreditarse mediante 2 copias simple de contratos o constancias o certificados o cualquier otra documentación que, de manera fehaciente demuestre la experiencia por la implementación y prestación de este servicio o mediante comprobantes de pago cuya cancelación acredite documental y fehacientemente a través de vouchers de depósito, reporte de estado de cuenta o que la cancelación conste en el mismo documento.</p>	Observación OEC
13		11 7	<p>Deberá adecuar el momento de presentación de la documentación del perfil del personal clave (para firma de contrato), salvo lo relacionado a la experiencia del personal clave que será al momento de la presentación de ofertas como lo estipula los requisitos de calificación.</p> <p>Asimismo, tener en cuenta lo siguiente:</p> <ul style="list-style-type: none">- La colegiatura y habilitación será exigida para el inicio efectivo del servicio; por otro lado deberá indicar su despacho, desde cuando se contabiliza la experiencia laboral si desde la colegiatura o partir desde la obtención del título o bachiller según corresponda para cada perfil.- Sólo se debe requerir el tiempo de experiencia mínimo en la actividad requerida del personal clave requerido conforme al cargo o denominación de la posición que ocupará el personal clave requerido para ejecutar la prestación objeto de la convocatoria.- La experiencia se calcula por el tiempo de experiencia y no por la cantidad de proyectos participados.	Observación OEC
14			<p>A fin de facilitar la supervisión de la ejecución del requerimiento, se solicita al área usuaria resumir en un cuadro todas las actividades, entregables y plazos previstos en las especificaciones técnicas</p>	Observación OEC

15			Subcontratación Indicar en las EETT, si procede la subcontratación en el presente requerimiento.	Observación OEC
16	5.2 .2. 1.1 .1	15	Se pide "Debe tener mínimo una memoria RAM de 16GB " Al respecto se entrega 16 GB, de forma agrupada mediante 2 Tarjetas de control de 8GB. Sirvase a confirmar se aceptarán 2 tarjetas de 8GB.	INGECORP
17	5.2 .2. 1.1 .1	15	Se pide "Debe tener mínimo una memoria Flash de 16GB " Al respecto, el almacenamiento propuesto por cada fabricante varía de acuerdo a la capacidad o tamaños de su sistema operativo y configuraciones, es decir no es indispensable contar con una memoria Flash elevada si el sistema esta correctamente estructurado por cada fabricante, definiendo capacidades óptimas para su propio sistema operativo y configuraciones almacenadas. Por lo tanto, sírvase a confirmar se aceptaran memoria Flash mínima de 2GB.	INGECORP
18	5.2 .2. 1.1 .1	15	Se pide "Cada Switch Core debe incluir 8 transceivers de 100Gbps (SFP28) para fibra óptica monomodo de 10Km para la conexión con el Border Node (Switch Core) y Distribución y switches ToR ubicados en el DC. Asimismo, 1 transceivers de 10Gbps para interconexión entre Cores". Al respecto, sírvase a confirmar se aceptarán soluciones similares o superiores a 10Gbps para la interconexion entre cores.	INGECORP
19	5.2 .2. 1.1 .1	15	Se pide "Contar con puerto serial de consola o puerto USB para gestión" Sírvase a confirmar se aceptarán modos de gestión similares: Contar con puerto serial de consola o puerto USB para gestión o puerto RJ45 consola.	INGECORP
20	5.2 .2. 1.1 .1	15	Se pide "Debe tener 32 puertos de red 40/100G (QSFP/QSFP28) como mínimo ". Al respecto se pide que se soporte 32 puertos de 40/100G, de los cuales solo se usarán 8 transceiver de 100G. Esto implica que, según el diseño actual, existe un exceso de capacidad en términos de puertos de alta velocidad. Además, es relevante considerar la eficiencia y el costo del diseño. Tener 32 puertos de 100G cuando solo se utilizarán 8 implica una inversión innecesaria en recursos de red de alto rendimiento. Además, esto puede tener un impacto en el presupuesto y el consumo energético, ya que la energía requerida para mantener 32 puertos de 100G operativos es significativamente mayor que para 8 puertos. Por lo tanto, sírvase a confirmar que el Switch de core debe ser capaz de soportar al menos 24 puertos de 100G. Esta cantidad permitirá cubrir las necesidades actuales y futuras de la red, sin incurrir en una inversión excesiva en recursos	INGECORP
21	5.2 .2. 1.1 .1	15	Se pide "Debe permitir MC-LAG". Al respecto, MC-LAG es una tecnología que permite a múltiples dispositivos de red, como switches, trabajar juntos como un único dispositivo lógico para proporcionar redundancia y alta disponibilidad. El CSS es una configuración en la que múltiples switches se combinan para funcionar como una única unidad lógica. Por lo tanto, la tecnología MC-LAG (Multi-Chassis Link Aggregation Group) y el CSS (Cluster de Switch) son conceptos relacionados que se utilizan en redes empresariales y de centros de datos para mejorar la redundancia y la disponibilidad de la red. En base a lo anterior, sírvase a confirmar se aceptará MC-LAG o CSS.	INGECORP
22	5.2 .2. 1.1 .1	15	Se pide "Debe incluir todos los componentes necesarios para realizar el stacking virtual " Al respecto, Tanto el stacking virtual como el CSS Cluster de Switch tienen como objetivo principal crear una entidad lógica única a partir de múltiples switches físicos. Ambas tecnologías permiten la administración y configuración simplificadas de los switches, lo que mejora la eficiencia operativa y la disponibilidad de la red. Por lo tanto, sírvase a confirmar se aceptará una solución equivalente a stacking virtual mediante CSS.	INGECORP

23	5.2 .2 1.1 .1	15	<p>Se pide "Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow, SPAN, ERSPAN".</p> <p>Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sírvase a confirmar en el requerimiento: Netflow o sFlow o similares.</p> <p>Además, se pide soportar ERSPAN que es una tecnología que permite la copia y el envío de tráfico de red desde una interfaz o varias interfaces de red en un switch a un dispositivo de análisis remoto a través de una red IP. Sírvase a confirmar se aceptarán tecnologías similares con SPAN, RSPAN o ERSPAN.</p>	INGECORP
24	5.2 .2 1.1 .1	16	<p>Se pide "Debe ser máximo de 1 Rack Unit (RU) "</p> <p>Debido a la cantidad de puertos de alto rendimiento (100G) el Switch debe contar con altas capacidades de reenvío siendo superior, sírvase a confirmar que aceptará capacidades entre 1 (RU) y 10 (RU).</p>	INGECORP
25	5.2 .2 1.1 .1	16	<p>Se pide "Debe incluir los componentes necesarios para su instalación en rack de 19". "</p> <p>Debido a la cantidad de puertos de alto rendimiento (100G) el Switch debe contar con altas capacidades de reenvío siendo superior, sírvase a confirmar que aceptará capacidades entre 19". o 1 (RU) y 10 (RU).</p>	INGECORP
26	5.2 .2 1.1 .1	16	<p>Se pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)"</p> <p>En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo, y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque de flash seguro, para asegurar la integridad y autenticidad de nuestro hardware y software. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras necesidades específicas.</p> <p>Por lo tanto, sírvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque de flash seguro.</p>	INGECORP
27	5.2 .2 1.1 .1	16	<p>Se pide "TACACS+"</p> <p>TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS.</p> <p>Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS</p>	INGECORP
28	5.2 .2 1.1 .1	16	<p>Se pide "RADSec"</p> <p>RadSec es un protocolo de seguridad que se utiliza para asegurar las comunicaciones entre servidores RADIUS (Remote Authentication Dial-In User Service) y clientes, garantizando la confidencialidad e integridad de los datos transmitidos. Esta tecnología es fundamental en entornos de autenticación y autorización de usuarios, especialmente en redes donde la seguridad es una prioridad.</p> <p>Al respecto, en el mercado existen distintas soluciones similares a Radsec como la verificación de seguridad por parte del servidor RADIUS a los usuarios que utilizan el protocolo Extensible Authentication Protocol over LAN (EAPoL). Esta información tiene como objetivo notificar a los usuarios acerca de los elementos que requieren verificaciones de seguridad adicionales, garantizando así que estén plenamente informados y conscientes de las medidas de seguridad aplicadas en nuestra red.</p> <p>Por lo tanto, sírvase a confirmar se aceptará soluciones RADSec o similar.</p>	INGECORP

29	5.2 .2 1.1 .1	16	<p>Se pide "CoPP (Control Plane Policy)"</p> <p>El CoPP (Cisco) utiliza filtros de acceso para limitar el tráfico que se dirige al plano de control, lo que ayuda a prevenir la saturación y los ataques de denegación de servicio contra el dispositivo.</p> <p>El equipo propuesto ofrece características de seguridad similares como la autenticación de usuario y la protección contra ataques de inundación, (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, Defense Against Fragmentation Attacks, Defense Against TCP SYN Flood Packets, Defense Against UDP Flood Attacks, Defense Against ICMP Flood Attacks).</p> <p>Por lo tanto, aunque el CoPP es una función específica de los dispositivos Cisco, los switches propuestos ofrecen características de seguridad similares que protegen el dispositivo contra ataques malintencionados y garantizar que el tráfico importante tenga prioridad sobre otros tipos de tráfico.</p> <p>En conclusión, sirvase a confirmar se aceptará CoPP o características de seguridad similares como (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, etc).</p>	INGECORP
30	5.2 .2 1.1 .1	16	<p>Se pide "Root Guard"</p> <p>Al respecto, se debe tener en cuenta que existen fabricantes en el mercado que denominan de otra forma a estas funcionalidades. Por ejemplo, a "STP root guard" también se le denomina "Root protection".</p> <p>Por tanto, se sugiere respetuosamente a la entidad considerar qu en el requerimiento se solicite Root Guard o equivalente.</p>	INGECORP
31	5.2 .2 1.1 .1	16	<p>Se pide "Private VLAN"</p> <p>(Private VLAN) es una tecnología que permite segmentar un VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos.</p> <p>Se provee lo mismo mediante Super-VLAN (S-VLAN). Al igual que PVLAN, S-VLAN permite segmentar una VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos para mejorar la seguridad y el aislamiento entre dispositivos y usuarios en una misma red.</p> <p>Por lo tanto, sirvase a confirmar que se aceptará Private VLAN o similar.</p>	INGECORP
32	5.2 .2 1.1 .1	18	<p>Se pide "Deberá contar con mecanismos de seguridad de IPv6 First-Hop".</p> <p>IPv6 First-Hop, es una función de seguridad que se utiliza para proteger el tráfico de IPv6 , como los enlaces Ethernet. Esta función se utiliza para proteger contra amenazas como los ataques de spoofing y los ataques de inundación.</p> <p>Se provee lo mismo, la función equivalente a IPv6 First Hop Security de Cisco se conoce como IPv6 Secure Neighbor Discovery (SEND). Esta función se utiliza para proteger el tráfico de IPv6 en los enlaces de capa 2, como los enlaces Ethernet. La función utiliza una combinación de autenticación, criptografía y verificación de estado para asegurar que los dispositivos de la red puedan confiar en los mensajes de descubrimiento de vecinos IPv6 que se intercambian en la capa 2.</p> <p>Por lo tanto, se entrega la misma función, sirvase a confirmar se aceptará IPv6 First-Hop o IPv6 Secure Neighbor Discovery.</p>	INGECORP
33	5.2 .2 1.1 .1	18	<p>Se pide "Deberá contar con mecanismos para garantizar que el sistema operativo sea íntegro y consistente en todos los switches".</p> <p>Al respecto, para cumplir con el siguiente requisito existen distintas formas de garantizar esta seguridad. Para mantener la seguridad y la coherencia en nuestra infraestructura de red, existen sluciones equivalente como el arranque de flash seguro.</p> <p>Por lo tanto, srivase a confirmar se aceptará: "Deberá contar con mecanismos para garantizar que el sistema operativo sea íntegro y consistente en todos los switches o arranque seguro de flash".</p>	INGECORP
34	5.2 .2	18	<p>Se pide: "Deberá contar con mecanismos que prevengan ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos".</p>	INGECORP

1.1 .1		<p>Al respecto, el requisito de "Deberá contar con mecanismos que prevengan ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos" guarda una similitud fundamental con la implementación de un "arranque de flash seguro". Ambos objetivos se centran en salvaguardar la autenticidad e integridad del software o firmware en nuestros equipos. Al implementar un "arranque de flash seguro," establecemos una barrera efectiva contra posibles ataques de intermediarios maliciosos, ya que garantiza que el software o firmware se inicie desde una fuente confiable y que no haya sido comprometido durante el proceso de inicio. En esencia, ambas medidas buscan prevenir manipulaciones no autorizadas del software/firmware y garantizar que los equipos se ejecuten con la autenticidad e integridad necesarias para mantener la seguridad de nuestra infraestructura de red.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "Deberá contar con mecanismos que prevengan ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos o arranque seguro de flash".</p>	
35	5.2 .2 1.1 .1	<p>Se pide "El Switch propuesto deberá soportar funcionalidades que ayuden a identificar amenazas o anomalías en la red incluso descubrimiento malware en el tráfico cifrado".</p> <p>Al respecto, lo anterior es similar a la capacidad de soportar "firmas digitales y certificados." Ambos enfoques tienen como objetivo principal fortalecer la seguridad de la red y detectar posibles amenazas, incluyendo aquellas que pueden ocultarse en el tráfico cifrado.</p> <p>La implementación de firmas digitales y certificados es un mecanismo efectivo para verificar la autenticidad y la integridad de los datos en la red. Al verificar las firmas digitales de los datos y utilizar certificados para autenticar la identidad de los dispositivos y usuarios, podemos asegurar que la información transmitida no ha sido alterada y proviene de fuentes confiables.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "El Switch propuesto deberá soportar funcionalidades que ayuden a identificar amenazas o anomalías en la red incluso descubrimiento malware en el tráfico cifrado o arranque seguro de flash".</p>	INGECORP
36	5.2 .2 1.1 .1	<p>Se pide "Debe soportar e implementar mecanismos de encolamiento Shaped Round Robin (SRR) y Committed Information Rate (CIR)".</p> <p>Debido a que existen funciones similares: Al respecto, la tecnología "Shaped Round Robin (SRR)" y el soporte para "Weighted Round Robin (WRR)" son dos enfoques similares utilizados en la gestión del tráfico de red en switches y routers. Aunque no son idénticos en su funcionamiento, comparten similitudes fundamentales en términos de asignación de prioridad y equidad en la distribución del tráfico.</p> <p>Tanto SRR como WRR se centran en la programación de cómo se maneja el tráfico en una cola de salida del dispositivo de red. SRR, en particular, se utiliza para asignar un peso o una prioridad a cada flujo de tráfico en la cola y determinar cómo se atienden estos flujos en función de su peso o prioridad. Por otro lado, WRR asigna pesos específicos a diferentes flujos de tráfico y distribuye el ancho de banda disponible en función de estos pesos, lo que le permite otorgar prioridad a ciertos flujos sobre otros.</p> <p>Por lo tanto sirvase a confirmar se aceptará: "Debe soportar e implementar mecanismos de encolamiento Shaped Round Robin (SRR) o WRR, y Committed Information Rate (CIR)"</p>	INGECORP
37	5.2 .2 1.1 .1	<p>Se pide "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo".</p> <p>Al respecto, el requisito de incluir una etiqueta RFID (RFID Tag) en el switch propuesto, ya sea interna o externa, tiene un propósito específico que no está directamente relacionado con el funcionamiento de la red en sí. En lugar de sumar a la funcionalidad de la red, se centra en aspectos relacionados con la administración y el mantenimiento de los equipos de red. La inclusión de una etiqueta RFID tiene más que ver con la gestión y la identificación eficiente de los dispositivos que conforman la red.</p> <p>Por lo anterior, sirvase a confirmar esta característica será considerada como opcional:</p>	INGECORP

			"El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo u opcional".	
38	5.2 .2 1.1 .1	18	Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sirvase a confirmar en el requerimiento: Netflow o sFlow o similares.	INGECORP
39	5.2 .2 1.1 .1	18	Se pide "802.1v". IEEE 802.1v se relaciona con la etiqueta de VLAN IEEE 802.1v, que agrega información de prioridad de 802.1p a las tramas Ethernet etiquetadas con VLAN. Esta etiqueta se utiliza en las redes VLAN para mantener la calidad de servicio (QoS) incluso cuando el tráfico viaja a través de enlaces troncales que conectan diferentes switches. IEEE 802.1p: Este estándar se refiere a la asignación de prioridades a los paquetes Ethernet en función de los bits de prioridad contenidos en la cabecera de los paquetes. IEEE 802.1p permite la clasificación y la priorización del tráfico en diferentes clases de servicio, lo que garantiza que los paquetes críticos, como voz o video, reciban un trato preferencial en la red. Al respecto, El estándar IEEE 802.1v y la característica IEEE 802.1p están estrechamente relacionados en el contexto de la gestión de calidad de servicio (QoS) en redes Ethernet y VLAN (Virtual LAN). Por lo tanto, sirvase a confirmar se aceptará: "IEEE 802.1v o 802.1p".	INGECORP
40	5.2 .2 1.1 .2	19	Se pide "Debe tener mínimo una memoria RAM de 16GB " Al respecto se entrega 16 GB, de forma agrupada mediante 2 Tarjetas de control de 8GB. Sirvase a confirmar se aceptarán 2 tarjetas de 8GB.	INGECORP
41	5.2 .2 1.1 .2	19	Se pide "Debe tener mínimo una memoria Flash de 16GB " Al respecto, el almacenamiento propuesto por cada fabricante varía de acuerdo a la capacidad o tamaños de su sistema operativo y configuraciones, es decir no es indispensable contar con una memoria Flash elevada si el sistema está correctamente estructurado por cada fabricante, definiendo capacidades óptimas para su propio sistema operativo y configuraciones almacenadas. Por lo tanto sirvase a confirmar se aceptaran memoria Flash mínima de 2GB.	INGECORP
42	5.2 .2 1.1 .2	20	Se pide "Debe permitir MC-LAG". Al respecto, MC-LAG es una tecnología que permite a múltiples dispositivos de red, como switches, trabajar juntos como un único dispositivo lógico para proporcionar redundancia y alta disponibilidad. El CSS es una configuración en la que múltiples switches se combinan para funcionar como una única unidad lógica. Por lo tanto, la tecnología MC-LAG (Multi-Chassis Link Aggregation Group) y el CSS (Cluster de Switch) son conceptos relacionados que se utilizan en redes empresariales y de centros de datos para mejorar la redundancia y la disponibilidad de la red. En base a lo anterior, sirvase a confirmar se aceptará MC-LAG o CSS.	INGECORP
43	5.2 .2 1.1 .2	20	Se pide "Debe incluir todos los componentes necesarios para realizar el stacking virtual " Al respecto, Tanto el stacking virtual como el CSS Cluster de Switch tienen como objetivo principal crear una entidad lógica única a partir de múltiples switches físicos. Ambas tecnologías permiten la administración y configuración simplificadas de los switches, lo que mejora la eficiencia operativa y la disponibilidad de la red. Por lo tanto, sirvase a confirmar se aceptará una solución equivalente a stacking virtual mediante CSS.	INGECORP
44	5.2 .2 1.1 .2	21	Se pide "Debe permitir no menos de 27000 entradas ACL ". El número de ACL (Listas de Control de Acceso) en un switch de distribución, en este caso, 27000 ACL, no necesariamente es determinante para su funcionamiento eficaz en esa ubicación específica dentro de la red. Los switches de distribución a menudo se utilizan para gestionar y enrutar el tráfico entre VLANs y para aplicar	INGECORP

		<p>políticas de seguridad y control de acceso en la red. La cantidad de ACL requerida dependerá de la complejidad y las necesidades específicas de la red.</p> <p>En el contexto de la solicitud, es importante señalar que la cantidad de ACL solicitada para el switch core fue de 4000 ACL, lo que indica que esta cifra se consideró adecuada para las operaciones de toda la red. Sin embargo, es posible que en los switches de distribución no sea necesario un número tan elevado de ACL debido a su ubicación y función en la topología de red.</p> <p>En base a lo anterior, sirvase a confirmar se aceptará como mínimo 4000 ACL.</p>	
45	5.2 .2 1.1 .2	21 <p>Se pide "Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow, SPAN, ERSPAN".</p> <p>Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sirvase a confirmar en el requerimiento: Netflow o sFlow o similares.</p> <p>Además, se pide soportar ERSPAN que es una tecnología que permite la copia y el envío de tráfico de red desde una interfaz o varias interfaces de red en un switch a un dispositivo de análisis remoto a través de una red IP. Sirvase a confirmar se aceptarán tecnologías similares con SPAN, RSPAN o ERSPAN.</p>	INGECORP
46	5.2 .2 1.1 .2	21 <p>Se pide "Debe ser máximo de 1 Rack Unit (RU) "</p> <p>Debido a la cantidad de puertos de alto rendimiento (100G) el Switch debe contar con altas capacidades de reenvío siendo superior, sirvase a confirmar que aceptará capacidades entre 1 (RU) y 10 (RU).</p>	INGECORP
47	5.2 .2 1.1 .2	21 <p>Se pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)"</p> <p>En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo, y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque de flash seguro, para asegurar la integridad y autenticidad de nuestro hardware y software. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras necesidades específicas.</p> <p>Por lo tanto sirvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque de flash seguro.</p>	INGECORP
48	5.2 .2 1.1 .2	21 <p>Se pide "TACACS+"</p> <p>TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS.</p> <p>Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS</p>	INGECORP
49	5.2 .2 1.1 .2	21 <p>Se pide "RADSec"</p> <p>RadSec es un protocolo de seguridad que se utiliza para asegurar las comunicaciones entre servidores RADIUS (Remote Authentication Dial-In User Service) y clientes, garantizando la confidencialidad e integridad de los datos transmitidos. Esta tecnología es fundamental en entornos de autenticación y autorización de usuarios, especialmente en redes donde la seguridad es una prioridad.</p> <p>Al respecto, en el mercado existen distintas soluciones similares a Radsec como la verificación de seguridad por parte del servidor RADIUS a los usuarios que utilizan el protocolo Extensible Authentication Protocol over LAN (EAPoL). Esta información tiene como objetivo notificar a los usuarios acerca de los elementos que requieren verificaciones de seguridad adicionales, garantizando así que estén plenamente informados y conscientes de las medidas de seguridad aplicadas en nuestra red.</p>	INGECORP

			Por lo tanto, sirvase a confirmar se aceptará soluciones RADSec o similar.	
50	5.2 .2 1.1 .2	21	<p>Se pide "CoPP (Control Plane Policy)"</p> <p>El CoPP (Cisco) utiliza filtros de acceso para limitar el tráfico que se dirige al plano de control, lo que ayuda a prevenir la saturación y los ataques de denegación de servicio contra el dispositivo.</p> <p>El equipo propuesto ofrece características de seguridad similares como la autenticación de usuario y la protección contra ataques de inundación, (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, Defense Against Fragmentation Attacks, Defense Against TCP SYN Flood Packets, Defense Against UDP Flood Attacks, Defense Against ICMP Flood Attacks).</p> <p>Por lo tanto, aunque el CoPP es una función específica de los dispositivos Cisco, los switches propuestos ofrecen características de seguridad similares que protegen el dispositivo contra ataques malintencionados y garantizar que el tráfico importante tenga prioridad sobre otros tipos de tráfico.</p> <p>En conclusión, sirvase a confirmar se aceptará CoPP o características de seguridad similares como (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, etc).</p>	INGECORP
51	5.2 .2 1.1 .2	21	<p>Se pide "Root Guard"</p> <p>Al respecto, se debe tener en cuenta que existen fabricantes en el mercado que denominan de otra forma a estas funcionalidades. Por ejemplo, a "STP root guard" también se le denomina "Root protection".</p> <p>Por tanto, se sugiere respetuosamente a la entidad considerar qu en el requerimiento se solicite Root Guard o equivalente.</p>	INGECORP
52	5.2 .2 1.1 .2	21	<p>Se pide "Private VLAN"</p> <p>(Private VLAN) es una tecnología que permite segmentar un VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos.</p> <p>Se provee lo mismo mediante Super-VLAN (S-VLAN). Al igual que PVLAN, S-VLAN permite segmentar una VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos para mejorar la seguridad y el aislamiento entre dispositivos y usuarios en una misma red.</p> <p>Por lo tanto, sirvase a confirmar que se aceptará Private VLAN o similar.</p>	INGECORP
53	5.2 .2 1.1 .2	21	<p>Se pide "Deberá contar con mecanismos de seguridad de IPv6 First-Hop".</p> <p>IPv6 First-Hop, es una función de seguridad que se utiliza para proteger el tráfico de IPv6 , como los enlaces Ethernet. Esta función se utiliza para proteger contra amenazas como los ataques de spoofing y los ataques de inundación.</p> <p>Se provee lo mismo, la función equivalente a IPv6 First Hop Security de Cisco se conoce como IPv6 Secure Neighbor Discovery (SEND). Esta función se utiliza para proteger el tráfico de IPv6 en los enlaces de capa 2, como los enlaces Ethernet. La función utiliza una combinación de autenticación, criptografía y verificación de estado para asegurar que los dispositivos de la red puedan confiar en los mensajes de descubrimiento de vecinos IPv6 que se intercambian en la capa 2.</p> <p>Por lo tanto, se entrega la misma función, sirvase a confirmar se aceptará IPv6 First-Hop o IPv6 Secure Neighbor Discovery.</p>	INGECORP
54	5.2 .2 1.1 .2	22	<p>Se pide "Deberá contar con mecanismos para garantizar que el sistema operativo sea íntegro y consistente en todos los switches".</p> <p>Al respecto, para cumplir con el siguiente requisito existen distintas formas de garantizar esta seguridad. Para mantener la seguridad y la coherencia en nuestra infraestructura de red, existen sluciones equivalente como el arranque de flash seguro.</p> <p>Por lo tanto, srivase a confirmar se aceptará: "Deberá contar con mecanismos para garantizar que el sistema operativo sea íntegro y consistente en todos los switches o arranque seguro de flash".</p>	INGECORP

55	5.2 .2 1.1 .2	22	<p>Se pide: "Deberá contar con mecanismos que prevengan ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos".</p> <p>Al respecto, el requisito de "Deberá contar con mecanismos que prevengan ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos" guarda una similitud fundamental con la implementación de un "arranque de flash seguro". Ambos objetivos se centran en salvaguardar la autenticidad e integridad del software o firmware en nuestros equipos. Al implementar un "arranque de flash seguro," establecemos una barrera efectiva contra posibles ataques de intermediarios maliciosos, ya que garantiza que el software o firmware se inicie desde una fuente confiable y que no haya sido comprometido durante el proceso de inicio. En esencia, ambas medidas buscan prevenir manipulaciones no autorizadas del software/firmware y garantizar que los equipos se ejecuten con la autenticidad e integridad necesarias para mantener la seguridad de nuestra infraestructura de red.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "Deberá contar con mecanismos que prevengan ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos o arranque seguro de flash".</p>	INGECORP
56	5.2 .2 1.1 .2	22	<p>Se pide "El Switch propuesto deberá soportar funcionalidades que ayuden a identificar amenazas o anomalías en la red incluso descubrimiento malware en el tráfico cifrado".</p> <p>Al respecto, lo anterior es similar a la capacidad de soportar "firmas digitales y certificados." Ambos enfoques tienen como objetivo principal fortalecer la seguridad de la red y detectar posibles amenazas, incluyendo aquellas que pueden ocultarse en el tráfico cifrado.</p> <p>La implementación de firmas digitales y certificados es un mecanismo efectivo para verificar la autenticidad y la integridad de los datos en la red. Al verificar las firmas digitales de los datos y utilizar certificados para autenticar la identidad de los dispositivos y usuarios, podemos asegurar que la información transmitida no ha sido alterada y proviene de fuentes confiables.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "El Switch propuesto deberá soportar funcionalidades que ayuden a identificar amenazas o anomalías en la red incluso descubrimiento malware en el tráfico cifrado o arranque seguro de flash".</p>	INGECORP
57	5.2 .2 1.1 .2	22	<p>Se pide "Debe soportar e implementar mecanismos de encolamiento Shaped Round Robin (SRR) y Committed Information Rate (CIR)".</p> <p>Debido a que existen funciones similares: Al respecto, la tecnología "Shaped Round Robin (SRR)" y el soporte para "Weighted Round Robin (WRR)" son dos enfoques similares utilizados en la gestión del tráfico de red en switches y routers. Aunque no son idénticos en su funcionamiento, comparten similitudes fundamentales en términos de asignación de prioridad y equidad en la distribución del tráfico.</p> <p>Tanto SRR como WRR se centran en la programación de cómo se maneja el tráfico en una cola de salida del dispositivo de red. SRR, en particular, se utiliza para asignar un peso o una prioridad a cada flujo de tráfico en la cola y determinar cómo se atienden estos flujos en función de su peso o prioridad. Por otro lado, WRR asigna pesos específicos a diferentes flujos de tráfico y distribuye el ancho de banda disponible en función de estos pesos, lo que le permite otorgar prioridad a ciertos flujos sobre otros.</p> <p>Por lo tanto sirvase a confirmar se aceptará: "Debe soportar e implementar mecanismos de encolamiento Shaped Round Robin (SRR) o WRR, y Committed Information Rate (CIR)"</p>	INGECORP
58	5.2 .2 1.1 .2	23	<p>Se pide "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo".</p> <p>Al respecto, el requisito de incluir una etiqueta RFID (RFID Tag) en el switch propuesto, ya sea interna o externa, tiene un propósito específico que no está directamente relacionado con el funcionamiento de la red en sí. En lugar de sumar a la funcionalidad de la red, se centra en aspectos relacionados con la administración y el mantenimiento de los equipos de red. La inclusión de una etiqueta RFID tiene más que ver con la gestión y la identificación eficiente de los dispositivos que conforman la red.</p>	INGECORP

			<p>Por lo anterior, sirvase a confirmar esta característica será considerada como opcional:</p> <p>"El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo o opcional".</p>	
59	5.2 .2 1.1 .2	23	<p>Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sirvase a confirmar en el requerimiento: Netflow o sFlow o similares.</p>	INGECORP
60	5.2 .2 1.1 .2	23	<p>Se pide "802.1v".</p> <p>IEEE 802.1v se relaciona con la etiqueta de VLAN IEEE 802.1v, que agrega información de prioridad de 802.1p a las tramas Ethernet etiquetadas con VLAN. Esta etiqueta se utiliza en las redes VLAN para mantener la calidad de servicio (QoS) incluso cuando el tráfico viaja a través de enlaces troncales que conectan diferentes switches.</p> <p>IEEE 802.1p: Este estándar se refiere a la asignación de prioridades a los paquetes Ethernet en función de los bits de prioridad contenidos en la cabecera de los paquetes. IEEE 802.1p permite la clasificación y la priorización del tráfico en diferentes clases de servicio, lo que garantiza que los paquetes críticos, como voz o video, reciban un trato preferencial en la red.</p> <p>Al respecto, El estándar IEEE 802.1v y la característica IEEE 802.1p están estrechamente relacionados en el contexto de la gestión de calidad de servicio (QoS) en redes Ethernet y VLAN (Virtual LAN). Por lo tanto, sirvase a confirmar se aceptará: "IEEE 802.1v o 802.1p".</p>	INGECORP
61	5.2 .2 1.1 .3	24	<p>Se pide "El switch propuesto debete tener al menos 8GB de memoria RAM y 16GB de memoria Flash"</p> <p>La capacidad de memoria RAM en un switch será relativa a las características del equipo: por ejemplo, el tamaño del sistema operativo, el tamaño de su configuración, el tamaño de los logs que maneja, entre otros. Si el equipo ha sido diseñado de forma tal que optimice sus recursos, entonces el tamaño de la RAM no necesita ser tan grande.</p> <p>Lo mismo sucederá con la capacidad del Flash. Este será requerido en función de las características del equipo en sí.</p> <p>Por lo anterior, se sugiere respetuosamente a la entidad:</p> <ol style="list-style-type: none"> 1. Solicitar en el switch una capacidad RAM no menor a 4 GB, y 2. Solicitar en el switch una capacidad flash no menor a 2 GB. 	INGECORP
62	5.2 .2 1.1 .3	24	<p>Se pide "El switch propuesto debe soportar contenedores, para segurar máxima flexibilidad y aislamiento del sistema operativo principal.</p> <p>Este enunciado significa que el switch que se está considerando debe ser capaz de trabajar con contenedores de software. Esto es importante para garantizar que la red tenga la mayor flexibilidad posible y para separar de manera efectiva el sistema operativo principal de otros componentes.</p> <p>Al respecto para garantizar este requerimiento muchos fabricantes en el mercado implementan sistemas operativos modular.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "El switch propuesto debe soportar contenedores, para asegurar máxima flexibilidad y aislamiento del sistema operativo principal o contar con un sistema operativo modular"</p>	INGECORP
63	5.2 .2 1.1 .3	24	<p>Se pide "Debe permitir no menos de 8000 entradas ACL"</p> <p>Sirvase a confirmar se aceptará una capacidad de 8000 entradas ACL entre IPv4 y IPv6.</p>	INGECORP
64	5.2 .2 1.1 .3	24	<p>Se pide "El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking."</p> <p>Debido a que muchos fabricantes implenta Stacking de forma lógica o física, sírvase a confirmar que también será válido la realización de stacking atraves de puertos de servicio dedicados para stacking.</p>	INGECORP

65	5.2 .2 1.1 .3	25	<p>Se pide "Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow, SPAN, ERSPAN".</p> <p>Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sirvase a confirmar en el requerimiento: Netflow o sFlow o similares.</p> <p>Además, se pide soportar ERSPAN que es una tecnología que permite la copia y el envío de tráfico de red desde una interfaz o varias interfaces de red en un switch a un dispositivo de análisis remoto a través de una red IP. Sirvase a confirmar se aceptarán tecnologías similares con SPAN, RSPAN o ERSPAN.</p>	INGECORP
66	5.2 .2 1.1 .3	25	<p>Se pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)"</p> <p>En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo, y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque de flash seguro, para asegurar la integridad y autenticidad de nuestro hardware y software. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras necesidades específicas.</p> <p>Por lo tanto, sirvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque de flash seguro.</p>	INGECORP
67	5.2 .2 1.1 .3	25	<p>Se pide "TACACS+"</p> <p>TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS.</p> <p>Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS</p>	INGECORP
68	5.2 .2 1.1 .3	25	<p>Se pide "RADSec"</p> <p>RadSec es un protocolo de seguridad que se utiliza para asegurar las comunicaciones entre servidores RADIUS (Remote Authentication Dial-In User Service) y clientes, garantizando la confidencialidad e integridad de los datos transmitidos. Esta tecnología es fundamental en entornos de autenticación y autorización de usuarios, especialmente en redes donde la seguridad es una prioridad.</p> <p>Al respecto, en el mercado existen distintas soluciones similares a Radsec como la verificación de seguridad por parte del servidor RADIUS a los usuarios que utilizan el protocolo Extensible Authentication Protocol over LAN (EAPoL). Esta información tiene como objetivo notificar a los usuarios acerca de los elementos que requieren verificaciones de seguridad adicionales, garantizando así que estén plenamente informados y conscientes de las medidas de seguridad aplicadas en nuestra red.</p> <p>Por lo tanto, sirvase a confirmar se aceptará soluciones RADSec o similar.</p>	INGECORP
69	5.2 .2 1.1 .3	25	<p>Se pide "CoPP (Control Plane Policy)"</p> <p>El CoPP (Cisco) utiliza filtros de acceso para limitar el tráfico que se dirige al plano de control, lo que ayuda a prevenir la saturación y los ataques de denegación de servicio contra el dispositivo.</p> <p>El equipo propuesto ofrece características de seguridad similares como la autenticación de usuario y la protección contra ataques de inundación, (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, Defense Against Fragmentation Attacks, Defense Against TCP SYN Flood Packets, Defense Against UDP Flood Attacks, Defense Against ICMP Flood Attacks).</p> <p>Por lo tanto, aunque el CoPP es una función específica de los dispositivos Cisco, los switches propuestos ofrecen características de seguridad similares que protegen el dispositivo contra ataques malintencionados y garantizar que el tráfico importante tenga prioridad sobre otros tipos de tráfico.</p>	INGECORP

			En conclusión, sirvase a confirmar se aceptará CoPP o características de seguridad similares como (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, etc).	
70	5.2 .2. 1.1 .3	25	<p>Se pide "Root Guard"</p> <p>Al respecto, se debe tener en cuenta que existen fabricantes en el mercado que denominan de otra forma a estas funcionalidades. Por ejemplo, a "STP root guard" también se le denomina "Root protection". Por tanto, se sugiere respetuosamente a la entidad considerar qu en el requerimiento se solicite Root Guard o equivalente.</p>	INGECORP
71	5.2 .2. 1.1 .3	25	<p>Se pide "Private VLAN"</p> <p>(Private VLAN) es una tecnología que permite segmentar un VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos.</p> <p>Se provee lo mismo mediante Super-VLAN (S-VLAN). Al igual que PVLAN, S-VLAN permite segmentar una VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos para mejorar la seguridad y el aislamiento entre dispositivos y usuarios en una misma red.</p> <p>Por lo tanto, sirvase a confirmar que se aceptará Private VLAN o similar.</p>	INGECORP
72	5.2 .2. 1.1 .3	25	<p>Se pide "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo".</p> <p>Al respecto, el requisito de incluir una etiqueta RFID (RFID Tag) en el switch propuesto, ya sea interna o externa, tiene un propósito específico que no está directamente relacionado con el funcionamiento de la red en sí. En lugar de sumar a la funcionalidad de la red, se centra en aspectos relacionados con la administración y el mantenimiento de los equipos de red. La inclusión de una etiqueta RFID tiene más que ver con la gestión y la identificación eficiente de los dispositivos que conforman la red.</p> <p>Por lo anterio, sirvase a confirar esta característica será considerada como opcional: "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo o opcional".</p>	INGECORP
73	5.2 .2. 1.1 .3	26	<p>Se pide: "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. ".</p> <p>Al respecto, el requisito de "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. " guarda una similitud fundamental con la implementación de un "arranque de flash seguro". Ambos objetivos se centran en salvaguardar la autenticidad e integridad del software o firmware en nuestros equipos. Al implementar un "arranque de flash seguro," establecemos una barrera efectiva contra posibles ataques de intermediarios maliciosos, ya que garantiza que el software o firmware se inicie desde una fuente confiable y que no haya sido comprometido durante el proceso de inicio. En esencia, ambas medidas buscan prevenir manipulaciones no autorizadas del software/firmware y garantizar que los equipos se ejecuten con la autenticidad e integridad necesarias para mantener la seguridad de nuestra infraestructura de red.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software o arranque seguro de flash".</p>	INGECORP

74	5.2 .2. 1.1 .3	26	<p>Se pide "El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware."</p> <p>Al respecto, en el mercado muchos fabricantes realizan este procesamiento de Transmisión de paquetes IPv6 en hardware, implica que el switch tiene la capacidad de procesar y enrutar paquetes IPv6 utilizando recursos de hardware o de manera lógica.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware o de manera lógica"</p>	INGECORP
75	5.2 .2. 1.1 .3	26	<p>Se pide "802.1v".</p> <p>IEEE 802.1v se relaciona con la etiqueta de VLAN IEEE 802.1v, que agrega información de prioridad de 802.1p a las tramas Ethernet etiquetadas con VLAN. Esta etiqueta se utiliza en las redes VLAN para mantener la calidad de servicio (QoS) incluso cuando el tráfico viaja a través de enlaces troncales que conectan diferentes switches.</p> <p>IEEE 802.1p: Este estándar se refiere a la asignación de prioridades a los paquetes Ethernet en función de los bits de prioridad contenidos en la cabecera de los paquetes. IEEE 802.1p permite la clasificación y la priorización del tráfico en diferentes clases de servicio, lo que garantiza que los paquetes críticos, como voz o video, reciban un trato preferencial en la red.</p> <p>Al respecto, El estándar IEEE 802.1v y la característica IEEE 802.1p están estrechamente relacionados en el contexto de la gestión de calidad de servicio (QoS) en redes Ethernet y VLAN (Virtual LAN). Por lo tanto, sirvase a confirmar se aceptará: "IEEE 802.1v o 802.1p".</p>	INGECORP
76	5.2 .2. 1.1 .4	27	<p>Se pide "El switch propuesto debete tener al menos 8GB de memoria RAM y 16GB de memoria Flash"</p> <p>La capacidad de memoria RAM en un switch será relativa a las características del equipo: por ejemplo, el tamaño del sistema operativo, el tamaño de su configuración, el tamaño de los logs que maneja, entre otros. Si el equipo ha sido diseñado de forma tal que optimice sus recursos, entonces el tamaño de la RAM no necesita ser tan grande.</p> <p>Lo mismo sucederá con la capacidad del Flash. Este será requerido en función de las características del equipo en sí.</p> <p>Por lo anterior, se sugiere respetuosamente a la entidad:</p> <ol style="list-style-type: none"> 1. Solicitar en el switch una capacidad RAM no menor a 4 GB, y 2. Solicitar en el switch una capacidad flash no menor a 2 GB. 	INGECORP
77	5.2 .2. 1.1 .4	27	<p>Se pide "El switch propuesto debe soportar contenedores, para segurar máxima flexibilidad y aislamiento del sistema operativo principal.</p> <p>Este enunciado significa que el switch que se está considerando debe ser capaz de trabajar con contenedores de software. Esto es importante para garantizar que la red tenga la mayor flexibilidad posible y para separar de manera efectiva el sistema operativo principal de otros componentes.</p> <p>Al respecto para garantizar este requerimiento muchos fabricantes en el mercado implementan sistemas operativos modular.</p> <p>Por lo tanto, sírvase a confirmar se aceptará: "El switch propuesto debe soportar contenedores, para asegurar máxima flexibilidad y aislamiento del sistema operativo principal o contar con un sistema operativo modular"</p>	INGECORP
78	5.2 .2. 1.1 .4	27	<p>Se pide "Debe permitir no menos de 8000 entradas ACL"</p> <p>Sírvase a confirmar se aceptará una capacidad de 8000 entradas ACL entre IPv4 y IPv6.</p>	INGECORP
79	5.2 .2. 1.1 .4	27	<p>Se pide "El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking."</p> <p>Debido a que muchos fabricantes implenta Stacking de forma logica o fisica, sirvase a confirmar que también será válido la realización de stacking atraves de puertos de servicio dedicados para stacking.</p>	INGECORP

80	5.2 .2 1.1 .4	<p>Se pide "Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow, SPAN, ERSPAN".</p> <p>Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sirvase a confirmar en el requerimiento: Netflow o sFlow o similares.</p> <p>Además, se pide soportar ERSPAN que es una tecnología que permite la copia y el envío de tráfico de red desde una interfaz o varias interfaces de red en un switch a un dispositivo de análisis remoto a través de una red IP. Sirvase a confirmar se aceptarán tecnologías similares con SPAN, RSPAN o ERSPAN.</p>	INGECORP
81	5.2 .2 1.1 .4	<p>Se pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)"</p> <p>En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo, y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque de flash seguro, para asegurar la integridad y autenticidad de nuestro hardware y software. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras necesidades específicas.</p> <p>Por lo tanto, sirvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque de flash seguro.</p>	INGECORP
82	5.2 .2 1.1 .4	<p>Se pide "TACACS+"</p> <p>TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS.</p> <p>Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS</p>	INGECORP
83	5.2 .2 1.1 .4	<p>Se pide "RADSec"</p> <p>RadSec es un protocolo de seguridad que se utiliza para asegurar las comunicaciones entre servidores RADIUS (Remote Authentication Dial-In User Service) y clientes, garantizando la confidencialidad e integridad de los datos transmitidos. Esta tecnología es fundamental en entornos de autenticación y autorización de usuarios, especialmente en redes donde la seguridad es una prioridad.</p> <p>Al respecto, en el mercado existen distintas soluciones similares a Radsec como la verificación de seguridad por parte del servidor RADIUS a los usuarios que utilizan el protocolo Extensible Authentication Protocol over LAN (EAPoL). Esta información tiene como objetivo notificar a los usuarios acerca de los elementos que requieren verificaciones de seguridad adicionales, garantizando así que estén plenamente informados y conscientes de las medidas de seguridad aplicadas en nuestra red.</p> <p>Por lo tanto, sirvase a confirmar se aceptará soluciones RADSec o similar.</p>	INGECORP
84	5.2 .2 1.1 .4	<p>Se pide "CoPP (Control Plane Policy)"</p> <p>El CoPP (Cisco) utiliza filtros de acceso para limitar el tráfico que se dirige al plano de control, lo que ayuda a prevenir la saturación y los ataques de denegación de servicio contra el dispositivo.</p> <p>El equipo propuesto ofrece características de seguridad similares como la autenticación de usuario y la protección contra ataques de inundación, (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, Defense Against Fragmentation Attacks, Defense Against TCP SYN Flood Packets, Defense Against UDP Flood Attacks, Defense Against ICMP Flood Attacks).</p> <p>Por lo tanto, aunque el CoPP es una función específica de los dispositivos Cisco, los switches propuestos ofrecen características de seguridad similares que protegen el dispositivo contra ataques malintencionados y garantizar que el tráfico importante tenga prioridad sobre otros tipos de tráfico.</p>	INGECORP

			En conclusión, sirvase a confirmar se aceptará CoPP o características de seguridad similares como (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, etc).	
85	5.2 .2. 1.1 .4	28	<p>Se pide "Root Guard"</p> <p>Al respecto, se debe tener en cuenta que existen fabricantes en el mercado que denominan de otra forma a estas funcionalidades. Por ejemplo, a "STP root guard" también se le denomina "Root protection". Por tanto, se sugiere respetuosamente a la entidad considerar qu en el requerimiento se solicite Root Guard o equivalente.</p>	INGECORP
86	5.2 .2. 1.1 .4	28	<p>Se pide "Private VLAN"</p> <p>(Private VLAN) es una tecnología que permite segmentar un VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos.</p> <p>Se provee lo mismo mediante Super-VLAN (S-VLAN). Al igual que PVLAN, S-VLAN permite segmentar una VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos para mejorar la seguridad y el aislamiento entre dispositivos y usuarios en una misma red.</p> <p>Por lo tanto, sirvase a confirmar que se aceptará Private VLAN o similar.</p>	INGECORP
87	5.2 .2. 1.1 .4	28	<p>Se pide "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo".</p> <p>Al respecto, el requisito de incluir una etiqueta RFID (RFID Tag) en el switch propuesto, ya sea interna o externa, tiene un propósito específico que no está directamente relacionado con el funcionamiento de la red en sí. En lugar de sumar a la funcionalidad de la red, se centra en aspectos relacionados con la administración y el mantenimiento de los equipos de red. La inclusión de una etiqueta RFID tiene más que ver con la gestión y la identificación eficiente de los dispositivos que conforman la red.</p> <p>Por lo anterior, sirvase a confimar esta característica será considerada como opcional: "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo o opcional".</p>	INGECORP
88	5.2 .2. 1.1 .4		<p>Se pide: "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. ".</p> <p>Al respecto, el requisito de "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. " guarda una similitud fundamental con la implementación de un "arranque de flash seguro". Ambos objetivos se centran en salvaguardar la autenticidad e integridad del software o firmware en nuestros equipos. Al implementar un "arranque de flash seguro," establecemos una barrera efectiva contra posibles ataques de intermediarios maliciosos, ya que garantiza que el software o firmware se inicie desde una fuente confiable y que no haya sido comprometido durante el proceso de inicio. En esencia, ambas medidas buscan prevenir manipulaciones no autorizadas del software/firmware y garantizar que los equipos se ejecuten con la autenticidad e integridad necesarias para mantener la seguridad de nuestra infraestructura de red.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software o arranque seguro de flash".</p>	INGECORP

89	5.2 .2 1.1 .4	29	<p>Se pide "El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware."</p> <p>Al respecto, en el mercado muchos fabricantes realizan este procesamiento de Transmisión de paquetes IPv6 en hardware, implica que el switch tiene la capacidad de procesar y enrutar paquetes IPv6 utilizando recursos de hardware o de manera lógica.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware o de manera lógica"</p>	INGECORP
90	5.2 .2 1.1 .4	29	<p>Se pide "802.1v".</p> <p>IEEE 802.1v se relaciona con la etiqueta de VLAN IEEE 802.1v, que agrega información de prioridad de 802.1p a las tramas Ethernet etiquetadas con VLAN. Esta etiqueta se utiliza en las redes VLAN para mantener la calidad de servicio (QoS) incluso cuando el tráfico viaja a través de enlaces troncales que conectan diferentes switches.</p> <p>IEEE 802.1p: Este estándar se refiere a la asignación de prioridades a los paquetes Ethernet en función de los bits de prioridad contenidos en la cabecera de los paquetes. IEEE 802.1p permite la clasificación y la priorización del tráfico en diferentes clases de servicio, lo que garantiza que los paquetes críticos, como voz o video, reciban un trato preferencial en la red.</p> <p>Al respecto, El estándar IEEE 802.1v y la característica IEEE 802.1p están estrechamente relacionados en el contexto de la gestión de calidad de servicio (QoS) en redes Ethernet y VLAN (Virtual LAN). Por lo tanto, sirvase a confirmar se aceptará: "IEEE 802.1v o 802.1p"</p>	INGECORP
91	5.2 .2 1.1 .5	30	<p>Se pide "El switch propuesto debete tener al menos 8GB de memoria RAM y 16GB de memoria Flash"</p> <p>La capacidad de memoria RAM en un switch será relativa a las características del equipo: por ejemplo, el tamaño del sistema operativo, el tamaño de su configuración, el tamaño de los logs que maneja, entre otros. Si el equipo ha sido diseñado de forma tal que optimice sus recursos, entonces el tamaño de la RAM no necesita ser tan grande.</p> <p>Lo mismo sucederá con la capacidad del Flash. Este será requerido en función de las características del equipo en sí.</p> <p>Por lo anterior, se sugiere respetuosamente a la entidad:</p> <ol style="list-style-type: none"> 1. Solicitar en el switch una capacidad RAM no menor a 4 GB, y 2. Solicitar en el switch una capacidad flash no menor a 2 GB. 	INGECORP
92	5.2 .2 1.1 .5	30	<p>Se pide "El switch propuesto debe soportar contenedores, para segurar máxima flexibilidad y aislamiento del sistema operativo principal.</p> <p>Este enunciado significa que el switch que se está considerando debe ser capaz de trabajar con contenedores de software. Esto es importante para garantizar que la red tenga la mayor flexibilidad posible y para separar de manera efectiva el sistema operativo principal de otros componentes.</p> <p>Al respecto para garantizar este requerimiento muchos fabricantes en el mercado implementan sistemas operativos modular.</p> <p>Por lo tanto sirvase a confirmar se aceptará: "El switch propuesto debe soportar contenedores, para asegurar máxima flexibilidad y aislamiento del sistema operativo principal o contar con un sistema operativo modular"</p>	INGECORP
93	5.2 .2 1.1 .5	30	<p>Se pide "Debe permitir no menos de 8000 entradas ACL"</p> <p>Sirvase a confirmar se aceptará una capacidad de 8000 entradas ACL entre IPv4 y IPv6.</p>	INGECORP
94	5.2 .2 1.1 .5	30	<p>Se pide "El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking."</p> <p>Debido a que muchos fabricantes implenta Stacking de forma logica o fisica, sirvase a confirmar que también será válido la realización de stacking atraves de puertos de servicio dedicados para stacking.</p>	INGECORP

95	5.2 .2. 1.1 .5	30	<p>Se pide "Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow, SPAN, ERSPAN".</p> <p>Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sirvase a confirmar en el requerimiento: Netflow o sFlow o similares.</p> <p>Además, se pide soportar ERSPAN que es una tecnología que permite la copia y el envío de tráfico de red desde una interfaz o varias interfaces de red en un switch a un dispositivo de análisis remoto a través de una red IP. Sirvase a confirmar se aceptarán tecnologías similares con SPAN, RSPAN o ERSPAN.</p>	INGECORP
96	5.2 .2. 1.1 .5	30	<p>Se pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)"</p> <p>En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo, y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque de flash seguro, para asegurar la integridad y autenticidad de nuestro hardware y software. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras necesidades específicas.</p> <p>Por lo tanto sirvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque de flash seguro.</p>	INGECORP
97	5.2 .2. 1.1 .5	31	<p>Se pide "RADSec"</p> <p>RadSec es un protocolo de seguridad que se utiliza para asegurar las comunicaciones entre servidores RADIUS (Remote Authentication Dial-In User Service) y clientes, garantizando la confidencialidad e integridad de los datos transmitidos. Esta tecnología es fundamental en entornos de autenticación y autorización de usuarios, especialmente en redes donde la seguridad es una prioridad.</p> <p>Al respecto, en el mercado existen distintas soluciones similares a Radsec como la verificación de seguridad por parte del servidor RADIUS a los usuarios que utilizan el protocolo Extensible Authentication Protocol over LAN (EAPoL). Esta información tiene como objetivo notificar a los usuarios acerca de los elementos que requieren verificaciones de seguridad adicionales, garantizando así que estén plenamente informados y conscientes de las medidas de seguridad aplicadas en nuestra red.</p> <p>Por lo tanto, sirvase a confirmar se aceptará soluciones RADSec o similar.</p>	INGECORP
98	5.2 .2. 1.1 .5	31	<p>Se pide "CoPP (Control Plane Policy)"</p> <p>El CoPP (Cisco) utiliza filtros de acceso para limitar el tráfico que se dirige al plano de control, lo que ayuda a prevenir la saturación y los ataques de denegación de servicio contra el dispositivo.</p> <p>El equipo propuesto ofrece características de seguridad similares como la autenticación de usuario y la protección contra ataques de inundación, (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, Defense Against Fragmentation Attacks, Defense Against TCP SYN Flood Packets, Defense Against UDP Flood Attacks, Defense Against ICMP Flood Attacks).</p> <p>Por lo tanto, aunque el CoPP es una función específica de los dispositivos Cisco, los switches propuestos ofrecen características de seguridad similares que protegen el dispositivo contra ataques malintencionados y garantizar que el tráfico importante tenga prioridad sobre otros tipos de tráfico.</p> <p>En conclusión, sirvase a confirmar se aceptará CoPP o características de seguridad similares como (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, etc).</p>	INGECORP
99	5.2 .2. 1.1 .5	31	<p>Se pide "Root Guard"</p> <p>Al respecto, se debe tener en cuenta que existen fabricantes en el mercado que denominan de otra forma a estas funcionalidades. Por ejemplo, a "STP root guard" también se le denomina "Root protection".</p>	INGECORP

			Por tanto, se sugiere respetuosamente a la entidad considerar que en el requerimiento se solicite Root Guard o equivalente.	
10 0	5.2 .2 1.1 .5	31	<p>Se pide "Private VLAN"</p> <p>(Private VLAN) es una tecnología que permite segmentar un VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos.</p> <p>Se provee lo mismo mediante Super-VLAN (S-VLAN). Al igual que PVLAN, S-VLAN permite segmentar una VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos para mejorar la seguridad y el aislamiento entre dispositivos y usuarios en una misma red.</p> <p>Por lo tanto, sírvase a confirmar que se aceptará Private VLAN o similar.</p>	INGECORP
10 1	5.2 .2 1.1 .5	31	<p>Se pide "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo".</p> <p>Al respecto, el requisito de incluir una etiqueta RFID (RFID Tag) en el switch propuesto, ya sea interna o externa, tiene un propósito específico que no está directamente relacionado con el funcionamiento de la red en sí. En lugar de sumar a la funcionalidad de la red, se centra en aspectos relacionados con la administración y el mantenimiento de los equipos de red. La inclusión de una etiqueta RFID tiene más que ver con la gestión y la identificación eficiente de los dispositivos que conforman la red.</p> <p>Por lo anterior, sírvase a confirmar esta característica será considerada como opcional: "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo o opcional".</p>	INGECORP
10 2	5.2 .2 1.1 .5	31	<p>Se pide: "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. ".</p> <p>Al respecto, el requisito de "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. " guarda una similitud fundamental con la implementación de un "arranque de flash seguro". Ambos objetivos se centran en salvaguardar la autenticidad e integridad del software o firmware en nuestros equipos. Al implementar un "arranque de flash seguro," establecemos una barrera efectiva contra posibles ataques de intermediarios maliciosos, ya que garantiza que el software o firmware se inicie desde una fuente confiable y que no haya sido comprometido durante el proceso de inicio. En esencia, ambas medidas buscan prevenir manipulaciones no autorizadas del software/firmware y garantizar que los equipos se ejecuten con la autenticidad e integridad necesarias para mantener la seguridad de nuestra infraestructura de red.</p> <p>Por lo tanto, sírvase a confirmar se aceptará: "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software o arranque seguro de flash".</p>	INGECORP
10 3	5.2 .2 1.1 .5	31	<p>Se pide "El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware."</p> <p>Al respecto, en el mercado muchos fabricantes realizan este procesamiento de Transmisión de paquetes IPv6 en hardware, implica que el switch tiene la capacidad de procesar y enrutar paquetes IPv6 utilizando recursos de hardware o de manera lógica.</p>	INGECORP

			Por lo tanto, sírvase a confirmar se aceptará: "El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware o de manera lógica"	
10	5.2 .2 4 1.1 .5	31	<p>Se pide "802.1v".</p> <p>IEEE 802.1v se relaciona con la etiqueta de VLAN IEEE 802.1v, que agrega información de prioridad de 802.1p a las tramas Ethernet etiquetadas con VLAN. Esta etiqueta se utiliza en las redes VLAN para mantener la calidad de servicio (QoS) incluso cuando el tráfico viaja a través de enlaces troncales que conectan diferentes switches.</p> <p>IEEE 802.1p: Este estándar se refiere a la asignación de prioridades a los paquetes Ethernet en función de los bits de prioridad contenidos en la cabecera de los paquetes. IEEE 802.1p permite la clasificación y la priorización del tráfico en diferentes clases de servicio, lo que garantiza que los paquetes críticos, como voz o video, reciban un trato preferencial en la red.</p> <p>Al respecto, El estándar IEEE 802.1v y la característica IEEE 802.1p están estrechamente relacionados en el contexto de la gestión de calidad de servicio (QoS) en redes Ethernet y VLAN (Virtual LAN). Por lo tanto, sírvase a confirmar se aceptará: "IEEE 802.1v o 802.1p".</p>	INGECORP
10	5.2 .2 5 1.1 .6	32	<p>Se pide "Debe tener mínimo una memoria RAM de 16GB "</p> <p>La capacidad de memoria RAM en un switch será relativa a las características del equipo: por ejemplo, el tamaño del sistema operativo, el tamaño de su configuración, el tamaño de los logs que maneja, entre otros. Si el equipo ha sido diseñado de forma tal que optimice sus recursos, entonces el tamaño de la RAM no necesita ser tan grande.</p> <p>Por lo anterior, se sugiere respetuosamente a la entidad:</p> <ol style="list-style-type: none"> 1. Solicitar en el switch una capacidad RAM no menor a 4 GB 	INGECORP
10	5.2 .2 6 1.1 .6	32	<p>Se pide "Debe tener mínimo una memoria Flash o SSD de 32GB "</p> <p>La capacidad de memoria Flash en un switch será relativa a las características del equipo: por ejemplo, el tamaño del sistema operativo, el tamaño de su configuración, el tamaño de los logs que maneja, entre otros. Si el equipo ha sido diseñado de forma tal que optimice sus recursos, entonces el tamaño de la flash no necesita ser tan grande.</p> <p>Por lo anterior, se sugiere respetuosamente a la entidad:</p> <ol style="list-style-type: none"> 1. Solicitar en el switch una capacidad flash no menor a 4 GB 	INGECORP
10	5.2 .2 7 1.1 .6	32	<p>Se pide "Debe permitir MC-LAG".</p> <p>Al respecto, MC-LAG es una tecnología que permite a múltiples dispositivos de red, como switches, trabajar juntos como un único dispositivo lógico para proporcionar redundancia y alta disponibilidad. En el mercado existen tecnologías similares pero con otras denominaciones como M-LAG.</p> <p>En base a lo anterior, sírvase a confirmar se aceptará MC-LAG o M-LAG.</p>	INGECORP
10	5.2 .2 8 1.1 .6	32	<p>Se pide "Debe tener un rendimiento mínimo de 1Bpps"</p> <p>Al respecto, El switch propuesto se destaca no solo por su capacidad para soportar MPPS, sino también por su impresionante capacidad de ancho de banda en Tbps. Además, El switch propuesto se ha diseñado para optimizar el uso de sus recursos, lo que lo distingue como una solución que no exige MPPS extremadamente elevados para garantizar un rendimiento óptimo. El dispositivo ha sido configurado de manera que los MPPS establecidos por el fabricante cumplen plenamente con los requisitos y permiten un funcionamiento óptimo en términos de conmutación y procesamiento de paquetes. Esto se traduce en una disponibilidad del 99.999%.</p> <p>Por lo tanto, sírvase a confirmar se aceptará: "Debe tener un rendimiento mínimo de 940 Mpps"</p>	INGECORP
10	5.2 .2 9 1.1 .6	32	<p>Se pide "El sistema operativo debe contar con mecanismos de servicio continuo con el objetivo de evitar interrupción del servicio ante operaciones de mantenimiento y actualización de software."</p>	INGECORP

			Debido a que existen soluciones diversas por cada fabricante para ofrecer alta disponibilidad sirvase a confirmar se aceptará: "El sistema operativo debe contar con mecanismos de servicio continuo con el objetivo de evitar interrupción del servicio ante operaciones de mantenimiento y actualización de software. O soportar stacking o cluster"	
11 0	5.2 .2 1.1 .6	33	Se pide "Debe incluir herramientas de telemetría, NetFlow o sFlow, SPAN, ERSPAN" ERSPAN que es una tecnología que permite la copia y el envío de tráfico de red desde una interfaz o varias interfaces de red en un switch a un dispositivo de análisis remoto a través de una red IP. Sirvase a confirmar se aceptarán tecnologías similares con SPAN, RSPAN o ERSPAN.	INGECORP
11 1	5.2 .2 1.1 .6	32	Se pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)" En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo, y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque de flash seguro, para asegurar la integridad y autenticidad de nuestro hardware y software. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras necesidades específicas. Por lo tanto sirvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque de flash seguro.	INGECORP
11 2	5.2 .2 1.1 .6	32	Se pide "TACACS+" TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS. Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS	INGECORP
11 3	5.2 .2 1.1 .6	32	Se pide "CoPP (Control Plane Policy)" El CoPP (Cisco) utiliza filtros de acceso para limitar el tráfico que se dirige al plano de control, lo que ayuda a prevenir la saturación y los ataques de denegación de servicio contra el dispositivo. El equipo propuesto ofrece características de seguridad similares como la autenticación de usuario y la protección contra ataques de inundación, (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, Defense Against Fragmentation Attacks, Defense Against TCP SYN Flood Packets, Defense Against UDP Flood Attacks, Defense Against ICMP Flood Attacks). Por lo tanto, aunque el CoPP es una función específica de los dispositivos Cisco, los switches propuestos ofrecen características de seguridad similares que protegen el dispositivo contra ataques malintencionados y garantizar que el tráfico importante tenga prioridad sobre otros tipos de tráfico. En conclusión, sirvase a confirmar se aceptará CoPP o características de seguridad similares como (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, etc).	INGECORP
11 4	5.2 .2 1.1 .6	32	Se pide "Root Guard" Al respecto, se debe tener en cuenta que existen fabricantes en el mercado que denominan de otra forma a estas funcionalidades. Por ejemplo, a "STP root guard" también se le denomina "Root protection". Por tanto, se sugiere respetuosamente a la entidad considerar qu en el requerimiento se solicite Root Guard o equivalente.	INGECORP
11 5	5.2 .2 1.1 .6	32	Se pide "Private VLAN" (Private VLAN) es una tecnología que permite segmentar un VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos. Se provee lo mismo mediante Super-VLAN (S-VLAN). Al igual que PVLAN, S-VLAN permite segmentar una	INGECORP

		VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos para mejorar la seguridad y el aislamiento entre dispositivos y usuarios en una misma red.	
		Por lo tanto, sirvase a confirmar que se aceptará Private VLAN o similar.	
11 6	5.2 .2. 1.1 .6	32 Se pide "802.1v". IEEE 802.1v se relaciona con la etiqueta de VLAN IEEE 802.1v, que agrega información de prioridad de 802.1p a las tramas Ethernet etiquetadas con VLAN. Esta etiqueta se utiliza en las redes VLAN para mantener la calidad de servicio (QoS) incluso cuando el tráfico viaja a través de enlaces troncales que conectan diferentes switches. IEEE 802.1p: Este estándar se refiere a la asignación de prioridades a los paquetes Ethernet en función de los bits de prioridad contenidos en la cabecera de los paquetes. IEEE 802.1p permite la clasificación y la priorización del tráfico en diferentes clases de servicio, lo que garantiza que los paquetes críticos, como voz o video, reciban un trato preferencial en la red. Al respecto, El estándar IEEE 802.1v y la característica IEEE 802.1p están estrechamente relacionados en el contexto de la gestión de calidad de servicio (QoS) en redes Ethernet y VLAN (Virtual LAN). Por lo tanto, sirvase a confirmar se aceptará: "IEEE 802.1v o 802.1p".	INGECORP
11 7	5.2 .2. 1.2 .1	34 Se pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)". En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo, y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque seguro o Bootload, para asegurar la integridad y autenticidad. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras necesidades específicas. Por lo tanto sirvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque seguro o BootLoad.	INGECORP
11 8	5.2 .2. 1.2 .1	35 Se pide " Deberá soportar RESTCONF (RFC 8040) para proporcionar una interfaz de programabilidad estándar y permitir el acceso a parámetros de configuración. " Al respecto, RESTCONF (RFC 8040) proporciona una interfaz de programabilidad estándar y permitir el acceso a parámetros de configuración para la gestión y configuración de dispositivos de red. Sin embargo, es relevante destacar que, a través del protocolo NETCONF, se puede lograr un objetivo similar de programabilidad y configuración de manera efectiva. Por lo tanto, sirvase a confirmar se aceptará " Deberá soportar RESTCONF (RFC 8040) para proporcionar una interfaz de programabilidad estándar y permitir el acceso a parámetros de configuración, o soportar NETCONF"	INGECORP
11 9	5.2 .2. 1.2 .1	35 Se pide "TACACS+" TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS. Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS	INGECORP
12 0	5.2 .2. 1.2 .1	35 Se pide "RFC 3576" El RFC 3576 especifica el protocolo de extensión RADIUS (Remote Authentication Dial-In User Service) conocido como "Dynamic Authorization Extensions to RADIUS." Este protocolo extiende las capacidades de RADIUS para proporcionar autorización dinámica en entornos de acceso a la red, como redes de acceso remoto y redes inalámbricas. Sin embargo, es importante destacar que RADIUS en sí mismo, sin la extensión proporcionada por RFC 3576, ya ofrece funcionalidades similares y es ampliamente utilizado en el mercado por distintos fabricantes para la autenticación y autorización de usuarios en redes.	INGECORP

			Por lo tanto, sirvase a confirmar se aceptará: "RFC 3576 o soportar RADIUS"	
12 1	5.2 .2 1.2 .1	35	<p>Se pide "Debe incluir visibilidad de las aplicaciones consumidas por los usuarios por medio de NBAR o DPI".</p> <p>Al respecto, se menciona la necesidad de utilizar tecnologías como NBAR (Network-Based Application Recognition) o DPI (Deep Packet Inspection) para obtener visibilidad sobre las aplicaciones consumidas por los usuarios en una red. Sin embargo, es relevante destacar que existe una alternativa efectiva y moderna conocida como SAC (Smart Application Control) que ofrece funcionalidades similares y, en algunos aspectos, puede superar las capacidades de NBAR y DPI.</p> <p>SAC es una tecnología avanzada que combina la detección y el control de aplicaciones en la red. Al igual que NBAR y DPI, SAC es capaz de identificar y clasificar las aplicaciones que se están utilizando en la red. Sin embargo, a diferencia de DPI, que a veces puede ser invasivo y consumir recursos significativos, SAC suele ser menos intrusivo y más eficiente en términos de recursos.</p> <p>Por lo tanto sirvase a confirmar se aceptará: " Debe incluir visibilidad de las aplicaciones consumidas por los usuarios por medio de NBAR o DPI o soportar SAC"</p>	INGECORP
12 2	5.2 .2 1.2 .1	35	<p>Se pide " Debe de incluir la capacidad de identificar los dispositivos inalámbricos y crear políticas de acuerdo con la identidad del dispositivo (Android, iPhone, Etc.)."</p> <p>Al respecto, la característica de identificación de dispositivos y la aplicación de políticas basadas en la identidad debería ser implementada en la plataforma de gestión de la red en lugar de la controladora WLAN debido a los beneficios de centralización y coherencia en la gestión de toda la red, tanto inalámbrica como cableada. Un enfoque centralizado simplifica la administración, garantiza la uniformidad de las políticas en toda la red, ofrece una mayor escalabilidad y facilita la integración con otros servicios de red, lo que resulta en una gestión más eficiente y eficaz de los dispositivos inalámbricos y las políticas de seguridad basadas en la identidad.</p> <p>Por lo tanto, sirvase a confirmar que: "Debe de incluir la capacidad de identificar los dispositivos inalámbricos y crear políticas de acuerdo con la identidad del dispositivo (Android, iPhone, Etc.) o también será válido si esta función será soportada por la plataforma de gestión de forma centralizada."</p>	INGECORP
12 3	5.2 .2 1.2 .1	36	<p>Se pide "Permitir la configuración y gestión a través de un navegador web estándar (HTTP, HTTPS), SSH y puerto serial. "</p> <p>Sirvase a confirmar se aceptarán modos de gestión similares: "Permitir la configuración y gestión a través de un navegador web estándar (HTTP, HTTPS), SSH y puerto serial o puerto consola RJ45"</p>	INGECORP
12 4	5.2 .2 1.2 .2	37	<p>Se pide "Debe incluir OFDM con 37 resource units".</p> <p>Al respecto, OFDM con 37 resource units se utiliza para transmitir una sola señal o asignar todas las subportadoras a un solo usuario, actualmente existen soluciones superiores como OFDMA. Aunque ambos enfoques utilizan la tecnología de modulación OFDM, OFDMA lleva la eficiencia y la capacidad de asignación de recursos a un nivel superior al permitir una asignación dinámica y eficiente de subconjuntos de subportadoras a diferentes usuarios. Mientras que OFDM con 37 resource units asigna todas las subportadoras a un solo usuario, OFDMA permite que múltiples usuarios compartan el espectro de frecuencia de manera eficaz, lo que resulta en una mejor capacidad de adaptación a las necesidades cambiantes de la red y una mayor capacidad para manejar múltiples conexiones simultáneas. Esto lo convierte en la elección preferida para entornos de red con alta densidad de usuarios y una demanda constante de asignación de recursos dinámicos, donde OFDMA ofrece un rendimiento superior y una mayor eficiencia en la asignación de recursos.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "Debe incluir OFDM con 37 resource units o debe incluir OFDMA"</p>	INGECORP
12 5	5.2 .2	37	<p>"Se pide ""Debe incluir un módulo de plataforma confiable (TPM o TAM) ""</p> <p>Al respecto, Trusted Platform Module (TPM) o Trusted Anchor Module (TAM), que son componentes de</p>	INGECORP

	1.2 .1	<p>seguridad utilizados para almacenar claves y certificados de manera segura, y para garantizar que el hardware y el software del dispositivo no hayan sido comprometidos.</p> <p>A diferencia de TPM o TAM, muchos fabricante en el mercado suele utilizar métodos de cifrado, autenticación y control de acceso avanzados en sus dispositivos para proteger la integridad y la confidencialidad de los datos de la red y los usuarios o de CAPWAP. Estos métodos pueden incluir protocolos de cifrado, autenticación de usuarios, detección de intrusiones y otras técnicas de seguridad estándar de la industria.</p> <p>Por lo tanto sirvase a confirmar se aceptará "Debe incluir un módulo de plataforma confiable (TPM o TAM) o CAPWAP o similare"</p>	
12 6	5.2 .2.39 1.5	<p>Se pide "Debe manejar el inventario de los dispositivos de red, recopilando la dirección IP, la MAC Address "</p> <p>Al respecto, debido a que muchos fabricantes en el mercado manejan distintos terminos para recopilar información de los dispositivos de red (dirección IP, la MAC Address), mediante inventario o listas de dispositivos.</p> <p>Al base a lo anterior sirvase a confirmar se aceptará: "Debe manejar el inventario o listas de dispositivos de red, recopilando la dirección IP, la MAC Address "</p>	INGECORP
12 7	5.2 .2.39 1.5	<p>Se pide "Obtención de información de inventario de los equipos."</p> <p>Al respecto, debido a que muchos fabricantes en el mercado manejan distintos terminos para recopilar información de los dispositivos de red (dirección IP, la MAC Address), mediante inventario o listas de dispositivos.</p> <p>Al base a lo anterior sirvase a confirmar se aceptará: "Obtención de información de inventario o lista de los equipos. "</p>	INGECORP
12 8	5.2 .2.40 1.5	<p>Se pide "Debe incluir workflows intuitivos ".</p> <p>Al respecto, muchos fabricantes definen los medianos de implementación intuitiva a través de workflows o GUI wizard, proporcionado flujos de trabajo diseñados de manera que sean fáciles de comprender y utilizar de forma natural, incluso para usuarios sin experiencia técnica avanzada.</p> <p>Por lo tanto, sirvase a confirmar se aceptara: "Debe incluir workflows intuitivos o GUI wizard"</p>	INGECORP
12 9	5.2 .2.40 1.5	<p>Pide "Debe permitir la integración con soluciones terceras por medio de herramientas de automatización que facilitan la transferencia de datos (Webhooks) para el envío de notificaciones "</p> <p>Al respecto, la plataforma debe ser capaz de conectarse y trabajar con soluciones de terceros a través de la automatización mediante Webhooks. Esto permite la transferencia de datos, mejorando la eficiencia y la interoperabilidad del sistema al permitir que eventos y acciones se comuniquen de manera automática y eficiente entre diferentes sistemas.</p> <p>En el mercado existen distintas denominaciones para funciones de automatización que facilita la transferencia de datos como Webhooks o RESTful API.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "Debe permitir la integración con soluciones terceras por medio de herramientas de automatización que facilitan la transferencia de datos (Webhooks) para el envío de notificaciones o soporta RESTful API".</p>	INGECORP
13 0	5.2 .2.41 1.5	<p>Se pide "Capacidad de generar informes de los siguientes tipos: Lista de clientes wireless, lista de access points, información de configuración de los controladores WLAN, uso de la red, access points no autorizados (rogue) detectados, esto de manera manual y automática agendada mensual y semanalmente."</p> <p>Debido a que muchos fabricantes no presentan las mismas denominaciones para generar informes de lista de clientes wireless, lista de access point, controladores WLAN, uso de la red, APS Rogue, Sirvase a confirmar que se aceptará la opción de generar informes de manera manual y automática mediante: tipo de dispositivo, vendors, modelo, uso de puerto y terminales.</p>	INGECORP

		<p>Por lo tanto se sugiere respetuosamente a la entidad considerar:</p> <p>"Capacidad de generar informes de los siguientes tipos: Lista de clientes wireless, lista de access points, información de configuración de los controladores WLAN, uso de la red, access points no autorizados (rogue) detectados, esto de manera manual y automática agendada mensual y semanalmente. o generar informes de tipo de dispositivo, vendors, modelo, uso de puerto y terminales, esto de manera manual y automática agendada mensual y semanalmente"</p>	
13 1	5.2 .2 1.5	41 <p>Se pide "Debe incluir una solución que permita el uso de algoritmos avanzados de análisis de comportamiento; para identificar patrones de tráfico, usando análisis de la información de eventos que ocurren dentro de un flujo de datos aplicando técnicas de machine learning, con el objetivo de detectar potenciales amenazas de seguridad. a través de la inclusión de hardware y software adicional que permita descifrar el tráfico para su análisis."</p> <p>En el mercado existen diversas alternativas para realizar el analisis de comportamientos aplicando tecnicas de machine learning no solo mediante la inclusión de hardware y software adicional que permita descifrar el tráfico para su análisis, sino que a través de una arquitectura integrada de recopilación de datos a través de telemetria, plataforma de analisis de big data y un motor de IA.</p> <p>Por lo tanto, se solicita respetuosamente a la entidad considerar: "Debe incluir una solución que permita el uso de algoritmos avanzados de análisis de comportamiento; para identificar patrones de tráfico, usando análisis de la información de eventos que ocurren dentro de un flujo de datos aplicando técnicas de machine learning, con el objetivo de detectar potenciales amenazas de seguridad. a través de la inclusión de hardware y software adicional que permita descifrar el tráfico para su análisis o a través de una plataforma de análisis de big data que recibe datos del dispositivo a través de la tecnología Telemetry y analiza y muestra los datos de la red a través de algoritmos inteligentes".</p>	INGECORP
13 2	5.2 .2 1.6	42 <p>Se pide "Debe incluir TACACS+ para la autenticación de los usuarios de gestión de la infraestructura de red "</p> <p>TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS.</p> <p>Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS</p>	INGECORP
13 3	5.2 .2 1.6	42 <p>Se pide "Para la gestión y autenticación de acceso a la red, se debe implementar el servicio RADIUS y/o TACACS+, que incluya el licenciamiento necesario para el Sistema Operativo, el servicio RADIUS o TACACS+ y un Servicio NTP."</p> <p>TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS.</p> <p>Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS</p>	INGECORP
13 4	5.2 .2 1.6	45 <p>Se pide "Debe garantizar que para el acceso a la red se validen y verifiquen los requisitos mínimos de cumplimiento y aquellos que no cumplan las reglas definidas por CORPAC S.A., serán enviados un segmento de cuarentena. Debe considerar como mínimo un licenciamiento para 200 dispositivos."</p> <p>Al respecto, debido a que existen diversas formas para restringir el acceso a la red como cuarentena, listas negras, bloqueo, que garanticen el requerimiento de garantizar la seguridad de acceso a la red. Se solicita respetuosamente a la entidad considerar lo siguiente:</p> <p>"Debe garantizar que para el acceso a la red se validen y verifiquen los requisitos mínimos de cumplimiento y aquellos que no cumplan las reglas definidas por CORPAC S.A., serán enviados un segmento de cuarentena o se definirá en listas negras o bloqueados directamente. Debe considerar como mínimo un licenciamiento para 200 dispositivos."</p>	INGECORP

13 5	5.2 .2. 1.6	43	<p>Se pide "El usuario debe validarse contra un dominio existente utilizando sus credenciales. En caso la red maneje esquemas de multidominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario."</p> <p>Al respecto, el requerimiento se refiere a los procedimientos de autenticación en una red donde los usuarios deben verificar su identidad utilizando credenciales, como un nombre de usuario y una contraseña, en un dominio específico. Por lo tanto para una mayor aclaración del requerimiento se solicita respetuosamente a la entidad considerar lo siguiente:</p> <p>"El usuario debe validarse contra un dominio existente utilizando sus credenciales. En caso la red maneje esquemas de multidominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario; o los usuarios deben proporcionar información de autenticación que será verificada por un servidor o sistema de autenticación en un dominio específico."</p>	INGECORP
13 6	5.2 .2. 1.6	45	<p>Se pide "EAP-FAST "</p> <p>Al respecto, "EAP-FAST" es un protocolo de autenticación propietario desarrollado por Cisco que establece un túnel de seguridad para proteger las credenciales del usuario y utiliza un proceso similar al desafío y respuesta para la autenticación. En el mercado existen protocolos similares como "EAP-TTLS-PAP" que es un estándar más ampliamente aceptado, también establece un túnel de seguridad (TTLS) para proteger las credenciales y utiliza el protocolo PAP (Password Authentication Protocol) para la autenticación del usuario.</p> <p>Por lo tanto sirvase a confirmar que se aceptará: "EAP-FAST o EAP-TTLS-PAP"</p>	INGECORP
13 7			<p>Se adjunta las consultas y observaciones a los Términos de referencia de la RENOVACION DE LA RED LAN DE CORPAC, se valida que solo la marca CISCO esta cumpliendo con todos los requerimientos técnicos solicitados.</p> <p>Asimismo; debe señalarse que, el artículo 29 del Reglamento del Texto Único Ordenado de la Ley de Contrataciones del Estado -en adelante el Reglamento; establece que es el área usuaria la responsable de elaborar el requerimiento, debiendo éste contener todas las características, exigencias y condiciones para la ejecución de la contratación.</p> <p>Así, el artículo 32 del Reglamento establece que, el órgano encargado de las contrataciones sobre la base del requerimiento realizará el estudio de mercado orientado a determinar el valor estimado, y la pluralidad de postores y marcas; así como, la posibilidad de distribuir la buena pro.</p> <p>En tal sentido, corresponde señalar que, en las compras públicas debe lograrse el mayor grado de eficacia de la contratación mediante mecanismos que promuevan el libre acceso y participación de proveedores, dado que un requisito de validez del procedimiento, y por consiguiente de la posterior adjudicación, es que se haya verificado una plural y efectiva concurrencia y competencia de agentes de mercado, de tal modo que si se advierte lo contrario, correspondería a la Entidad convocante sanear dicho aspecto (vicio de nulidad).</p>	INGECORP

ANEXO A.1

ABSOLUCION A LAS CONSULTAS Y/U OBSERVACIONES DEL ANEXO A

5.2 .2. 1.1 .1	15	Se pide "Debe tener mínimo una memoria RAM de 16GB " Al respecto se entrega 16 GB, de forma agrupada mediante 2 Tarjetas de control de 8GB. Sírvase a confirmar se aceptarán 2 tarjetas de 8GB.	INGECORP	El requerimiento hace referencia a la capacidad de memoria que debe tener el equipamiento; en este caso de 16GB; independientemente de cómo lo implemente cada fabricante; respetando la capacidad solicitada. En ese sentido se reformula requerimiento.	Debe tener mínimo la capacidad de memoria de RAM de 16GB.
5.2 .2. 1.1 .1	15	Se pide "Debe tener mínimo una memoria Flash de 16GB " Al respecto, el almacenamiento propuesto por cada fabricante varía de acuerdo a la capacidad o tamaños de su sistema operativo y configuraciones, es decir no es indispensable contar con una memoria Flash elevada si el sistema está correctamente estructurado por cada fabricante, definiendo capacidades óptimas para su propio sistema operativo y configuraciones almacenadas. Por lo tanto, sírvase a confirmar se aceptarán memoria Flash mínima de 2GB.	INGECORP	Tomando en consideración que la memoria flash sirve para el almacenamiento del sistema operativo y/o configuraciones; independientemente de cómo lo implemente cada fabricante; se aceptarán como mínimo la capacidad mínima de 2GB. En ese sentido se reformula requerimiento.	Debe tener mínimo la capacidad de memoria Flash de 2GB
5.2 .2. 1.1 .1	15	Se pide "Cada Switch Core debe incluir 8 transceivers de 100Gbps (SFP28) para fibra óptica monomodo de 10Km para la conexión con el Border Node (Switch Core) y Distribución y switches ToR ubicados en el DC. Asimismo, 1 transceivers de 10Gbps para interconexión entre Cores". Al respecto, sírvase a confirmar se aceptarán soluciones similares o superiores a 10Gbps para la interconexión entre cores.	INGECORP	Se precisa, que las especificaciones son requisitos mínimos, pudiendo el participante proponer mejoras sobre lo que se solicita. En este caso conexiones superiores para la interconexión entre CORES.	
5.2 .2. 1.1 .1	15	Se pide "Contar con puerto serial de consola o puerto USB para gestión" Sírvase a confirmar se aceptarán modos de gestión similares: Contar con puerto serial de consola o puerto USB para gestión o puerto RJ45 consola.	INGECORP	Se confirma, se reformula de la siguiente manera: Contar con puerto serial de consola o puerto USB o puerto RJ45 de consola para gestión.	Contar con puerto serial de consola o puerto USB o puerto RJ45 de consola para gestión.
5.2 .2. 1.1 .1	15	pide "Debe tener 32 puertos de red 40/100G (QSFP/QSFP28) como mínimo ". Al respecto se pide que se soporte 32 puertos de 40/100G, de los cuales solo se usarán 8 transceiver de 100G. Esto implica que, según el diseño actual, existe un exceso de capacidad en términos de puertos de alta velocidad. Además, es relevante considerar la eficiencia y el costo del diseño. Tener 32 puertos de 100G cuando solo se utilizarán 8 implica una inversión innecesaria en recursos de red de alto rendimiento. Además, esto puede tener un impacto en el presupuesto y el consumo energético, ya que la energía requerida para mantener 32 puertos de 100G operativos es significativamente mayor que para 8 puertos. Por lo tanto, sírvase a confirmar que el Switch de core debe ser capaz de soportar al menos 24 puertos de 100G. Esta cantidad permitirá cubrir las necesidades actuales y futuras de la red, sin incurrir en una inversión excesiva en recursos	INGECORP	Se precisa que, de la revaluación de esta característica, con respecto a la utilización de puertos (slot disponibles) para conexión de transceivers, se reformula el requerimiento, de la siguiente manera: Debe tener 24 puertos de red con soporte de 40/100G (QSFP/QSFP28) como mínimo.	Debe tener 24 puertos de red con soporte de 40/100G (QSFP/QSFP28) como mínimo.
5.2 .2. 1.1 .1	15	Se pide "Debe permitir MC-LAG". Al respecto, MC-LAG es una tecnología que permite a múltiples dispositivos de red, como switches, trabajar juntos como un único dispositivo lógico para proporcionar redundancia y alta disponibilidad. El CSS es una configuración en la que múltiples switches se combinan para funcionar como una única unidad lógica. Por lo tanto, la tecnología MC-LAG (Multi-Chassis Link Aggregation Group) y el CSS (Cluster de Switch) son	INGECORP	El requerimiento hace referencia a la capacidad de del sistema para funcionar con un dispositivo lógico agrupando varios dispositivos físicos, que permitan contar con escenarios de redundancia y alta disponibilidad, independientemente de cómo lo denomine cada fabricante. En ese sentido se reformula requerimiento.	Se elimina MC-LAG y se reemplaza por: Debe permitir tecnología de múltiples dispositivos para que trabaje como un único dispositivo lógico para proporcionar

		conceptos relacionados que se utilizan en redes empresariales y de centros de datos para mejorar la redundancia y la disponibilidad de la red. En base a lo anterior, sírvase a confirmar se aceptará MC-LAG o CSS.			redundancia y alta disponibilidad para entornos de redes empresariales y centro de datos.
5.2 .2. 1.1 .1	15	Se pide "Debe incluir todos los componentes necesarios para realizar el stacking virtual " Al respecto, Tanto el stacking virtual como el CSS Cluster de Switch tienen como objetivo principal crear una entidad lógica única a partir de múltiples switches físicos. Ambas tecnologías permiten la administración y configuración simplificada de los switches, lo que mejora la eficiencia operativa y la disponibilidad de la red. Por lo tanto, sírvase a confirmar se aceptará una solución equivalente a stacking virtual mediante CSS.	INGECORP	El requerimiento hace referencia a la capacidad de del sistema para funcionar con una unidad lógica agrupando varios dispositivos físicos, que permitan contar con escenarios de administración y configuración simplificada de estos dispositivos, logrando la eficiencia operativa y disponibilidad de la red; independientemente de cómo lo denomine cada fabricante. En ese sentido se reformula requerimiento.	Debe incluir todos los componentes necesarios para realizar el Stacking virtual o solución equivalente.
5.2 .2. 1.1 .1	15	Se pide "Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow, SPAN, ERSPAN ". Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sírvase a confirmar en el requerimiento: Netflow o sFlow o similares. Además, se pide soportar ERSPAN que es una tecnología que permite la copia y el envío de tráfico de red desde una interfaz o varias interfaces de red en un switch a un dispositivo de análisis remoto a través de una red IP. Sírvase a confirmar se aceptarán tecnologías similares con SPAN, RSPAN o ERSPAN.	INGECORP	Tomando en consideración que existe una diversidad de soluciones o tecnologías relacionadas a la captura y/o recolección de flujos utilizados para la supervisión de dispositivos de red; serán aceptados soluciones y/o tecnologías similares. En ese sentido se reformula requerimiento.	"Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow o soluciones similares, SPAN, ERSPAN o tecnologías similares".
5.2 .2. 1.1 .1	16	Se pide "Debe ser máximo de 1 Rack Unit (RU) " Debido a la cantidad de puertos de alto rendimiento (100G) el Switch debe contar con altas capacidades de reenvío siendo superior, sírvase a confirmar que aceptará capacidades entre 1 (RU) y 10 (RU).	INGECORP	Se precisa que, el espacio disponible para esta implementación es reducido; para soluciones de tipo chasis para el requerimiento solicitado esta no podrá exceder de 8 RU. Se reformula requerimiento.	Debe ser máximo de 1 Rack Unit (RU). Para soluciones de tipo chasis no deberá excederse de 8 RU (unidades de rack)
5.2 .2. 1.1 .1	16	Se pide "Debe incluir los componentes necesarios para su instalación en rack de 19". " Debido a la cantidad de puertos de alto rendimiento (100G) el Switch debe contar con altas capacidades de reenvío siendo superior, sírvase a confirmar que aceptará capacidades entre 19", o 1 (RU) y 10 (RU).	INGECORP	Se precisa que, para soluciones de tipo chasis para el requerimiento solicitado esta no podrá exceder de 8 RU e incluir todos los accesorios para tal fin. Se reformula requerimiento.	Debe incluir los componentes necesarios para su instalación en rack de 19" inclusive para soluciones de tipo chasis.
5.2 .2. 1.1 .1	16	Se pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)" En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo, y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque de flash seguro, para asegurar la integridad y autenticidad de nuestro hardware y software. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras necesidades específicas. Por lo tanto, sírvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque de flash seguro.	INGECORP	Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera: Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad de hardware y software.	Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.
5.2 .2. 1.1 .1	16	Se pide "TACACS+ " TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS. Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS	INGECORP	Se confirma, TACACS, TACACS+ o equivalentes	TACACS, TACACS+ o equivalentes

5.2 .2. 1.1 .1	16	<p>Se pide "RADSec"</p> <p>RadSec es un protocolo de seguridad que se utiliza para asegurar las comunicaciones entre servidores RADIUS (Remote Authentication Dial-In User Service) y clientes, garantizando la confidencialidad e integridad de los datos transmitidos. Esta tecnología es fundamental en entornos de autenticación y autorización de usuarios, especialmente en redes donde la seguridad es una prioridad.</p> <p>Al respecto, en el mercado existen distintas soluciones similares a Radsec como la verificación de seguridad por parte del servidor RADIUS a los usuarios que utilizan el protocolo Extensible Authentication Protocol over LAN (EAPoL). Esta información tiene como objetivo notificar a los usuarios acerca de los elementos que requieren verificaciones de seguridad adicionales, garantizando así que estén plenamente informados y conscientes de las medidas de seguridad aplicadas en nuestra red.</p> <p>Por lo tanto, sírvase a confirmar se aceptará soluciones RADSec o similar.</p>	INGECORP	Se confirma RADSec o similares	RADSec o similares
5.2 .2. 1.1 .1	16	<p>Se pide "CoPP (Control Plane Policy)"</p> <p>El CoPP (Cisco) utiliza filtros de acceso para limitar el tráfico que se dirige al plano de control, lo que ayuda a prevenir la saturación y los ataques de denegación de servicio contra el dispositivo.</p> <p>El equipo propuesto ofrece características de seguridad similares como la autenticación de usuario y la protección contra ataques de inundación, (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, Defense Against Fragmentation Attacks, Defense Against TCP SYN Flood Packets, Defense Against UDP Flood Attacks, Defense Against ICMP Flood Attacks).</p> <p>Por lo tanto, aunque el CoPP es una función específica de los dispositivos Cisco, los switches propuestos ofrecen características de seguridad similares que protegen el dispositivo contra ataques malintencionados y garantizar que el tráfico importante tenga prioridad sobre otros tipos de tráfico.</p> <p>En conclusión, sírvase a confirmar se aceptará CoPP o características de seguridad similares como (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, etc).</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.</p>	Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión
5.2 .2. 1.1 .1	16	<p>Se pide "Root Guard"</p> <p>Al respecto, se debe tener en cuenta que existen fabricantes en el mercado que denominan de otra forma a estas funcionalidades. Por ejemplo, a "STP root guard" también se le denomina "Root protection".</p> <p>Por tanto, se sugiere respetuosamente a la entidad considerar qu en el requerimiento se solicite Root Guard o equivalente.</p>	INGECORP	Se confirma Root Guard o equivalente	Root Guard o equivalente
5.2 .2. 1.1 .1	16	<p>Se pide "Private VLAN"</p> <p>(Private VLAN) es una tecnología que permite segmentar un VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos.</p> <p>Se provee lo mismo mediante Super-VLAN (S-VLAN). Al igual que PVLAN, S-VLAN permite segmentar una VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos para mejorar la seguridad y el aislamiento entre dispositivos y usuarios en una misma red.</p> <p>Por lo tanto, sírvase a confirmar que se aceptará Private VLAN o similar.</p>	INGECORP	Se confirma Private VLAN o similares	Private VLAN o similares
5.2 .2. 1.1 .1	18	<p>Se pide "Deberá contar con mecanismos de seguridad de IPv6 First-Hop".</p> <p>IPv6 First-Hop, es una función de seguridad que se utiliza para proteger el tráfico de IPv6, como los enlaces Ethernet. Esta función se utiliza para proteger contra amenazas como los ataques de spoofing y los ataques de inundación.</p> <p>Se provee lo mismo, la función equivalente a IPv6 First Hop Security de Cisco se conoce como IPv6 Secure Neighbor Discovery (SEND). Esta función se utiliza para proteger el tráfico de IPv6 en los enlaces de capa 2, como los enlaces Ethernet. La función utiliza una combinación de autenticación, criptografía y verificación de estado para asegurar que los dispositivos de la red puedan confiar en los mensajes de descubrimiento de vecinos IPv6 que se intercambian en la capa 2.</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Deberá contar con mecanismo y/o función de seguridad que utilice una combinación de autenticación, criptografía y verificación de estado para asegurar que los dispositivos de la red puedan confiar en los mensajes de descubrimiento de vecinos IPv6 que se intercambian en la capa 2.</p>	Deberá contar con mecanismo y/o función de seguridad que utilice una combinación de autenticación, criptografía y verificación de estado para asegurar que los dispositivos de la red puedan confiar en los mensajes de descubrimiento de vecinos IPv6 que se intercambian en la capa 2.

		Por lo tanto, se entrega la misma función, sirvase a confirmar se aceptará IPv6 First-Hop o IPv6 Secure Neighbor Discovery.			
5.2 .2. 1.1 .1	18	<p>Se pide "Deberá contar con mecanismos para garantizar que el sistema operativo sea íntegro y consistente en todos los switches".</p> <p>Al respecto, para cumplir con el siguiente requisito existen distintas formas de garantizar esta seguridad. Para mantener la seguridad y la coherencia en nuestra infraestructura de red, existen soluciones equivalentes como el arranque de flash seguro.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "Deberá contar con mecanismos para garantizar que el sistema operativo sea íntegro y consistente en todos los switches o arranque seguro de flash".</p>	INGECORP	Se precisa que, independientemente como implemente la solución para garantizar la seguridad del sistema operativo de cada fabricante o como se la denomine; se deberá contar con estos mecanismos para garantizar que el sistema operativo sea íntegro y consistente en todos los switches.	
5.2 .2. 1.1 .1	18	<p>Se pide: "Deberá contar con mecanismos que prevengan ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos".</p> <p>Al respecto, el requisito de "Deberá contar con mecanismos que prevengan ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos" guarda una similitud fundamental con la implementación de un "arranque de flash seguro". Ambos objetivos se centran en salvaguardar la autenticidad e integridad del software o firmware en nuestros equipos. Al implementar un "arranque de flash seguro," establecemos una barrera efectiva contra posibles ataques de intermediarios maliciosos, ya que garantiza que el software o firmware se inicie desde una fuente confiable y que no haya sido comprometido durante el proceso de inicio. En esencia, ambas medidas buscan prevenir manipulaciones no autorizadas del software/firmware y garantizar que los equipos se ejecuten con la autenticidad e integridad necesarias para mantener la seguridad de nuestra infraestructura de red.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "Deberá contar con mecanismos que prevengan ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos o arranque seguro de flash".</p>	INGECORP	Se precisa que, independientemente como implemente la solución, para prevenir ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos, de cada fabricante o como se la denomine; estos serán una barrera contra ataques de intermediarios maliciosos que prevengan manipulaciones no autorizadas del software/firmware en los equipos.	
5.2 .2. 1.1 .1	18	<p>Se pide "El Switch propuesto deberá soportar funcionalidades que ayuden a identificar amenazas o anomalías en la red incluso descubrimiento malware en el tráfico cifrado".</p> <p>Al respecto, lo anterior es similar a la capacidad de soportar "firmas digitales y certificados." Ambos enfoques tienen como objetivo principal fortalecer la seguridad de la red y detectar posibles amenazas, incluyendo aquellas que pueden ocultarse en el tráfico cifrado.</p> <p>La implementación de firmas digitales y certificados es un mecanismo efectivo para verificar la autenticidad y la integridad de los datos en la red. Al verificar las firmas digitales de los datos y utilizar certificados para autenticar la identidad de los dispositivos y usuarios, podemos asegurar que la información transmitida no ha sido alterada y proviene de fuentes confiables.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "El Switch propuesto deberá soportar funcionalidades que ayuden a identificar amenazas o anomalías en la red incluso descubrimiento malware en el tráfico cifrado o arranque seguro de flash".</p>	INGECORP	Se precisa que, independientemente como implemente la solución, sobre funcionalidades que ayuden a identificar amenazas o anomalías en la red incluso descubrimiento malware en el tráfico cifrado, de cada fabricante o como se la denomine; el objetivo es fortalecer la seguridad de la red detectando posibles amenazas, inclusive si es tráfico encriptado/cifrado; por lo tanto, se pide que pueda asegurarse que la información transmitida no haya sido alterada y que provenga de fuentes confiables.	
5.2 .2. 1.1 .1	18	<p>Se pide "Debe soportar e implementar mecanismos de encolamiento Shaped Round Robin (SRR) y Committed Information Rate (CIR)".</p> <p>Debido a que existen funciones similares: Al respecto, la tecnología "Shaped Round Robin (SRR)" y el soporte para "Weighted Round Robin (WRR)" son dos enfoques similares utilizados en la gestión del tráfico de red en switches y routers. Aunque no son idénticos en su funcionamiento, comparten similitudes fundamentales en términos de asignación de prioridad y equidad en la distribución del tráfico.</p> <p>Tanto SRR como WRR se centran en la programación de cómo se maneja el tráfico en una cola de salida del dispositivo de red. SRR, en particular, se utiliza para asignar un peso o una prioridad a cada flujo de tráfico en la cola y determinar cómo se atienden estos flujos en función de su peso o prioridad. Por otro lado, WRR</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Debe soportar e implementar mecanismos de encolamiento Shaped Round Robin (SRR) o WRR, y Committed Information Rate (CIR)"</p>	Debe soportar e implementar mecanismos de encolamiento Shaped Round Robin (SRR) o WRR, y Committed Information Rate (CIR)"

		<p>asigna pesos específicos a diferentes flujos de tráfico y distribuye el ancho de banda disponible en función de estos pesos, lo que le permite otorgar prioridad a ciertos flujos sobre otros</p> <p>Por lo tanto sirvase a confirmar se aceptará: "Debe soportar e implementar mecanismos de encolamiento Shaped Round Robin (SRR) o WRR, y Committed Information Rate (CIR)"</p>			
5.2 .2. 1.1 .1	18	<p>Se pide "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo".</p> <p>Al respecto, el requisito de incluir una etiqueta RFID (RFID Tag) en el switch propuesto, ya sea interna o externa, tiene un propósito específico que no está directamente relacionado con el funcionamiento de la red en sí. En lugar de sumar a la funcionalidad de la red, se centra en aspectos relacionados con la administración y el mantenimiento de los equipos de red. La inclusión de una etiqueta RFID tiene más que ver con la gestión y la identificación eficiente de los dispositivos que conforman la red.</p> <p>Por lo anterior, sirvase a confirmar esta característica será considerada como opcional: "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo u opcional".</p>	INGECORP	No se confirma, se requiere incluir esta característica sin limitación, puede ser interna o externa, puede ser del mismo fabricante o de terceros.	
5.2 .2. 1.1 .1	18	<p>Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sirvase a confirmar en el requerimiento: Netflow o sFlow o similares.</p>	INGECORP	Tomando en consideración que existe una diversidad de soluciones o tecnologías relacionadas a la captura y/o recolección de flujos utilizados para la supervisión de dispositivos de red; serán aceptados soluciones y/o tecnologías similares. En ese sentido se reformula requerimiento.	"Soporte instalado y operativo de sFlow o Netflow o soluciones similares".
5.2 .2. 1.1 .1	18	<p>Se pide "802.1v".</p> <p>IEEE 802.1v se relaciona con la etiqueta de VLAN IEEE 802.1v, que agrega información de prioridad de 802.1p a las tramas Ethernet etiquetadas con VLAN. Esta etiqueta se utiliza en las redes VLAN para mantener la calidad de servicio (QoS) incluso cuando el tráfico viaja a través de enlaces troncales que conectan diferentes switches.</p> <p>IEEE 802.1p: Este estándar se refiere a la asignación de prioridades a los paquetes Ethernet en función de los bits de prioridad contenidos en la cabecera de los paquetes. IEEE 802.1p permite la clasificación y la priorización del tráfico en diferentes clases de servicio, lo que garantiza que los paquetes críticos, como voz o video, reciban un trato preferencial en la red.</p> <p>Al respecto, El estándar IEEE 802.1v y la característica IEEE 802.1p están estrechamente relacionados en el contexto de la gestión de calidad de servicio (QoS) en redes Ethernet y VLAN (Virtual LAN). Por lo tanto, sirvase a confirmar se aceptará: "IEEE 802.1v o 802.1p".</p>	INGECORP	<p>Se confirma.</p> <p>Se reformula requerimiento de soporte:</p> <p>IEEE 802.1v o 802.1p</p>	IEEE 802.1v o 802.1p
5.2 .2. 1.1 .2	19	<p>Se pide "Debe tener mínimo una memoria RAM de 16GB "</p> <p>Al respecto se entrega 16 GB, de forma agrupada mediante 2 Tarjetas de control de 8GB. Sirvase a confirmar se aceptarán 2 tarjetas de 8GB.</p>	INGECORP	El requerimiento hace referencia a la capacidad de memoria que debe tener el equipamiento; en este caso de 16GB; independientemente de cómo lo implemente cada fabricante; respetando la capacidad solicitada. En ese sentido se reformula requerimiento.	Debe tener mínimo la capacidad de memoria de RAM de 16GB.
5.2 .2. 1.1 .2	19	<p>Se pide "Debe tener mínimo una memoria Flash de 16GB "</p> <p>Al respecto, el almacenamiento propuesto por cada fabricante varía de acuerdo a la capacidad o tamaños de su sistema operativo y configuraciones, es decir no es indispensable contar con una memoria Flash elevada si el sistema está correctamente estructurado por cada fabricante, definiendo capacidades óptimas para su propio sistema operativo y configuraciones almacenadas.</p> <p>Por lo tanto sirvase a confirmar se aceptaran memoria Flash mínima de 2GB.</p>	INGECORP	Tomando en consideración que la memoria flash sirve para el almacenamiento del sistema operativo y/o configuraciones; independientemente de cómo lo implemente cada fabricante; se aceptaran como mínimo la capacidad mínima de 2GB; este puede ser brindado en forma individual o forma agrupada. En ese sentido se reformula requerimiento.	Debe tener mínimo la capacidad de memoria Flash de 2GB
5.2 .2.	20	<p>Se pide "Debe permitir MC-LAG".</p> <p>Al respecto, MC-LAG es una tecnología que permite a múltiples dispositivos de red, como switches, trabajar</p>	INGECORP	El requerimiento hace referencia a la capacidad de del sistema para funcionar con una unidad lógica agrupando varios dispositivos físicos, que permitan	Se elimina MC-LAG y se reemplaza por:

1.1 .2	<p>juntos como un único dispositivo lógico para proporcionar redundancia y alta disponibilidad. El CSS es una configuración en la que múltiples switches se combinan para funcionar como una única unidad lógica.</p> <p>Por lo tanto, la tecnología MC-LAG (Multi-Chassis Link Aggregation Group) y el CSS (Cluster de Switch) son conceptos relacionados que se utilizan en redes empresariales y de centros de datos para mejorar la redundancia y la disponibilidad de la red.</p> <p>En base a lo anterior, sírvase a confirmar se aceptará MC-LAG o CSS.</p>		<p>contar con escenarios de redundancia y alta disponibilidad, independientemente de cómo lo denomine cada fabricante. En ese sentido se reformula requerimiento.</p>	<p>Debe permitir tecnología de múltiples dispositivos para que trabaje como un único dispositivo lógico para proporcionar redundancia y alta disponibilidad para entornos de redes empresariales y centro de datos.</p>
5.2 .2 20 1.1 .2	<p>Se pide "Debe incluir todos los componentes necesarios para realizar el stacking virtual "</p> <p>Al respecto, Tanto el stacking virtual como el CSS Cluster de Switch tienen como objetivo principal crear una entidad lógica única a partir de múltiples switches físicos. Ambas tecnologías permiten la administración y configuración simplificadas de los switches, lo que mejora la eficiencia operativa y la disponibilidad de la red.</p> <p>Por lo tanto, sírvase a confirmar se aceptará una solución equivalente a stacking virtual mediante CSS.</p>	INGECORP	<p>El requerimiento hace referencia a la capacidad de del sistema para funcionar con una unidad lógica agrupando varios dispositivos físicos, que permitan contar con escenarios de administración y configuración simplificada de estos dispositivos, logrando la eficiencia operativa y disponibilidad de la red; independientemente de como lo denomine cada fabricante. En ese sentido se reformula requerimiento.</p>	<p>Debe incluir todos los componentes necesarios para realizar el Stacking virtual o solución equivalente.</p>
5.2 .2 21 1.1 .2	<p>Se pide "Debe permitir no menos de 27000 entradas ACL ".</p> <p>El número de ACL (Listas de Control de Acceso) en un switch de distribución, en este caso, 27000 ACL, no necesariamente es determinante para su funcionamiento eficaz en esa ubicación específica dentro de la red. Los switches de distribución a menudo se utilizan para gestionar y enrutar el tráfico entre VLANs y para aplicar políticas de seguridad y control de acceso en la red. La cantidad de ACL requerida dependerá de la complejidad y las necesidades específicas de la red.</p> <p>En el contexto de la solicitud, es importante señalar que la cantidad de ACL solicitada para el switch core fue de 4000 ACL, lo que indica que esta cifra se consideró adecuada para las operaciones de toda la red. Sin embargo, es posible que en los switches de distribución no sea necesario un número tan elevado de ACL debido a su ubicación y función en la topología de red.</p> <p>En base a lo anterior, sírvase a confirmar se aceptará como mínimo 4000 ACL.</p>	INGECORP	<p>Con la finalidad de pluralidad de participantes, se reformula requerimiento, de la siguiente manera:</p> <p>Debe permitir no menos de 4000 entradas ACL</p>	<p>Debe permitir no menos de 4000 entradas ACL</p>
5.2 .2 21 1.1 .2	<p>Se pide "Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow, SPAN, ERSPAN ".</p> <p>Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sírvase a confirmar en el requerimiento: Netflow o sFlow o similares.</p> <p>Además, se pide soportar ERSPAN que es una tecnología que permite la copia y el envío de tráfico de red desde una interfaz o varias interfaces de red en un switch a un dispositivo de análisis remoto a través de una red IP. Sírvase a confirmar se aceptarán tecnologías similares con SPAN, RSPAN o ERSPAN.</p>	INGECORP	<p>Tomando en consideración que existe una diversidad de soluciones o tecnologías relacionadas a la captura y/o recolección de flujos utilizados para la supervisión de dispositivos de red; serán aceptadas soluciones y/o tecnologías similares. En ese sentido se reformula requerimiento.</p>	<p>"Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow o soluciones similares, SPAN, ERSPAN o tecnologías similares".</p>
5.2 .2 21 1.1 .2	<p>Se pide "Debe ser máximo de 1 Rack Unit (RU) "</p> <p>Debido a la cantidad de puertos de alto rendimiento (100G) el Switch debe contar con altas capacidades de reenvío siendo superior, sírvase a confirmar que aceptará capacidades entre 1 (RU) y 10 (RU).</p>	INGECORP	<p>Se precisa que, el espacio disponible para esta implementación es reducido; por lo tanto, para soluciones de tipo chasis para el requerimiento solicitado esta no podrá exceder de 8 RU. Se reformula requerimiento.</p>	<p>Debe ser máximo de 1 Rack Unit (RU). Para soluciones de tipo chasis no deberá excederse de 8 RU (unidades de rack)</p>
5.2 .2 21 1.1 .2	<p>Se pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)"</p> <p>En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo, y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque de flash seguro, para asegurar la integridad y autenticidad de nuestro hardware y software. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de</p>	<p>Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.</p>

		necesidades específicas. Por lo tanto sirvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque de flash seguro.		cifrado, para asegurar la integridad y autenticidad del hardware y software.	
5.2 .2 1.1 .2	21	Se pide "TACACS+" TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS. Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS	INGECORP	Se confirma, TACACS, TACACS+ o equivalentes	TACACS, TACACS+ o equivalentes
5.2 .2 1.1 .2	21	Se pide "RADSec" RadSec es un protocolo de seguridad que se utiliza para asegurar las comunicaciones entre servidores RADIUS (Remote Authentication Dial-In User Service) y clientes, garantizando la confidencialidad e integridad de los datos transmitidos. Esta tecnología es fundamental en entornos de autenticación y autorización de usuarios, especialmente en redes donde la seguridad es una prioridad. Al respecto, en el mercado existen distintas soluciones similares a Radsec como la verificación de seguridad por parte del servidor RADIUS a los usuarios que utilizan el protocolo Extensible Authentication Protocol over LAN (EAPoL). Esta información tiene como objetivo notificar a los usuarios acerca de los elementos que requieren verificaciones de seguridad adicionales, garantizando así que estén plenamente informados y conscientes de las medidas de seguridad aplicadas en nuestra red. Por lo tanto, sirvase a confirmar se aceptará soluciones RADSec o similar.	INGECORP	Se confirma RADSec o similares	RADSec o similares
5.2 .2 1.1 .2	21	Se pide "CoPP (Control Plane Policy)" El CoPP (Cisco) utiliza filtros de acceso para limitar el tráfico que se dirige al plano de control, lo que ayuda a prevenir la saturación y los ataques de denegación de servicio contra el dispositivo. El equipo propuesto ofrece características de seguridad similares como la autenticación de usuario y la protección contra ataques de inundación, (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, Defense Against Fragmentation Attacks, Defense Against TCP SYN Flood Packets, Defense Against UDP Flood Attacks, Defense Against ICMP Flood Attacks). Por lo tanto, aunque el CoPP es una función específica de los dispositivos Cisco, los switches propuestos ofrecen características de seguridad similares que protegen el dispositivo contra ataques malintencionados y garantizar que el tráfico importante tenga prioridad sobre otros tipos de tráfico. En conclusión, sirvase a confirmar se aceptará CoPP o características de seguridad similares como (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, etc).	INGECORP	Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera: Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.	Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.
5.2 .2 1.1 .2	21	Se pide "Root Guard" Al respecto, se debe tener en cuenta que existen fabricantes en el mercado que denominan de otra forma a estas funcionalidades. Por ejemplo, a "STP root guard" también se le denomina "Root protection". Por tanto, se sugiere respetuosamente a la entidad considerar qu en el requerimiento se solicite Root Guard o equivalente.	INGECORP	Se confirma Root Guard o equivalente	Root Guard o equivalente
5.2 .2 1.1 .2	21	Se pide "Private VLAN" (Private VLAN) es una tecnología que permite segmentar un VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos. Se provee lo mismo mediante Super-VLAN (S-VLAN). Al igual que PVLAN, S-VLAN permite segmentar una VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos para mejorar la seguridad y el aislamiento entre dispositivos y usuarios en una misma red.	INGECORP	Se confirma Private VLAN o similares	Private VLAN o similares

		Por lo tanto, sírvase a confirmar que se aceptará Private VLAN o similar.			
5.2 .2 1.1 .2	21	<p>Se pide "Deberá contar con mecanismos de seguridad de IPv6 First-Hop".</p> <p>IPv6 First-Hop, es una función de seguridad que se utiliza para proteger el tráfico de IPv6, como los enlaces Ethernet. Esta función se utiliza para proteger contra amenazas como los ataques de spoofing y los ataques de inundación.</p> <p>Se provee lo mismo, la función equivalente a IPv6 First Hop Security de Cisco se conoce como IPv6 Secure Neighbor Discovery (SEND). Esta función se utiliza para proteger el tráfico de IPv6 en los enlaces de capa 2, como los enlaces Ethernet. La función utiliza una combinación de autenticación, criptografía y verificación de estado para asegurar que los dispositivos de la red puedan confiar en los mensajes de descubrimiento de vecinos IPv6 que se intercambian en la capa 2.</p> <p>Por lo tanto, se entrega la misma función, sírvase a confirmar se aceptará IPv6 First-Hop o IPv6 Secure Neighbor Discovery.</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Deberá contar con mecanismo y/o función de seguridad que utilice una combinación de autenticación, criptografía y verificación de estado para asegurar que los dispositivos de la red puedan confiar en los mensajes de descubrimiento de vecinos IPv6 que se intercambian en la capa 2.</p>	Deberá contar con mecanismo y/o función de seguridad que utilice una combinación de autenticación, criptografía y verificación de estado para asegurar que los dispositivos de la red puedan confiar en los mensajes de descubrimiento de vecinos IPv6 que se intercambian en la capa 2.
5.2 .2 1.1 .2	22	<p>Se pide "Deberá contar con mecanismos para garantizar que el sistema operativo sea íntegro y consistente en todos los switches".</p> <p>Al respecto, para cumplir con el siguiente requisito existen distintas formas de garantizar esta seguridad. Para mantener la seguridad y la coherencia en nuestra infraestructura de red, existen soluciones equivalentes como el arranque de flash seguro.</p> <p>Por lo tanto, sírvase a confirmar se aceptará: "Deberá contar con mecanismos para garantizar que el sistema operativo sea íntegro y consistente en todos los switches o arranque seguro de flash".</p>	INGECORP	<p>Se precisa que, independientemente como implemente la solución para garantizar la seguridad del sistema operativo de cada fabricante o como se la denomine; se deberá contar con estos mecanismos para garantizar que el sistema operativo sea íntegro y consistente en todos los switches.</p>	
5.2 .2 1.1 .2	22	<p>Se pide: "Deberá contar con mecanismos que prevengan ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos".</p> <p>Al respecto, el requisito de "Deberá contar con mecanismos que prevengan ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos" guarda una similitud fundamental con la implementación de un "arranque de flash seguro". Ambos objetivos se centran en salvaguardar la autenticidad e integridad del software o firmware en nuestros equipos. Al implementar un "arranque de flash seguro," establecemos una barrera efectiva contra posibles ataques de intermediarios maliciosos, ya que garantiza que el software o firmware se inicie desde una fuente confiable y que no haya sido comprometido durante el proceso de inicio. En esencia, ambas medidas buscan prevenir manipulaciones no autorizadas del software/firmware y garantizar que los equipos se ejecuten con la autenticidad e integridad necesarias para mantener la seguridad de nuestra infraestructura de red.</p> <p>Por lo tanto, sírvase a confirmar se aceptará: "Deberá contar con mecanismos que prevengan ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos o arranque seguro de flash".</p>	INGECORP	<p>Se precisa que, independientemente como implemente la solución, para prevenir ataques de tipo hombre en el medio que puedan comprometer la autenticidad e integridad del software/firmware instalado en los equipos, de cada fabricante o como se la denomine; estos serán una barrera contra ataques de intermediarios maliciosos que prevengan manipulaciones no autorizadas del software/firmware en los equipos.</p>	
5.2 .2 1.1 .2	22	<p>Se pide "El Switch propuesto deberá soportar funcionalidades que ayuden a identificar amenazas o anomalías en la red incluso descubrimiento malware en el tráfico cifrado".</p> <p>Al respecto, lo anterior es similar a la capacidad de soportar "firmas digitales y certificados." Ambos enfoques tienen como objetivo principal fortalecer la seguridad de la red y detectar posibles amenazas, incluyendo aquellas que pueden ocultarse en el tráfico cifrado.</p> <p>La implementación de firmas digitales y certificados es un mecanismo efectivo para verificar la autenticidad y la integridad de los datos en la red. Al verificar las firmas digitales de los datos y utilizar certificados para autenticar la identidad de los dispositivos y usuarios, podemos asegurar que la información transmitida no ha sido alterada y proviene de fuentes confiables.</p>	INGECORP	<p>Se precisa que, independientemente como implemente la solución, sobre funcionalidades que ayuden a identificar amenazas o anomalías en la red incluso descubrimiento malware en el tráfico cifrado, de cada fabricante o como se la denomine; el objetivo es fortalecer la seguridad de la red detectando posibles amenazas, inclusive si es tráfico encriptado/cifrado; por lo tanto, se pide que pueda asegurarse que la información transmitida no haya sido alterada y que provenga de fuentes confiables.</p>	

		Por lo tanto, sirvase a confirmar se aceptará: "El Switch propuesto deberá soportar funcionalidades que ayuden a identificar amenazas o anomalías en la red incluso descubrimiento malware en el tráfico cifrado o arranque seguro de flash".			
5.2 .2 1.1 .2	22	<p>Se pide "Debe soportar e implementar mecanismos de encolamiento Shaped Round Robin (SRR) y Committed Information Rate (CIR)".</p> <p>Debido a que existen funciones similares: Al respecto, la tecnología "Shaped Round Robin (SRR)" y el soporte para "Weighted Round Robin (WRR)" son dos enfoques similares utilizados en la gestión del tráfico de red en switches y routers. Aunque no son idénticos en su funcionamiento, comparten similitudes fundamentales en términos de asignación de prioridad y equidad en la distribución del tráfico.</p> <p>Tanto SRR como WRR se centran en la programación de cómo se maneja el tráfico en una cola de salida del dispositivo de red. SRR, en particular, se utiliza para asignar un peso o una prioridad a cada flujo de tráfico en la cola y determinar cómo se atienden estos flujos en función de su peso o prioridad. Por otro lado, WRR asigna pesos específicos a diferentes flujos de tráfico y distribuye el ancho de banda disponible en función de estos pesos, lo que le permite otorgar prioridad a ciertos flujos sobre otros</p> <p>Por lo tanto sirvase a confirmar se aceptará: "Debe soportar e implementar mecanismos de encolamiento Shaped Round Robin (SRR) o WRR, y Committed Information Rate (CIR)"</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Debe soportar e implementar mecanismos de encolamiento Shaped Round Robin (SRR) o WRR, y Committed Information Rate (CIR)"</p>	Debe soportar e implementar mecanismos de encolamiento Shaped Round Robin (SRR) o WRR, y Committed Information Rate (CIR)"
5.2 .2 1.1 .2	23	<p>Se pide "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo".</p> <p>Al respecto, el requisito de incluir una etiqueta RFID (RFID Tag) en el switch propuesto, ya sea interna o externa, tiene un propósito específico que no está directamente relacionado con el funcionamiento de la red en sí. En lugar de sumar a la funcionalidad de la red, se centra en aspectos relacionados con la administración y el mantenimiento de los equipos de red. La inclusión de una etiqueta RFID tiene más que ver con la gestión y la identificación eficiente de los dispositivos que conforman la red.</p> <p>Por lo anterior, sirvase a confirmar esta característica será considerada como opcional: "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo o opcional".</p>	INGECORP	No se confirma, se requiere incluir esta característica sin limitación, puede ser interna o externa, puede ser del mismo fabricante o de terceros.	
5.2 .2 1.1 .2	23	Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sirvase a confirmar en el requerimiento: Netflow o sFlow o similares.	INGECORP	Tomando en consideración que existe una diversidad de soluciones o tecnologías relacionadas a la captura y/o recolección de flujos utilizados para la supervisión de dispositivos de red; serán aceptados soluciones y/o tecnologías similares. En ese sentido se reformula requerimiento.	"Soporte instalado y operativo de sFlow o Netflow o soluciones similares".
5.2 .2 1.1 .2	23	<p>Se pide "802.1v".</p> <p>IEEE 802.1v se relaciona con la etiqueta de VLAN IEEE 802.1v, que agrega información de prioridad de 802.1p a las tramas Ethernet etiquetadas con VLAN. Esta etiqueta se utiliza en las redes VLAN para mantener la calidad de servicio (QoS) incluso cuando el tráfico viaja a través de enlaces troncales que conectan diferentes switches.</p> <p>IEEE 802.1p: Este estándar se refiere a la asignación de prioridades a los paquetes Ethernet en función de los bits de prioridad contenidos en la cabecera de los paquetes. IEEE 802.1p permite la clasificación y la priorización del tráfico en diferentes clases de servicio, lo que garantiza que los paquetes críticos, como voz o video, reciban un trato preferencial en la red.</p> <p>Al respecto, El estándar IEEE 802.1v y la característica IEEE 802.1p están estrechamente relacionados en el contexto de la gestión de calidad de servicio (QoS) en redes Ethernet y VLAN (Virtual LAN). Por lo tanto, sirvase a confirmar se aceptará: "IEEE 802.1v o 802.1p".</p>	INGECORP	<p>Se confirma.</p> <p>Se reformula requerimiento de soporte:</p> <p>IEEE 802.1v o 802.1p</p>	IEEE 802.1v o 802.1p

5.2 .2 1.1 .3	24	<p>Se pide "El switch propuesto debete tener al menos 8GB de memoria RAM y 16GB de memoria Flash"</p> <p>La capacidad de memoria RAM en un switch será relativa a las características del equipo: por ejemplo, el tamaño del sistema operativo, el tamaño de su configuración, el tamaño de los logs que maneja, entre otros. Si el equipo ha sido diseñado de forma tal que optimice sus recursos, entonces el tamaño de la RAM no necesita ser tan grande.</p> <p>Lo mismo sucederá con la capacidad del Flash. Este será requerido en función de las características del equipo en sí.</p> <p>Por lo anterior, se sugiere respetuosamente a la entidad:</p> <ol style="list-style-type: none"> 1. Solicitar en el switch una capacidad RAM no menor a 4 GB, y 2. Solicitar en el switch una capacidad flash no menor a 2 GB. 	INGECORP	<p>Se precisa que, de acuerdo con nuestros registros de funcionamiento actual, los equipos deben contar con al menos 8GB de memoria RAM y 2GB de memoria Flash.</p> <p>Se actualizan las especificaciones.</p>	El switch propuesto debe tener al menos 8GB de memoria RAM y 2GB de memoria Flash
5.2 .2 1.1 .3	24	<p>Se pide "El switch propuesto debe soportar contenedores, para segurar máxima flexibilidad y aislamiento del sistema operativo principal.</p> <p>Este enunciado significa que el switch que se está considerando debe ser capaz de trabajar con contenedores de software. Esto es importante para garantizar que la red tenga la mayor flexibilidad posible y para separar de manera efectiva el sistema operativo principal de otros componentes.</p> <p>Al respecto para garantizar este requerimiento muchos fabricantes en el mercado implementan sistemas operativos modular.</p> <p>Por lo tanto, sírvase a confirmar se aceptará: "El switch propuesto debe soportar contenedores, para asegurar máxima flexibilidad y aislamiento del sistema operativo principal o contar con un sistema operativo modular"</p>	INGECORP	<p>Se precisa que, con la finalidad de homogenizar la concepción de la flexibilidad y aislamiento del sistema operativo modular, el requerimiento será reformulado de la siguiente manera:</p> <p>El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal</p>	El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal
5.2 .2 1.1 .3	24	<p>Se pide "Debe permitir no menos de 8000 entradas ACL"</p> <p>Sírvase a confirmar se aceptará una capacidad de 8000 entradas ACL entre IPv4 y IPv6.</p>	INGECORP	Se confirma, la capacidad de 8000 entradas ACL serán para la lista de control de accesos de IPV4 e IPV6.	Debe permitir no menos de 8000 entradas ACL IPv4 e IPV6
5.2 .2 1.1 .3	24	<p>Se pide "El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking."</p> <p>Debido a que muchos fabricantes implenta Stacking de forma lógica o física, sírvase a confirmar que también será válido la realización de stacking atraves de puertos de servicio dedicados para stacking.</p>	INGECORP	No se confirma, los puertos de servicio son para servicio; y los puertos para Stacking son para el apilamiento.	
5.2 .2 1.1 .3	25	<p>Se pide "Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow, SPAN, ERSPAN "</p> <p>Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sírvase a confirmar en el requerimiento: Netflow o sFlow o similares.</p> <p>Además, se pide soportar ERSPAN que es una tecnología que permite la copia y el envío de tráfico de red desde una interfaz o varias interfaces de red en un switch a un dispositivo de análisis remoto a través de una red IP. Sírvase a confirmar se aceptarán tecnologías similares con SPAN, RSPAN o ERSPAN.</p>	INGECORP	Tomando en consideración que existe una diversidad de soluciones o tecnologías relacionadas a la captura y/o recolección de flujos utilizados para la supervisión de dispositivos de red; serán aceptados soluciones y/o tecnologías similares. En ese sentido se reformula requerimiento.	"Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow o soluciones similares, SPAN, ERSPAN o tecnologías similares".
5.2 .2 1.1 .3	25	<p>Se pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)"</p> <p>En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo, y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque de flash seguro, para asegurar la integridad y autenticidad de nuestro hardware y software. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras necesidades específicas.</p> <p>Por lo tanto, sírvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque de flash seguro.</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.</p>	Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.

5.2 .2 1.1 .3	25	<p>Se pide "TACACS+"</p> <p>TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS.</p> <p>Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS</p>	INGECORP	Se confirma, TACACS, TACACS+ o equivalentes	TACACS, TACACS+ o equivalentes
5.2 .2 1.1 .3	25	<p>Se pide "RADSec"</p> <p>RadSec es un protocolo de seguridad que se utiliza para asegurar las comunicaciones entre servidores RADIUS (Remote Authentication Dial-In User Service) y clientes, garantizando la confidencialidad e integridad de los datos transmitidos. Esta tecnología es fundamental en entornos de autenticación y autorización de usuarios, especialmente en redes donde la seguridad es una prioridad.</p> <p>Al respecto, en el mercado existen distintas soluciones similares a Radsec como la verificación de seguridad por parte del servidor RADIUS a los usuarios que utilizan el protocolo Extensible Authentication Protocol over LAN (EAPoL). Esta información tiene como objetivo notificar a los usuarios acerca de los elementos que requieren verificaciones de seguridad adicionales, garantizando así que estén plenamente informados y conscientes de las medidas de seguridad aplicadas en nuestra red.</p> <p>Por lo tanto, sirvase a confirmar se aceptará soluciones RADSec o similar.</p>	INGECORP	Se confirma RADSec o similares	RADSec o similares
5.2 .2 1.1 .3	25	<p>Se pide "CoPP (Control Plane Policy)"</p> <p>El CoPP (Cisco) utiliza filtros de acceso para limitar el tráfico que se dirige al plano de control, lo que ayuda a prevenir la saturación y los ataques de denegación de servicio contra el dispositivo.</p> <p>El equipo propuesto ofrece características de seguridad similares como la autenticación de usuario y la protección contra ataques de inundación, (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, Defense Against Fragmentation Attacks, Defense Against TCP SYN Flood Packets, Defense Against UDP Flood Attacks, Defense Against ICMP Flood Attacks).</p> <p>Por lo tanto, aunque el CoPP es una función específica de los dispositivos Cisco, los switches propuestos ofrecen características de seguridad similares que protegen el dispositivo contra ataques malintencionados y garantizar que el tráfico importante tenga prioridad sobre otros tipos de tráfico.</p> <p>En conclusión, sirvase a confirmar se aceptará CoPP o características de seguridad similares como (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, etc).</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.</p>	Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.
5.2 .2 1.1 .3	25	<p>Se pide "Root Guard"</p> <p>Al respecto, se debe tener en cuenta que existen fabricantes en el mercado que denominan de otra forma a estas funcionalidades. Por ejemplo, a "STP root guard" también se le denomina "Root protection".</p> <p>Por tanto, se sugiere respetuosamente a la entidad considerar que en el requerimiento se solicite Root Guard o equivalente.</p>	INGECORP	Se confirma Root Guard o equivalente	Root Guard o equivalente
5.2 .2 1.1 .3	25	<p>Se pide "Private VLAN"</p> <p>(Private VLAN) es una tecnología que permite segmentar un VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos.</p> <p>Se provee lo mismo mediante Super-VLAN (S-VLAN). Al igual que PVLAN, S-VLAN permite segmentar una VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos para mejorar la seguridad y el aislamiento entre dispositivos y usuarios en una misma red.</p> <p>Por lo tanto, sirvase a confirmar que se aceptará Private VLAN o similar.</p>	INGECORP	Se confirma Private VLAN o similares	Private VLAN o similares

5.2 .2 1.1 .3	25	<p>Se pide "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo".</p> <p>Al respecto, el requisito de incluir una etiqueta RFID (RFID Tag) en el switch propuesto, ya sea interna o externa, tiene un propósito específico que no está directamente relacionado con el funcionamiento de la red en sí. En lugar de sumar a la funcionalidad de la red, se centra en aspectos relacionados con la administración y el mantenimiento de los equipos de red. La inclusión de una etiqueta RFID tiene más que ver con la gestión y la identificación eficiente de los dispositivos que conforman la red.</p> <p>Por lo anterior, servirse a confirmar esta característica será considerada como opcional: "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo o opcional".</p>	INGECORP	No se confirma, se requiere incluir esta característica sin limitación, puede ser interna o externa, puede ser del mismo fabricante o de terceros.	
5.2 .2 1.1 .3	26	<p>Se pide: "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. ".</p> <p>Al respecto, el requisito de "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. " guarda una similitud fundamental con la implementación de un "arranque de flash seguro". Ambos objetivos se centran en salvaguardar la autenticidad e integridad del software o firmware en nuestros equipos. Al implementar un "arranque de flash seguro," establecemos una barrera efectiva contra posibles ataques de intermediarios maliciosos, ya que garantiza que el software o firmware se inicie desde una fuente confiable y que no haya sido comprometido durante el proceso de inicio. En esencia, ambas medidas buscan prevenir manipulaciones no autorizadas del software/firmware y garantizar que los equipos se ejecuten con la autenticidad e integridad necesarias para mantener la seguridad de nuestra infraestructura de red.</p> <p>Por lo tanto, servirse a confirmar se aceptará: "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software o arranque seguro de flash".</p>	INGECORP	Se precisa que, independientemente como implemente la solución, que incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma, de cada fabricante o como se la denomine; estos serán una barrera efectiva contra ataques de intermediarios maliciosos que prevengan manipulaciones no autorizadas del software/firmware en los equipos.	
5.2 .2 1.1 .3	26	<p>Se pide "El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware."</p> <p>Al respecto, en el mercado muchos fabricantes realizan este procesamiento de Transmisión de paquetes IPv6 en hardware, implica que el switch tiene la capacidad de procesar y enrutar paquetes IPv6 utilizando recursos de hardware o de manera lógica.</p> <p>Por lo tanto, servirse a confirmar se aceptará: "El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware o de manera lógica"</p>	INGECORP	<p>Con la finalidad de no limitar a los participantes, se confirma que la transmisión de paquetes sea en hardware o de manera lógica. Se reformula requerimiento:</p> <p>El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware o de manera lógica.</p>	El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware o de manera lógica.
5.2 .2 1.1 .3	26	<p>Se pide "802.1v".</p> <p>IEEE 802.1v se relaciona con la etiqueta de VLAN IEEE 802.1v, que agrega información de prioridad de 802.1p a las tramas Ethernet etiquetadas con VLAN. Esta etiqueta se utiliza en las redes VLAN para mantener la calidad de servicio (QoS) incluso cuando el tráfico viaja a través de enlaces troncales que conectan diferentes switches.</p> <p>IEEE 802.1p: Este estándar se refiere a la asignación de prioridades a los paquetes Ethernet en función de los bits de prioridad contenidos en la cabecera de los paquetes. IEEE 802.1p permite la clasificación y la priorización del tráfico en diferentes clases de servicio, lo que garantiza que los paquetes críticos, como voz o video, reciban un trato preferencial en la red.</p>	INGECORP	<p>Se confirma.</p> <p>Se reformula requerimiento de soporte:</p> <p>IEEE 802.1v o 802.1p</p>	IEEE 802.1v o 802.1p

		Al respecto, El estándar IEEE 802.1v y la característica IEEE 802.1p están estrechamente relacionados en el contexto de la gestión de calidad de servicio (QoS) en redes Ethernet y VLAN (Virtual LAN). Por lo tanto, sirvase a confirmar se aceptará: "IEEE 802.1v o 802.1p".			
5.2 .2 1.1 .4	27	<p>Se pide "El switch propuesto debete tener al menos 8GB de memoria RAM y 16GB de memoria Flash"</p> <p>La capacidad de memoria RAM en un switch será relativa a las características del equipo: por ejemplo, el tamaño del sistema operativo, el tamaño de su configuración, el tamaño de los logs que maneja, entre otros. Si el equipo ha sido diseñado de forma tal que optimice sus recursos, entonces el tamaño de la RAM no necesita ser tan grande.</p> <p>Lo mismo sucederá con la capacidad del Flash. Este será requerido en función de las características del equipo en sí.</p> <p>Por lo anterior, se sugiere respetuosamente a la entidad:</p> <ol style="list-style-type: none"> 1. Solicitar en el switch una capacidad RAM no menor a 4 GB, y 2. Solicitar en el switch una capacidad flash no menor a 2 GB. 	INGECORP	<p>Se precisa que, de acuerdo con nuestros registros de funcionamiento actual, los equipos deben contar con al menos 8GB de memoria RAM y 2GB de memoria Flash.</p> <p>Se actualizan las especificaciones.</p>	El switch propuesto debe tener al menos 8GB de memoria RAM y 2GB de memoria Flash
5.2 .2 1.1 .4	27	<p>Se pide "El switch propuesto debe soportar contenedores, para segurar máxima flexibilidad y aislamiento del sistema operativo principal.</p> <p>Este enunciado significa que el switch que se está considerando debe ser capaz de trabajar con contenedores de software. Esto es importante para garantizar que la red tenga la mayor flexibilidad posible y para separar de manera efectiva el sistema operativo principal de otros componentes.</p> <p>Al respecto para garantizar este requerimiento muchos fabricantes en el mercado implementan sistemas operativos modular.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "El switch propuesto debe soportar contenedores, para asegurar máxima flexibilidad y aislamiento del sistema operativo principal o contar con un sistema operativo modular"</p>	INGECORP	<p>Se precisa que, con la finalidad de homogenizar la concepción de la flexibilidad y aislamiento del sistema operativo modular, el requerimiento será reformulado de la siguiente manera:</p> <p>El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal</p>	El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal
5.2 .2 1.1 .4	27	<p>Se pide "Debe permitir no menos de 8000 entradas ACL"</p> <p>Sirvase a confirmar se aceptará una capacidad de 8000 entradas ACL entre IPv4 y IPv6.</p>	INGECORP	Se confirma, la capacidad de 8000 entradas ACL serán para la lista de control de accesos de IPv4 e IPv6.	Debe permitir no menos de 8000 entradas ACL IPv4 e IPv6
5.2 .2 1.1 .4	27	<p>Se pide "El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking."</p> <p>Debido a que muchos fabricantes implenta Stacking de forma logica o fisica, sirvase a confirmar que también será válido la realización de stacking atraves de puertos de servicio dedicados para stacking.</p>	INGECORP	No se confirma, los puertos de servicio son para servicio; y los puertos para Stacking son para el apilamiento.	
5.2 .2 1.1 .4		<p>Se pide "Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow, SPAN, ERSPAN".</p> <p>Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sirvase a confirmar en el requerimiento: Netflow o sFlow o similares.</p> <p>Además, se pide soportar ERSPAN que es una tecnología que permite la copia y el envío de tráfico de red desde una interfaz o varias interfaces de red en un switch a un dispositivo de análisis remoto a través de una red IP. Sirvase a confirmar se aceptarán tecnologías similares con SPAN, RSPAN o ERSPAN.</p>	INGECORP	Tomando en consideración que existe una diversidad de soluciones o tecnologías relacionadas a la captura y/o recolección de flujos utilizados para la supervisión de dispositivos de red; serán aceptados soluciones y/o tecnologías similares. En ese sentido se reformula requerimiento.	"Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow o soluciones similares, SPAN, ERSPAN o tecnologías similares".
5.2 .2 1.1 .4	28	<p>e pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)"</p> <p>En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo, y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque de flash seguro, para asegurar la integridad y autenticidad de nuestro hardware y software. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras necesidades específicas.</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.</p>	Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.

		Por lo tanto, sírvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque de flash seguro.			
5.2 .2 1.1 .4	28	<p>Se pide "TACACS+"</p> <p>TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS.</p> <p>Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS</p>	INGECORP	Se confirma, TACACS, TACACS+ o equivalentes	TACACS, TACACS+ o equivalentes
5.2 .2 1.1 .4	28	<p>Se pide "RADSec"</p> <p>RadSec es un protocolo de seguridad que se utiliza para asegurar las comunicaciones entre servidores RADIUS (Remote Authentication Dial-In User Service) y clientes, garantizando la confidencialidad e integridad de los datos transmitidos. Esta tecnología es fundamental en entornos de autenticación y autorización de usuarios, especialmente en redes donde la seguridad es una prioridad.</p> <p>Al respecto, en el mercado existen distintas soluciones similares a Radsec como la verificación de seguridad por parte del servidor RADIUS a los usuarios que utilizan el protocolo Extensible Authentication Protocol over LAN (EAPoL). Esta información tiene como objetivo notificar a los usuarios acerca de los elementos que requieren verificaciones de seguridad adicionales, garantizando así que estén plenamente informados y conscientes de las medidas de seguridad aplicadas en nuestra red.</p> <p>Por lo tanto, sírvase a confirmar se aceptará soluciones RADSec o similar.</p>	INGECORP	Se confirma RADSec o similares	RADSec o similares
5.2 .2 1.1 .4	28	<p>Se pide "CoPP (Control Plane Policy)"</p> <p>El CoPP (Cisco) utiliza filtros de acceso para limitar el tráfico que se dirige al plano de control, lo que ayuda a prevenir la saturación y los ataques de denegación de servicio contra el dispositivo.</p> <p>El equipo propuesto ofrece características de seguridad similares como la autenticación de usuario y la protección contra ataques de inundación, (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, Defense Against Fragmentation Attacks, Defense Against TCP SYN Flood Packets, Defense Against UDP Flood Attacks, Defense Against ICMP Flood Attacks).</p> <p>Por lo tanto, aunque el CoPP es una función específica de los dispositivos Cisco, los switches propuestos ofrecen características de seguridad similares que protegen el dispositivo contra ataques malintencionados y garantizar que el tráfico importante tenga prioridad sobre otros tipos de tráfico.</p> <p>En conclusión, sírvase a confirmar se aceptará CoPP o características de seguridad similares como (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, etc).</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.</p>	Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.
5.2 .2 1.1 .4	28	<p>Se pide "Root Guard"</p> <p>Al respecto, se debe tener en cuenta que existen fabricantes en el mercado que denominan de otra forma a estas funcionalidades. Por ejemplo, a "STP root guard" también se le denomina "Root protection".</p> <p>Por tanto, se sugiere respetuosamente a la entidad considerar que en el requerimiento se solicite Root Guard o equivalente.</p>	INGECORP	Se confirma Root Guard o equivalente	Root Guard o equivalente
5.2 .2 1.1 .4	28	<p>Se pide "Private VLAN"</p> <p>(Private VLAN) es una tecnología que permite segmentar un VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos.</p> <p>Se provee lo mismo mediante Super-VLAN (S-VLAN). Al igual que PVLAN, S-VLAN permite segmentar una VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos para mejorar la seguridad y el aislamiento entre dispositivos y usuarios en una misma red.</p>	INGECORP	Se confirma Private VLAN o similares	Private VLAN o similares

		Por lo tanto, sirvase a confirmar que se aceptará Private VLAN o similar.			
5.2 .2 1.1 .4	28	<p>Se pide "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo".</p> <p>Al respecto, el requisito de incluir una etiqueta RFID (RFID Tag) en el switch propuesto, ya sea interna o externa, tiene un propósito específico que no está directamente relacionado con el funcionamiento de la red en sí. En lugar de sumar a la funcionalidad de la red, se centra en aspectos relacionados con la administración y el mantenimiento de los equipos de red. La inclusión de una etiqueta RFID tiene más que ver con la gestión y la identificación eficiente de los dispositivos que conforman la red.</p> <p>Por lo anterior, sirvase a confirmar esta característica será considerada como opcional: "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo o opcional".</p>	INGECORP	No se confirma, se requiere incluir esta característica sin limitación, puede ser interna o externa, puede ser del mismo fabricante o de terceros.	
5.2 .2 1.1 .4		<p>Se pide: "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. ".</p> <p>Al respecto, el requisito de "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. " guarda una similitud fundamental con la implementación de un "arranque de flash seguro". Ambos objetivos se centran en salvaguardar la autenticidad e integridad del software o firmware en nuestros equipos. Al implementar un "arranque de flash seguro," establecemos una barrera efectiva contra posibles ataques de intermediarios maliciosos, ya que garantiza que el software o firmware se inicie desde una fuente confiable y que no haya sido comprometido durante el proceso de inicio. En esencia, ambas medidas buscan prevenir manipulaciones no autorizadas del software/firmware y garantizar que los equipos se ejecuten con la autenticidad e integridad necesarias para mantener la seguridad de nuestra infraestructura de red.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software o arranque seguro de flash".</p>	INGECORP	Se precisa que, independientemente como implemente la solución, que incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma, de cada fabricante o como se la denomine; estos serán una barrera efectiva contra ataques de intermediarios maliciosos que prevengan manipulaciones no autorizadas del software/firmware en los equipos.	
5.2 .2 1.1 .4	29	<p>Se pide "El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware."</p> <p>Al respecto, en el mercado muchos fabricantes realizan este procesamiento de Transmisión de paquetes IPv6 en hardware, implica que el switch tiene la capacidad de procesar y enrutar paquetes IPv6 utilizando recursos de hardware o de manera lógica.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware o de manera lógica"</p>	INGECORP	<p>Con la finalidad de no limitar a los participantes, se confirma que la transmisión de paquetes sea en hardware o de manera lógica. Se reformula requerimiento:</p> <p>El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware o de manera lógica.</p>	El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware o de manera lógica.
5.2 .2 1.1 .4	29	<p>Se pide "802.1v".</p> <p>IEEE 802.1v se relaciona con la etiqueta de VLAN IEEE 802.1v, que agrega información de prioridad de 802.1p a las tramas Ethernet etiquetadas con VLAN. Esta etiqueta se utiliza en las redes VLAN para mantener la calidad de servicio (QoS) incluso cuando el tráfico viaja a través de enlaces troncales que conectan diferentes switches.</p> <p>IEEE 802.1p: Este estándar se refiere a la asignación de prioridades a los paquetes Ethernet en función de los bits de prioridad contenidos en la cabecera de los paquetes. IEEE 802.1p permite la clasificación y la</p>	INGECORP	<p>Se confirma.</p> <p>Se reformula requerimiento de soporte:</p> <p>IEEE 802.1v o 802.1p</p>	IEEE 802.1v o 802.1p

		<p>priorización del tráfico en diferentes clases de servicio, lo que garantiza que los paquetes críticos, como voz o video, reciban un trato preferencial en la red.</p> <p>Al respecto, El estándar IEEE 802.1v y la característica IEEE 802.1p están estrechamente relacionados en el contexto de la gestión de calidad de servicio (QoS) en redes Ethernet y VLAN (Virtual LAN). Por lo tanto, sirvase a confirmar se aceptará: "IEEE 802.1v o 802.1p".</p>			
5.2 .2. 1.1 .5	30	<p>Se pide "El switch propuesto debete tener al menos 8GB de memoria RAM y 16GB de memoria Flash"</p> <p>La capacidad de memoria RAM en un switch será relativa a las características del equipo: por ejemplo, el tamaño del sistema operativo, el tamaño de su configuración, el tamaño de los logs que maneja, entre otros. Si el equipo ha sido diseñado de forma tal que optimice sus recursos, entonces el tamaño de la RAM no necesita ser tan grande.</p> <p>Lo mismo sucederá con la capacidad del Flash. Este será requerido en función de las características del equipo en sí.</p> <p>Por lo anterior, se sugiere respetuosamente a la entidad:</p> <ol style="list-style-type: none"> 1. Solicitar en el switch una capacidad RAM no menor a 4 GB, y 2. Solicitar en el switch una capacidad flash no menor a 2 GB. 	INGECORP	<p>Se precisa que, de acuerdo con nuestros registros de funcionamiento actual, los equipos deben contar con al menos 8GB de memoria RAM y 2GB de memoria Flash.</p> <p>Se actualizan las especificaciones.</p>	El switch propuesto debe tener al menos 8GB de memoria RAM y 2GB de memoria Flash
5.2 .2. 1.1 .5	30	<p>Se pide "El switch propuesto debe soportar contenedores, para segurar máxima flexibilidad y aislamiento del sistema operativo principal.</p> <p>Este enunciado significa que el switch que se está considerando debe ser capaz de trabajar con contenedores de software. Esto es importante para garantizar que la red tenga la mayor flexibilidad posible y para separar de manera efectiva el sistema operativo principal de otros componentes.</p> <p>Al respecto para garantizar este requerimiento muchos fabricantes en el mercado implementan sistemas operativos modular.</p> <p>Por lo tanto sirvase a confirmar se aceptará: "El switch propuesto debe soportar contenedores, para asegurar máxima flexibilidad y aislamiento del sistema operativo principal o contar con un sistema operativo modular"</p>	INGECORP	<p>Se precisa que, con la finalidad de homogenizar la concepción de la flexibilidad y aislamiento del sistema operativo modular, el requerimiento será reformulado de la siguiente manera:</p> <p>El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal</p>	El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal
5.2 .2. 1.1 .5	30	<p>Se pide "Debe permitir no menos de 8000 entradas ACL"</p> <p>Sirvase a confirmar se aceptará una capacidad de 8000 entradas ACL entre IPv4 y IPv6.</p>	INGECORP	Se confirma, la capacidad de 8000 entradas ACL serán para la lista de control de accesos de IPV4 e IPV6.	Debe permitir no menos de 8000 entradas ACL IPv4 e IPV6
5.2 .2. 1.1 .5	30	<p>Se pide "El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking."</p> <p>Debido a que muchos fabricantes implenta Stacking de forma logica o fisica, sirvase a confirmar que también será válido la realización de stacking atraves de puertos de servicio dedicados para stacking.</p>	INGECORP	No se confirma, los puertos de servicio son para servicio; y los puertos para Stacking son para el apilamiento.	
5.2 .2. 1.1 .5	30	<p>Se pide "Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow, SPAN, ERSPAN".</p> <p>Muchos fabricantes en el mercado ofrecen diferentes protocolos de muestreo, entre ellos sFlow, Netflow o Netstream. Por tanto, sirvase a confirmar en el requerimiento: Netflow o sFlow o similares.</p> <p>Además, se pide soportar ERSPAN que es una tecnología que permite la copia y el envío de tráfico de red desde una interfaz o varias interfaces de red en un switch a un dispositivo de análisis remoto a través de una red IP. Sirvase a confirmar se aceptarán tecnologías similares con SPAN, RSPAN o ERSPAN.</p>	INGECORP	Tomando en consideración que existe una diversidad de soluciones o tecnologías relacionadas a la captura y/o recolección de flujos utilizados para la supervisión de dispositivos de red; serán aceptados soluciones y/o tecnologías similares. En ese sentido se reformula requerimiento.	"Debe soportar e implementar herramientas de telemetría, Full Flexible Netflow o sFlow o soluciones similares, SPAN, ERSPAN o tecnologías similares".
5.2 .2. 1.1 .5	30	<p>Se pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)"</p> <p>En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo, y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque de flash seguro.</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura</p>	Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura para asegurar la integridad y

		<p>para asegurar la integridad y autenticidad de nuestro hardware y software. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras necesidades específicas.</p> <p>Por lo tanto sirvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque de flash seguro.</p>		<p>incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.</p>	<p>autenticidad del hardware y software.</p>
5.2 .2. 1.1 .5	31	<p>Se pide "RADSec"</p> <p>RadSec es un protocolo de seguridad que se utiliza para asegurar las comunicaciones entre servidores RADIUS (Remote Authentication Dial-In User Service) y clientes, garantizando la confidencialidad e integridad de los datos transmitidos. Esta tecnología es fundamental en entornos de autenticación y autorización de usuarios, especialmente en redes donde la seguridad es una prioridad.</p> <p>Al respecto, en el mercado existen distintas soluciones similares a Radsec como la verificación de seguridad por parte del servidor RADIUS a los usuarios que utilizan el protocolo Extensible Authentication Protocol over LAN (EAPoL). Esta información tiene como objetivo notificar a los usuarios acerca de los elementos que requieren verificaciones de seguridad adicionales, garantizando así que estén plenamente informados y conscientes de las medidas de seguridad aplicadas en nuestra red.</p> <p>Por lo tanto, sirvase a confirmar se aceptará soluciones RADSec o similar.</p>	INGECORP	<p>Se confirma RADSec o similares</p>	<p>RADSec o similares</p>
5.2 .2. 1.1 .5	31	<p>Se pide "CoPP (Control Plane Policy)"</p> <p>El CoPP (Cisco) utiliza filtros de acceso para limitar el tráfico que se dirige al plano de control, lo que ayuda a prevenir la saturación y los ataques de denegación de servicio contra el dispositivo.</p> <p>El equipo propuesto ofrece características de seguridad similares como la autenticación de usuario y la protección contra ataques de inundación, (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, Defense Against Fragmentation Attacks, Defense Against TCP SYN Flood Packets, Defense Against UDP Flood Attacks, Defense Against ICMP Flood Attacks).</p> <p>Por lo tanto, aunque el CoPP es una función específica de los dispositivos Cisco, los switches propuestos ofrecen características de seguridad similares que protegen el dispositivo contra ataques malintencionados y garantizar que el tráfico importante tenga prioridad sobre otros tipos de tráfico.</p> <p>En conclusión, sirvase a confirmar se aceptará CoPP o características de seguridad similares como (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, etc).</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.</p>	<p>Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.</p>
5.2 .2. 1.1 .5	31	<p>Se pide "Root Guard"</p> <p>Al respecto, se debe tener en cuenta que existen fabricantes en el mercado que denominan de otra forma a estas funcionalidades. Por ejemplo, a "STP root guard" también se le denomina "Root protection".</p> <p>Por tanto, se sugiere respetuosamente a la entidad considerar que en el requerimiento se solicite Root Guard o equivalente.</p>	INGECORP	<p>Se confirma Root Guard o equivalente</p>	<p>Root Guard o equivalente</p>
5.2 .2. 1.1 .5	31	<p>Se pide "Private VLAN"</p> <p>(Private VLAN) es una tecnología que permite segmentar un VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos.</p> <p>Se provee lo mismo mediante Super-VLAN (S-VLAN). Al igual que PVLAN, S-VLAN permite segmentar una VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos para mejorar la seguridad y el aislamiento entre dispositivos y usuarios en una misma red.</p> <p>Por lo tanto, sirvase a confirmar que se aceptará Private VLAN o similar.</p>	INGECORP	<p>Se confirma Private VLAN o similares</p>	<p>Private VLAN o similares</p>
5.2 .2. 1.1 .5	31	<p>Se pide "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo".</p>	INGECORP	<p>No se confirma, se requiere incluir esta característica sin limitación, puede ser interna o externa, puede ser del mismo fabricante o de terceros.</p>	

		<p>Al respecto, el requisito de incluir una etiqueta RFID (RFID Tag) en el switch propuesto, ya sea interna o externa, tiene un propósito específico que no está directamente relacionado con el funcionamiento de la red en sí. En lugar de sumar a la funcionalidad de la red, se centra en aspectos relacionados con la administración y el mantenimiento de los equipos de red. La inclusión de una etiqueta RFID tiene más que ver con la gestión y la identificación eficiente de los dispositivos que conforman la red.</p> <p>Por lo anterior, sírvase a confirmar esta característica será considerada como opcional: "El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo o opcional".</p>			
5.2 .2 1.1 .5	31	<p>Se pide: "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. ".</p> <p>Al respecto, el requisito de "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. " guarda una similitud fundamental con la implementación de un "arranque de flash seguro". Ambos objetivos se centran en salvaguardar la autenticidad e integridad del software o firmware en nuestros equipos. Al implementar un "arranque de flash seguro," establecemos una barrera efectiva contra posibles ataques de intermediarios maliciosos, ya que garantiza que el software o firmware se inicie desde una fuente confiable y que no haya sido comprometido durante el proceso de inicio. En esencia, ambas medidas buscan prevenir manipulaciones no autorizadas del software/firmware y garantizar que los equipos se ejecuten con la autenticidad e integridad necesarias para mantener la seguridad de nuestra infraestructura de red.</p> <p>Por lo tanto, sírvase a confirmar se aceptará: "Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software o arranque seguro de flash".</p>	INGECORP	Se precisa que, independientemente como implemente la solución, que incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma, de cada fabricante o como se la denomine; estos serán una barrera efectiva contra ataques de intermediarios maliciosos que prevengan manipulaciones no autorizadas del software/firmware en los equipos.	
5.2 .2 1.1 .5	31	<p>Se pide "El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware."</p> <p>Al respecto, en el mercado muchos fabricantes realizan este procesamiento de Transmisión de paquetes IPv6 en hardware, implica que el switch tiene la capacidad de procesar y enrutar paquetes IPv6 utilizando recursos de hardware o de manera lógica.</p> <p>Por lo tanto, sírvase a confirmar se aceptará: "El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware o de manera lógica"</p>	INGECORP	<p>Con la finalidad de no limitar a los participantes, se confirma que la transmisión de paquetes sea en hardware o de manera lógica. Se reformula requerimiento:</p> <p>El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware o de manera lógica.</p>	El switch propuesto debe soportar transmisión de paquetes IPv6 en hardware o de manera lógica.
5.2 .2 1.1 .5	31	<p>Se pide "802.1v". IEEE 802.1v se relaciona con la etiqueta de VLAN IEEE 802.1v, que agrega información de prioridad de 802.1p a las tramas Ethernet etiquetadas con VLAN. Esta etiqueta se utiliza en las redes VLAN para mantener la calidad de servicio (QoS) incluso cuando el tráfico viaja a través de enlaces troncales que conectan diferentes switches.</p> <p>IEEE 802.1p: Este estándar se refiere a la asignación de prioridades a los paquetes Ethernet en función de los bits de prioridad contenidos en la cabecera de los paquetes. IEEE 802.1p permite la clasificación y la priorización del tráfico en diferentes clases de servicio, lo que garantiza que los paquetes críticos, como voz o video, reciban un trato preferencial en la red.</p> <p>Al respecto, El estándar IEEE 802.1v y la característica IEEE 802.1p están estrechamente relacionados en el contexto de la gestión de calidad de servicio (QoS) en redes Ethernet y VLAN (Virtual LAN). Por lo tanto, sírvase a confirmar se aceptará: "IEEE 802.1v o 802.1p".</p>	INGECORP	<p>Se confirma. Se reformula requerimiento de soporte:</p> <p>IEEE 802.1v o 802.1p</p>	IEEE 802.1v o 802.1p

5.2 .2. 1.1 .6	32	<p>Se pide "Debe tener mínimo una memoria RAM de 16GB "</p> <p>La capacidad de memoria RAM en un switch será relativa a las características del equipo: por ejemplo, el tamaño del sistema operativo, el tamaño de su configuración, el tamaño de los logs que maneja, entre otros. Si el equipo ha sido diseñado de forma tal que optimice sus recursos, entonces el tamaño de la RAM no necesita ser tan grande.</p> <p>Por lo anterior, se sugiere respetuosamente a la entidad:</p> <ol style="list-style-type: none"> 1. Solicitar en el switch una capacidad RAM no menor a 4 GB 	INGECORP	<p>No se confirma, los switches Tipo VI para DC, deben contar con 16GB.</p>	
5.2 .2. 1.1 .6	32	<p>Se pide "Debe tener mínimo una memoria Flash o SSD de 32GB "</p> <p>La capacidad de memoria Flash en un switch será relativa a las características del equipo: por ejemplo, el tamaño del sistema operativo, el tamaño de su configuración, el tamaño de los logs que maneja, entre otros. Si el equipo ha sido diseñado de forma tal que optimice sus recursos, entonces el tamaño de la flash no necesita ser tan grande.</p> <p>Por lo anterior, se sugiere respetuosamente a la entidad:</p> <ol style="list-style-type: none"> 1. Solicitar en el switch una capacidad flash no menor a 4 GB 	INGECORP	<p>Se precisa que la dimensión de memoria flash para este tipo de Switch será mínimo de 4GB. Se reformula requerimiento, de la siguiente manera:</p> <p>Debe tener mínimo una memoria Flash de 4GB o SSD de 32GB</p>	Debe tener mínimo una memoria Flash de 4GB o SSD de 32GB
5.2 .2. 1.1 .6	32	<p>Se pide "Debe permitir MC-LAG".</p> <p>Al respecto, MC-LAG es una tecnología que permite a múltiples dispositivos de red, como switches, trabajar juntos como un único dispositivo lógico para proporcionar redundancia y alta disponibilidad. En el mercado existen tecnologías similares pero con otras denominaciones como M-LAG.</p> <p>En base a lo anterior, sirvase a confirmar se aceptará MC-LAG o M-LAG.</p>	INGECORP	<p>El requerimiento hace referencia a la capacidad de del sistema para funcionar con un dispositivo lógico agrupando varios dispositivos físicos, que permitan contar con escenarios de redundancia y alta disponibilidad, independientemente de como lo denomine cada fabricante. En ese sentido se reformula requerimiento.</p>	<p>Se elimina MC-LAG y se reemplaza por:</p> <p>Debe permitir tecnología de múltiples dispositivos para que trabaje como un único dispositivo lógico para proporcionar redundancia y alta disponibilidad para entornos de redes empresariales y centro de datos.</p>
5.2 .2. 1.1 .6	32	<p>Se pide "Debe tener un rendimiento mínimo de 1Bpps"</p> <p>Al respecto, El switch propuesto se destaca no solo por su capacidad para soportar MPPS, sino también por su impresionante capacidad de ancho de banda en Tbps. Además, El switch propuesto se ha diseñado para optimizar el uso de sus recursos, lo que lo distingue como una solución que no exige MPPS extremadamente elevados para garantizar un rendimiento óptimo. El dispositivo ha sido configurado de manera que los MPPS establecidos por el fabricante cumplen plenamente con los requisitos y permiten un funcionamiento óptimo en términos de conmutación y procesamiento de paquetes. Esto se traduce en una disponibilidad del 99.999%.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "Debe tener un rendimiento mínimo de 940 Mpps"</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular y ampliar los participantes, se reformula el requerimiento de la siguiente manera:</p> <p>Debe tener un rendimiento mínimo de 940Mpps.</p>	Debe tener un rendimiento mínimo de 940Mpps.
5.2 .2. 1.1 .6	32	<p>Se pide "El sistema operativo debe contar con mecanismos de servicio continuo con el objetivo de evitar interrupción del servicio ante operaciones de mantenimiento y actualización de software."</p> <p>Debido a que existen soluciones diversas por cada fabricante para ofrecer alta disponibilidad sirvase a confirmar se aceptará: "El sistema operativo debe contar con mecanismos de servicio continuo con el objetivo de evitar interrupción del servicio ante operaciones de mantenimiento y actualización de software. O soportar stacking o cluster"</p>	INGECORP	<p>No se confirma, el requerimiento es claro independientemente si es clúster, Stacking o independiente.</p>	
5.2 .2. 1.1 .6	33	<p>Se pide "Debe incluir herramientas de telemetría, NetFlow o sFlow, SPAN, ERSPAN"</p> <p>ERSPAN que es una tecnología que permite la copia y el envío de tráfico de red desde una interfaz o varias interfaces de red en un switch a un dispositivo de análisis remoto a través de una red IP. Sirvase a confirmar se aceptarán tecnologías similares con SPAN, RSPAN o ERSPAN.</p>	INGECORP	<p>Tomando en consideración que existe una diversidad de soluciones o tecnologías relacionadas a la captura y/o recolección de flujos utilizados para la supervisión de dispositivos de red; serán aceptados soluciones y/o tecnologías similares. En ese sentido se reformula requerimiento.</p>	Debe incluir herramientas de telemetría, NetFlow o sFlow, SPAN, ERSPAN
5.2 .2.	32	<p>Se pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)"</p> <p>En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo,</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p>	Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma

1.1 .6	<p>y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque de flash seguro, para asegurar la integridad y autenticidad de nuestro hardware y software. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras necesidades específicas.</p> <p>Por lo tanto sirvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque de flash seguro.</p>		Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.	segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.
5.2 .2 32 1.1 .6	<p>Se pide "TACACS+"</p> <p>TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS.</p> <p>Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS</p>	INGECORP	Se confirma, TACACS, TACACS+ o equivalentes	TACACS, TACACS+ o equivalentes
5.2 .2 32 1.1 .6	<p>Se pide "CoPP (Control Plane Policy)"</p> <p>El CoPP (Cisco) utiliza filtros de acceso para limitar el tráfico que se dirige al plano de control, lo que ayuda a prevenir la saturación y los ataques de denegación de servicio contra el dispositivo. El equipo propuesto ofrece características de seguridad similares como la autenticación de usuario y la protección contra ataques de inundación, (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, Defense Against Fragmentation Attacks, Defense Against TCP SYN Flood Packets, Defense Against UDP Flood Attacks, Defense Against ICMP Flood Attacks).</p> <p>Por lo tanto, aunque el CoPP es una función específica de los dispositivos Cisco, los switches propuestos ofrecen características de seguridad similares que protegen el dispositivo contra ataques malintencionados y garantizar que el tráfico importante tenga prioridad sobre otros tipos de tráfico.</p> <p>En conclusión, sirvase a confirmar se aceptará CoPP o características de seguridad similares como (CPU Attack Defense, Port Attack Defense, Defense Against Malformed Packet Attacks, etc).</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.</p>	Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.
5.2 .2 32 1.1 .6	<p>Se pide "Root Guard"</p> <p>Al respecto, se debe tener en cuenta que existen fabricantes en el mercado que denominan de otra forma a estas funcionalidades. Por ejemplo, a "STP root guard" también se le denomina "Root protection". Por tanto, se sugiere respetuosamente a la entidad considerar que en el requerimiento se solicite Root Guard o equivalente.</p>	INGECORP	Se confirma Root Guard o equivalente	Root Guard o equivalente
5.2 .2 32 1.1 .6	<p>Se pide "Private VLAN"</p> <p>(Private VLAN) es una tecnología que permite segmentar un VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos.</p> <p>Se provee lo mismo mediante Super-VLAN (S-VLAN). Al igual que P-VLAN, S-VLAN permite segmentar una VLAN en sub-VLANs más pequeños con diferentes niveles de aislamiento entre ellos para mejorar la seguridad y el aislamiento entre dispositivos y usuarios en una misma red.</p> <p>Por lo tanto, sirvase a confirmar que se aceptará Private VLAN o similar.</p>	INGECORP	Se confirma Private VLAN o similares	Private VLAN o similares
5.2 .2 32 1.1 .6	<p>Se pide "802.1p".</p> <p>IEEE 802.1p se relaciona con la etiqueta de VLAN IEEE 802.1p, que agrega información de prioridad de 802.1p a las tramas Ethernet etiquetadas con VLAN. Esta etiqueta se utiliza en las redes VLAN para mantener la calidad de servicio (QoS) incluso cuando el tráfico viaja a través de enlaces troncales que conectan diferentes switches.</p> <p>IEEE 802.1p: Este estándar se refiere a la asignación de prioridades a los paquetes Ethernet en función de los</p>	INGECORP	<p>Se confirma.</p> <p>Se reformula requerimiento de soporte:</p> <p>IEEE 802.1p o 802.1p</p>	IEEE 802.1p o 802.1p

		bits de prioridad contenidos en la cabecera de los paquetes. IEEE 802.1p permite la clasificación y la priorización del tráfico en diferentes clases de servicio, lo que garantiza que los paquetes críticos, como voz o video, reciban un trato preferencial en la red. Al respecto, El estándar IEEE 802.1v y la característica IEEE 802.1p están estrechamente relacionados en el contexto de la gestión de calidad de servicio (QoS) en redes Ethernet y VLAN (Virtual LAN). Por lo tanto, sirvase a confirmar se aceptará: "IEEE 802.1v o 802.1p".			
5.2 .2 1.2 .1	34	Se pide "TAM (Trusted Anchor Module) o TPM (Trusted Platform Module)" En el mercado existen diversos enfoques para verificar la autenticidad del hardware y el código de un equipo, y esto no se limita exclusivamente a la utilización de un módulo de hardware o chip específico. Dado este contexto, estamos abiertos a considerar y aceptar tanto la implementación de un TAM (Trusted Anchor Module) como la utilización de un TPM (Trusted Platform Module), o incluso la opción de un arranque seguro o Bootload, para asegurar la integridad y autenticidad. Esta flexibilidad nos permite adaptarnos a las soluciones de seguridad disponibles en el mercado que mejor se ajusten a nuestras necesidades específicas. Por lo tanto sirvase a confirmar se aceptará Trusted Platform Module (TPM) o Trusted Anchor Module (TAM) o arranque seguro o BootLoad.	INGECORP	Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera: Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.	Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.
5.2 .2 1.2 .1	35	Se pide " Deberá soportar RESTCONF (RFC 8040) para proporcionar una interfaz de programabilidad estándar y permitir el acceso a parámetros de configuración. " Al respecto, RESTCONF (RFC 8040) proporciona una interfaz de programabilidad estándar y permitir el acceso a parámetros de configuración para la gestión y configuración de dispositivos de red. Sin embargo, es relevante destacar que, a través del protocolo NETCONF, se puede lograr un objetivo similar de programabilidad y configuración de manera efectiva. Por lo tanto, sirvase a confirmar se aceptará " Deberá soportar RESTCONF (RFC 8040) para proporcionar una interfaz de programabilidad estándar y permitir el acceso a parámetros de configuración, o soportar NETCONF"	INGECORP	Se precisa que, de la reevaluación de esta característica, y al ser protocolos con el mismo objetivo, se reformula el requerimiento, de la siguiente manera: Deberá soportar NETCONF (RFC 6241) o RESTCONF (RFC 8040) para proporcionar una interfaz de programabilidad estándar y permitir el acceso a parámetros de configuración	Deberá soportar NETCONF (RFC 6241) o RESTCONF (RFC 8040) para proporcionar una interfaz de programabilidad estándar y permitir el acceso a parámetros de configuración
5.2 .2 1.2 .1	35	Se pide "TACACS+ " TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS. Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS	INGECORP	Se confirma, TACACS, TACACS+ o equivalentes	TACACS, TACACS+ o equivalentes
5.2 .2 1.2 .1	35	Se pide "RFC 3576 " El RFC 3576 especifica el protocolo de extensión RADIUS (Remote Authentication Dial-In User Service) conocido como "Dynamic Authorization Extensions to RADIUS." Este protocolo extiende las capacidades de RADIUS para proporcionar autorización dinámica en entornos de acceso a la red, como redes de acceso remoto y redes inalámbricas. Sin embargo, es importante destacar que RADIUS en sí mismo, sin la extensión proporcionada por RFC 3576, ya ofrece funcionalidades similares y es ampliamente utilizado en el mercado por distintos fabricantes para la autenticación y autorización de usuarios en redes. Por lo tanto, sirvase a confirmar se aceptará: "RFC 3576 o soportar RADIUS"	INGECORP	Dado que el protocolo Radius ya se esta solicitando, el RFC 3576 será opcional. Se reformula requerimiento: Opcionalmente RFC 3576.	Opcionalmente RFC 3576.
5.2 .2 1.2 .1	35	Se pide "Debe incluir visibilidad de las aplicaciones consumidas por los usuarios por medio de NBAR o DPI ". Al respecto, se menciona la necesidad de utilizar tecnologías como NBAR (Network-Based Application Recognition) o DPI (Deep Packet Inspection) para obtener visibilidad sobre las aplicaciones consumidas por los usuarios en una red. Sin embargo, es relevante destacar que existe una alternativa efectiva y moderna conocida como SAC (Smart Application Control) que ofrece funcionalidades similares y, en algunos aspectos, puede superar las capacidades de NBAR y DPI.	INGECORP	Se precisa que, con la finalidad de homogenizar la concepción de este requerimiento se reformula de la siguiente manera: Debe incluir visibilidad de las aplicaciones consumidas por los usuarios, combinando la detección y el control de aplicaciones en la red, identificando y clasificando información de Capa 4 a	Debe incluir visibilidad de las aplicaciones consumidas por los usuarios, combinando la detección y el control de aplicaciones en la red, identificando y clasificando información de Capa 4 a Capa 7 de las aplicaciones que se están utilizando en la red; que luego

		<p>SAC es una tecnología avanzada que combina la detección y el control de aplicaciones en la red. Al igual que NBAR y DPI, SAC es capaz de identificar y clasificar las aplicaciones que se están utilizando en la red. Sin embargo, a diferencia de DPI, que a veces puede ser invasivo y consumir recursos significativos, SAC suele ser menos intrusivo y más eficiente en términos de recursos.</p> <p>Por lo tanto sirvase a confirmar se aceptará: "Debe incluir visibilidad de las aplicaciones consumidas por los usuarios por medio de NBAR o DPI o soportar SAC"</p>		<p>Capa 7 de las aplicaciones que se están utilizando en la red; que luego permitan configurar ACL por aplicación o categoría de aplicación y acelerar el ancho de banda para aplicaciones de misión crítica para priorización del tráfico y QoS; utilizando como tecnologías como pueden ser control de aplicaciones, inspección profunda de paquetes, reconocimiento de aplicaciones basado en red, o una combinación de las mismas.</p>	<p>permitan configurar ACL por aplicación o categoría de aplicación y acelerar el ancho de banda para aplicaciones de misión crítica para priorización del tráfico y QoS; utilizando como tecnologías como pueden ser control de aplicaciones, inspección profunda de paquetes, reconocimiento de aplicaciones basado en red, o una combinación de las mismas.</p>
5.2 .2 1.2 .1	35	<p>Se pide "Debe de incluir la capacidad de identificar los dispositivos inalámbricos y crear políticas de acuerdo con la identidad del dispositivo (Android, iPhone, Etc.)."</p> <p>Al respecto, la característica de identificación de dispositivos y la aplicación de políticas basadas en la identidad debería ser implementada en la plataforma de gestión de la red en lugar de la controladora WLAN debido a los beneficios de centralización y coherencia en la gestión de toda la red, tanto inalámbrica como cableada. Un enfoque centralizado simplifica la administración, garantiza la uniformidad de las políticas en toda la red, ofrece una mayor escalabilidad y facilita la integración con otros servicios de red, lo que resulta en una gestión más eficiente y eficaz de los dispositivos inalámbricos y las políticas de seguridad basadas en la identidad.</p> <p>Por lo tanto, sírvase a confirmar que: "Debe de incluir la capacidad de identificar los dispositivos inalámbricos y crear políticas de acuerdo con la identidad del dispositivo (Android, iPhone, Etc.) o también será válido si esta función será soportada por la plataforma de gestión de forma centralizada."</p>	INGECORP	<p>Se precisa que, la solución de controlador wireless, debe estar en la capacidad de identificar los dispositivos inalámbricos y crear políticas de acuerdo con la identidad del dispositivo; sin la necesidad de otros elementos externos, en forma independiente; sin la posibilidad de realizarlo a través de un centro de gestión centralizado.</p>	
5.2 .2 1.2 .1	36	<p>Se pide "Permitir la configuración y gestión a través de un navegador web estándar (HTTP, HTTPS), SSH y puerto serial."</p> <p>Sírvase a confirmar se aceptarán modos de gestión similares: "Permitir la configuración y gestión a través de un navegador web estándar (HTTP, HTTPS), SSH y puerto serial o puerto consola RJ45"</p>	INGECORP	<p>Se confirma, se reformula de la siguiente manera: Permitir la configuración y gestión a través de un navegador web estándar (HTTP, HTTPS), SSH y puerto serial o puerto de consola RJ45.</p>	<p>Permitir la configuración y gestión a través de un navegador web estándar (HTTP, HTTPS), SSH y puerto serial o puerto de consola RJ45.</p>
5.2 .2 1.2 .2	37	<p>Se pide "Debe incluir OFDM con 37 resource units".</p> <p>Al respecto, OFDM con 37 resource units se utiliza para transmitir una sola señal o asignar todas las subportadoras a un solo usuario, actualmente existen soluciones superiores como OFDMA. Aunque ambos enfoques utilizan la tecnología de modulación OFDM, OFDMA lleva la eficiencia y la capacidad de asignación de recursos a un nivel superior al permitir una asignación dinámica y eficiente de subconjuntos de subportadoras a diferentes usuarios. Mientras que OFDM con 37 resource units asigna todas las subportadoras a un solo usuario, OFDMA permite que múltiples usuarios compartan el espectro de frecuencia de manera eficaz, lo que resulta en una mejor capacidad de adaptación a las necesidades cambiantes de la red y una mayor capacidad para manejar múltiples conexiones simultáneas. Esto lo convierte en la elección preferida para entornos de red con alta densidad de usuarios y una demanda constante de asignación de recursos dinámicos, donde OFDMA ofrece un rendimiento superior y una mayor eficiencia en la asignación de recursos.</p> <p>Por lo tanto, sírvase a confirmar se aceptará: "Debe incluir OFDM con 37 resource units o debe incluir OFDMA"</p>	INGECORP	<p>Se precisa y aclara que las unidades serán asignadas en entornos de OFDM o OFDMA. Se reformula requerimiento.</p> <p>Debe incluir OFDM/OFDMA con 37 resource units</p>	<p>"Debe incluir OFDM/OFDMA con 37 resource units"</p>
5.2 .2 1.2 .1	37	<p>"Se pide ""Debe incluir un módulo de plataforma confiable (TPM o TAM) ""</p> <p>Al respecto, Trusted Platform Module (TPM) o Trusted Anchor Module (TAM), que son componentes de seguridad utilizados para almacenar claves y certificados de manera segura, y para garantizar que el hardware y el software del dispositivo no hayan sido comprometidos.</p> <p>A diferencia de TPM o TAM, muchos fabricante en el mercado suele utilizar métodos de cifrado, autenticación y control de acceso avanzados en sus dispositivos para proteger la integridad y la confidencialidad de los datos de la red y los usuarios o de CAPWAP. Estos métodos pueden incluir protocolos de cifrado, autenticación de</p>	INGECORP	<p>Con la finalidad de aclarar los términos y no limitar alguna denominación en particular, se reformula el requerimiento de la siguiente manera:</p> <p>Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.</p>	<p>Debe incluir un componente que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.</p>

		<p>usuarios, detección de intrusiones y otras técnicas de seguridad estándar de la industria.</p> <p>Por lo tanto sirvase a confirmar se aceptará "Debe incluir un módulo de plataforma confiable (TPM o TAM) o CAPWAP o similar"</p>			
5.2 .2 1.5	39	<p>Se pide "Debe manejar el inventario de los dispositivos de red, recopilando la dirección IP, la MAC Address "</p> <p>Al respecto, debido a que muchos fabricantes en el mercado manejan distintos terminos para recopilar información de los dispositivos de red (dirección IP, la MAC Address), mediante inventario o listas de dispositivos.</p> <p>Al base a lo anterior sirvase a confirmar se aceptará: "Debe manejar el inventario o listas de dispositivos de red, recopilando la dirección IP, la MAC Address "</p>	INGECORP	<p>Con la finalidad de ampliar el concepto de inventario se amplía la terminología:</p> <p>"Debe manejar el registro o inventario o lista de los dispositivos de red, recopilando la dirección IP, la MAC Address</p>	"Debe manejar el registro o inventario o lista de los dispositivos de red, recopilando la dirección IP, la MAC Address
5.2 .2 1.5	39	<p>Se pide "Obtención de información de inventario de los equipos."</p> <p>Al respecto, debido a que muchos fabricantes en el mercado manejan distintos terminos para recopilar información de los dispositivos de red (dirección IP, la MAC Address), mediante inventario o listas de dispositivos.</p> <p>Al base a lo anterior sirvase a confirmar se aceptará: "Obtención de información de inventario o lista de los equipos. "</p>	INGECORP	<p>Con la finalidad de ampliar el concepto de inventario se amplía la terminología:</p> <p>Obtención de información de registro o inventario o lista inventario de los equipos.</p>	Obtención de información de registro o inventario o lista inventario de los equipos.
5.2 .2 1.5	40	<p>Se pide "Debe incluir workflows intuitivos ".</p> <p>Al respecto, muchos fabricantes definen los medianos de implementación intuitiva a través de workflows o GUI wizard, proporcionando flujos de trabajo diseñados de manera que sean fáciles de comprender y utilizar de forma natural, incluso para usuarios sin experiencia técnica avanzada.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "Debe incluir workflows intuitivos o GUI wizard"</p>	INGECORP	<p>Se confirma.</p> <p>Debe incluir workflows intuitivos o GUI wizard</p>	Debe incluir workflows intuitivos o GUI wizard.
5.2 .2 1.5	40	<p>Pide "Debe permitir la integración con soluciones terceras por medio de herramientas de automatización que facilitan la transferencia de datos (Webhooks) para el envío de notificaciones "</p> <p>Al respecto, la plataforma debe ser capaz de conectarse y trabajar con soluciones de terceros a través de la automatización mediante Webhooks. Esto permite la transferencia de datos, mejorando la eficiencia y la interoperabilidad del sistema al permitir que eventos y acciones se comuniquen de manera automática y eficiente entre diferentes sistemas.</p> <p>En el mercado existen distintas denominaciones para funciones de automatización que facilita la transferencia de datos como Webhooks o RESTful API.</p> <p>Por lo tanto, sirvase a confirmar se aceptará: "Debe permitir la integración con soluciones terceras por medio de herramientas de automatización que facilitan la transferencia de datos (Webhooks) para el envío de notificaciones o soporta RESTful API".</p>	INGECORP	<p>Con la finalidad de homogenizar el requerimiento e incorporar las diferentes herramientas por las cuales los fabricantes implementan la automatización del envío de notificaciones, se reformula requerimiento, de la siguiente manera:</p> <p>Debe permitir la integración con soluciones terceras por medio de herramientas de automatización que facilitan la transferencia de datos para el envío de notificaciones</p>	Debe permitir la integración con soluciones terceras por medio de herramientas de automatización que facilitan la transferencia de datos para el envío de notificaciones
5.2 .2 1.5	41	<p>Se pide "Capacidad de generar informes de los siguientes tipos: Lista de clientes wireless, lista de access points, información de configuración de los controladores WLAN, uso de la red, access points no autorizados (rogue) detectados, esto de manera manual y automática agendada mensual y semanalmente."</p> <p>Debido a que muchos fabricantes no presentan las mismas denominaciones para generar informes de lista de clientes wireless, lista de access point, controladores WLAN, uso de la red, APS Rogue, Sirvase a confirmar que se aceptará la opción de generar informes de manera manual y automática mediante: tipo de dispositivo, vendors, modelo, uso de puerto y terminales.</p> <p>Por lo tanto se sugiere respetuosamente a la entidad considerar:</p> <p>"Capacidad de generar informes de los siguientes tipos: Lista de clientes wireless, lista de access points, información de configuración de los controladores WLAN, uso de la red, access points no autorizados (rogue) detectados, esto de manera manual y automática agendada mensual y</p>	INGECORP	<p>Con la finalidad de homogenizar el requerimiento e incorporar las diferentes denominaciones que puedan manejar los fabricantes, se reformula de la siguiente manera:</p> <p>Capacidad de generar informes de los siguientes tipos: Lista de clientes wireless o lista de tipo de dispositivo cliente, lista de access points o lista de tipo de dispositivo punto de acceso inalámbrico, información de configuración de los controladores WLAN, uso de la red o uso de puerto y terminales, (rogue) detectados o lista de punto de acceso NO autorizados, esto de manera manual y automática</p>	Capacidad de generar informes de los siguientes tipos: Lista de clientes wireless o lista de tipo de dispositivo cliente, lista de access points o lista de tipo de dispositivo punto de acceso inalámbrico, información de configuración de los controladores WLAN, uso de la red o uso de puerto y terminales, access points no autorizados (rogue) detectados o lista de punto de acceso NO autorizados, esto de manera manual y automática

		semanalmente. o generar informes de tipo de dispositivo, vendors, modelo, uso de puerto y terminales, esto de manera manual y automática agendada mensual y semanalmente"		manera manual y automática agendada mensual y semanalmente"	agendada mensual y semanalmente"
5.2 .2 1.5	41	<p>Se pide "Debe incluir una solución que permita el uso de algoritmos avanzados de análisis de comportamiento; para identificar patrones de tráfico, usando análisis de la información de eventos que ocurren dentro de un flujo de datos aplicando técnicas de machine learning, con el objetivo de detectar potenciales amenazas de seguridad. a través de la inclusión de hardware y software adicional que permita descifrar el tráfico para su análisis."</p> <p>En el mercado existen diversas alternativas para realizar el analisis de comportamientos aplicando tecnicas de machine learning no solo mediante la inclusión de hardware y software adicional que permita descifrar el tráfico para su análisis, sino que a través de una arquitectura integrada de recopilación de datos a través de telemetria, plataforma de analisis de big data y un motor de IA.</p> <p>Por lo tanto, se solicita respetuosamente a la entidad considerar: "Debe incluir una solución que permita el uso de algoritmos avanzados de análisis de comportamiento; para identificar patrones de tráfico, usando análisis de la información de eventos que ocurren dentro de un flujo de datos aplicando técnicas de machine learning, con el objetivo de detectar potenciales amenazas de seguridad. a través de la inclusión de hardware y software adicional que permita descifrar el tráfico para su análisis o a través de una plataforma de análisis de big data que recibe datos del dispositivo a través de la tecnología Telemetry y analiza y muestra los datos de la red a través de algoritmos inteligentes".</p>	INGECORP	<p>Con la finalidad de homogenizar el requerimiento e incorporar las diferentes denominaciones y/o tecnologías que puedan manejar los fabricantes, se reformula de la siguiente manera:</p> <p>Debe incluir una solución que permita el uso de algoritmos avanzados de análisis de comportamiento; para identificar patrones de tráfico, usando análisis de la información de eventos que ocurren dentro de un flujo de datos aplicando técnicas de machine learning, o plataforma de análisis de big data Telemetry que analice y muestre los datos de la red a través de algoritmos inteligentes; con el objetivo de detectar potenciales amenazas de seguridad, a través de la inclusión de hardware y software adicional que permita descifrar el tráfico para su análisis.</p>	Debe incluir una solución que permita el uso de algoritmos avanzados de análisis de comportamiento; para identificar patrones de tráfico, usando análisis de la información de eventos que ocurren dentro de un flujo de datos aplicando técnicas de machine learning, o plataforma de análisis de big data Telemetry que analice y muestre los datos de la red a través de algoritmos inteligentes; con el objetivo de detectar potenciales amenazas de seguridad, a través de la inclusión de hardware y software adicional que permita descifrar el tráfico para su análisis.
5.2 .2 1.6	42	<p>Se pide "Debe incluir TACACS+ para la autenticación de los usuarios de gestión de la infraestructura de red "</p> <p>TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS.</p> <p>Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS</p>	INGECORP	Se confirma, TACACS, TACACS+ o equivalentes	TACACS, TACACS+ o equivalentes
5.2 .2 1.6	42	<p>Se pide "Para la gestión y autenticación de acceso a la red, se debe implementar el servicio RADIUS y/o TACACS+, que incluya el licenciamiento necesario para el Sistema Operativo, el servicio RADIUS o TACACS+ y un Servicio NTP."</p> <p>TACACS+ es la denominación que algunos fabricantes usan para denominar una versión del standard TACACS con algunas mejoras. Otros fabricantes proponen versiones mejoradas de TACACS compatibles con TACACS+. Por ejemplo, HWTACACS.</p> <p>Por lo anterior, se solicita respetuosamente a la entidad incluir en su requerimiento el término "TACACS+ o equivalentes", a fin de validar estándares compatibles con TACACS</p>	INGECORP	Se confirma, TACACS, TACACS+ o equivalentes	TACACS, TACACS+ o equivalentes
5.2 .2 1.6	45	<p>Se pide "Debe garantizar que para el acceso a la red se validen y verifiquen los requisitos mínimos de cumplimiento y aquellos que no cumplan las reglas definidas por CORPAC S.A., serán enviados un segmento de cuarentena. Debe considerar como mínimo un licenciamiento para 200 dispositivos."</p> <p>Al respecto, debido a que existen diversas formas para restringir el acceso a la red como cuarentena, listas negras, bloqueo, que garantizan el requerimiento de garantizar la seguridad de acceso a la red. Se solicita respetuosamente a la entidad considerar lo siguiente:</p> <p>"Debe garantizar que para el acceso a la red se validen y verifiquen los requisitos mínimos de cumplimiento y aquellos que no cumplan las reglas definidas por CORPAC S.A., serán enviados un segmento de cuarentena o se definirá en listas negras o bloqueados directamente. Debe considerar como mínimo un licenciamiento para 200 dispositivos."</p>	INGECORP	Se precisa que, aquellos dispositivos que no validen o verifiquen los mínimos de cumplimiento y que no cumplan las reglas definidas por CORPAC serán enviados a un segmento llamados cuarentena o segmentos de dispositivos bloqueados o segmento de dispositivos en lista negra o segmento de dispositivos en aislamiento o segmento de dispositivos en confinamiento, etc.; lo que se quiere lograr es que estos 200 dispositivos licenciados deben permanecer en esta zona y que se actualicen cumpliendo las reglas definidas o políticas de la Entidad, respecto al acceso de estos terminales o clientes.	

5.2 .2 1.6	43	<p>Se pide "El usuario debe validarse contra un dominio existente utilizando sus credenciales. En caso la red maneje esquemas de multidominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario."</p> <p>Al respecto, el requerimiento se refiere a los procedimientos de autenticación en una red donde los usuarios deben verificar su identidad utilizando credenciales, como un nombre de usuario y una contraseña, en un dominio específico. Por lo tanto para una mayor aclaración del requerimiento se solicita respetuosamente a la entidad considerar lo siguiente:</p> <p>"El usuario debe validarse contra un dominio existente utilizando sus credenciales. En caso la red maneje esquemas de multidominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario; o los usuarios deben proporcionar información de autenticación que será verificada por un servidor o sistema de autenticación en un dominio específico."</p>	INGECORP	<p>Se precisa que un usuario se valida con su nombre de usuario y su contraseña contra un dominio específico, ya sea se tenga un solo dominio o múltiples dominios; por lo que la solución de control de acceso del fabricante debe estipular que esto sea transparente para el usuario; con relación al autenticación a la red.</p>	
5.2 .2 1.6	45	<p>Se pide "EAP-FAST "</p> <p>Al respecto, "EAP-FAST" es un protocolo de autenticación propietario desarrollado por Cisco que establece un túnel de seguridad para proteger las credenciales del usuario y utiliza un proceso similar al desafío y respuesta para la autenticación. En el mercado existen protocolos similares como "EAP-TTLS-PAP" que es un estándar más ampliamente aceptado, también establece un túnel de seguridad (TTLS) para proteger las credenciales y utiliza el protocolo PAP (Password Authentication Protocol) para la autenticación del usuario.</p> <p>Por lo tanto sirvase a confirmar que se aceptará: "EAP-FAST o EAP-TTLS-PAP"</p>	INGECORP	<p>Se precisa que, EAP-FAST será opcional.</p>	EAP-FAST (Opcional)
		<p>Se adjunta las consultas y observaciones a los Términos de referencia de la RENOVACION DE LA RED LAN DE CORPAC, se valida que solo la marca CISCO esta cumpliendo con todos los requerimientos técnicos solicitados.</p> <p>Asimismo; debe señalarse que, el artículo 29 del Reglamento del Texto Único Ordenado de la Ley de Contrataciones del Estado -en adelante el Reglamento; establece que es el área usuaria la responsable de elaborar el requerimiento, debiendo éste contener todas las características, exigencias y condiciones para la ejecución de la contratación.</p> <p>Así, el artículo 32 del Reglamento establece que, el órgano encargado de las contrataciones sobre la base del requerimiento realizará el estudio de mercado orientado a determinar el valor estimado, y la pluralidad de postores y marcas; así como, la posibilidad de distribuir la buena pro.</p> <p>En tal sentido, corresponde señalar que, en las compras públicas debe lograrse el mayor grado de eficacia de la contratación mediante mecanismos que promuevan el libre acceso y participación de proveedores, dado que un requisito de validez del procedimiento, y por consiguiente de la posterior adjudicación, es que se haya verificado una plural y efectiva concurrencia y competencia de agentes de mercado, de tal modo que si se advierte lo contrario, correspondería a la Entidad convocante sanear dicho aspecto (vicio de nulidad).</p>	INGECORP	<p>Se precisa, que la absolución de estas consultas y observaciones están basadas en la necesidad de la Entidad y procura las mayor pluralidad y participación de las empresas.</p>	

ANEXO B

ITEM 9 DEL NUMERAL 2.8 OBSERVACIONES AL REQUERIMIENTO

N° de orden	Términos de Referencia o Especificaciones Técnicas o Requisitos de calificación		Consulta y/u Observación	Corresponde a consulta y/u observación del OEC o de las empresas invitadas en la indagación de mercado
	Numeral	Pág.		
1	5.2.2.1.1.2	20	Considerando que la frecuencia del CPU podría ajustarse para satisfacer mejor las necesidades del proyecto actual, sin innecesario tan alto valor, y dado que el rendimiento de un switch de red LAN se evalúa principalmente en función de su capacidad de conmutación, reenvío de tráfico y otras características operativas. Es importante destacar que la frecuencia del CPU no es el factor determinante ya que en la práctica, el servicio de red se mide por la capacidad de transmisión alcanzada mediante el switching y el reenvío del equipo. Por lo tanto, le solicitamos confirmar como válido un CPU con una frecuencia de 1.4 GHz precisado en el equipo con respaldo del fabricante.	Consulta de la empresa GRUPO INGECORP S.A.C.
2	5.2.2.1.1.2	20	Considerando que la capacidad de la memoria RAM puede ajustarse para satisfacer mejor las necesidades del proyecto actual, sin que sea de tan alto valor innecesario, y dado que el rendimiento de un switch de red LAN se evalúa principalmente en función de su capacidad de conmutación, reenvío de tráfico y otras características operativas. Es importante destacar que la capacidad de la memoria RAM no es el factor determinante ya que en la práctica, el servicio de red se mide por la capacidad de transmisión alcanzada mediante el switching y el reenvío del equipo. Por lo tanto, le solicitamos confirmar como válida una memoria RAM de 8GB precisada en el equipo con respaldo del fabricante.	Consulta de la empresa GRUPO INGECORP S.A.C.
3	5.2.2.1.1.2	21	Para evitar la sobrecarga innecesaria derivada de la encapsulación GRE de paquetes en ERSPAN y asegurar una capacidad de análisis de tráfico local adecuada, es recomendable utilizar los puertos de origen y destino en el mismo switch para la captura del tráfico. Esto optimiza el	

			<p>uso del ancho de banda para los datos de los servicios de la entidad y reduce la latencia, ya que el tráfico no será encapsulado. Además, al minimizar la sobrecarga de encapsulación, se disminuye el riesgo de interrupciones en el servicio.</p> <p>Por ello, se solicita a la entidad modificar el requerimiento a:</p> <p>"Debe soportar e implementar herramientas de telemetría, como Full Flexible NetFlow, sFlow o soluciones similares, así como SPAN o ERSPAN o tecnologías equivalentes."</p>	Consulta de la empresa GRUPO INGECCOR S.A.C.
4	5.2.2.1.1.2	21	Sírvase, prever que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.	Consulta de la empresa GRUPO INGECCOR S.A.C.
5	5.2.2.1.1.2	23	<p>Sírvase precisar que se refiere a la característica "IPv6 SEND" presente en múltiples fabricantes, como por ejemplo:</p> <ul style="list-style-type: none"> • Cisco IOS con el RFC 3971. • Juniper Networks con el RFC 3971. • ARUBA con el RFC 3971. 	Consulta de la empresa GRUPO INGECCOR S.A.C.
6	5.2.2.1.1.2	23	Sírvase, prever que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo donde previo a ello el sistema operativo (software) y de esta manera quedará confirmada la ejecución del software auténtico.	Consulta de la empresa GRUPO INGECCOR S.A.C.
7	5.2.2.1.1.2	23	Al respecto, en el mercado se despliegan distintos mecanismos para alta disponibilidad en modo Activo/Activo, para una mayor pluralidad de postores sírvase a confirmar que también se aceptará stacking y/o M-LAG.	Consulta de la empresa GRUPO INGECCOR S.A.C.
8	5.2.2.1.1.3	25	Sírvase precisar que se refiere o que será válido el cumplimiento con un sistema operativo modular	Consulta de la empresa GRUPO INGECCOR S.A.C.
9	5.2.2.1.1.3	25	<p>Basado en el análisis de la capacidad del switch y los requerimientos de la red, es recomendable ajustar el número de ACLs permitidas a 6000. Esta medida ayudará a mantener el equilibrio entre la seguridad de la red y el rendimiento del hardware, asegurando una operación más estable y eficiente del switch, además que la entidad no está indicando como usará tan alto valor de ACL.</p> <p>Por lo anterior, sírvase confirmar que también se aceptarán equipos con 6000 entradas ACL.</p>	Consulta de la empresa GRUPO INGECCOR S.A.C.
10	5.2.2.1.1.3	26	Para evitar la sobrecarga innecesaria derivada de la encapsulación GRE de paquetes en ERSPAN y asegurar una capacidad de análisis de tráfico local adecuada, es recomendable utilizar los puertos de origen y destino en el mismo switch para la captura del tráfico. Esto optimiza el	

			<p>uso del ancho de banda para los datos de los servicios de la entidad y reduce la latencia, ya que el tráfico no será encapsulado. Además, al minimizar la sobrecarga de encapsulación, se disminuye el riesgo de interrupciones en el servicio.</p> <p>Por ello, se solicita a la entidad modificar el requerimiento a:</p> <p>"Debe soportar e implementar herramientas de telemetría, como Full Flexible NetFlow, sFlow o soluciones similares, así como SPAN o ERSPAN o tecnologías equivalentes."</p>	Consulta de la empresa GRUPO INGECORP S.A.C.
11	5.2.2.1.1.3	26	<p>Sírvase, preavisar que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.</p>	Consulta de la empresa GRUPO INGECORP S.A.C.
12	5.2.2.1.1.4	28	<p>Sírvase precisar que se refiere o que será válido el cumplimiento con un sistema operativo modular</p>	Consulta de la empresa GRUPO INGECORP S.A.C.
13	5.2.2.1.1.4	28	<p>Basado en el análisis de la capacidad del switch y los requerimientos de la red, es recomendable ajustar el número de ACLs permitidas a 6000. Esta medida ayudará a mantener el equilibrio entre la seguridad de la red y el rendimiento del hardware, asegurando una operación más estable y eficiente del switch, además que la entidad no está indicando como usará tan alto valor de ACL.</p> <p>Por lo anterior, sírvase confirmar que también se aceptarán equipos con 6000 entradas ACL.</p>	Consulta de la empresa GRUPO INGECORP S.A.C.
14	5.2.2.1.1.4	28	<p>Para evitar la sobrecarga innecesaria derivada de la encapsulación GRE de paquetes en ERSPAN y asegurar una capacidad de análisis de tráfico local adecuada, es recomendable utilizar los puertos de origen y destino en el mismo switch para la captura del tráfico. Esto optimiza el uso del ancho de banda para los datos de los servicios de la entidad y reduce la latencia, ya que el tráfico no será encapsulado. Además, al minimizar la sobrecarga de encapsulación, se disminuye el riesgo de interrupciones en el servicio.</p> <p>Por ello, se solicita a la entidad modificar el requerimiento a:</p> <p>"Debe soportar e implementar herramientas de telemetría, como Full Flexible NetFlow, sFlow o soluciones similares, así como SPAN o ERSPAN o tecnologías equivalentes."</p>	Consulta de la empresa GRUPO INGECORP S.A.C.
15	5.2.2.1.1.4	28	<p>(Debe incluir un componente en hardware que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.) Sírvase, preavisar que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se</p>	Consulta de la empresa GRUPO INGECORP S.A.C.

			almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.	
16	5.2.2.1.1.4	28	(Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma). Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. Sirvase, preavisar que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.	Consulta de la empresa GRUPO INGECORP S.A.C.
17	5.2.2.1.1.6	34	Considerando que la capacidad de la memoria RAM puede ajustarse para satisfacer mejor las necesidades del proyecto actual, sin que sea de tan alto valor innecesario, y dado que el rendimiento de un switch de red en el DATA CENTER se evalúa principalmente en función de su capacidad de conmutación, reenvío de tráfico y otras características operativas. Es importante destacar que la capacidad de la memoria RAM no es el factor determinante ya que en la práctica, el servicio de red se mide por la capacidad de transmisión alcanzada mediante el switching y el reenvío del equipo. Por lo tanto, le solicitamos confirmar como válida una memoria RAM de 4GB precisada en el equipo con respaldo del fabricante.	Consulta de la empresa GRUPO INGECORP S.A.C.
18	5.2.2.1.1.6	34	Dado que existen diversas soluciones ofrecidas por diferentes fabricantes y que este requerimiento puede cumplirse utilizando equipos configurados en activo/activo mediante dos switches en alta disponibilidad, y que esta funcionalidad permite evitar interrupciones del servicio durante operaciones de mantenimiento y actualización de software. Sirvase modificar el requerimiento de la siguiente manera: "El sistema operativo debe contar con mecanismos que aseguren la continuidad del servicio durante operaciones de mantenimiento y actualización de software. Es válido usando M-LAG.	Consulta de la empresa GRUPO INGECORP S.A.C.
19	5.2.2.1.1.6	34	(Debe incluir un componente en hardware que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.) Sirvase, preavisar que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.	Consulta de la empresa GRUPO INGECORP S.A.C.
20	5.2.2.1.2.1	36	Sirvase precisar a qué se refiere la expresión "4096 WLANS", aparentemente se quiso decir "4096 VLANS".	Consulta de la empresa GRUPO INGECORP S.A.C.


21	5.2.2.1.2.1	36	(Debe incluir un componente en hardware que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.). Sírvase, prever que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.	Consulta de la empresa GRUPO INGECORP S.A.C.
22	5.2.2.1.2.1	36	NETCONF es un protocolo para la gestión de redes que se basa en estándares abiertos. Los diferentes RFC relacionados con NETCONF en una controladora WLAN son elegidos por los fabricantes por lo cual podría no ser la misma para todos los casos. Por ello sírvase confirmar que se aceptará el RFC de NETCONF conforme el que usa cada fabricante.	Consulta de la empresa GRUPO INGECORP S.A.C.
23	5.2.2.1.2.1	37	La fiabilidad de un switch de red LAN no siempre está directamente relacionada con su antigüedad en el mercado, sino con su diseño, la calidad de los componentes, y el historial de rendimiento. Un switch que lleva más de 3 años en el mercado puede haber pasado por un riguroso proceso de validación y pruebas, permitiendo a los fabricantes identificar y corregir problemas en sus primeras versiones. Durante este tiempo, los fabricantes también pueden haber lanzado actualizaciones de firmware y correcciones que mejoran aún más su rendimiento y estabilidad. Si el modelo ha sido bien recibido y tiene un historial positivo de rendimiento, su antigüedad no necesariamente significa que sea menos fiable que un modelo más reciente. Por lo anterior, sírvase que la entidad aceptará equipos con antigüedad en el mercado no mayor a 4 años de lanzamiento.	Consulta de la empresa GRUPO INGECORP S.A.C.
24	5.2.2.1.2.2	38	Se pide "Debe incluir OFDM con 37 resource units". Al respecto, OFDM con 37 resource units se utiliza para transmitir una sola señal o asignar todas las subportadoras a un solo usuario, actualmente existen soluciones superiores como OFDMA. Aunque ambos enfoques utilizan la tecnología de modulación OFDM, OFDMA lleva la eficiencia y la capacidad de asignación de recursos a un nivel superior al permitir una asignación dinámica y eficiente de subconjuntos de subportadoras a diferentes usuarios. Mientras que OFDM con 37 resource units asigna todas las subportadoras a un solo usuario, OFDMA permite que múltiples usuarios compartan el espectro de frecuencia de manera eficaz, lo que resulta en una mejor capacidad de adaptación a las necesidades cambiantes de la red y una mayor capacidad para manejar múltiples conexiones simultáneas. Esto lo convierte en la elección preferida para entornos de red con alta densidad de usuarios y una demanda constante de asignación de recursos dinámicos, donde OFDMA ofrece un rendimiento superior y una mayor eficiencia en la asignación de recursos.	Consulta de la empresa GRUPO INGECORP S.A.C.

			Por lo tanto, sírvase a confirmar se aceptará: "Debe incluir OFDM con 37 resource units o debe incluir OFDMA"	
25	5.2.2.1.2.2	38	Sírvase, prever que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.	Consulta de la empresa GRUPO INGECORP S.A.C.
26	5.2.2.1.2.2	39	La fiabilidad de un switch de red LAN no siempre está directamente relacionada con su antigüedad en el mercado, sino con su diseño, la calidad de los componentes, y el historial de rendimiento. Un switch que lleva más de 3 años en el mercado puede haber pasado por un riguroso proceso de validación y pruebas, permitiendo a los fabricantes identificar y corregir problemas en sus primeras versiones. Durante este tiempo, los fabricantes también pueden haber lanzado actualizaciones de firmware y correcciones que mejoran aún más su rendimiento y estabilidad. Si el modelo ha sido bien recibido y tiene un historial positivo de rendimiento, su antigüedad no necesariamente significa que sea menos fiable que un modelo más reciente. Por lo anterior, sírvase que la entidad aceptará equipos con antigüedad en el mercado no mayor a 4 años de lanzamiento.	Consulta de la empresa GRUPO INGECORP S.A.C.
27	5.2.2.1.3	41	(Según tdrs: Incluir visibilidad de las aplicaciones en capa 7, con capacidad de al menos 3000 para usuarios conectados vía LAN y WLAN). Favor de considerar 1000 aplicaciones	Consulta de la empresa GRUPO INGECORP S.A.C.
28	5.2.2.1.3	41	Pide "Debe permitir la integración con soluciones terceras por medio de herramientas de automatización que facilitan la transferencia de datos (Webhooks) para el envío de notificaciones "	Consulta de la empresa GRUPO INGECORP S.A.C.
29	5.2.2.1.4	45	Incluir los protocolos Radius y TACACS+. O SIMILAR	Consulta de la empresa GRUPO INGECORP S.A.C.
30	5.2.2.1.4	45	Al respecto, debido a que existen diversas formas para restringir el acceso a la red como cuarentena, listas negras, bloqueo, que garantizan el requerimiento de garantizar la seguridad de acceso a la red. Se solicita respetuosamente a la entidad considerar lo siguiente: "Debe garantizar que para el acceso a la red se validen y verifiquen los requisitos mínimos de cumplimiento y aquellos que no cumplan las reglas definidas por CORPAC S.A., serán enviados un segmento de cuarentena o se definirá en listas negras o bloqueados directamente	Consulta de la empresa GRUPO INGECORP S.A.C.
31	5.2.2.1.4	46	Se pide "El usuario debe validarse contra un dominio existente utilizando sus credenciales. En caso la red maneje esquemas de multidominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario."	Consulta de la empresa GRUPO INGECORP S.A.C.

			<p>Al respecto, el requerimiento se refiere a los procedimientos de autenticación en una red donde los usuarios deben verificar su identidad utilizando credenciales, como un nombre de usuario y una contraseña, en un dominio específico. Por lo tanto para una mayor aclaración del requerimiento se solicita respetuosamente a la entidad considerar lo siguiente:</p> <p>"El usuario debe validarse contra un dominio existente utilizando sus credenciales. En caso la red maneje esquemas de multidominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario; o los usuarios deben proporcionar información de autenticación que será verificada por un servidor o sistema de autenticación en un dominio específico."</p>	
32	5.3.1.8	82	<p>En el numeral 5.3.1.8 VISITA DE CAMPO página N° 82 de las ESPECIFICACIONES TECNICAS DE LA RENOVACION DE LA RED LAN SEDE CENTRAL, se precisa:</p> <p>"El postor podrá realizar visitas de campo a las diferentes instalaciones de CORPAC S.A. para cotizar todo lo necesario para la correcta implementación del servicio solicitado."</p> <p>En tal sentido, solicitamos confirmar si aún se puede solicitar una VISITA DE CAMPO, a fin de poder cotizar de manera certera el servicio.</p>	<p>Consulta de la empresa IDELCOM S.A.C.</p>

ANEXO B.1

ABSOLUCION A LAS CONSULTAS Y/U OBSERVACIONES DEL ANEXO B

Requerimiento efectuado con los siguientes documentos				EE.TT. V8 31.07.2024			
N° de orden	Consultas y observaciones efectuadas por OEC o por Proveedores invitados a indagación de mercado			Absolución de las consultas y observaciones realizada usuaria			
	Términos de Referencia o Especificaciones Técnicas o Requisitos de calificación		Consulta y/u Observación	Corresponde a consulta y/u observación del OEC o de las empresas invitadas en la indagación de mercado	Análisis respecto de la consulta u observación. (Precisar si se acoge o no se acoge. En caso de no acoger sustentar los motivos)	Precisión de aquello que se incorporará en los TDR o EEETT o Requisitos de calificación, de corresponder	
	Numeral	Pág.					
1	5.2.2.1.1.2	20	Considerando que la frecuencia del CPU podría ajustarse para satisfacer mejor las necesidades del proyecto actual, sin innecesario tan alto valor, y dado que el rendimiento de un switch de red LAN se evalúa principalmente en función de su capacidad de conmutación, reenvío de tráfico y otras características operativas. Es importante destacar que la frecuencia del CPU no es el factor determinante ya que en la práctica, el servicio de red se mide por la capacidad de transmisión alcanzada mediante el switching y el reenvío del equipo. Por lo tanto, le solicitamos confirmar como válido un CPU con una frecuencia de 1.4 GHz precisado en el equipo con respaldo del fabricante.	Consulta de la empresa GRUPO INGECORP S.A.C.	Tomando en consideración que para el Switch de Tipo II el factor determinante es la capacidad de conmutación, se aceptara CPU mínimo de 1.4 Ghz, siempre y cuando no impacte en el rendimiento de los equipos	El switch deberá contar con CPU mínimo de 1.4 Ghz siempre y cuando no impacte en el rendimiento de los equipos	
2	5.2.2.1.1.2	20	Considerando que la capacidad de la memoria RAM puede ajustarse para satisfacer mejor las necesidades del proyecto actual, sin que sea de tan alto valor innecesario, y dado que el rendimiento de un switch de red LAN se evalúa principalmente en función de su capacidad de conmutación, reenvío de tráfico y otras características operativas. Es importante destacar que la capacidad de la memoria RAM no es el factor determinante ya que en la práctica, el servicio de red se mide por la capacidad de transmisión alcanzada mediante el switching y el reenvío del equipo. Por lo tanto, le solicitamos confirmar como válida una memoria RAM de 8GB precisada en el equipo con respaldo del fabricante.	Consulta de la empresa GRUPO INGECORP S.A.C.	En concordancia la capacidad de conmutación del equipamiento del Tipo II; y dado que gran parte del proceso lo asume la solución de automatización, administración y gestión de la infraestructura campus de la RED LAN, se aceptarán como mínimo la capacidad de memoria RAM de 8GB, siempre y cuando no impacte en el rendimiento de los equipos.	Debe tener mínimo la capacidad de memoria RAM de 8GB siempre y cuando no impacte en el rendimiento de los equipos	
3	5.2.2.1.1.2	21	Para evitar la sobrecarga innecesaria derivada de la encapsulación GRE de paquetes en ERSPAN y asegurar una capacidad de análisis de tráfico local adecuada, es recomendable utilizar los puertos de origen y destino en el mismo switch para la captura del tráfico. Esto optimiza el		Tomando en consideración que se requiere el soporte e implementar herramientas de telemetría y que	Debe soportar e implementar herramientas de telemetría como Full Flexible Netflow o sFlow o soluciones	

			<p>uso del ancho de banda para los datos de los servicios de la entidad y reduce la latencia, ya que el tráfico no será encapsulado. Además, al minimizar la sobrecarga de encapsulación, se disminuye el riesgo de interrupciones en el servicio.</p> <p>Por ello, se solicita a la entidad modificar el requerimiento a:</p> <p>"Debe soportar e implementar herramientas de telemetría, como Full Flexible NetFlow, sFlow o soluciones similares, así como SPAN o ERSPAN o tecnologías equivalentes."</p>	<p>Consulta de la empresa GRUPO INGECORP S.A.C.</p>	<p>es requisito de la Entidad, realizar los reflejos de los puertos a nivel local y remoto, tanto en redes de L2 y L3, se reformula el requerimiento para mejor entendimiento:</p> <p>Debe soportar e implementar herramientas de telemetría, como Full Flexible NetFlow o sFlow o soluciones similares, así como SPAN o tecnologías similares o equivalentes, RSPAN o tecnologías similares o equivalentes, ERSPAN o tecnologías similares o equivalentes.</p>	<p>similares; así como SPAN o tecnologías similares o equivalentes, RSPAN o tecnologías similares o equivalentes, ERSPAN o tecnologías similares o equivalentes.</p>
4	5.2.2.1.1.2	21	<p>Sírvase, preavisar que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.</p>	<p>Consulta de la empresa GRUPO INGECORP S.A.C.</p>	<p>En el numeral indicado no figura la consulta realizada, sobre capacidad de arranque seguro.</p>	
5	5.2.2.1.1.2	23	<p>Sírvase precisar que se refiere a la característica "IPv6 SEND" presente en múltiples fabricantes, como por ejemplo:</p> <ul style="list-style-type: none"> • Cisco IOS con el RFC 3971. • Juniper Networks con el RFC 3971. • ARUBA con el RFC 3971. 	<p>Consulta de la empresa GRUPO INGECORP S.A.C..</p>	<p>En el numeral indicado no figura la consulta realizada, sobre IPv6 SEND.</p>	
6	5.2.2.1.1.2	23	<p>Sírvase, preavisar que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo donde previo a ello el sistema operativo (software) y de esta manera quedará confirmada la ejecución del software auténtico.</p>	<p>Consulta de la empresa GRUPO INGECORP S.A.C.</p>	<p>En el numeral indicado no figura la consulta realizada, sobre capacidad de arranque seguro.</p>	
7	5.2.2.1.1.2	23	<p>Al respecto, en el mercado se despliegan distintos mecanismos para alta disponibilidad en modo Activo/Activo, para una mayor pluralidad de postores sírvase a confirmar que también se aceptará stacking y/o M-LAG.</p>	<p>Consulta de la empresa GRUPO INGECORP S.A.C.</p>	<p>Independiente del nombre que utilice la solución de equipos de networking a proponer, el mecanismo a utilizar debe hacer operar a los equipos en alta disponibilidad en modo ACTIVO/ACTIVO, siempre y cuando no haya indisponibilidad del servicio.</p>	<p>Los dos Switches de Core deberán trabajar de tal manera que operan en alta disponibilidad, en modo Activo/Activo, siempre y cuando no haya indisponibilidad del servicio.</p> <p>Garantizar que no existan escenarios de inestabilidad en capa 2 (L2) ocasionados por lazos (Loops) en</p>

						enlaces redundantes, por lo cual todos los enlaces redundantes deberán operar de modo Activo/Activo siempre y cuando no haya indisponibilidad del servicio. Se deberá de contar con mecanismos de protección ante la caída del enlace entre los dos Switches de Core.
8	5.2.2.1.1.3	25	Sírvase precisar que se refiere o que será válido el cumplimiento con un sistema operativo modular	Consulta de la empresa GRUPO INGECORP S.A.C.	Con relación al sistema operativo para mejor entendimiento del mismo, se reformula el requerimiento, de la siguiente manera: El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.	El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.
9	5.2.2.1.1.3	25	Basado en el análisis de la capacidad del switch y los requerimientos de la red, es recomendable ajustar el número de ACLs permitidas a 6000. Esta medida ayudará a mantener el equilibrio entre la seguridad de la red y el rendimiento del hardware, asegurando una operación más estable y eficiente del switch, además que la entidad no está indicando como usará tan alto valor de ACL. Por lo anterior, sírvase confirmar que también se aceptarán equipos con 6000 entradas ACL.	Consulta de la empresa GRUPO INGECORP S.A.C.	No se confirma. Existe en el mercado equipamiento para satisfacer este requisito.	
10	5.2.2.1.1.3	26	Para evitar la sobrecarga innecesaria derivada de la encapsulación GRE de paquetes en ERSPAN y asegurar una capacidad de análisis de tráfico local adecuada, es recomendable utilizar los puertos de origen y destino en el mismo switch para la captura del tráfico. Esto optimiza el uso del ancho de banda para los datos de los servicios de la entidad y reduce la latencia, ya que el tráfico no será encapsulado. Además, al minimizar la sobrecarga de encapsulación, se disminuye el riesgo de interrupciones en el servicio. Por ello, se solicita a la entidad modificar el requerimiento a: "Debe soportar e implementar herramientas de telemetría, como Full Flexible NetFlow, sFlow o soluciones similares, así como SPAN o ERSPAN o tecnologías equivalentes."	Consulta de la empresa GRUPO INGECORP S.A.C.	Tomando en consideración que se requiere el soporte e implementar herramientas de telemetría y que es requisito de la Entidad, realizar los reflejos de los puertos a nivel local y remoto, tanto en redes de L2 y L3, se reformula el requerimiento para mejor entendimiento: Debe soportar e implementar herramientas de telemetría, como Full Flexible NetFlow o sFlow o soluciones similares, así como SPAN o tecnologías similares o equivalentes, RSPAN o tecnologías similares o equivalentes, ERSPAN o	Debe soportar e implementar herramientas de telemetría como Full Flexible Netflow o sFlow o soluciones similares; así como SPAN o tecnologías similares o equivalentes, RSPAN o tecnologías similares o equivalentes, ERSPAN o tecnologías similares o equivalentes.

					tecnologías similares o equivalentes.	
11	5.2.2.1.1.3	26	Sírvase, preavisar que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.	Consulta de la empresa GRUPO INGECORP S.A.C.	Con la finalidad de mayor pluralidad se reformula el requerimiento: Debe incluir un componente en hardware o software que permita verificar la legitimidad del hardware y software de forma segura, para asegurar la integridad y autenticidad del hardware y software.	Debe incluir un componente en hardware o software que permita verificar la legitimidad del hardware y software de forma segura, para asegurar la integridad y autenticidad del hardware y software.
12	5.2.2.1.1.4	28	Sírvase precisar que se refiere o que será válido el cumplimiento con un sistema operativo modular	Consulta de la empresa GRUPO INGECORP S.A.C.	Con relación al sistema operativo para mejor entendimiento del mismo, se reformula el requerimiento, de la siguiente manera: El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.	El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.
13	5.2.2.1.1.4	28	Basado en el análisis de la capacidad del switch y los requerimientos de la red, es recomendable ajustar el número de ACLs permitidas a 6000. Esta medida ayudará a mantener el equilibrio entre la seguridad de la red y el rendimiento del hardware, asegurando una operación más estable y eficiente del switch, además que la entidad no está indicando como usará tan alto valor de ACL. Por lo anterior, sírvase confirmar que también se aceptarán equipos con 6000 entradas ACL.	Consulta de la empresa GRUPO INGECORP S.A.C.	No se confirma. Existe en el mercado equipamiento para satisfacer este requisito.	
14	5.2.2.1.1.4	28	Para evitar la sobrecarga innecesaria derivada de la encapsulación GRE de paquetes en ERSPAN y asegurar una capacidad de análisis de tráfico local adecuada, es recomendable utilizar los puertos de origen y destino en el mismo switch para la captura del tráfico. Esto optimiza el uso del ancho de banda para los datos de los servicios de la entidad y reduce la latencia, ya que el tráfico no será encapsulado. Además, al minimizar la sobrecarga de encapsulación, se disminuye el riesgo de interrupciones en el servicio. Por ello, se solicita a la entidad modificar el requerimiento a:	Consulta de la empresa GRUPO INGECORP S.A.C.	Tomando en consideración que se requiere el soporte e implementar herramientas de telemetría y que es requisito de la Entidad, realizar los reflejos de los puertos a nivel local y remoto, tanto en redes de L2 y L3, se reformula el requerimiento para mejor entendimiento: Debe soportar e implementar herramientas de telemetría, como Full Flexible NetFlow o sFlow o soluciones similares, así como	Debe soportar e implementar herramientas de telemetría, como Full Flexible NetFlow o sFlow o soluciones similares, así como

			"Debe soportar e implementar herramientas de telemetría, como Full Flexible NetFlow, sFlow o soluciones similares, así como SPAN o ERSPAN o tecnologías equivalentes."		SPAN o tecnologías similares o equivalentes, RSPAN o tecnologías similares o equivalentes, ERSPAN o tecnologías similares o equivalentes.	
15	5.2.2.1.1.4	28	(Debe incluir un componente en hardware que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.) Sirvase, preavisar que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.	Consulta de la empresa GRUPO INGECORP S.A.C.	Con la finalidad de mayor pluralidad se reformula el requerimiento: Debe incluir un componente en hardware o software que permita verificar la legitimidad del hardware y software de forma segura, para asegurar la integridad y autenticidad del hardware y software.	Debe incluir un componente en hardware o software que permita verificar la legitimidad del hardware y software de forma segura, para asegurar la integridad y autenticidad del hardware y software.
16	5.2.2.1.1.4	28	(Se requiere que la plataforma de hardware y software de los equipos de comunicaciones incluyan mecanismos de seguridad que verifiquen el buen funcionamiento del sistema operativo, y que garanticen la seguridad contra la manipulación indebida interna y/o externa contra la plataforma). Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software. Sirvase, preavisar que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.	Consulta de la empresa GRUPO INGECORP S.A.C.	Este requisito debe cumplirse independientemente del nombre que utilice esta implementación por parte del fabricante.	
17	5.2.2.1.1.6	34	Considerando que la capacidad de la memoria RAM puede ajustarse para satisfacer mejor las necesidades del proyecto actual, sin que sea de tan alto valor innecesario, y dado que el rendimiento de un switch de red en el DATA CENTER se evalúa principalmente en función de su capacidad de conmutación, reenvío de tráfico y otras características operativas. Es importante destacar que la capacidad de la memoria RAM no es el factor determinante ya que en la práctica, el servicio de red se mide por la capacidad de transmisión alcanzada mediante el switching y el reenvío del equipo. Por lo tanto, le solicitamos confirmar como válida una memoria RAM de 4GB precisada en el equipo con respaldo del fabricante.	Consulta de la empresa GRUPO INGECORP S.A.C.	En concordancia la capacidad de conmutación del equipamiento del Tipo VI; y dado que gran parte del proceso lo asume la solución de automatización, administración y gestión de la infraestructura campus de la RED LAN, se aceptarán como mínimo la capacidad de memoria RAM de 4GB, siempre y cuando no impacte en el rendimiento de los equipos.	Debe tener mínimo una memoria RAM de 4GB siempre y cuando no impacte en el rendimiento de los equipos
18	5.2.2.1.1.6	34	Dado que existen diversas soluciones ofrecidas por diferentes fabricantes y que este requerimiento puede cumplirse utilizando equipos configurados en activo/activo mediante dos switches en alta disponibilidad, y que esta funcionalidad permite evitar interrupciones del	Consulta de la empresa GRUPO INGECORP S.A.C.	Independiente del nombre que utilice la solución de equipos de networking a proponer, el mecanismo a utilizar debe hacer operar a los equipos en alta	Debe permitir tecnología de hasta 2 dispositivos para que trabaje como un único dispositivo lógico para proporcionar redundancia y alta disponibilidad (en modo

			servicio durante operaciones de mantenimiento y actualización de software. Sirvase modificar el requerimiento de la siguiente manera: "El sistema operativo debe contar con mecanismos que aseguren la continuidad del servicio durante operaciones de mantenimiento y actualización de software. Es válido usando M-LAG.		disponibilidad en modo ACTIVO/ACTIVO, siempre y cuando no haya indisponibilidad del servicio.	Activo/Activo), para entornos de redes empresariales y centro de datos; siempre y cuando no haya indisponibilidad del servicio
19	5.2.2.1.1.6	34	(Debe incluir un componente en hardware que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.) Sirvase, prever que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.	Consulta de la empresa GRUPO INGECORP S.A.C.	Con la finalidad de mayor pluralidad se reformula el requerimiento: Debe incluir un componente en hardware o software que permita verificar la legitimidad del hardware y software de forma segura, para asegurar la integridad y autenticidad del hardware y software.	Debe incluir un componente en hardware o software que permita verificar la legitimidad del hardware y software de forma segura, para asegurar la integridad y autenticidad del hardware y software
20	5.2.2.1.2.1	36	Sírvase precisar a qué se refiere la expresión "4096 VLANs", aparentemente se quiso decir "4096 VLANs".	Consulta de la empresa GRUPO INGECORP S.A.C.	Se confirma son VLAN 4096 VLAN	El equipo deberá soportar por lo menos 16000 dispositivos clientes y 4096 VLANs.
21	5.2.2.1.2.1	36	(Debe incluir un componente en hardware que permita verificar la legitimidad del hardware y software de forma segura incluyendo contraseñas, certificados o claves de cifrado, para asegurar la integridad y autenticidad del hardware y software.). Sírvase, prever que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.	Consulta de la empresa GRUPO INGECORP S.A.C.	Con la finalidad de mayor pluralidad se reformula el requerimiento: Debe incluir un componente en hardware o software que permita verificar la legitimidad del hardware y software de forma segura, para asegurar la integridad y autenticidad del hardware y software.	Debe incluir un componente en hardware o software que permita verificar la legitimidad del hardware y software de forma segura, para asegurar la integridad y autenticidad del hardware y software.
22	5.2.2.1.2.1	36	NETCONF es un protocolo para la gestión de redes que se basa en estándares abiertos. Los diferentes RFC relacionados con NETCONF en una controladora WLAN son elegidos por los fabricantes por lo cual podría no ser la misma para todos los casos. Por ello sírvase confirmar que se aceptará el RFC de NETCONF conforme el que usa cada fabricante.	Consulta de la empresa GRUPO INGECORP S.A.C.	Con la finalidad de evitar restricción en el uso del netconf o restconf se elimina la referencia. Deberá soportar NETCONF o RESTCONF para proporcionar una interfaz de programabilidad estándar y permitir el acceso a parámetros de configuración	Deberá soportar NETCONF o RESTCONF para proporcionar una interfaz de programabilidad estándar y permitir el acceso a parámetros de configuración.

23	5.2.2.1.2.1	37	<p>La fiabilidad de un switch de red LAN no siempre está directamente relacionada con su antigüedad en el mercado, sino con su diseño, la calidad de los componentes, y el historial de rendimiento. Un switch que lleva más de 3 años en el mercado puede haber pasado por un riguroso proceso de validación y pruebas, permitiendo a los fabricantes identificar y corregir problemas en sus primeras versiones. Durante este tiempo, los fabricantes también pueden haber lanzado actualizaciones de firmware y correcciones que mejoran aún más su rendimiento y estabilidad. Si el modelo ha sido bien recibido y tiene un historial positivo de rendimiento, su antigüedad no necesariamente significa que sea menos fiable que un modelo más reciente.</p> <p>Por lo anterior, sírvase que la entidad aceptará equipos con antigüedad en el mercado no mayor a 4 años de lanzamiento.</p>	Consulta de la empresa GRUPO INGECORP S.A.C.	<p>No se confirma, se precisa y se amplía que los equipos deben estar a la vanguardia y con un horizonte de utilización de 5 años, con el máximo nivel de licenciamiento para las capacidades de automatización, control y analítica; deben estar preparados y habilitados para escalamiento a las normas de la industria.</p>	<p>El licenciamiento de toda la solución de Networking debe ser a nombre de CORPAC y a perpetuidad, debe incluir el máximo nivel de licenciamiento preparado y habilitado para las capacidades de automatización, control y analítica; deberá contemplarse la garantía de fabricante durante 3 años contados a partir de la finalización de la implementación ya la entrega de los servicios operativos</p>
24	5.2.2.1.2.2	38	<p>Se pide "Debe incluir OFDM con 37 resource units".</p> <p>Al respecto, OFDM con 37 resource units se utiliza para transmitir una sola señal o asignar todas las subportadoras a un solo usuario, actualmente existen soluciones superiores como OFDMA. Aunque ambos enfoques utilizan la tecnología de modulación OFDM, OFDMA lleva la eficiencia y la capacidad de asignación de recursos a un nivel superior al permitir una asignación dinámica y eficiente de subconjuntos de subportadoras a diferentes usuarios. Mientras que OFDM con 37 resource units asigna todas las subportadoras a un solo usuario, OFDMA permite que múltiples usuarios compartan el espectro de frecuencia de manera eficaz, lo que resulta en una mejor capacidad de adaptación a las necesidades cambiantes de la red y una mayor capacidad para manejar múltiples conexiones simultáneas. Esto lo convierte en la elección preferida para entornos de red con alta densidad de usuarios y una demanda constante de asignación de recursos dinámicos, donde OFDMA ofrece un rendimiento superior y una mayor eficiencia en la asignación de recursos.</p> <p>Por lo tanto, sírvase a confirmar se aceptará: "Debe incluir OFDM con 37 resource units o debe incluir OFDMA"</p>	Consulta de la empresa GRUPO INGECORP S.A.C.	<p>Con la finalidad de contar con mejor eficiencia y capacidad de asignación de recursos se reformula el requerimiento:</p> <p>"Debe incluir OFDM con 37 resource units o debe incluir OFDMA "</p>	<p>Debe incluir OFDM con 37 resource units o debe incluir OFDMA.</p>
25	5.2.2.1.2.2	38	<p>Sírvase, preavisar que se refiere a la capacidad de arranque seguro (Secure Boot) en la memoria Flash del switch LAN, ya que la memoria Flash es el hardware donde se almacena el firmware del equipo (software) y de esta manera quedará confirmada la ejecución del software auténtico.</p>	Consulta de la empresa GRUPO INGECORP S.A.C.	<p>En el numeral indicado no figura la consulta realizada sobre capacidad de arranque seguro.</p>	
26	5.2.2.1.2.2	39	<p>La fiabilidad de un switch de red LAN no siempre está directamente relacionada con su antigüedad en el mercado, sino con su diseño, la calidad de los componentes, y el historial de rendimiento. Un switch que lleva más de 3 años en el mercado puede haber pasado por un riguroso proceso de validación y pruebas, permitiendo a los fabricantes identificar y corregir problemas en sus primeras versiones. Durante este tiempo,</p>	Consulta de la empresa GRUPO INGECORP S.A.C.	<p>No se confirma, se precisa y se amplía que los equipos deben estar a la vanguardia y con un horizonte de utilización de 5 años, con el máximo nivel de licenciamiento para las capacidades de</p>	<p>El licenciamiento de toda la solución de Networking debe ser a nombre de CORPAC y a perpetuidad, debe incluir el máximo nivel de licenciamiento preparado y habilitado para las capacidades de</p>

			<p>los fabricantes también pueden haber lanzado actualizaciones de firmware y correcciones que mejoran aún más su rendimiento y estabilidad. Si el modelo ha sido bien recibido y tiene un historial positivo de rendimiento, su antigüedad no necesariamente significa que sea menos fiable que un modelo más reciente.</p> <p>Por lo anterior, sírvase que la entidad aceptará equipos con antigüedad en el mercado no mayor a 4 años de lanzamiento.</p>		<p>automatización, control y analítica; deben estar preparados y habilitados para escalamiento a las normas de la industria.</p>	<p>automatización, control y analítica; deberá contemplarse la garantía de fabricante durante 3 años contados a partir de la finalización de la implementación ya la entrega de los servicios operativos.</p>
27	5.2.2.1.3	41	<p>(Según tdrs: Incluir visibilidad de las aplicaciones en capa 7, con capacidad de al menos 3000 para usuarios conectados vía LAN y WLAN). Favor de considerar 1000 aplicaciones</p>	<p>Consulta de la empresa GRUPO INGECORP S.A.C.</p>	<p>Se aclara que la visibilidad de al menos es para 3000 usuarios. En cuanto a las aplicaciones la visibilidad debe considerarse como mínimo 1000 aplicaciones.</p>	<p>Incluir visibilidad de las aplicaciones en capa 7, con capacidad de al menos 3000 para usuarios conectados vía LAN y WLAN. En cuanto a las aplicaciones la visibilidad debe considerarse como mínimo 1000 aplicaciones</p>
28	5.2.2.1.3	41	<p>Pide "Debe permitir la integración con soluciones terceras por medio de herramientas de automatización que facilitan la transferencia de datos (Webhooks) para el envío de notificaciones "</p>	<p>Consulta de la empresa GRUPO INGECORP S.A.C.</p>	<p>Se aclara que la solución puede utilizar cualquier medio de automatización para el envío de notificaciones. Este dependerá de la forma en que brinda la solución tecnológica a este requerimiento</p>	
29	5.2.2.1.4	45	<p>Incluir los protocolos Radius y TACACS+. O SIMILAR</p>	<p>Consulta de la empresa GRUPO INGECORP S.A.C.</p>	<p>Se actualiza requerimiento: Incluir los protocolos Radius y TACACS o TACACS+ o equivalentes.</p>	<p>Incluir los protocolos Radius y TACACS+ o equivalentes.</p>
30	5.2.2.1.4	45	<p>Al respecto, debido a que existen diversas formas para restringir el acceso a la red como cuarentena, listas negras, bloqueo, que garantizan el requerimiento de garantizar la seguridad de acceso a la red. Se solicita respetuosamente a la entidad considerar lo siguiente:</p> <p>"Debe garantizar que para el acceso a la red se validen y verifiquen los requisitos mínimos de cumplimiento y aquellos que no cumplan las reglas definidas por CORPAC S.A., serán enviados un segmento de cuarentena o se definirá en listas negras o bloqueados directamente</p>	<p>Consulta de la empresa GRUPO INGECORP S.A.C.</p>	<p>Se reformula el requerimiento: Debe garantizar que para el acceso a la red se validen y verifiquen los requisitos mínimos de cumplimiento y aquellos que no cumplan las reglas definidas por CORPAC S.A., serán enviados un segmento considerado de lista negra o bloqueo o de cuarentena, con la finalidad de que la plataforma o solución propuesta permita realizar los procesos de remediación para que los dispositivos cumplan los requisitos de acceso a la red.</p>	<p>Debe garantizar que para el acceso a la red se validen y verifiquen los requisitos mínimos de cumplimiento y aquellos que no cumplan las reglas definidas por CORPAC S.A., serán enviados un segmento considerado como lista negra o lista de bloqueados o de cuarentena, con la finalidad de que la plataforma o solución propuesta permita realizar los procesos de remediación para que los dispositivos cumplan los requisitos de acceso a la red. Debe considerarse como mínimo un licenciamiento para 100 usuarios donde cada uno puede utilizar hasta 3 dispositivos o poder integrarse con una plataforma de cumplimiento en donde estará licenciada para 100</p>

						usuarios y cada uno de estos pueda utilizar 3 dispositivos
31	5.2.2.1.4	46	<p>Se pide "El usuario debe validarse contra un dominio existente utilizando sus credenciales. En caso la red maneje esquemas de multidominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario."</p> <p>Al respecto, el requerimiento se refiere a los procedimientos de autenticación en una red donde los usuarios deben verificar su identidad utilizando credenciales, como un nombre de usuario y una contraseña, en un dominio específico. Por lo tanto para una mayor aclaración del requerimiento se solicita respetuosamente a la entidad considerar lo siguiente:</p> <p>"El usuario debe validarse contra un dominio existente utilizando sus credenciales. En caso la red maneje esquemas de multidominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario; o los usuarios deben proporcionar información de autenticación que será verificada por un servidor o sistema de autenticación en un dominio específico."</p>	Consulta de la empresa GRUPO INGECORP S.A.C.	<p>Para aclarar el requerimiento se reformula de la siguiente manera:</p> <p>El usuario debe validarse contra un dominio existente proporcionando información de autenticación utilizando sus credenciales, verificada por un servidor o sistema de autenticación en un dominio específico. En caso la red maneje esquemas de multidominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario.</p>	El usuario debe validarse contra un dominio existente proporcionando información de autenticación utilizando sus credenciales, siendo verificadas por un servidor o sistema de autenticación en un dominio específico. En caso la red maneje esquemas de multidominio, la solución de control de acceso deberá asegurar que ello sea transparente para el usuario.
32	5.3.1.8	82	<p>En el numeral 5.3.1.8 VISITA DE CAMPO página N° 82 de las ESPECIFICACIONES TECNICAS DE LA RENOVACION DE LA RED LAN SEDE CENTRAL, se precisa:</p> <p>"El postor podrá realizar visitas de campo a las diferentes instalaciones de CORPAC S.A. para cotizar todo lo necesario para la correcta implementación del servicio solicitado."</p> <p>En tal sentido, solicitamos confirmar si aún se puede solicitar una VISITA DE CAMPO, a fin de poder cotizar de manera certera el servicio.</p>	Consulta de la empresa IDELCOM S.A.C.	Se confirma, podrán ser coordinadas con el Área Usuaría	

ANEXO C

ITEM 10 DEL NUMERAL 2.8 OBSERVACIONES AL REQUERIMIENTO

N° de orden	Términos de Referencia o Especificaciones Técnicas o Requisitos de calificación		Consulta y/u Observación	Corresponde a consulta y/u observación del OEC o de las empresas invitadas en la indagación de mercado
	Numeral	Pág.		
1	5.2.2.1.1.1	14	El switch deberá contar con CPU mínimo de 2.2 Ghz. "Para tener una mejor eficiencia y reasignar los recursos dependiendo de la carga sirvase permitir una arquitectura multi-core a nivel de CPU".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
2	5.2.2.1.1.1	14	Debe tener mínimo la capacidad de memoria Flash o SSD de 2GB. "Para tener una capacidad de ampliación de almacenamiento mediante USB o disco SATA SSD para instalación de aplicaciones mediante contenedores o similares . sirvase permitir solo la memoria flash de al menos 16GB y la memoria SSD pueda tener la capacidad de soportar hasta 960GB"	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
3	5.2.2.1.1.1	14	Debe incluir todos los componentes necesarios para realizar el stacking virtual o solución equivalente. "Sirvase considerar solo la tecnología de stacking virtual ya que aumentaría la eficacia operativa y potencia las comunicaciones sin interrupciones y el ancho de banda del sistema a escala".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
4	5.2.2.1.1.1	18	Los dos Switches de Core deberán trabajar de tal manera que operan en alta disponibilidad, en modo Activo/Activo o ser capaz de asegurar la operación de la plataforma ante un escenario de falla o actualización, manteniendo la conmutación tanto en capa2 como en capa3 por medio de una solución del tipo Fabric o SDN.	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.

			"Sirvase permitir trabajar la alta disponibilidad en modo activo / pasivo, teniendo en cuenta que un switch es el activo y funciona como plano de control y gestion mientras que el otro es el de reserva".	
5	5.2.2.1.1.1	18	Los dos Switches de Core deberán trabajar de tal manera que operan en alta disponibilidad, en modo Activo/Activo. "Sirvase permitir trabajar la alta disponibilidad en modo activo / pasivo, teniendo en cuenta que un switch es el activo y funciona como plano de control y gestion mientras que el otro es el de reserva".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
6	5.2.2.1.1.2	20	El switch deberá contar con CPU mínimo de 2.2 Ghz "Para tener una mejor eficiencia y reasignar los recursos dependiendo de la carga sirvase permitir una arquitectura multi-core a nivel de CPU".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
7	5.2.2.1.1.2	20	Debe tener mínimo la capacidad de memoria Flash o SSD de 2GB. "Para tener una capacidad de ampliación de almacenamiento mediante USB o disco SATA SSD para instalación de aplicaciones mediante contenedores o similares . sirvase permitir solo la memoria flash de al menos 16GB y la memoria SSD pueda tener la capacidad de soportar hasta 960GB".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
8	5.2.2.1.1.2	20	Debe tener 32 puertos de red 40/100G (QSFP/QSFP28) como mínimo. "De acuerdo al diagrama de bloques de arquitectura de interconexión y no desperdiciar puertos sirvase permitir al menos 24 puertos de red 40Gbps QSFP y al menos 8 puertos de 100Gbps".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
9	5.2.2.1.1.2	20	Debe incluir todos los componentes necesarios para realizar el stacking virtual o solución equivalente. "Sirvase considerar solo la tecnología de stacking virtual ya que aumentaría la eficacia operativa y potencia las comunicaciones sin interrupciones y el ancho de banda del sistema a escala".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
10	5.2.2.1.1.2	23	Los dos Switches de Core deberán trabajar de tal manera que operan en alta disponibilidad, en modo Activo/Activo. "Sirvase permitir trabajar la alta disponibilidad en modo activo / pasivo, teniendo en cuenta que un switch es el activo y funciona como plano de control y gestion mientras que el otro es el de reserva".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
11	5.2.2.1.1.3	25	Debe ser non-blocking. Tener mínimo un rendimiento de 396Gbps. "Por rendimiento y tener una mayor capacidad de switching al momento de conectar Acces point con capacidad de puertos hasta 5Gbps , sirvase permitir tener un rendimiento de al menos 800Gbps y así poder discriminar equipos con menor capacidad de conmutación".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.

12	5.2.2.1.1.3	25	Debe tener un rendimiento mínimo de 396Mpps. "Por rendimiento y tener una mayor capacidad de forwarding rate al momento de conectar Acces point con capacidad de puertos hasta 5Gbps, sirvase permitir tener un rendimiento de al menos 800Mpps y así poder discriminar equipos con menor capacidad de transmisión de paquetes".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.
13	5.2.2.1.1.3	25	El stacking debe tener un rendimiento no menor a 160Gbps. "Por rendimiento y capacidad de conmutación entre los switches sirvase considerar tener un rendimiento de stacking no menor a 320 Gbps".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.
14	5.2.2.1.1.4	28	Debe ser non-blocking. Tener mínimo un rendimiento de 440Gbps. "Por rendimiento y tener una mayor capacidad de switching al momento de conectar Acces point con capacidad de puertos hasta 5Gbps, sirvase permitir tener un rendimiento de al menos 600Gbps y así poder discriminar equipos con menor capacidad de conmutación".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.
15	5.2.2.1.1.4	28	Debe tener un rendimiento mínimo de 330Mpps. "Para la pluralidad de marca sirvase permitir tener un rendimiento de al menos 327Mpps sin afectar o cambiar la solución de switches"	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.
16	5.2.2.1.1.4	28	El stacking debe tener un rendimiento no menor a 160Gbps. "Por rendimiento y capacidad de conmutación entre los switches sirvase considerar tener un rendimiento de stacking no menor a 320 Gbps".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.
17	5.2.2.1.1.5	31	Debe ser non-blocking. Tener mínimo un rendimiento de 440Gbps. "Por rendimiento y tener una mayor capacidad de switching al momento de conectar Acces point con capacidad de puertos hasta 5Gbps, sirvase permitir tener un rendimiento de al menos 600Gbps y así poder discriminar equipos con menor capacidad de conmutación".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.
18	5.2.2.1.1.4	31	Debe tener un rendimiento mínimo de 470Mpps. "Para la pluralidad de marca sirvase permitir tener un rendimiento de al menos 327Mpps sin afectar o cambiar la solución de switches".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.
19	5.2.2.1.1.5	31	El stacking debe tener un rendimiento no menor a 160Gbps. "Por rendimiento y capacidad de conmutación entre los switches sirvase considerar tener un rendimiento de stacking no menor a 320 Gbps".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN

				COMUNICACION Y SEGURIDAD S.A.C.
20	5.2.2.1.2.1	36	Se requiere una herramienta en hardware (Appliance) en alta disponibilidad que va a tunelizar las comunicaciones inalámbricas y que permita configurar y gestionar los puntos de accesos inalámbrico de forma centraliza con soporte de por lo menos 2000 APs. Este tendrá las siguientes funcionalidades: "Para no sobre dimensionar la solucion y propuesta sirvase permitir al controlador wireless soportar por lo menos 250 Aps".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
21	5.2.2.1.2.1	36	El equipo deberá soportar por lo menos 16000 dispositivos clientes y 4096 WLANS. "Para no sobre dimensionar la solucion y propuesta sirvase permitir al controlador wireless soportar por lo menos 5000 dispositivos clientes".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
22	5.2.2.1.2.1	36	Deberá manejar un rendimiento no menor a 18Gbps "Para no sobre dimensionar la solucion y propuesta sirvase permitir al controlador wireless soportar por lo menos 5 Gbps".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
23	5.2.1	13	El licenciamiento de toda la solución de Networking debe ser a nombre de CORPAC y a perpetuidad; deberá contemplarse la garantía de fabricante durante 3 años contados a partir de la finalización de la implementación y a la entrega de los servicios operativos. "Sirvase aclarar para el licenciamiento de toda la solucion networking sea por suscripcion por el tiempo del proyecto 3 años".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
24	5.2.2.1.3	39	La solución de automatización, administración y gestión de la infraestructura campus con todos sus componentes de hardware y software serán implementados en alta disponibilidad sen un entorno ON PREMISE utilizando appliances de propósito específico, la cual debe ser del mismo fabricante de los Switches de Core, Distribución, Acceso y de la solución de WLAN, con motivo de asegurar su correcta integración, utilizando licenciamiento del tipo perpetuo. La solución debe ser catalogada por el fabricante como un controlador para redes SDN o El software de consola de gestión deberá ser desarrollado por el mismo fabricante de los Switches de Core ofertados. Asimismo, se deberá incluir el sistema operativo, su licenciamiento y todo el hardware (rackeable) necesario para su puesta en operación. Podrá ser instalado en entorno virtual, el proveedor se encargará de colocar el hardware necesario y las licencias del software correspondiente (tal como hypervisor o equivalente) si la oferta es en entorno virtual. "Sirvase aclarar para el licenciamiento de toda la solucion networking sea por suscripcion por el tiempo del proyecto 3 años".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.

25	8	95	<p>Se requiere para el Líder de Networking LAN que acredite como mínimo cinco (5) años de experiencia como arquitecto y/o líder técnico en plataformas de networking LAN y WLAN.</p> <p>Sírvase confirmar si con la finalidad de poder tener una mayor participación de postores se podrá acreditar como mínimo tres (3) años de experiencia como arquitecto y/o líder técnico y/o especialista en plataformas de networking LAN y WLAN.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
26	8	95	<p>Se requiere para el Líder de Networking LAN que acredite contar con certificaciones técnicas oficiales vigentes de nivel experto o avanzado en Enterprise o Datacom o Switching o Wireless de al menos dos (02) fabricantes reconocidos (incluyendo al fabricante de los equipos de networking propuestos).</p> <p>Se observa que este requerimiento vulnera el principio de libre concurrencia al exigir requisitos desproporcionados y que limitan la pluralidad de postores, además de no configurar ventaja alguna para la Entidad el requerir las certificaciones técnicas oficiales vigentes en al menos dos (2) fabricantes reconocidos.</p> <p>Solicitamos para este profesional sea requerido el contar con la certificación técnica vigente de nivel experto o avanzado en Enterprise o Datacom o Switching o Wireless del fabricante de los equipos propuestos.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
27	8	95	<p>Se requiere para el Implementador de Networking LAN que acredite certificación técnica oficial vigente de nivel profesional en Enterprise o Switching o Datacom del fabricante propuesto.</p> <p>Sírvase confirmar que la acreditación de la certificación técnica oficial vigente de nivel profesional en Enterprise o Switching o Datacom requerida podrá ser de cualquier fabricante.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
28	8	96	<p>Se requiere para el Implementador de Networking WLAN que acredite certificación técnica oficial vigente de nivel profesional en Wireless del fabricante propuesto.</p> <p>Sírvase confirmar que la acreditación de la certificación técnica oficial vigente de nivel profesional en Wireless requerida podrá ser de cualquier fabricante.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
29	8	95	<p>Se requiere para el Especialista en Cableado Estructurado Certificado oficial o carta de fabricante de la solución de cableado estructurado de la plataforma a operar.</p> <p>Sírvase confirmar que la acreditación requerida podrá ser de cualquier fabricante de cableado estructurado</p>	Consulta de la empresa ITALTEL PERU S.A.C..
30	8	96	Se requiere para el Residente 1 Presencial como mínimo certificación en materia de switching y routing por parte del fabricante de los equipos	

			<p>de la solución; a nivel asociado, técnico, especialista o ingeniero de red (según la denominación propia del fabricante y demostrable según documentación del fabricante) y que se encuentre vigente durante toda la ejecución del servicio complementario.)</p> <p>Sírvase confirmar que se aceptarán certificaciones en materia de switching y routing por parte de cualquier fabricante; a nivel asociado, técnico, especialista o ingeniero de red y que se encuentre vigente durante toda la ejecución del servicio complementario.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
31	8	97	<p>Se requiere para el Residente 2 Presencial como mínimo Certificación y/o acreditación respectiva del sistema de cableado a operar vigente durante toda la ejecución del servicio complementario.</p> <p>Sírvase confirmar que se aceptarán Certificación y/o acreditación de cualquier sistema de cableado.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
32	5.2.1	13	<p>Con respecto al SISTEMA DE NETWORKING (INFRAESTRUCTURA ACTIVA), se menciona lo siguiente: "Todos los transceivers a proveer como parte de la solución deberán poseer conectores tipo LC, el postor deberá considerar y garantizar en su propuesta que permita interoperabilidad de los transceivers de la solución propuesta siendo estos propietarios o de terceros compatibles con la solución."</p> <p>Con la finalidad de asegurar la interoperabilidad de los transceivers de la solución propuesta, sírvase confirmar que los transceivers deberán ser del mismo fabricante (propietarios) de la solución a ofertar, descartándose de esta manera la provisión de transceivers compatibles o de terceros que podrían causar incompatibilidades e incluso pérdida de garantía de los equipos que conformarán el SISTEMA DE NETWORKING (INFRAESTRUCTURA ACTIVA).</p>	Consulta de la empresa ITALTEL PERU S.A.C..
33	7	93	<p>Con respecto al Plazo de Entrega, se menciona lo siguiente: "El plazo para la Entrega de componentes del sistema de Networking (Infraestructura activa) y renovación de garantías de la infraestructura pasiva y activa de la Sede Central de CORPAC S.A. será máximo de sesenta (60) días calendarios, se contabilizará desde el día siguiente de la firma del contrato.</p> <p>Considerando que, los tiempos de entrega por parte del fabricante de los equipos que conforman el sistema de Networking (Infraestructura Activa), oscilan entre 90 a 120 días calendario, vemos que 60 días calendario no es suficiente tiempo para entregar los mismos, por lo que se solicita extender el tiempo de entrega de los componentes del Sistema de Networking a 90 días calendario.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
34	7	94	Con respecto al Plazo de Implementación – ETAPA 1, se menciona lo siguiente:	

			<p>"El plazo para la implementación de la presente contratación del Sistema de Networking (Infraestructura Activa), será de ciento cincuenta (50) días calendarios a partir del día siguiente de la fecha máxima del plazo de entrega de equipos. Este plazo incluye el suministro, instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), hasta que la solución funcione correctamente."</p> <p>Respecto al plazo se indica en letras ciento cincuenta y en números (50), sírvase confirmar que lo correcto es, ciento cincuenta (150) días calendarios, en letras y número respectivamente.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
35	7	94	<p>Con respecto al Plazo de Implementación – ETAPA 1, se menciona lo siguiente:</p> <p>"El plazo para la implementación de la presente contratación del Sistema de Networking (Infraestructura Activa), será de ciento cincuenta (50) días calendarios a partir del día siguiente de la fecha máxima del plazo de entrega de equipos. Este plazo incluye el suministro, instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), hasta que la solución funcione correctamente."</p> <p>Teniendo en cuenta que el plazo inicia desde la fecha máxima del plazo de entrega de equipos, sírvase confirmar que el texto referente a lo que incluye dicho plazo, quedaría de la siguiente forma: "Este plazo incluye la instalación y configuración y todo lo relacionado al sistema de Networking (infraestructura Activa), hasta que la solución funcione correctamente"</p>	Consulta de la empresa ITALTEL PERU S.A.C..
36	7	93	<p>Con respecto a los Plazos de la Prestación Principal se menciona lo siguiente:</p> <p>"El plazo total de la prestación principal es de 150 días calendarios, se contabiliza al día siguiente de la firma del contrato. Este plazo contempla la entrega e implementación y puesta en marcha."</p> <p>Teniendo en cuenta la secuencia y las etapas que componen la Prestación Principal (como son: Plazo de Entrega, Plazo de Implementación y sus respectivas Etapas), sírvase aclarar que el plazo total de la Prestación Principal es de 280 días calendarios, considerando un Plazo de Entrega de los componentes del Sistema de Networking de 90 días calendarios.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
37	8	95	<p>Con respecto al Perfil del Personal Clave – Líder de Networking LAN, se menciona lo siguiente:</p> <p>"Un (01) Ingeniero Electrónico o Sistemas o Telecomunicaciones, Titulado, Colegiado y habilitado, que acrediten como mínimo cinco (05) años de experiencia como arquitecto y/o líder técnico en plataformas de Networking LAN y WLAN."</p>	

			<p>Teniendo en cuenta que, en las constancias de trabajo del personal, las funciones del Arquitecto y/o Líder de Networking, por lo general se describen como Arquitecto y/o Líder de Técnico en Networking o Plataformas de Networking (lo cual ya incluye LAN y WLAN), por favor, sírvase confirmar que el requerimiento del perfil podrá quedar de la siguiente manera:</p> <p>"Un (01) Ingeniero Electrónico o Sistemas o Telecomunicaciones, Titulado, Colegiado y habilitado, que acrediten como mínimo cinco (05) años de experiencia como arquitecto y/o líder técnico en Networking o Plataformas de Networking."</p>	Consulta de la empresa ITALTEL PERU S.A.C..
38	8	95	<p>Con respecto al Perfil del Personal Clave – Líder de Networking LAN, se menciona lo siguiente:</p> <p>"Constancias de experiencia mínima de cinco (05) años de experiencia como arquitecto y/o líder técnico en networking LAN y WLAN."</p> <p>Teniendo en cuenta que, en las constancias de trabajo del personal, las funciones del Arquitecto y/o Líder de Networking, por lo general se describen como Arquitecto y/o Líder de Técnico en Networking o Plataformas de Networking (lo cual ya incluye LAN y WLAN), por favor, sírvase confirmar que el requerimiento de la experiencia podrá quedar de la siguiente manera:</p> <p>"Constancias de experiencia mínima de cinco (05) años de experiencia como arquitecto y/o líder técnico en Networking o Plataformas de Networking"</p>	Consulta de la empresa ITALTEL PERU S.A.C..
39	8	95	<p>Con respecto al Perfil del Personal Clave – Líder de Networking LAN, se menciona lo siguiente:</p> <p>"El líder de networking implementador propuesto por el postor debe contar con certificaciones técnicas oficiales vigentes de nivel experto o avanzado en Enterprise o Datacom o Switching o Wireless de al menos dos (02) fabricantes reconocidos (incluyendo al fabricante de los equipos de networking propuestos)."</p> <p>Sírvase confirmar que se aceptarán certificaciones técnicas oficiales vigentes de nivel experto o avanzado en Enterprise o Datacom o Switching o Wireless del fabricante de los equipos de networking ofertados.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
40	8	96	<p>Con Respecto al Perfil del Personal Clave – Implementador de Networking LAN, se menciona lo siguiente:</p> <p>"Un (01) Bachiller o Ingeniero o técnico titulado Electrónico o Sistemas o Telecomunicaciones o redes y comunicaciones, como mínimo con tres (03) años de experiencia realizando tareas de implementación soporte y/o mantenimiento de networking LAN usando la tecnología SDN o fabric"</p> <p>Teniendo en cuenta que, en las constancias de trabajo del personal, las funciones de los Ingenieros y/o Técnicos, por lo general se describen</p>	Consulta de la empresa ITALTEL PERU S.A.C..

			<p>como servicios de implementación, soporte y/o mantenimientos de redes LAN de forma general y no precisamente usando la Tecnología SDN o Fabric, lo cual no implica que el personal no este calificado para realizarlas, por favor, sírvase confirmar que el requerimiento del perfil podrá quedar de la siguiente manera:</p> <p>"Un (01) Bachiller o Ingeniero o técnico titulado Electrónico o Sistemas o Telecomunicaciones o redes y comunicaciones, como mínimo con tres (03) años de experiencia realizando tareas de implementación soporte y/o mantenimiento de networking LAN"</p>	
41	8	96	<p>Con Respecto al Perfil del Personal Clave – Implementador de Networking LAN, se menciona lo siguiente:</p> <p>"Constancias de experiencia mínima de tres (03) años realizando tareas de implementación y/o soporte y/o mantenimiento de networking LAN usando la tecnología SDN o fabric."</p> <p>Teniendo en cuenta que, en las constancias de trabajo del personal, las funciones de los Ingenieros y/o Técnicos, por lo general se describen como servicios de implementación, soporte y/o mantenimientos de redes LAN de forma general y no precisamente usando la Tecnología SDN o Fabric, lo cual no implica que el personal no este calificado para realizarlas, por favor, sírvase confirmar que el requerimiento del perfil podrá quedar de la siguiente manera:</p> <p>"Constancias de experiencia mínima de tres (03) años realizando tareas de implementación y/o soporte y/o mantenimiento de networking LAN."</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>
42	8	96	<p>Con Respecto al Perfil del Personal Clave – Implementador de Networking WLAN, se menciona lo siguiente:</p> <p>"Un (01) Bachiller o Ingeniero o técnico titulado Electrónico o Sistemas o Telecomunicaciones o redes y comunicaciones, como mínimo con tres (03) años de experiencia realizando tareas de implementación soporte y/o mantenimiento de networking WLAN usando la tecnología SDN o fabric"</p> <p>Teniendo en cuenta que, en las constancias de trabajo del personal, las funciones de los Ingenieros y/o Técnicos, por lo general se describen como servicios de implementación, soporte y/o mantenimientos de redes WLAN o Redes Inalámbricas o Redes WiFi de forma general y no precisamente usando la Tecnología SDN o Fabric, lo cual no implica que el personal no este calificado para realizarlas, por favor, sírvase confirmar que el requerimiento del perfil podrá quedar de la siguiente manera:</p> <p>"Un (01) Bachiller o Ingeniero o técnico titulado Electrónico o Sistemas o Telecomunicaciones o redes y comunicaciones, como mínimo con tres (03) años de experiencia realizando tareas de implementación soporte y/o mantenimiento de networking WLAN o Redes Inalámbricas o Redes WiFi"</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>

43	8	96	<p>Con Respecto al Perfil del Personal Clave – Implementador de Networking WLAN, se menciona lo siguiente: "Constancias de experiencia mínima de tres (03) años realizando tareas de implementación y/o soporte y/o mantenimiento de networking WLAN usando la tecnología SDN o fabric.."</p> <p>Teniendo en cuenta que, en las constancias de trabajo del personal, las funciones de los Ingenieros y/o Técnicos, por lo general se describen como servicios de implementación, soporte y/o mantenimientos de redes WLAN o Redes Inalámbricas o Redes WiFi de forma general y no precisamente usando la Tecnología SDN o Fabric, lo cual no implica que el personal no este calificado para realizarlas, por favor, sírvase confirmar que el requerimiento del perfil podrá quedar de la siguiente manera: "Constancias de experiencia mínima de tres (03) años realizando tareas de implementación y/o soporte y/o mantenimiento de networking WLAN o Redes Inalámbricas, o Redes WiFi."</p>	Consulta de la empresa ITALTEL PERU S.A.C..
44	9.1.4	99	<p>Con respecto a la TRANSFERENCIA TECNOLÓGICA, se menciona lo siguiente: "Entrenamiento de 40 horas como mínimo para cuatro 2 personas en el uso de los equipos de redes LAN/WAN que corresponda a los niveles intermedio y avanzado del equipamiento propuesto y relacionado a las implementaciones realizadas para la operación del sistema dentro de CORPAC S.A."</p> <p>Por favor sírvase aclarar si el entrenamiento indicado de 40 horas como mínimo, es para cuatro (04) o para dos (02) personas.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
45	3.1.3	126	<p>Se indica: "El servicio de operación de redes y comunicaciones TI para CORPAC S.A. deberá configurar un Call Center con suficientes líneas de acceso telefónico integradas al Sistema de Mesa de Servicio para la revisión de la calidad y elaboración de reportes e informes de gestión"</p> <p>Confirma que el CALL CENTER es propiedad de Corpac, y que se requiere configurar con nuestra plataforma de Gestión de ticket</p>	Consulta de la empresa ITALTEL PERU S.A.C..
46	6	96	<p>Se indica: "PROFESIONAL RESIDENTE 1 PRESENCIAL (un personal por cada TURNO DE 8 HORAS total 3" Considerando la regulación peruana, se debe considerar un recurso como "descansero", por lo que se debe considerar como 4 personas para cubrir adecuadamente esta posición.</p> <p>Sírvase confirmar que se deberán de considerar 04 personas en total.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
47	5.3.1.4	80	<p>Se indica: Rango de frecuencia: 40 – 70 Hz</p> <p>Consulta:</p>	Consulta de la empresa ITALTEL PERU S.A.C..

			Favor confirmar que para potencias medias de 6KVA y 10KVA, se aceptarán rangos de +/- 4Hz; es decir, en el rango de 46Hz - 64Hz	
48	5.3.1.4	81	Se indica: Toma de entrada: 4 x IEC C13 + 4 x IEC C19 + cableado fijo en caja de distribución de energía. Consulta: Favor confirmar que se aceptará para las tomas IEC 19 de los UPS puedan tener mínimo 1 salida C19, ya que en su mayoría los equipos de TI se conectan a las tomas C13.	Consulta de la empresa ITALTEL PERU S.A.C..
49	5.3.1.4	81	Se indica: Tiempo de recarga: 3 horas al 90% de capacidad después de descarga completa al 100% de carga. Consulta: Favor confirmar que para potencias medias de 6 KVA y 10 KVA se aceptará que el tiempo de recarga tenga un rango de 7 a 9 horas al 90%.	Consulta de la empresa ITALTEL PERU S.A.C..
50	5.3.1.4	81	Se indica: Ruido audible: <55 dB, a 1 metro de la parte posterior <50 dBA, a 1 metro de la parte frontal o de los laterales. Consulta: Favor confirmar que para potencias medias de 6 KVA y 10 KVA se aceptará ruido audible a 1 metro <58 dB	Consulta de la empresa ITALTEL PERU S.A.C..
51	5.3.1.4	79	Se indica: Si bien los cuartos de comunicación tendrán los gabinetes con aire acondicionado del tipo autocontenido según la capacidad de cada uno de estos, sin embargo, la entidad está solicitando adicionalmente instalar equipos de refrigeración del tipo confort mínimo de 12000BTU, como sistema redundante en dichos ambientes. Consulta: Dado que el equipo de confort no es un aire de precisión por lo cual no tiene la funcionalidad para climatizar a equipos de TI este no puede conectarse al aire de precisión y trabajar en redundancia. Favor confirmar, que solo se suministrará el aire de confort y no trabajará en redundancia con el equipo de precisión por lo expuesto anteriormente.	Consulta de la empresa ITALTEL PERU S.A.C..
52	5.3.1.10	83	Se dice: Adicionalmente al objeto de la contratación de equipamiento, CORPAC S.A. requiere renovar la garantía y el soporte de algunos componentes de la infraestructura pasiva implementada que tenga la garantía vigente del fabricante, a manera referencial se muestra el listado de todos los componentes implementados en los diversos nodos de telecomunicaciones en el Aeropuerto Sede Central:	Consulta de la empresa ITALTEL PERU S.A.C..

			<p>Consulta: Favor confirmar que la renovación de garantía y soporte de algunos componentes de la infraestructura también aplica para los equipos activos mientras la garantía de fabricante se encuentre vigente lo que aplica también para los equipos de la marca RITTAL y SIEMON.</p>	
53	5.3.1.10	87	<p>Se dice: DETAC (RENOVACION DE SOPORTE)</p> <p>Consulta: De acuerdo con lo indicado por el fabricante RITTAL, los sistemas DETAC tienen un tiempo de vida útil de 10 años por lo que no calificarían para tener garantía de fábrica. Favor confirmar que el postor deberá de considerar equipos DETAC's nuevos.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
54	5.3.1.8	82	<p>Se dice: VISITA DE CAMPO</p> <p>El postor podrá realizar visitas de campo a las diferentes instalaciones de CORPAC S.A. para cotizar todo lo necesario para la correcta implementación del servicio solicitado. Las visitas podrán coordinarse mediante carta o correo electrónico con mínimo 2 días de anticipación, alcanzando copia del Documento Oficial del Identidad del personal que efectuara la visita.</p> <p>Consulta: Para confirmar qué equipos tienen la garantía vigente. Favor confirmar que el fabricante o postor deberá de hacer el levantamiento de información del estatus actual de la base instalada (servicio de inspección), de encontrarse observaciones en el funcionamiento de los equipos, alarmas, piezas dañadas, se deberá de hacer el respectivo correctivo para que la garantía tenga validez.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
55	5.2.2.1.1.1	14	<p>Se menciona: El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean cómo un único switch desde una perspectiva lógica, manteniendo un único plano de control y gestión, mientras que el plano de datos o transmisión será de tipo distribuido y que garantice la alta disponibilidad en capa 2 y capa 3</p> <p>Consulta: Con el objetivo de una mayor pluralidad de fabricantes, empleando el uso de protocolos estándares de la industria, sírvase a confirmar que se puede cumplir la especificación solicitada mediante el uso de enlaces LACP, garantizando HA en capa 2 y capa 3. Considerando finalmente la siguiente especificación: El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean cómo un único switch desde una perspectiva lógica para lograr agregar enlaces con LACP y garantizar HA en capa 2 y capa 3</p>	Consulta de la empresa ITALTEL PERU S.A.C..

56	5.2.2.1.1.1	16	<p>Se menciona: Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.</p> <p>Consulta: Con el objetivo de una mayor pluralidad de fabricantes, sírvase a confirmar que se podrá cumplir la especificación a través de funcionalidades como Control Plane Policing (CoPP) o similares.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
57	5.2.2.1.1.1	18	<p>Se menciona: IEEE 802.1x suplicant.</p> <p>Consulta: Debido a que esta funcionalidad es principalmente utilizada en la capa de acceso, y con el objetivo de brindar una mayor pluralidad de fabricantes, sírvase a confirmar que lo solicitado será considerado como opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..
58	5.2.2.1.1.2	20	<p>Se menciona: El switch deberá contar con CPU mínimo de 2.2 Ghz</p> <p>Consulta: Debido a que la principal funcionalidad del switch involucra el uso de altos niveles de Throughput y Switching capacity, teniendo el CPU un rol menos determinante en el performance del equipo, ya que esto dependerá de la arquitectura de cada fabricante, sírvase a confirmar que el switch deberá contar con CPU mínimo de 1.8 GHz</p>	Consulta de la empresa ITALTEL PERU S.A.C..
59	5.2.2.1.1.2	20	<p>Se menciona: El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean como un único switch desde una perspectiva lógica, manteniendo un único plano de control y gestión, mientras que el plano de datos será de tipo distribuido y garantice la alta disponibilidad en capa 2 y capa 3.</p> <p>Consulta: Con el objetivo de una mayor pluralidad de fabricantes, empleando el uso de protocolos estándares de la industria, sírvase a confirmar que se puede cumplir la especificación solicitada mediante el uso de enlaces LACP, garantizando HA en capa 2 y capa 3. Considerando finalmente la siguiente especificación: El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean como un único switch desde una</p>	Consulta de la empresa ITALTEL PERU S.A.C..

			perspectiva lógica para lograr agregar enlaces con LACP y garantizar HA en capa 2 y capa 3	
60	5.2.2.1.1.2	20	Se menciona: Debe tener 32 puertos de red 40/100G (QSFP/QSFP28) como mínimo Consulta: Debido a que en las bases se requieren la interconexión de un máximo de 18 nodos lo cual requiere 18 puertos, con la finalidad de permitir una mayor pluralidad de fabricantes, y con el objetivo de evitar sobredimensionar la solución, sírvase confirmar que será válido ofertar soluciones que cuenten con 20 puertos, tal que se cubra con el mínimo necesario para la interconexión de nodos	Consulta de la empresa ITALTEL PERU S.A.C..
61	5.2.2.1.1.2	20	Se menciona: Debe tener 32 puertos de red 40/100G (QSFP/QSFP28) como mínimo Consulta: Sírvase a confirmar que también serán válidas proponer soluciones que cuenten con puertos a velocidades de 50G	Consulta de la empresa ITALTEL PERU S.A.C..
62	5.2.2.1.1.2	20	Se menciona: Debe permitir no menos de 4096 VLAN IDs y soportar e implementar protocolo 802.1q Consulta: Para una mayor pluralidad de fabricantes, se solicita confirmar que la cantidad de VLAN IDs permitidas sea no menor a 4000.	Consulta de la empresa ITALTEL PERU S.A.C..
63	5.2.2.1.1.2	21	Se menciona: RADIUS, TACACS, TACACS+ o equivalentes, ACL IPv4, ACL IPv6, BDPU Guard, BPDU Filter, Root Guard o equivalente, Private VLAN o similares, DHCP Snooping, MLD Snooping. Consulta: Debido a que TACACS y TACACS+ (asociado al siguiente RFC 8907) tienen funcionalidades integrables con distintos fabricantes, ambos siendo estándares de la industria, sírvase a confirmar que no se podrá cumplir esta especificación con protocolos equivalentes o propietarios.	Consulta de la empresa ITALTEL PERU S.A.C..
64	5.2.2.1.1.2	21	Se menciona: Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión. Consulta:	Consulta de la empresa ITALTEL PERU S.A.C..

			Con el objetivo de una mayor pluralidad de fabricantes, sírvase a confirmar que se podrá cumplir la especificación a través de funcionalidades como Control Plane Policing (CoPP) o similares.	
65	5.2.2.1.1.2	23	Se menciona: Deberá contar con mecanismo y/o función de seguridad que utilice una combinación de autenticación, criptografía y verificación de estado para asegurar que los dispositivos de la red puedan confiar en los mensajes de descubrimiento de vecinos IPv6 que se intercambian en la capa 2. Consulta: Debido a que esta especificación está orientada exclusivamente a un solo fabricante, sírvase a confirmar que lo solicitado será considerado como opcional	Consulta de la empresa ITALTEL PERU S.A.C..
66	5.2.2.1.1.3	25	Se menciona: El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal. Consulta: Debido a que esta especificación está orientada a un solo fabricante, sírvase a confirmar que lo solicitado será considerado como opcional	Consulta de la empresa ITALTEL PERU S.A.C..
67	5.2.2.1.1.3	25	Se menciona: El switch propuesto debe contar con al menos 48 puertos 10/100/1000 Base-T RJ45 con soporte PoE/PoE+, en todos sus puertos. Consulta: Debido a que la velocidad de funcionamiento de los dispositivos finales tienden a aumentar con el paso de los años, y en pro de mantener una arquitectura de red acorde a las nuevas tendencias y estándares de la industria, sírvase a confirmar que el switch propuesto deba contar como mínimo con 48 puertos 100M//1G/2.5G/5G, Base-T RJ45 con soporte PoE/PoE+ en todos sus puertos	Consulta de la empresa ITALTEL PERU S.A.C..
68	5.2.2.1.1.3	25	Se menciona: El switch propuesto debe contar con al menos 2 puertos 40GE de uplink. Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, se solicita confirmar que se podrán proponer soluciones con puertos de uplink a 50GE.	69Consulta de la empresa ITALTEL PERU S.A.C..
69	5.2.2.1.1.3	25	Se menciona: Debe incluir 2 transceivers de 40Gbps (SFP28) para fibra óptica monomodo 10Km Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, sírvase a confirmar que se podrán proponer soluciones con puertos de 50Gbps(SFP28) para fibra óptica monomodo 10Km	Consulta de la empresa ITALTEL PERU S.A.C..

70	5.2.2.1.1.3	25	<p>Se menciona: El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking.</p> <p>Consulta: Con el objetivo de tener una mayor pluralidad de fabricantes, sírvase en confirmar que se podrá realizar el stacking de los switches por medio de puertos de uplink adicionales, con ello se ahorra costos en agregar módulos dedicados para los puertos de stacking del equipo</p>	Consulta de la empresa ITALTEL PERU S.A.C..
71	5.2.2.1.1.3	26	<p>Se menciona: Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.</p> <p>Consulta: Con el objetivo de una mayor pluralidad de fabricantes, sírvase a confirmar que se podrá cumplir la especificación a través de funcionalidades como Control Plane Policing (CoPP) o similares.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
72	5.2.2.1.1.3	26	<p>Se menciona: El switch propuesto debe soportar puertos Uplinks Modulares o Fijos con opciones de tasas de transmisión de 10Gbps y 40 Gbps.</p> <p>Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, se solicita confirmar que se podrán proponer soluciones de switches con uplink modulares o fijos con velocidad de transmisión de 10Gbps y 50 Gbps</p>	Consulta de la empresa ITALTEL PERU S.A.C..
73	5.2.2.1.1.3	26	<p>Se menciona: Configuración automática de QoS.</p> <p>Consultar: Debido a que esta característica está orientada exclusivamente al fabricante Cisco, sírvase a confirmar que esta característica sea opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..
74	5.2.2.1.1.3	26	<p>Se menciona: El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo.</p> <p>Consulta:</p>	Consulta de la empresa ITALTEL PERU S.A.C..

			Debido a que esta característica está orientada exclusivamente al fabricante Cisco, sírvase a confirmar que esta característica será opcional.	
75	5.2.2.1.1.4	28	Se menciona: El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal. Consulta: Debido a que esta funcionalidad está orientada al fabricante Cisco, sírvase a confirmar que esta funcionalidad será opcional	Consulta de la empresa ITALTEL PERU S.A.C..
76	5.2.2.1.1.4	28	Se menciona: El switch propuesto debe contar con al menos 24 puertos 10/100/1000 Base-T RJ45 con soporte PoE/PoE+, en todos sus puertos. Consulta: Debido a que la velocidad de funcionamiento de los dispositivos finales tienden a aumentar con el paso de los años, y en pro de mantener una arquitectura de red acorde a las nuevas tendencias y estándares de la industria, sírvase a confirmar que el switch propuesto deba contar como mínimo con 24 puertos 100M//1G/2.5G/5G, Base-T RJ45 con soporte PoE/PoE+ en todos sus puertos	Consulta de la empresa ITALTEL PERU S.A.C..
77	5.2.2.1.1.4	28	Se menciona: El switch propuesto debe contar con al menos 2 puertos 40GE de uplink. Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, se solicita confirmar que se podrán proponer soluciones con puertos de uplink a 50GE.	Consulta de la empresa ITALTEL PERU S.A.C..
78	5.2.2.1.1.4	28	Se menciona: Debe incluir 2 transceivers de 40Gbps (SFP28) para fibra óptica monomodo 10Km Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, sírvase a confirmar que se podrán proponer soluciones con puertos de 50Gbps(SFP28) para fibra óptica monomodo 10Km	Consulta de la empresa ITALTEL PERU S.A.C..
79	5.2.2.1.1.4	28	Se menciona: El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking. Consulta: Con el objetivo de tener una mayor pluralidad de fabricantes, sírvase en confirmar que se podrá realizar el stacking de los switches por medio de puertos de uplink adicionales, con ello se ahorra costos en agregar módulos dedicados para los puertos de stacking del equipo.	Consulta de la empresa ITALTEL PERU S.A.C..

80	5.2.2.1.1.4	29	<p>Se menciona: RADIUS, TACACS, TACACS+ o equivalentes, ACL IPv4, ACL IPv6, BDPU Guard, BDPU Filter, Root Guard o equivalente, Private VLAN o similares, DHCP Snooping, MLD Snooping.</p> <p>Consulta: Debido a que TACACS y TACACS+ (asociado al siguiente RFC 8907) tienen funcionalidades integrables con distintos fabricantes, ambos siendo estándares de la industria, Sírvese a confirmar que no se podrá cumplir esta especificación con protocolos equivalentes o propietarios.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
81	5.2.2.1.1.4	29	<p>Se menciona: Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.</p> <p>Consulta: Con el objetivo de una mayor pluralidad de fabricantes, sírvase a confirmar que se podrá cumplir la especificación a través de funcionalidades como Control Plane Policing (CoPP) o similares.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
82	5.2.2.1.1.4	29	<p>Se menciona: El switch propuesto debe soportar puertos Uplinks Modulares o Fijos con opciones de tasas de transmisión de 10Gbps y 40 Gbps.</p> <p>Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, se solicita confirmar que se podrán proponer soluciones de switches con uplink modulares o fijos con velocidad de transmisión de 10Gbps y 50 Gbps</p>	Consulta de la empresa ITALTEL PERU S.A.C..
83	5.2.2.1.1.4	29	<p>Se menciona: Configuración automática de QoS.</p> <p>Consulta: Debido a que esta característica está orientada exclusivamente al fabricante Cisco, Sírvese a confirmar que lo solicitado será considerado como opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..
84	5.2.2.1.1.4	29	<p>Se menciona: El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo.</p> <p>Consulta:</p>	Consulta de la empresa ITALTEL PERU S.A.C..

			Debido a que esta característica está orientada exclusivamente al fabricante Cisco, sírvase a confirmar que lo solicitado será considerado como opcional	
85	5.2.2.1.1.5	31	Se menciona: El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal. Consulta: Debido a que esta funcionalidad está orientada al fabricante Cisco, Sírvase a confirmar que esta funcionalidad será opcional	Consulta de la empresa ITALTEL PERU S.A.C..
86	5.2.2.1.1.5	31	Se menciona: El switch propuesto debe contar con al menos 2 puertos 40GE de uplink. Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, se solicita confirmar que se podrán proponer soluciones con puertos de uplink a 50GE.	Consulta de la empresa ITALTEL PERU S.A.C..
87	5.2.2.1.1.5	31	Se menciona: Debe incluir 2 transceivers de 40Gbps (SFP28) para fibra óptica monomodo 10Km Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, Sírvase a confirmar que se podrán proponer soluciones con puertos de 50Gbps(SFP28) para fibra óptica monomodo 10Km	Consulta de la empresa ITALTEL PERU S.A.C..
88	5.2.2.1.1.5	31	Se menciona: El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking. Consulta: Con el objetivo de tener una mayor pluralidad de fabricantes, Sírvase en confirmar que se podrá realizar el stacking de los switches por medio de puertos de uplink adicionales, con ello se ahorra costos en agregar módulos dedicados para los puertos de stacking del equipo.	Consulta de la empresa ITALTEL PERU S.A.C..
89	5.2.2.1.1.5	32	Se menciona: RADIUS, TACACS, TACACS+ o equivalentes, ACL IPv4, ACL IPv6, BDPU Guard, BPDU Filter, Root Guard o equivalente, Private VLAN o similares, DHCP Snooping, MLD Snooping. Consulta: Debido a que TACACS y TACACS+ (asociado al siguiente RFC 8907) tienen funcionalidades integrables con distintos fabricantes, ambos siendo estándares de la industria, Sírvase a confirmar que no se podrá cumplir esta especificación con protocolos equivalentes o propietarios.	Consulta de la empresa ITALTEL PERU S.A.C..
90	5.2.2.1.1.5	32	Se menciona:	

			<p>El switch propuesto debe soportar puertos Uplinks Modulares o Fijos con opciones de tasas de transmisión de 10Gbps y 40 Gbps.</p> <p>Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, se solicita confirmar que se podrán proponer soluciones de switches con uplink modulares o fijos con velocidad de transmisión de 10Gbps y 50 Gbps</p>	Consulta de la empresa ITALTEL PERU S.A.C..
91	5.2.2.1.1.5	32	<p>Se menciona: Configuración automática de QoS.</p> <p>Consulta: Debido a que esta característica está orientada exclusivamente al fabricante Cisco, sírvase a confirmar que esta característica sea opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..
92	5.2.2.1.1.5	32	<p>Se menciona: El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo.</p> <p>Consulta: Debido a que esta característica está orientada exclusivamente al fabricante Cisco, sírvase a confirmar que esta característica será opcional.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
93	5.2.2.1.1.6	34	<p>Se menciona: RADIUS, TACACS, TACACS+ o equivalentes, ACL IPv4, ACL IPv6, BDPU Guard, BDPU Filter, Root Guard o equivalente, Private VLAN o similares, DHCP Snooping, MLD Snooping.</p> <p>Consulta: Debido a que TACACS y TACACS+ (asociado al siguiente RFC 8907) tienen funcionalidades integrables con distintos fabricantes, ambos siendo estándares de la industria, Sírvase a confirmar que no se podrá cumplir esta especificación con protocolos equivalentes o propietarios.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
94	5.2.2.1.2.1	36	<p>Se menciona: El equipo deberá soportar por lo menos 16000 dispositivos clientes y 4096 WLANS.</p> <p>Consulta: Para una mayor pluralidad de fabricantes Sírvase confirmar que el equipo a ofertar soporte por lo menos 10000 dispositivos clientes.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
95	5.2.2.1.2.1	36	<p>Se menciona: El equipo deberá soportar por lo menos 16000 dispositivos clientes y 4096 WLANS.</p> <p>Consulta:</p>	Consulta de la empresa ITALTEL PERU S.A.C..

			Para una mayor pluralidad de fabricantes, se solicita confirmar que la cantidad de VLANs permitidas sean no menor a 4000.	
96	5.2.2.1.2.1	36	Se menciona: Implementar barrido continuo de RF, programado bajo demanda de puntos de acceso con identificación de clientes irregulares. Consulta: Con el objetivo de una mayor pluralidad de postores, Sírvase a confirmar que el añadido 'con identificación de clientes irregulares' podrá ser opcional	Consulta de la empresa ITALTEL PERU S.A.C..
97	5.2.2.1.2.1	37	Se menciona: Deberá soportar NETCONFF (RFC 6241) o RESTCONF (RFC 8040) para proporcionar una interfaz de programabilidad estándar y permitir el acceso a parámetros de configuración. Consulta: Con el objetivo de una mayor pluralidad de postores, Sírvase a confirmar que la especificación podrá ser cumplida con RESTAPI o similares	Consulta de la empresa ITALTEL PERU S.A.C..
98	5.2.2.1.2.1	37	Se menciona: Debe incluir visibilidad de las aplicaciones consumidas por los usuarios, combinando la detección y el control de aplicaciones en la red, identificando y clasificando información de Capa 4 a Capa 7 de las aplicaciones que se están utilizando en la red; que luego permitan configurar ACL por aplicación o categoría de aplicación y acelerar el ancho de banda para aplicaciones de misión crítica para priorización del tráfico y QoS; utilizando como tecnologías que pueden ser control de aplicaciones, inspección profunda de paquetes, reconocimiento de aplicaciones basado en red, o una combinación de las mismas. Consulta: Debido a que la especificación está orientada a un solo fabricante, Sírvase a confirmar que lo solicitado será considerado como opcional	Consulta de la empresa ITALTEL PERU S.A.C..
99	5.2.2.1.2.1	37	Se menciona: Actualización en vivo de los Access Points Consulta: Con el objetivo de simplificar la gestión de la solución, Sírvase a confirmar que la especificación será cumplida con la solución requerida en el numeral 5.2.2.1.4 - PLATAFORMA DE GESTIÓN Y AUTENTICACION DE ACCESO A LA RED	Consulta de la empresa ITALTEL PERU S.A.C..
100	5.2.2.1.2.2	38	Se menciona: Despliegue de políticas de Calidad de Servicio (QoS) de manera automatizada en base al listado de aplicaciones críticas, no críticas y por defecto. Este despliegue será basado en las aplicaciones que son las reconocidas por la solución del fabricante y aplicaciones	

			personalizadas que corresponden a la Entidad en base a puertos TCP o UDP o IP Consulta: Debido a que la especificación está orientada a un solo fabricante, sírvase a confirmar que lo solicitado será considerado como opcional	Consulta de la empresa ITALTEL PERU S.A.C..
101	5.2.2.1.3	39	Se menciona: La solución de automatización, administración y gestión de la infraestructura campus con todos sus componentes de hardware y software serán implementados en alta disponibilidad sen un entorno ON PREMISE utilizando appliances de propósito específico Consulta: Sírvase en confirmar que también se aceptarán soluciones en nube tipo SaaS para la administración y gestión de los equipos (Switching y WiFi)	Consulta de la empresa ITALTEL PERU S.A.C..
102	5.2.2.1.3	39	Se menciona: Utilizando licenciamiento del tipo perpetuo. Consulta: Sírvase en confirmar que también se aceptaran licenciamiento bajo un esquema de suscripción garantizando el soporte y correcto funcionamiento de este.	Consulta de la empresa ITALTEL PERU S.A.C..
103	5.2.2.1.3	40	Se menciona: Verificaciones antes y después de realizar el despliegue de nuevas versiones de software en los switches. Consulta: Las verificaciones de software del sistema operativo se realiza antes de realizar el despliegue de los equipos, Sírvase en confirmar que esta funcionalidad será considerada como opcional.	Consulta de la empresa ITALTEL PERU S.A.C..
104	5.2.2.1.3	40	Se menciona: Despliegue de políticas de Calidad de Servicio (QoS). Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..
105	5.2.2.1.3	40	Se menciona: El sistema de administración dispondrá de una función que centralice las configuraciones de los equipos permitiendo mantener copia de la configuración con múltiples versiones de las mismas. Deberá permitir realizar el respaldo, la restitución y la comparación de archivos de configuración Consulta:	Consulta de la empresa ITALTEL PERU S.A.C..

			Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	
106	5.2.2.1.3	40	Se menciona: Tendrá una función que permitirá establecer una fecha u horario donde se aplicará la tarea en forma automática. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..
107	5.2.2.1.3	40	Se menciona: Organización jerárquica de equipos en plantas, plantas en edificios y edificios en proyectos. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..
108	5.2.2.1.3	41	Se menciona: Capacidad de generar informes de los siguientes tipos: Lista de clientes wireless o lista de tipo de dispositivo cliente Consulta: Sírvase en confirmar que la lista de clientes Wireless a exportar, será los que se encuentren activos en el dashboard	Consulta de la empresa ITALTEL PERU S.A.C..
109	5.2.2.1.3	41	Se menciona: Información de configuración de los controladores WLAN Consulta: Sírvase en confirmar que la información de los controladores WLAN se verá la información en cada equipo.	Consulta de la empresa ITALTEL PERU S.A.C..
110	5.2.2.1.3	41	Se menciona: Deberá permitir configurar para que automáticamente almacene el respaldo de las configuraciones de los equipos inalámbricos, por ejemplo, cada mes, cada semana, etc. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..

111	5.2.2.1.3	42	<p>Se menciona: Debe incluir una solución que permita el uso de algoritmos avanzados de análisis de comportamiento; para identificar patrones de tráfico, usando análisis de la información de eventos que ocurren dentro de un flujo de datos aplicando técnicas de machine learning, o plataforma de análisis de big data Telemetry que analice y muestre los datos de la red a través de algoritmos inteligentes; con el objetivo de detectar potenciales amenazas de seguridad, a través de la inclusión de hardware y software adicional que permita descifrar el tráfico para su análisis.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
112	5.2.2.1.3	42	<p>Se menciona: Soporte de descubrimiento vía SNMP o tablas de enrutamiento o tablas ARP etc., o cualquier otro mecanismo que brinde el fabricante para automatizar este proceso.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
113	5.2.2.1.3	42	<p>Se menciona: Soporte de la visualización de la configuración del servicio, la configuración y el monitoreo de la red virtual basada en topología y la consulta del estado del aprovisionamiento del servicio en tiempo real.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
114	5.2.2.1.3	42	<p>Se menciona: Soporte de programación de QoS basada en usuarios y prioridades de servicio. Esto debe permitir la implementación de diferentes políticas para diferentes usuarios y aplicaciones a través de la generación de control de políticas de ancho de banda.</p> <p>Consulta: Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.</p>	Consulta de la empresa ITALTEL PERU S.A.C..

115	5.2.2.1.3	42	<p>Se menciona: Soporte de monitoreo de red basado en mapas, inspección de red.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
116	5.2.2.1.3	42	<p>Se menciona: Soporte de visibilidad de experiencia en tiempo real del uso de aplicaciones de cada usuario en cada área.</p> <p>Consulta: Sirvase en confirmar que, para revisar la experiencia del uso de las aplicaciones, se pueda considerar un equipo adicional para que este monitoree el estado de la red inalámbrica</p>	Consulta de la empresa ITALTEL PERU S.A.C..
117	5.2.2.1.3	42	<p>Se menciona: Soporte de seguimiento de fallas, que permita identificar con rapidez a los dispositivos defectuosos, así como analizar las causas raíz de la mala calidad.</p> <p>Consulta: Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión</p>	Consulta de la empresa ITALTEL PERU S.A.C..
118	5.2.2.1.3	42	<p>Se menciona: Capacidad de evaluar conflictos de la red inalámbrica en tiempo real.</p> <p>Consulta: Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión</p>	Consulta de la empresa ITALTEL PERU S.A.C..
119	5.2.2.1.3	42	<p>Se menciona: Capacidad de comparar las ganancias de la red inalámbrica antes y después de la calibración.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
120	5.2.2.1.3	42	<p>Se menciona: Vistas de estadísticas de datos multidimensionales basadas en diferentes niveles y regiones</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sirvase en confirmar que esta</p>	Consulta de la empresa ITALTEL PERU S.A.C..

			funcionalidad será considerada como opcional dentro de la plataforma de gestión.	
121	5.2.2.1.3	43	Se menciona: Permite enviar informes de salud de la red al administrador en tiempo real o periódicamente. Consulta: Sírvese en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión	Consulta de la empresa ITALTEL PERU S.A.C..
122	5.2.2.1.3	43	Se menciona: El servidor debe contar con la funcionalidad de Syslog. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvese en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..
123	5.2.2.1.3	43	Se menciona: Monitoreo de seguridad y verificación de la salud de la red para poder determinar si la red tiene las políticas de seguridad óptimas a nivel de configuración. Consulta: Sírvese en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión	Consulta de la empresa ITALTEL PERU S.A.C..
124	5.2.2.1.3	43	Se menciona: Permitir el monitoreo de servicios de video y voz sobre wireless. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvese en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..
125	5.2.2.1.3	43	Se menciona: Permitir visualizar la cantidad de clientes conectados, habilitar capturas en tiempo real, listar amenazas detectadas Consulta: Sírvese en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión	Consulta de la empresa ITALTEL PERU S.A.C..
126	5.2.2.1.3	43	Se menciona: La solución debe de permitir realizar backups automáticos de la configuración del sistema. Consulta:	Consulta de la empresa ITALTEL PERU S.A.C..

			Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	
127	5.2.2.1.3	43	Se menciona: Inventarios debe al menos dar información de número de serie y versión de imagen de sistema operativo. Consulta: Sírvase en confirmar que esta información pueda ser exportada desde la página de inicio de la plataforma de gestión y no como reporte.	Consulta de la empresa ITALTEL PERU S.A.C..
128	5.2.2.1.3	43	Se menciona: Permite a los usuarios importar vistas de topología y planificar ubicaciones de AP para ver la distribución de la ubicación de fallas. Consulta: Sírvase en confirmar que esta información de la distribución de la ubicación de fallas será considerada como opcional La funcionalidad de distribución de la ubicación de fallas está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..
129	5.2.2.1.3	43	Se menciona: Permitir correlacionar la información de la red/wifi/analíticos/control de acceso en un solo dashboard. Consulta: Sírvase en aclarar que el control de acceso se realizara a traves de la plataforma de control de Acceso (NAC)	Consulta de la empresa ITALTEL PERU S.A.C..
130	5.2.2.1.3	43	Se menciona: Permite a los usuarios importar datos de planificación de la red y comparar los datos de planificación con los datos reales de funcionamiento de la red para mostrar las diferencias entre ellos. Consulta: Sírvase en confirmar que esta información de la distribución de la ubicación de fallas, sea considerada como opcional	Consulta de la empresa ITALTEL PERU S.A.C..
131	5.2.2.1.3	43	Se menciona: Debe tener la capacidad de ser un servidor syslog. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..

132	5.2.2.1.3	43	<p>Se menciona: Debe de poder hacer backup de las configuraciones</p> <p>Consulta: Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión</p>	Consulta de la empresa ITALTEL PERU S.A.C..
133	5.2.2.1.3	44	<p>Se menciona: Protocolos de análisis de tiempo de respuesta de aplicaciones, análisis de tráfico de voz y video.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
134	5.2.2.1.3	44	<p>Se menciona: Los dashboard deben de ser configurables y se puede personalizar la ventana de vista de dashboard.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
135	5.2.2.1.4	45	<p>Se menciona: Para la gestión y autenticación de acceso a la red, se debe implementar el servicio RADIUS y/o TACACS, TACACS+ o equivalentes, que incluya el licenciamiento necesario para el Sistema Operativo, el servicio RADIUS o TACACS o TACACS+ y un Servicio NTP.</p> <p>Consulta: Sirvase en confirmar que la funcionalidad de NTP sea considerada como opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..
136	5.2.2.1.4	46	<p>Se menciona: El sistema de control de acceso debe permitir integrarse al controlador SDN</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sirvase en confirmar que esta funcionalidad será considerada como opcional.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
137	5.2.2.1.4	47	<p>Se menciona: Debe permitir vincular información a cuentas de usuario y cuentas MAC, incluyendo la dirección IP, la dirección MAC (no aplicable a cuentas MAC) y la información del dispositivo de acceso. Esta información se debe utilizar para restringir los comportamientos de acceso del usuario,</p>	Consulta de la empresa ITALTEL PERU S.A.C..

			<p>por ejemplo, los usuarios solo pueden acceder a la red a través de la dirección IP vinculada a su cuenta respectiva.</p> <p>Consulta: Sírvese en confirmar que esta funcionalidad, será considerada como opcional</p>	
138	5.2.2.1.4	48	<p>Se menciona: Debe permitir la gestión de lista negra de usuarios. Se debe poder agregar manualmente usuarios a la lista negra o configurar la función de bloqueo automático de usuarios que ingresan contraseñas incorrectas varias veces consecutivas y usuarios con direcciones IP o MAC específicas. Los usuarios en la lista negra tienen denegado el acceso a la red</p> <p>Consulta: Sírvese en confirmar que esta funcionalidad, será considerada como opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..
139	5.2.2.1.4	48	<p>Se menciona: Admite la gestión de PPSK (Clave Precompartida por Usuario). Se pueden establecer diferentes PPSK para diferentes usuarios en la misma red Wi-Fi.</p> <p>Consulta: Sírvese en confirmar que esta funcionalidad, será considerada como opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..
140	5.2.2.1.4	48	<p>Se menciona: Si una regla personalizada contiene múltiples condiciones coincidentes, un terminal solo coincide con la regla cuando la puntuación total de las condiciones coincidentes en esta regla alcanza la puntuación mínima requerida.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvese en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de control de Acceso.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
141	5.2.2.1.4	48	<p>Se menciona: Debe utilizar inteligencia artificial para agrupar terminales no identificados después de recopilar huellas digitales de terminales.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvese en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de control de Acceso.</p>	Consulta de la empresa ITALTEL PERU S.A.C..

142	5.2.2.1.4	48	<p>Se menciona: Autenticación mediante código de acceso: El usuario ingresa el código de acceso en la página del portal de autenticación. En este modo, los códigos de acceso deben ser creados y distribuidos previamente por los administradores.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de control de Acceso</p>	Consulta de la empresa ITALTEL PERU S.A.C..
143	5.2.2.1.4	48	<p>Se menciona: Además, el usuario puede optar por asociar un número de teléfono móvil con la cuenta durante la autenticación por SMS.</p> <p>Consulta: Sírvase en confirmar que esta funcionalidad, será considerada como opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..
144	5.2.2.1.6	52	<p>Se menciona: En el caso de Overlay distribuido: Se deberá contemplar cualquier componente de hardware adicional redundante para que permita a los usuarios de los diferentes segmentos de red creados consumir servicios que estarán ubicados en un punto común (Data Centers). Para ello se deberá hacer uso de VRF Leaking.</p> <p>Aclaración: Las configuraciones de VRF leaking están asociadas al fabricante Cisco, Sírvase en aclarar que esta configuración será opcional o reemplazado con la configuración indicada por el fabricante.</p>	Consulta de la empresa ITALTEL PERU S.A.C..
145	5.2.2.1.6	52	<p>Se menciona: En el caso de Overlay distribuido: Independiente del tipo de Overlay a desplegar. Se deberá realizar una integración con el NAC para poder asignar los SGT o Roles correspondientes que permitan manejar una microsegmentación.</p> <p>Aclaración: Las configuraciones de SGT es asociada a Cisco. Sírvase en aclarar que se realizará las integraciones con el NAC de acuerdo con las soluciones brindadas por el fabricante propuesto</p>	Consulta de la empresa ITALTEL PERU S.A.C..
146	5.2.2.1.6	52	<p>Se menciona: Implementación de las políticas para el ingreso de operadores de red con TACACAS, TACACS+ o equivalente, para Autenticación, Autorización y Accounting.</p> <p>Consulta:</p>	Consulta de la empresa ITALTEL PERU S.A.C..

			Debido a que TACACS y TACACS+ (asociado al siguiente RFC 8907) tienen funcionalidades integrables con distintos fabricantes, ambos siendo estándares de la industria, Sirvase a confirmar que no se podrá cumplir esta especificación con protocolos equivalentes.	
147	5.2.2.1.4	45	Se menciona: Para la gestión y autenticación de acceso a la red, se debe implementar el servicio RADIUS y/o TACACS, TACACS+ o equivalentes, que incluya el licenciamiento necesario para el Sistema Operativo, el servicio RADIUS o TACACS o TACACS+ y un Servicio NTP. Consulta: Debido a que TACACS y TACACS+ (asociado al siguiente RFC 8907) tienen funcionalidades integrables con distintos fabricantes, ambos siendo estándares de la industria, Sirvase a confirmar que no se podrá cumplir esta especificación con protocolos equivalentes.	Consulta de la empresa ITALTEL PERU S.A.C..
148	5.2.2.1.2.1	36	Se menciona: El equipo deberá soportar por lo menos 16000 dispositivos clientes y 4096 WLANS. Consulta: Sirvase confirmar que el termino WLANS hace referencia a VLANs.	Consulta de la empresa ITALTEL PERU S.A.C..
149	5.1	5	Se dice: PRESTACIÓN PRINCIPAL SISTEMA DE CABLEADO ESTRUCTURADO OPTIMIZACION DEL CABLEADO ESTRUCTURADO IMPLEMENTACIÓN DE 3 NUEVOS NODOS RENOVACIÓN DE EQUIPAMIENTO PASIVO EN 16 NODOS ACTUALES (CONTROL DE ACCESO, CCTV, AA DE CONFORT DE CONTINGENCIA, SISTEMA DE UPS) Y EN 2 SALAS (SALA CARRIER Y SALA BLANCA). Consulta: Favor de especificar cuál es el alcance del presente proyecto para las 2 salas (SALA CARRIER Y SALA BLANCA)	Consulta de la empresa ITALTEL PERU S.A.C..
149	5.3.1.4 – B	75	Dice: Compresión De Video: Corriente principal: H.264 (MPEG-4 Parte 10/AVC), Subtransmisión: H.265 PEG-H Parte 2/HEVC) Consulta: La especificación indicada corresponde a un modelo discontinuado. Con el objetivo de poder presentar un equipo actual, se solicita se acepte la siguiente modificación: Debe decir: "Compresión De Video:	Consulta de la empresa ITALTEL PERU S.A.C..

			H.264 (MPEG-4 Parte 10/AVC), Baseline perfil, Main perfil, y High perfil H.265 (MPEG-H Parte 2/HEVC) Main perfil, MJPEG"	
150	5.3.1.4 – B	75	<p>Dice: Tipo H.264: Baseline perfil, Main perfil y Highperfil Tipo H.265: Main perfil, Motion JPEG</p> <p>Consulta: La especificación indicada corresponde a un modelo descontinuado. Con el objetivo de poder presentar un equipo actual, se solicita se acepte la siguiente modificación:</p> <p>Debe decir: "Tipo H.264: Baseline perfil, Main perfil, y High perfil Tipo H.265: Main perfil, MJPEG"</p>	Consulta de la empresa ITALTEL PERU S.A.C..
151	5.3.1.4 – B	76	<p>Dice: Seguridad: Protección por contraseña, filtrado de direcciones IP, HTTPSa, control de acceso a la red IEEE 802.1x (EAP-TLS)a, autenticación Digest, registro de acceso de usuarios, gestión centralizada de certificados, protección contra retrasos de fuerza bruta, firmware firmado, arranque seguro vídeo firmado, pulsación de tecla segura (con certificación CC EAL4)</p> <p>Consulta: La especificación indicada corresponde a un modelo descontinuado. Con el objetivo de poder presentar un equipo actual, se solicita se acepte la siguiente modificación:</p> <p>Debe decir: "Seguridad perimetral: - Software: Firmware firmado, protección contra retrasos de fuerza bruta, autenticación Digest y flujo de código de autorización OpenID OAuth 2.0 RFC6749 para gestión centralizada de cuentas ADFS, protección mediante contraseña, cifrado de tarjeta SD AES-XTS-Plain64 de 256 bits - Hardware: Plataforma de ciberseguridad Axis Edge Vault Elemento seguro (CC EAL 6+), seguridad de sistema en un chip (TEE), ID de dispositivo de Axis, almacén de claves seguro, vídeo firmado, arranque seguro, sistema de archivos cifrado (AES-XTS-Plain64 256 bits) Seguridad de red</p>	Consulta de la empresa ITALTEL PERU S.A.C..

			IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2), IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), X.509 Certificado PKI, firewall basado en host"	
152	General	General	Consulta: Sírvese a confirmar si se enviará el detalle de los planos en autocad de los 16 nodos existentes + 02 salas (SALA CARRIER Y SALA BLANCA)	Consulta de la empresa ITALTEL PERU S.A.C..
153	5.3.1.5.1.1	79	Con respecto a la Estación de Monitoreo de la Solución de CCTV, se menciona lo siguiente: • Debe contar con un procesador i7 última generación. Consulta: Considerando que la Estación de Monitoreo propio del fabricante de la solución de CCTV, con procesador i7 ha sido discontinuado y con el objetivo de poder presentar un equipo actual, se solicita se acepte la siguiente modificación como mínimo: "• Debe contar con un procesador i3 última generación."	Consulta de la empresa ITALTEL PERU S.A.C..

ANEXO C.1

ABSOLUCION A LAS CONSULTAS Y/U OBSERVACIONES DEL ANEXO C

N° de orden	Términos de Referencia o Especificaciones Técnicas o Requisitos de calificación		Consulta y/u Observación	Corresponde a consulta y/u observación del OEC o de las empresas invitadas en la indagación de mercado	Análisis respecto de la consulta u observación. (Precisar si se acoge o no se acoge. En caso de no acoger sustentar los motivos)	Precisión de aquello que se incorporará en los TDR o EEETT o Requisitos de calificación, de corresponder
	Numeral	Pág.				
1	5.2.2.1.1.1	14	El switch deberá contar con CPU mínimo de 2.2 Ghz. "Para tener una mejor eficiencia y reasignar los recursos dependiendo de la carga sirvase permitir una arquitectura multi-core a nivel de CPU".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se aclara que, con el fin de tener mayor pluralidad de postores, se permitirá una frecuencia de CPU de uno o más cores de 1.4 GHz.	El switch deberá contar con CPU mínimo de 1.4 Ghz de uno o mas cores.
2	5.2.2.1.1.1	14	Debe tener mínimo la capacidad de memoria Flash o SSD de 2GB. "Para tener una capacidad de ampliacion de almacenamiento mediante USB o disco SATA SSD para instalacion de aplicaciones mediante contenedores o similares . sirvase permitir solo la memoria flash de al menos 16GB y la memoria SSD pueda tener la capacidad de soportar hasta 960GB"	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se aclara que lo indicado restringe la participación de postores, por lo que no se acepta lo solicitado. Por otro lado las características solicitadas son requerimientos mínimos, el proveedor o postor puede ofertar mejoras al requerimiento.	
3	5.2.2.1.1.1	14	Debe incluir todos los componentes necesarios para realizar el stacking virtual o solución equivalente. "Sirvase considerar solo la tecnologia de stacking virtual ya que aumentaria la eficacia operativa y potencia las comunicaciones sin interrupciones y el ancho de banda del sistema a escala".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se aclara que lo indicado restringe la participación de postores, por lo que no se acepta lo solicitado. Por otro lado las características solicitadas son requerimientos mínimos, el proveedor o postor puede	

Fecha: 26/08/2024

					ofertar mejoras al requerimiento.	
4	5.2.2.1.1.1	18	Los dos Switches de Core deberán trabajar de tal manera que operan en alta disponibilidad, en modo Activo/Activo o ser capaz de asegurar la operación de la plataforma ante un escenario de falla o actualización, manteniendo la conmutación tanto en capa2 como en capa3 por medio de una solución del tipo Fabric o SDN. "Sirvase permitir trabajar la alta disponibilidad en modo activo / pasivo, teniendo en cuenta que un switch es el activo y funciona como plano de control y gestion mientras que el otro es el de reserva".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se aclara que, la solución activo-activo permite aprovechar toda la capacidad instalada de la solución, por lo cual no se acepta lo indicado.	
5	5.2.2.1.1.1	18	Los dos Switches de Core deberán trabajar de tal manera que operan en alta disponibilidad, en modo Activo/Activo. "Sirvase permitir trabajar la alta disponibilidad en modo activo / pasivo, teniendo en cuenta que un switch es el activo y funciona como plano de control y gestion mientras que el otro es el de reserva".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se aclara que, la solución activo-activo permite aprovechar toda la capacidad instalada de la solución, por lo cual no se acepta lo indicado.	
6	5.2.2.1.1.2	20	El switch deberá contar con CPU mínimo de 2.2 Ghz "Para tener una mejor eficiencia y reasignar los recursos dependiendo de la carga sirvase permitir una arquitectura multi-core a nivel de CPU".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se aclara que, con el fin de tener mayor pluralidad de postores, se permitirá una frecuencia de CPU de uno o más cores de 1.4 GHz.	El switch deberá contar con CPU mínimo de 1.4 Ghz de uno o mas cores.
7	5.2.2.1.1.2	20	Debe tener mínimo la capacidad de memoria Flash o SSD de 2GB. "Para tener una capacidad de ampliacion de almacenamiento mediante USB o disco SATA SSD para instalacion de aplicaciones mediante contenedores o similares . sirvase permitir solo la memoria flash de al menos 16GB y la memoria SSD pueda tener la capacidad de soportar hasta 960GB".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se aclara que lo indicado restringe la participación de postores, por lo que no se acepta lo solicitado. Por otro lado las características solicitadas son requerimientos mínimos, el proveedor o postor puede ofertar mejoras al requerimiento.	
8	5.2.2.1.1.2	20	Debe tener 32 puertos de red 40/100G (QSFP/QSFP28) como mínimo. "De acuerdo al diagrama de bloques de arquitectura de interconexion y no desperdiciar puertos sirvase permitir al menos 24 puertos de red 40Gbps QSFP y al menos 8 puertos de 100Gbps".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Es un requerimiento de la Entidad contar con un equipo de 32 puertos para crecimiento futuro. Asimismo lo puertos de 40/100 Gbps on para tener la flexibilidad de incrementar la capacidad de las conexiones según demanda. Se precisa que actualmente se tiene en porcentaje de ocupación y utilización del 59% de	

					puertos sin implementar nuevos nodos; y sin porcentaje de crecimiento.	
9	5.2.2.1.1.2	20	Debe incluir todos los componentes necesarios para realizar el stacking virtual o solución equivalente. "Sirvase considerar solo la tecnología de stacking virtual ya que aumentaría la eficacia operativa y potencia las comunicaciones sin interrupciones y el ancho de banda del sistema a escala".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se aclara que lo indicado restringe la participación de postores, por lo que no se acepta lo solicitado.	
10	5.2.2.1.1.2	23	Los dos Switches de Core deberán trabajar de tal manera que operan en alta disponibilidad, en modo Activo/Activo. "Sirvase permitir trabajar la alta disponibilidad en modo activo / pasivo, teniendo en cuenta que un switch es el activo y funciona como plano de control y gestion mientras que el otro es el de reserva".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se aclara que, la solución activo-activo permite aprovechar toda la capacidad instalada de la solución, por lo cual no se acepta lo indicado.	
11	5.2.2.1.1.3	25	Debe ser non-blocking. Tener mínimo un rendimiento de 396Gbps. "Por rendimiento y tener una mayor capacidad de switching al momento de conectar Acces point con capacidad de puertos hasta 5Gbps , sirvase permitir tener un rendimiento de al menos 800Gbps y así poder discriminar equipos con menor capacidad de conmutacion".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se confirma parcialmente, se considerará la capacidad de conmutación de 650 Gbps.	Debe ser non-blocking. Tener mínimo un rendimiento de 650Gbps
12	5.2.2.1.1.3	25	Debe tener un rendimiento mínimo de 396Mpps. "Por rendimiento y tener una mayor capacidad de forwarding rate al momento de conectar Acces point con capacidad de puertos hasta 5Gbps, sirvase permitir tener un rendimiento de al menos 800Mpps y así poder discriminar equipos con menor capacidad de transmision de paquetes".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se confirma parcialmente, se considerará la capacidad de conmutación de 450 Mpps.	Debe tener un rendimiento mínimo de 450Mpps
13	5.2.2.1.1.3	25	El stacking debe tener un rendimiento no menor a 160Gbps. "Por rendimiento y capacidad de conmutacion entre los switches sirvase considerar tener un rendimiento de stacking no menor a 320 Gbps".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se confirma, se considerará un rendimiento de stacking mínimo de 320 Gbps.	El stacking debe tener un rendimiento mínimo de 320Gbps
14	5.2.2.1.1.4	28	Debe ser non-blocking. Tener mínimo un rendimiento de 440Gbps. "Por rendimiento y tener una mayor capacidad de switching al momento de conectar Acces point con capacidad de puertos hasta 5Gbps , sirvase permitir tener un rendimiento de al menos 600Gbps y así poder discriminar equipos con menor capacidad de conmutacion".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se confirma parcialmente, se considerará la capacidad de conmutación de 600 Gbps.	Debe ser non-blocking. Tener mínimo un rendimiento de 600Gbps
15	5.2.2.1.1.4	28	Debe tener un rendimiento mínimo de 330Mpps. "Para la pluralidad de marca sirvase permitir tener un rendimiento de al menos 327Mpps sin afectar o cambiar la solucion de switches"	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	No se confirma, el valor mínimo de 330 Mpps es el valor mínimo requerido con el fin de tener el rendimiento adecuado de la solución.	

16	5.2.2.1.1.4	28	El stacking debe tener un rendimiento no menor a 160Gbps. "Por rendimiento y capacidad de conmutación entre los switches sirvase considerar tener un rendimiento de stacking no menor a 320 Gbps".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.	Se confirma, se considerará un rendimiento de stacking mínimo de 320 Gbps.	El stacking debe tener un rendimiento no menor a 320Gbps
17	5.2.2.1.1.5	31	Debe ser non-blocking. Tener mínimo un rendimiento de 440Gbps. "Por rendimiento y tener una mayor capacidad de switching al momento de conectar Acces point con capacidad de puertos hasta 5Gbps, sirvase permitir tener un rendimiento de al menos 600Gbps y así poder discriminar equipos con menor capacidad de conmutación".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.	Se confirma, se requiere un rendimiento de 600 Gbps de capacidad de conmutación.	Debe ser non-blocking. Tener mínimo un rendimiento de 600Gbps
18	5.2.2.1.1.4	31	Debe tener un rendimiento mínimo de 470Mpps. "Para la pluralidad de marca sirvase permitir tener un rendimiento de al menos 327Mpps sin afectar o cambiar la solución de switches".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.	Con el fin de permitir mayor pluralidad de postes, se permitirá un rendimiento mínimo de 440 Mpps.	Debe tener un rendimiento mínimo de 440Mpps
19	5.2.2.1.1.5	31	El stacking debe tener un rendimiento no menor a 160Gbps. "Por rendimiento y capacidad de conmutación entre los switches sirvase considerar tener un rendimiento de stacking no menor a 320 Gbps".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.	Se confirma, se considerará un rendimiento de stacking mínimo de 320 Gbps.	El stacking debe tener un rendimiento no menor a 320Gbps.
20	5.2.2.1.2.1	36	Se requiere una herramienta en hardware (Appliance) en alta disponibilidad que va a tunelizar las comunicaciones inalámbricas y que permita configurar y gestionar los puntos de accesos inalámbrico de forma centralizada con soporte de por lo menos 2000 APs. Este tendrá las siguientes funcionalidades: "Para no sobre dimensionar la solución y propuesta sirvase permitir al controlador wireless soportar por lo menos 250 Aps".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.	Se aclara que se requiere la capacidad de gestión de 2000 APs para en un futuro poder gestionar centralizadamente los APs de diversas sedes.	
21	5.2.2.1.2.1	36	El equipo deberá soportar por lo menos 16000 dispositivos clientes y 4096 VLANs. "Para no sobre dimensionar la solución y propuesta sirvase permitir al controlador wireless soportar por lo menos 5000 dispositivos clientes".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.	No se confirma, sin embargo el Controller Wireless soportará por lo menos 10000 dispositivos y no menos de 4000 VLANs.	El equipo deberá soportar por lo menos 10000 dispositivos clientes y no menos de 4000 VLANs.
22	5.2.2.1.2.1	36	Deberá manejar un rendimiento no menor a 18Gbps "Para no sobre dimensionar la solución y propuesta sirvase permitir al controlador wireless soportar por lo menos 5 Gbps".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.	No se confirma lo indicado, ya que el rendimiento en bps es uno de los valores más importantes de rendimiento de una solución inalámbrica.	
23	5.2.1	13	El licenciamiento de toda la solución de Networking debe ser a nombre de CORPAC y a perpetuidad; deberá contemplarse la garantía de	Consulta de la empresa	No se confirma lo indicado, con el fin de proteger la	La solución contempla el despliegue, implementación y configuración de la

			<p>fabricante durante 3 años contados a partir de la finalización de la implementación y a la entrega de los servicios operativos.</p> <p>"Sirvase aclarar para el licenciamiento de toda la solución networking sea por suscripción por el tiempo del proyecto 3 años".</p>	<p>PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.</p>	<p>inversión de la Entidad, el licenciamiento debe ser de tipo perpetuo.</p> <p>Asimismo, para clarificar las características y condiciones de la contratación referente al licenciamiento, la arquitectura del SDN deberá contar con el máximo nivel de licenciamiento para contar con las mejores capacidades de automatización, control y analítica.</p>	<p>red inalámbrica y la red local cableada en una arquitectura de Software Defined Network con el máximo nivel de licenciamiento que ofrezca el fabricante, para contar con las mejores capacidades de automatización, control y analítica.</p>
24	5.2.2.1.3	39	<p>La solución de automatización, administración y gestión de la infraestructura campus con todos sus componentes de hardware y software serán implementados en alta disponibilidad en un entorno ON PREMISE utilizando appliances de propósito específico, la cual debe ser del mismo fabricante de los Switches de Core, Distribución, Acceso y de la solución de WLAN, con motivo de asegurar su correcta integración, utilizando licenciamiento del tipo perpetuo. La solución debe ser catalogada por el fabricante como un controlador para redes SDN o El software de consola de gestión deberá ser desarrollado por el mismo fabricante de los Switches de Core ofertados. Asimismo, se deberá incluir el sistema operativo, su licenciamiento y todo el hardware (rackeable) necesario para su puesta en operación. Podrá ser instalado en entorno virtual, el proveedor se encargará de colocar el hardware necesario y las licencias del software correspondiente (tal como hypervisor o equivalente) si la oferta es en entorno virtual.</p> <p>"Sirvase aclarar para el licenciamiento de toda la solución networking sea por suscripción por el tiempo del proyecto 3 años".</p>	<p>Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACIÓN Y SEGURIDAD S.A.C.</p>	<p>No se confirma lo indicado, con el fin de proteger la inversión de la Entidad, el licenciamiento debe ser de tipo perpetuo.</p> <p>Asimismo, para clarificar las características y condiciones de la contratación referente al licenciamiento, la arquitectura del SDN deberá contar con el máximo nivel de licenciamiento para contar con las mejores capacidades de automatización, control y analítica.</p>	<p>La solución contempla el despliegue, implementación y configuración de la red inalámbrica y la red local cableada en una arquitectura de Software Defined Network con el máximo nivel de licenciamiento que ofrezca el fabricante, para contar con las mejores capacidades de automatización, control y analítica.</p>
25	8	95	<p>Se requiere para el Líder de Networking LAN que acredite como mínimo cinco (5) años de experiencia como arquitecto y/o líder técnico en plataformas de networking LAN y WLAN.</p> <p>Sirvase confirmar si con la finalidad de poder tener una mayor participación de postores se podrá acreditar como mínimo tres (3) años de experiencia como arquitecto y/o líder técnico y/o especialista en plataformas de networking LAN y WLAN.</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>	<p>No se confirma, dado que principalmente se requiere expertiz por el nivel de proyecto a implementar la experiencia en años es la requerida.</p>	
26	8	95	<p>Se requiere para el Líder de Networking LAN que acredite contar con certificaciones técnicas oficiales vigentes de nivel experto o avanzado en Enterprise o Datacom o Switching o Wireless de al menos dos (02) fabricantes reconocidos (incluyendo al fabricante de los equipos de networking propuestos).</p> <p>Se observa que este requerimiento vulnera el principio de libre</p>		<p>Dado que basado en lo acontecido en el servicio que actualmente se cuenta en CORPAC con relación a la RED LAN, se ha visto por necesario contar con el personal clave líder de</p>	

			<p>conurrencia al exigir requisitos desproporcionados y que limitan la pluralidad de postores, además de no configurar ventaja alguna para la Entidad el requerir las certificaciones técnicas oficiales vigentes en al menos dos (2) fabricantes reconocidos.</p> <p>Solicitamos para este profesional sea requerido el contar con la certificación técnica vigente de nivel experto o avanzado en Enterprise o Datacom o Switching o Wireless del fabricante de los equipos propuestos.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	networking y que cuenta con el expertiz requerido para la correcta transición desde una plataforma que viene operando en el Aeropuerto y que realice la migración en paralelo a los nuevos equipos propuestos.	
27	8	95	<p>Se requiere para el Implementador de Networking LAN que acredite certificación técnica oficial vigente de nivel profesional en Enterprise o Switching o Datacom del fabricante propuesto.</p> <p>Sírvase confirmar que la acreditación de la certificación técnica oficial vigente de nivel profesional en Enterprise o Switching o Datacom requerida podrá ser de cualquier fabricante.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma, el personal Implementador de Networking LAN debe contar con la acreditación respectiva del fabricante de los equipos propuestos	
28	8	96	<p>Se requiere para el Implementador de Networking WLAN que acredite certificación técnica oficial vigente de nivel profesional en Wireless del fabricante propuesto.</p> <p>Sírvase confirmar que la acreditación de la certificación técnica oficial vigente de nivel profesional en Wireless requerida podrá ser de cualquier fabricante.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma, el personal Implementador de Networking WLAN debe contar con la acreditación respectiva del fabricante de los equipos propuestos.	
29	8	95	<p>Se requiere para el Especialista en Cableado Estructurado Certificado oficial o carta de fabricante de la solución de cableado estructurado de la plataforma a operar.</p> <p>Sírvase confirmar que la acreditación requerida podrá ser de cualquier fabricante de cableado estructurado</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma, dado que es una solución administrable se requiere especialista del cableado estructurado a operar; por ende, el certificado oficial o carta de fabricante de la plataforma a operar.	
30	8	96	<p>Se requiere para el Residente 1 Presencial como mínimo certificación en materia de switching y routing por parte del fabricante de los equipos de la solución; a nivel asociado, técnico, especialista o ingeniero de red (según la denominación propia del fabricante y demostrable según documentación del fabricante) y que se encuentre vigente durante toda la ejecución del servicio complementario.)</p> <p>Sírvase confirmar que se aceptarán certificaciones en materia de switching y routing por parte de cualquier fabricante; a nivel asociado, técnico, especialista o ingeniero de red y que se encuentre vigente durante toda la ejecución del servicio complementario.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma, el personal Profesional Residente 1 Presencial, debe contar con la acreditación respectiva del fabricante de los equipos propuestos	
31	8	97	<p>Se requiere para el Residente 2 Presencial como mínimo Certificación y/o acreditación respectiva del sistema de cableado a operar vigente durante toda la ejecución del servicio complementario.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma, dado que es una solución administrable se requiere que el personal	

			Sírvase confirmar que se aceptarán Certificación y/o acreditación de cualquier sistema de cableado.		Residente 2 Presencial cuente con la certificación y/o acreditación del sistema del cableado estructurado a operar.	
32	5.2.1	13	<p>Con respecto al SISTEMA DE NETWORKING (INFRAESTRUCTURA ACTIVA), se menciona lo siguiente:</p> <p>"Todos los transceivers a proveer como parte de la solución deberán poseer conectores tipo LC, el postor deberá considerar y garantizar en su propuesta que permita interoperabilidad de los transceivers de la solución propuesta siendo estos propietarios o de terceros compatibles con la solución."</p> <p>Con la finalidad de asegurar la interoperabilidad de los transceivers de la solución propuesta, sírvase confirmar que los transceivers deberán ser del mismo fabricante (propietarios) de la solución a ofertar, descartándose de esta manera la provisión de transceivers compatibles o de terceros que podrían causar incompatibilidades e incluso pérdida de garantía de los equipos que conformarán el SISTEMA DE NETWORKING (INFRAESTRUCTURA ACTIVA).</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Tomando en consideración la experiencia que se ha tenido con diferentes plataformas de equipamiento LAN, los postores deben considerar en sus propuestas que los transceivers a implementar sean los más idóneos (ejemplo propietarios), y estén operando mientras exista la ejecución contractual; no limitando la opción de soluciones de interoperabilidad para efectos futuros de la ejecución contractual en donde el mercado ofrezca componentes compatibles para su operación en cuanto a la operatividad de enlaces de comunicaciones LAN.	
33	7	93	<p>Con respecto al Plazo de Entrega, se menciona lo siguiente:</p> <p>"El plazo para la Entrega de componentes del sistema de Networking (Infraestructura activa) y renovación de garantías de la infraestructura pasiva y activa de la Sede Central de CORPAC S.A. será máximo de sesenta (60) días calendarios, se contabilizará desde el día siguiente de la firma del contrato.</p> <p>Considerando que, los tiempos de entrega por parte del fabricante de los equipos que conforman el sistema de Networking (Infraestructura Activa), oscilan entre 90 a 120 días calendario, vemos que 60 días calendario no es suficiente tiempo para entregar los mismos, por lo que se solicita extender el tiempo de entrega de los componentes del Sistema de Networking a 90 días calendario.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Los plazos establecidos van acorde a la necesidad de la Entidad. En ese sentido, el plazo establecido es el requerido para la entrega de los componentes del sistema de networking (infraestructura activa) y el de renovación de las garantías de la Infraestructura pasiva.	
34	7	94	<p>Con respecto al Plazo de Implementación – ETAPA 1, se menciona lo siguiente:</p> <p>"El plazo para la implementación de la presente contratación del Sistema de Networking (Infraestructura Activa), será de ciento cincuenta (50) días calendarios a partir del día siguiente de la fecha máxima del plazo de entrega de equipos. Este plazo incluye el suministro,</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Efectivamente existe un error material, la Etapa 1 tiene un plazo de cincuenta días (50) calendarios.	El plazo para la implementación de la presente contratación del Sistema de Networking (Infraestructura Activa), será de cincuenta (50) días calendarios a partir del día siguiente de la fecha

			<p>instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), hasta que la solución funcione correctamente."</p> <p>Respecto al plazo se indica en letras ciento cincuenta y en números (50), sírvase confirmar que lo correcto es, ciento cincuenta (150) días calendarios, en letras y número respectivamente.</p>			<p>máxima del plazo de entrega de equipos. Este plazo incluye el suministro, instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), hasta que la solución funcione correctamente.</p>
35	7	94	<p>Con respecto al Plazo de Implementación – ETAPA 1, se menciona lo siguiente: "El plazo para la implementación de la presente contratación del Sistema de Networking (Infraestructura Activa), será de ciento cincuenta (50) días calendarios a partir del día siguiente de la fecha máxima del plazo de entrega de equipos. Este plazo incluye el suministro, instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), hasta que la solución funcione correctamente."</p> <p>Teniendo en cuenta que el plazo inicia desde la fecha máxima del plazo de entrega de equipos, sírvase confirmar que el texto referente a lo que incluye dicho plazo, quedaría de la siguiente forma: "Este plazo incluye la instalación y configuración y todo lo relacionado al sistema de Networking (infraestructura Activa), hasta que la solución funcione correctamente"</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>	<p>Se reformula para mejor entendimiento.</p> <p>Este plazo incluye la instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), - de todo lo suministrado y/o entregado durante el plazo de Entrega-, hasta que la solución funcione correctamente</p>	<p>Este plazo incluye la instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), - de todo lo suministrado y/o entregado durante el plazo de Entrega-, hasta que la solución funcione correctamente</p>
36	7	93	<p>Con respecto a los Plazos de la Prestación Principal se menciona lo siguiente: "El plazo total de la prestación principal es de 150 días calendarios, se contabiliza al día siguiente de la firma del contrato. Este plazo contempla la entrega e implementación y puesta en marcha."</p> <p>Teniendo en cuenta la secuencia y las etapas que componen la Prestación Principal (como son: Plazo de Entrega, Plazo de Implementación y sus respectivas Etapas), sírvase aclarar que el plazo total de la Prestación Principal es de 280 días calendarios, considerando un Plazo de Entrega de los componentes del Sistema de Networking de 90 días calendarios.</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>	<p>Los plazos establecidos van acorde a la necesidad de la Entidad. En ese sentido, el plazo y etapas establecidas son las requeridas para la entrega, implementación y puesta en marcha.</p>	
37	8	95	<p>Con respecto al Perfil del Personal Clave – Líder de Networking LAN, se menciona lo siguiente: "Un (01) Ingeniero Electrónico o Sistemas o Telecomunicaciones, Titulado, Colegiado y habilitado, que acrediten como mínimo cinco (05) años de experiencia como arquitecto y/o líder técnico en plataformas de Networking LAN y WLAN."</p> <p>Teniendo en cuenta que, en las constancias de trabajo del personal, las funciones del Arquitecto y/o Líder de Networking, por lo general se describen como Arquitecto y/o Líder de Técnico en Networking o</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>	<p>Se acoge parcialmente la consulta para el líder de networking; dado que principalmente se requiere expertiz por el nivel de proyecto a implementar la experiencia en años es la requerida. Con relación a la denominación en la</p>	<p>Un (01) Ingeniero Electrónico o Sistemas o Telecomunicaciones, Titulado, Colegiado y habilitado, que acrediten como mínimo cinco (05) años de experiencia como arquitecto y/o líder técnico y/o Responsable y/o Especialista y/o Ingeniero en Networking o en</p>

			Plataformas de Networking (lo cual ya incluye LAN y WLAN), por favor, sírvase confirmar que el requerimiento del perfil podrá quedar de la siguiente manera: "Un (01) Ingeniero Electrónico o Sistemas o Telecomunicaciones, Titulado, Colegiado y habilitado, que acrediten como mínimo cinco (05) años de experiencia como arquitecto y/o líder técnico en Networking o Plataformas de Networking."		experiencia en plataforma de Networking LAN y WLAN se realiza la actualización, consolidando consultas similares.	Plataformas de Networking LAN y WLAN.
38	8	95	Con respecto al Perfil del Personal Clave – Líder de Networking LAN, se menciona lo siguiente: "Constancias de experiencia mínima de cinco (05) años de experiencia como arquitecto y/o líder técnico en networking LAN y WLAN." Teniendo en cuenta que, en las constancias de trabajo del personal, las funciones del Arquitecto y/o Líder de Networking, por lo general se describen como Arquitecto y/o Líder de Técnico en Networking o Plataformas de Networking (lo cual ya incluye LAN y WLAN), por favor, sírvase confirmar que el requerimiento de la experiencia podrá quedar de la siguiente manera: "Constancias de experiencia mínima de cinco (05) años de experiencia como arquitecto y/o líder técnico en Networking o Plataformas de Networking"	Consulta de la empresa ITALTEL PERU S.A.C..	Se acoge parcialmente la consulta para el líder de Networking LAN, consolidando consultas similares.	Constancias de experiencia mínima de cinco (05) años de experiencia como arquitecto y/o líder técnico y/o Responsable y/o Especialista y/o Ingeniero en Networking o en Plataformas de Networking LAN y WLAN.
39	8	95	Con respecto al Perfil del Personal Clave – Líder de Networking LAN, se menciona lo siguiente: "El líder de networking implementador propuesto por el postor debe contar con certificaciones técnicas oficiales vigentes de nivel experto o avanzado en Enterprise o Datacom o Switching o Wireless de al menos dos (02) fabricantes reconocidos (incluyendo al fabricante de los equipos de networking propuestos)." Sírvase confirmar que se aceptarán certificaciones técnicas oficiales vigentes de nivel experto o avanzado en Enterprise o Datacom o Switching o Wireless del fabricante de los equipos de networking ofertados.	Consulta de la empresa ITALTEL PERU S.A.C..	Se precisa, dado que basado en lo acontecido en el servicio que actualmente se cuenta en CORPAC con relación a la RED LAN, se ha visto por necesario contar con el personal clave líder de networking y que cuenta con el expertiz requerido para la correcta transición desde una plataforma que viene operando en el Aeropuerto y que realice la migración en paralelo a los nuevos equipos propuestos.	
40	8	96	Con Respecto al Perfil del Personal Clave – Implementador de Networking LAN, se menciona lo siguiente: "Un (01) Bachiller o Ingeniero o técnico titulado Electrónico o Sistemas o Telecomunicaciones o redes y comunicaciones, como mínimo con tres (03) años de experiencia realizando tareas de implementación soporte y/o mantenimiento de networking LAN usando la tecnología SDN o fabric	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma lo indicado, dado que se requiere que el personal clave cuente con experiencia específicamente en Networking LAN usando la tecnología SDN o fabric, que no es comparable a la experiencia en redes usando las tecnologías tradicionales.	

			<p>Teniendo en cuenta que, en las constancias de trabajo del personal, las funciones de los Ingenieros y/o Técnicos, por lo general se describen como servicios de implementación, soporte y/o mantenimientos de redes LAN de forma general y no precisamente usando la Tecnología SDN o Fabric, lo cual no implica que el personal no este calificado para realizarlas, por favor, sírvase confirmar que el requerimiento del perfil podrá quedar de la siguiente manera:</p> <p>"Un (01) Bachiller o Ingeniero o técnico titulado Electrónico o Sistemas o Telecomunicaciones o redes y comunicaciones, como mínimo con tres (03) años de experiencia realizando tareas de implementación soporte y/o mantenimiento de networking LAN"</p>			
41	8	96	<p>Con Respecto al Perfil del Personal Clave – Implementador de Networking LAN, se menciona lo siguiente:</p> <p>"Constancias de experiencia mínima de tres (03) años realizando tareas de implementación y/o soporte y/o mantenimiento de networking LAN usando la tecnología SDN o fabric."</p> <p>Teniendo en cuenta que, en las constancias de trabajo del personal, las funciones de los Ingenieros y/o Técnicos, por lo general se describen como servicios de implementación, soporte y/o mantenimientos de redes LAN de forma general y no precisamente usando la Tecnología SDN o Fabric, lo cual no implica que el personal no este calificado para realizarlas, por favor, sírvase confirmar que el requerimiento del perfil podrá quedar de la siguiente manera:</p> <p>"Constancias de experiencia mínima de tres (03) años realizando tareas de implementación y/o soporte y/o mantenimiento de networking LAN."</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>	<p>No se confirma lo indicado, dado que se requiere que el personal clave cuente con experiencia específicamente en Networking LAN usando la tecnología SDN o fabric, que no es comparable a la experiencia en redes usando las tecnologías tradicionales.</p>	
42	8	96	<p>Con Respecto al Perfil del Personal Clave – Implementador de Networking WLAN, se menciona lo siguiente:</p> <p>"Un (01) Bachiller o Ingeniero o técnico titulado Electrónico o Sistemas o Telecomunicaciones o redes y comunicaciones, como mínimo con tres (03) años de experiencia realizando tareas de implementación soporte y/o mantenimiento de networking WLAN usando la tecnología SDN o fabric"</p> <p>Teniendo en cuenta que, en las constancias de trabajo del personal, las funciones de los Ingenieros y/o Técnicos, por lo general se describen como servicios de implementación, soporte y/o mantenimientos de redes WLAN o Redes Inalámbricas o Redes WiFi de forma general y no precisamente usando la Tecnología SDN o Fabric, lo cual no implica que el personal no este calificado para realizarlas, por favor, sírvase confirmar que el requerimiento del perfil podrá quedar de la siguiente manera:</p> <p>"Un (01) Bachiller o Ingeniero o técnico titulado Electrónico o Sistemas o Telecomunicaciones o redes y comunicaciones, como mínimo con tres (03) años de experiencia realizando tareas de implementación soporte</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>	<p>No se confirma lo indicado, dado que se requiere que el personal clave cuente con experiencia específicamente en Networking WLAN usando la tecnología SDN o fabric, que no es comparable a la experiencia en redes usando las tecnologías tradicionales.</p>	

			y/o mantenimiento de networking WLAN o Redes Inalámbricas o Redes WiFi"			
43	8	96	<p>Con Respecto al Perfil del Personal Clave – Implementador de Networking WLAN, se menciona lo siguiente: "Constancias de experiencia mínima de tres (03) años realizando tareas de implementación y/o soporte y/o mantenimiento de networking WLAN usando la tecnología SDN o fabric.."</p> <p>Teniendo en cuenta que, en las constancias de trabajo del personal, las funciones de los Ingenieros y/o Técnicos, por lo general se describen como servicios de implementación, soporte y/o mantenimientos de redes WLAN o Redes Inalámbricas o Redes WiFi de forma general y no precisamente usando la Tecnología SDN o Fabric, lo cual no implica que el personal no este calificado para realizarlas, por favor, sírvase confirmar que el requerimiento del perfil podrá quedar de la siguiente manera: "Constancias de experiencia mínima de tres (03) años realizando tareas de implementación y/o soporte y/o mantenimiento de networking WLAN o Redes Inalámbricas, o Redes WiFi."</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma lo indicado, dado que se requiere que el personal clave cuente con experiencia específicamente en Networking WLAN usando la tecnología SDN o fabric, que no es comparable a la experiencia en redes usando las tecnologías tradicionales.	
44	9.1.4	99	<p>Con respecto a la TRANSFERENCIA TECNOLÓGICA, se menciona lo siguiente: "Entrenamiento de 40 horas como mínimo para cuatro 2 personas en el uso de los equipos de redes LAN/WAN que corresponda a los niveles intermedio y avanzado del equipamiento propuesto y relacionado a las implementaciones realizadas para la operación del sistema dentro de CORPAC S.A."</p> <p>Por favor sírvase aclarar si el entrenamiento indicado de 40 horas como mínimo, es para cuatro (04) o para dos (02) personas.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Se precisa que son 4 personas.	Entrenamiento de 40 horas como mínimo para cuatro (04) personas en el uso de los equipos de redes LAN/WAN que corresponda a los niveles intermedio y avanzado del equipamiento propuesto y relacionado a las implementaciones realizadas para la operación del sistema dentro de CORPAC S.A.
45	3.1.3	126	<p>Se indica: "El servicio de operación de redes y comunicaciones TI para CORPAC S.A. deberá configurar un Call Center con suficientes líneas de acceso telefónico integradas al Sistema de Mesa de Servicio para la revisión de la calidad y elaboración de reportes e informes de gestión"</p> <p>Confirma que el CALL CENTER es propiedad de Corpac, y que se requiere configurar con nuestra plataforma de Gestión de ticket</p>	Consulta de la empresa ITALTEL PERU S.A.C..	<p>El Call Center, se refiere al Centro de llamadas que se realizara al personal rotativo a los Residentes de Turno, el cual debe ser un solo número y que registrarán y atenderán los tickets de atención generados por cada servicio, sistema de Networking (Infraestructura Activa) y del Sistema de Infraestructura Pasiva.</p> <p>CORPAC por otro lado asignara un teléfono IP interno para coordinaciones.</p>	

46	6	96	Se indica: "PROFESIONAL RESIDENTE 1 PRESENCIAL (un personal por cada TURNO DE 8 HORAS total 3" Considerando la regulación peruana, se debe considerar un recurso como "descansero", por lo que se debe considerar como 4 personas para cubrir adecuadamente esta posición. Sírvasse confirmar que se deberán de considerar 04 personas en total.	Consulta de la empresa ITALTEL PERU S.A.C..	Se confirma.	PROFESIONAL RESIDENTE 1 PRESENCIAL (un personal por cada Turno de 8 horas y 1 descansero – Total 4)
47	5.3.1.4	80	Se indica: Rango de frecuencia: 40 – 70 Hz Consulta: Favor confirmar que para potencias medias de 6KVA y 10KVA, se aceptarán rangos de +/- 4Hz; es decir, en el rango de 46Hz - 64Hz	Consulta de la empresa ITALTEL PERU S.A.C..	Los rangos solicitados están dentro del rango de frecuencias de requerimiento.	
48	5.3.1.4	81	Se indica: Toma de entrada: 4 x IEC C13 + 4 x IEC C19 + cableado fijo en caja de distribución de energía. Consulta: Favor confirmar que se aceptará para las tomas IEC 19 de los UPS puedan tener mínimo 1 salida C19, ya que en su mayoría los equipos de TI se conectan a las tomas C13.	Consulta de la empresa ITALTEL PERU S.A.C..	Se precisa que, en el requerimiento indica: 4 x IEC C13 + 2 x IEC C19 + cableado fijo en caja de distribución de energía.	
49	5.3.1.4	81	Se indica: Tiempo de recarga: 3 horas al 90% de capacidad después de descarga completa al 100% de carga. Consulta: Favor confirmar que para potencias medias de 6 KVA y 10 KVA se aceptará que el tiempo de recarga tenga un rango de 7 a 9 horas al 90%.	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma.	
50	5.3.1.4	81	Se indica: Ruido audible: <55 dB, a 1 metro de la parte posterior <50 dBA, a 1 metro de la parte frontal o de los laterales. Consulta: Favor confirmar que para potencias medias de 6 KVA y 10 KVA se aceptará ruido audible a 1 metro <58 dB	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma.	
51	5.3.1.4	79	Se indica: Si bien los cuartos de comunicación tendrán los gabinetes con aire acondicionado del tipo autocontenido según la capacidad de cada uno de estos, sin embargo, la entidad está solicitando adicionalmente instalar equipos de refrigeración del tipo confort mínimo de 12000BTU, como sistema redundante en dichos ambientes. Consulta: Dado que el equipo de confort no es un aire de precisión por lo cual no tiene la funcionalidad para climatizar a equipos de TI este no puede	Consulta de la empresa ITALTEL PERU S.A.C..	Se precisa que, el equipo solicitado es la contingencia ante la falta del sistema principal de refrigeración, y la cual es configurada utilizando el sistema de monitorización como el DETAC III, activándose	

			conectarse al aire de precisión y trabajar en redundancia. Favor confirmar, que solo se suministrará el aire de confort y no trabajará en redundancia con el equipo de precisión por lo expuesto anteriormente.		cuando no existe Aire Acondicionado de Precisión.	
52	5.3.1.10	83	Se dice: Adicionalmente al objeto de la contratación de equipamiento, CORPAC S.A. requiere renovar la garantía y el soporte de algunos componentes de la infraestructura pasiva implementada que tenga la garantía vigente del fabricante, a manera referencial se muestra el listado de todos los componentes implementados en los diversos nodos de telecomunicaciones en el Aeropuerto Sede Central: Consulta: Favor confirmar que la renovación de garantía y soporte de algunos componentes de la infraestructura también aplica para los equipos activos mientras la garantía de fabricante se encuentre vigente lo que aplica también para los equipos de la marca RITTAL y SIEMON.	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma, el requerimiento indica que componentes deben contar con Garantía y soporte; y cuales solo con soporte. Por otro lado, el proveedor debe considerar lo necesario para contar con la renovación respectiva de los componentes descritos.	
53	5.3.1.10	87	Se dice: DETAC (RENOVACION DE SOPORTE) Consulta: De acuerdo con lo indicado por el fabricante RITTAL, los sistemas DETAC tienen un tiempo de vida útil de 10 años por lo que no calificarían para tener garantía de fábrica. Favor confirmar que el postor deberá de considerar equipos DETAC's nuevos.	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma, el proveedor debe considerar lo necesario para contar con la renovación de la garantía y/o soporte. Por otro lado, los componentes DETAC fueron implementados en Agosto del año 2017.	
54	5.3.1.8	82	Se dice: VISITA DE CAMPO El postor podrá realizar visitas de campo a las diferentes instalaciones de CORPAC S.A. para cotizar todo lo necesario para la correcta implementación del servicio solicitado. Las visitas podrán coordinarse mediante carta o correo electrónico con mínimo 2 días de anticipación, alcanzando copia del Documento Oficial del Identidad del personal que efectuara la visita. Consulta: Para confirmar qué equipos tienen la garantía vigente. Favor confirmar que el fabricante o postor deberá de hacer el levantamiento de información del estatus actual de la base instalada (servicio de inspección), de encontrarse observaciones en el funcionamiento de los equipos, alarmas, piezas dañadas, se deberá de hacer el respectivo correctivo para que la garantía tenga validez.	Consulta de la empresa ITALTEL PERU S.A.C..	Se precisa que, el proveedor debe considerar lo necesario para contar con la renovación de la garantía y/o soporte, según corresponda. Para ello podrá realizar visitas de campo para tal fin.	
55	5.2.2.1.1.1	14	Se menciona: El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean como un único switch desde una perspectiva lógica, manteniendo un único plano de control y gestión, mientras que el plano de datos o transmisión será de tipo distribuido y que garantice la alta disponibilidad en capa 2 y capa 3		No se confirma. Sin embargo, con el fin de permitir mayor pluralidad de postores también se aceptará para la tecnología	El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean como un único switch desde

			<p>Consulta:</p> <p>Con el objetivo de una mayor pluralidad de fabricantes, empleando el uso de protocolos estándares de la industria, sírvase a confirmar que se puede cumplir la especificación solicitada mediante el uso de enlaces LACP, garantizando HA en capa 2 y capa 3. Considerando finalmente la siguiente especificación:</p> <p>El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean cómo un único switch desde una perspectiva lógica para lograr agregar enlaces con LACP y garantizar HA en capa 2 y capa 3</p>	Consulta de la empresa ITALTEL PERU S.A.C..	de virtualización que el plano de control y gestión también sean distribuidos.	una perspectiva lógica, manteniendo un único plano de control y gestión, mientras que el plano de datos o transmisión será de tipo distribuido y que garantice la alta disponibilidad en capa 2 y capa 3. También se aceptará para la tecnología de virtualización que el plano de control y gestión también sean distribuidos.
56	5.2.2.1.1.1	16	<p>Se menciona:</p> <p>Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.</p> <p>Consulta:</p> <p>Con el objetivo de una mayor pluralidad de fabricantes, sírvase a confirmar que se podrá cumplir la especificación a través de funcionalidades como Control Plane Policing (CoPP) o similares.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	<p>Se confirma.</p> <p>Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.</p>	Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.
57	5.2.2.1.1.1	18	<p>Se menciona:</p> <p>IEEE 802.1x suplicant.</p> <p>Consulta:</p> <p>Debido a que esta funcionalidad es principalmente utilizada en la capa de acceso, y con el objetivo de brindar una mayor pluralidad de fabricantes, sírvase a confirmar que lo solicitado será considerado como opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Se acoge la consulta.	Opcionalmente, IEEE 802.1x suplicant
58	5.2.2.1.1.2	20	<p>Se menciona:</p> <p>El switch deberá contar con CPU mínimo de 2.2 Ghz</p> <p>Consulta:</p> <p>Debido a que la principal funcionalidad del switch involucra el uso de altos niveles de Throughput y Switching capacity, teniendo el CPU un rol menos determinante en el performance del equipo, ya que esto dependerá de la arquitectura de cada fabricante, sírvase a confirmar que el switch deberá contar con CPU mínimo de 1.8 GHz</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Tomando en consideración que para el Switch de Tipo II el factor determinante es la capacidad de conmutación, se aceptara CPU mínimo de 1.4 Ghz, siempre y cuando no impacte en el rendimiento de los equipos	El switch deberá contar con CPU mínimo de 1.4 Ghz siempre y cuando no impacte en el rendimiento de los equipos
59	5.2.2.1.1.2	20	<p>Se menciona:</p> <p>El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean cómo un único switch desde una perspectiva lógica, manteniendo un único plano de control y gestión,</p>		No se confirma. Sin embargo, con el fin de permitir mayor pluralidad de postores también se aceptará para la tecnología	El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean cómo un único switch desde

			<p>mientras que el plano de datos será de tipo distribuido y garantice la alta disponibilidad en capa 2 y capa 3.</p> <p>Consulta: Con el objetivo de una mayor pluralidad de fabricantes, empleando el uso de protocolos estándares de la industria, sírvase a confirmar que se puede cumplir la especificación solicitada mediante el uso de enlaces LACP, garantizando HA en capa 2 y capa 3. Considerando finalmente la siguiente especificación:</p> <p>El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean como un único switch desde una perspectiva lógica para lograr agregar enlaces con LACP y garantizar HA en capa 2 y capa 3</p>	Consulta de la empresa ITALTEL PERU S.A.C..	de virtualización que el plano de control y gestión también sean distribuidos.	una perspectiva lógica, manteniendo un único plano de control y gestión, mientras que el plano de datos o transmisión será de tipo distribuido y que garantice la alta disponibilidad en capa 2 y capa 3. También se aceptará para la tecnología de virtualización que el plano de control y gestión también sean distribuidos.
60	5.2.2.1.1.2	20	<p>Se menciona: Debe tener 32 puertos de red 40/100G (QSFP/QSFP28) como mínimo</p> <p>Consulta: Debido a que en las bases se requieren la interconexión de un máximo de 18 nodos lo cual requiere 18 puertos, con la finalidad de permitir una mayor pluralidad de fabricantes, y con el objetivo de evitar sobredimensionar la solución, sírvase confirmar que será válido ofertar soluciones que cuenten con 20 puertos, tal que se cubra con el mínimo necesario para la interconexión de nodos</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Es un requerimiento de la Entidad contar con un equipo de 32 puertos para crecimiento futuro. Se precisa que actualmente se tiene en porcentaje de ocupación y utilización del 59% de puertos sin implementar nuevos nodos; y sin porcentaje de crecimiento.	
61	5.2.2.1.1.2	20	<p>Se menciona: Debe tener 32 puertos de red 40/100G (QSFP/QSFP28) como mínimo</p> <p>Consulta: Sírvase a confirmar que también serán válidas proponer soluciones que cuenten con puertos a velocidades de 50G</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
62	5.2.2.1.1.2	20	<p>Se menciona: Debe permitir no menos de 4096 VLAN IDs y soportar e implementar protocolo 802.1q</p> <p>Consulta:</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Se confirma que para equipo de Tipo II se aceptaran rango no menos de 4000	Debe permitir no menos de 4000 VLAN IDs y soportar e implementar protocolo 802.1q.

			Para una mayor pluralidad de fabricantes, se solicita confirmar que la cantidad de VLAN IDs permitidas sea no menor a 4000.			
63	5.2.2.1.1.2	21	Se menciona: RADIUS, TACACS, TACACS+ o equivalentes, ACL IPv4, ACL IPv6, BDPU Guard, BDPU Filter, Root Guard o equivalente, Private VLAN o similares, DHCP Snooping, MLD Snooping. Consulta: Debido a que TACACS y TACACS+ (asociado al siguiente RFC 8907) tienen funcionalidades integrables con distintos fabricantes, ambos siendo estándares de la industria, sírvase a confirmar que no se podrá cumplir esta especificación con protocolos equivalentes o propietarios.	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Con el fin de permitir mayor pluralidad de postores se ha solicitado lo indicado en el presente requerimiento.	
64	5.2.2.1.1.2	21	Se menciona: Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión. Consulta: Con el objetivo de una mayor pluralidad de fabricantes, sírvase a confirmar que se podrá cumplir la especificación a través de funcionalidades como Control Plane Policing (CoPP) o similares.	Consulta de la empresa ITALTEL PERU S.A.C..	Se confirma. Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.	Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.
65	5.2.2.1.1.2	23	Se menciona: Deberá contar con mecanismo y/o función de seguridad que utilice una combinación de autenticación, criptografía y verificación de estado para asegurar que los dispositivos de la red puedan confiar en los mensajes de descubrimiento de vecinos IPv6 que se intercambian en la capa 2. Consulta: Debido a que esta especificación está orientada exclusivamente a un solo fabricante, sírvase a confirmar que lo solicitado será considerado como opcional	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. El aseguramiento del vecino en IPv6 es una funcionalidad estándar de la industria.	
66	5.2.2.1.1.3	25	Se menciona: El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal. Consulta: Debido a que esta especificación está orientada a un solo fabricante, sírvase a confirmar que lo solicitado será considerado como opcional	Consulta de la empresa ITALTEL PERU S.A.C..	Se reformula requerimiento de la siguiente manera: El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.	El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.
67	5.2.2.1.1.3	25	Se menciona: El switch propuesto debe contar con al menos 48 puertos 10/100/1000 Base-T RJ45 con soporte PoE/PoE+, en todos sus puertos.		De la revisión en la sección 5.2.2.1.1.3 se solicita equipamiento del TIPO III.	El switch propuesto debe contar con al menos 48 puertos 10/100/1000 Base-T RJ45 con

			<p>Consulta: Debido a que la velocidad de funcionamiento de los dispositivos finales tienden a aumentar con el paso de los años, y en pro de mantener una arquitectura de red acorde a las nuevas tendencias y estándares de la industria, sírvase a confirmar que el switch propuesto deba contar como mínimo con 48 puertos 100M//1G/2.5G/5G, Base-T RJ45 con soporte PoE/PoE+ en todos sus puertos</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>	<p>Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento.</p> <p>Por otro lado, de la revisión, de esta característica para que tenga congruencia el requerimiento se actualiza el soporte de PoE/PoE+/PoE++, dado que los puertos solicitados debe cumplir con el soporte de 60W de potencia; por lo que se actualiza el requerimiento, en ese extremo</p>	<p>soporte PoE/PoE+/PoE++, en todos sus puertos.</p>
68	5.2.2.1.1.3	25	<p>Se menciona: El switch propuesto debe contar con al menos 2 puertos 40GE de uplink.</p> <p>Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, se solicita confirmar que se podrán proponer soluciones con puertos de uplink a 50GE.</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>	<p>Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.</p>	
69	5.2.2.1.1.3	25	<p>Se menciona: Debe incluir 2 transceivers de 40Gbps (SFP28) para fibra óptica monomodo 10Km</p> <p>Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, sírvase a confirmar que se podrán proponer soluciones con puertos de 50Gbps(SFP28) para fibra óptica monomodo 10Km</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>	<p>Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de</p>	

					todos los componentes para tal fin.	
70	5.2.2.1.1.3	25	<p>Se menciona: El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking.</p> <p>Consulta: Con el objetivo de tener una mayor pluralidad de fabricantes, sírvase en confirmar que se podrá realizar el stacking de los switches por medio de puertos de uplink adicionales, con ello se ahorra costos en agregar módulos dedicados para los puertos de stacking del equipo</p>	Consulta de la empresa ITALTEL PERU S.A.C..	<p>Con la finalidad de ampliar la participación de postores, se reformula el requerimiento:</p> <p>El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking o puertos de uplinks/servicios adicionales para stacking.</p>	El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos de uplinks/servicios adicionales para stacking.
71	5.2.2.1.1.3	26	<p>Se menciona: Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión.</p> <p>Consulta: Con el objetivo de una mayor pluralidad de fabricantes, sírvase a confirmar que se podrá cumplir la especificación a través de funcionalidades como Control Plane Policing (CoPP) o similares.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	<p>Se confirma.</p> <p>Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.</p>	Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.
72	5.2.2.1.1.3	26	<p>Se menciona: El switch propuesto debe soportar puertos Uplinks Modulares o Fijos con opciones de tasas de transmisión de 10Gbps y 40 Gbps.</p> <p>Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, se solicita confirmar que se podrán proponer soluciones de switches con uplink modulares o fijos con velocidad de transmisión de 10Gbps y 50 Gbps</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
73	5.2.2.1.1.3	26	<p>Se menciona: Configuración automática de QoS.</p> <p>Consultar:</p>		Sera opcional.	Opcionalmente, configuración automática de QoS.

			Debido a que esta característica está orientada exclusivamente al fabricante Cisco, sírvase a confirmar que esta característica sea opcional	Consulta de la empresa ITALTEL PERU S.A.C..		
74	5.2.2.1.1.3	26	<p>Se menciona: El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo.</p> <p>Consulta: Debido a que esta característica está orientada exclusivamente al fabricante Cisco, sírvase a confirmar que esta característica será opcional.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	<p>Precisar que de la revisión de esta sección 5.2.2.1.1.3 corresponde a Equipos Tipo III.</p> <p>Con Relación a esta etiqueta RFID que es requerida para identificación de los equipos que serán implementados en cada nodo LAN, se reformula el requerimiento para que su cumplimiento pueda ser también con código de barras o QR.</p> <p>El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) o QR o Código de Barra, ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo</p>	El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) o QR o Código de Barra, ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo
75	5.2.2.1.1.4	28	<p>Se menciona: El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal.</p> <p>Consulta: Debido a que esta funcionalidad está orientada al fabricante Cisco, sírvase a confirmar que esta funcionalidad será opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..	<p>Se reformula requerimiento de la siguiente manera:</p> <p>El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.</p>	El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.
76	5.2.2.1.1.4	28	<p>Se menciona: El switch propuesto debe contar con al menos 24 puertos 10/100/1000 Base-T RJ45 con soporte PoE/PoE+, en todos sus puertos.</p> <p>Consulta: Debido a que la velocidad de funcionamiento de los dispositivos finales tienden a aumentar con el paso de los años, y en pro de mantener una arquitectura de red acorde a las nuevas tendencias y estándares de la industria, sírvase a confirmar que el switch propuesto deba contar como</p>	Consulta de la empresa ITALTEL PERU S.A.C..	<p>Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento.</p> <p>Por otro lado, de la revisión, de esta característica para</p>	El switch propuesto debe contar con al menos 24 puertos 10/100/1000 Base-T RJ45 con soporte PoE/PoE+/PoE++, en todos sus puertos.

			mínimo con 24 puertos 100M//1G/2.5G/5G, Base-T RJ45 con soporte PoE/PoE+ en todos sus puertos		que tenga congruencia el requerimiento se actualiza el soporte de PoE/PoE+/PoE++, dado que los puertos solicitados deben cumplir con el soporte de 60W de potencia; por lo que se actualiza el requerimiento, en ese extremo	
77	5.2.2.1.1.4	28	Se menciona: El switch propuesto debe contar con al menos 2 puertos 40GE de uplink. Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, se solicita confirmar que se podrán proponer soluciones con puertos de uplink a 50GE.	Consulta de la empresa ITALTEL PERU S.A.C..	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
78	5.2.2.1.1.4	28	Se menciona: Debe incluir 2 transceivers de 40Gbps (SFP28) para fibra óptica monomodo 10Km Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, sírvase a confirmar que se podrán proponer soluciones con puertos de 50Gbps(SFP28) para fibra óptica monomodo 10Km	Consulta de la empresa ITALTEL PERU S.A.C..	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
79	5.2.2.1.1.4	28	Se menciona: El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking. Consulta: Con el objetivo de tener una mayor pluralidad de fabricantes, sírvase en confirmar que se podrá realizar el stacking de los switches por medio de	Consulta de la empresa ITALTEL PERU S.A.C..	Con la finalidad de ampliar la participación de postores, se reformula el requerimiento: El switch propuesto debe soportar apilamiento y la	El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking o puertos de uplinks/servicios adicionales para stacking.

			puertos de uplink adicionales, con ello se ahorra costos en agregar módulos dedicados para los puertos de stacking del equipo.		formación de stacks entre ellos utilizando puertos dedicados a Stacking o puertos de uplinks/servicios adicionales para stacking.	
80	5.2.2.1.1.4	29	Se menciona: RADIUS, TACACS, TACACS+ o equivalentes, ACL IPv4, ACL IPv6, BDPU Guard, BDPU Filter, Root Guard o equivalente, Private VLAN o similares, DHCP Snooping, MLD Snooping. Consulta: Debido a que TACACS y TACACS+ (asociado al siguiente RFC 8907) tienen funcionalidades integrables con distintos fabricantes, ambos siendo estándares de la industria, sírvase a confirmar que no se podrá cumplir esta especificación con protocolos equivalentes o propietarios.	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Con el fin de permitir mayor pluralidad de postores se ha solicitado lo indicado en el presente requerimiento.	
81	5.2.2.1.1.4	29	Se menciona: Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión. Consulta: Con el objetivo de una mayor pluralidad de fabricantes, sírvase a confirmar que se podrá cumplir la especificación a través de funcionalidades como Control Plane Policing (CoPP) o similares.	Consulta de la empresa ITALTEL PERU S.A.C..	Se confirma. Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.	Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.
82	5.2.2.1.1.4	29	Se menciona: El switch propuesto debe soportar puertos Uplinks Modulares o Fijos con opciones de tasas de transmisión de 10Gbps y 40 Gbps. Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, se solicita confirmar que se podrán proponer soluciones de switches con uplink modulares o fijos con velocidad de transmisión de 10Gbps y 50 Gbps	Consulta de la empresa ITALTEL PERU S.A.C..	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
83	5.2.2.1.1.4	29	Se menciona: Configuración automática de QoS.		Sera Opcional.	Opcionalmente, configuración automática de QoS.

			<p>Consulta: Debido a que esta característica está orientada exclusivamente al fabricante Cisco, Sírvese a confirmar que lo solicitado será considerado como opcional</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>		
84	5.2.2.1.1.4	29	<p>Se menciona: El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo.</p> <p>Consulta: Debido a que esta característica está orientada exclusivamente al fabricante Cisco, sírvase a confirmar que lo solicitado será considerado como opcional</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>	<p>Con Relación a esta etiqueta RFID que es requerida para identificación de los equipos que serán implementados en cada nodo LAN, se reformula el requerimiento para que su cumplimiento pueda ser también con código de barras o QR.</p> <p>El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) o QR o Código de Barra, ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo</p>	<p>El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) o QR o Código de Barra, ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo</p>
85	5.2.2.1.1.5	31	<p>Se menciona: El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal.</p> <p>Consulta: Debido a que esta funcionalidad está orientada al fabricante Cisco, Sírvese a confirmar que esta funcionalidad será opcional</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>	<p>Se reformula requerimiento de la siguiente manera:</p> <p>El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.</p>	<p>El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.</p>
86	5.2.2.1.1.5	31	<p>Se menciona: El switch propuesto debe contar con al menos 2 puertos 40GE de uplink.</p> <p>Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, se solicita confirmar que se podrán proponer soluciones con puertos de uplink a 50GE.</p>	<p>Consulta de la empresa ITALTEL PERU S.A.C..</p>	<p>Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.</p>	

87	5.2.2.1.1.5	31	<p>Se menciona: Debe incluir 2 transceivers de 40Gbps (SFP28) para fibra óptica monomodo 10Km</p> <p>Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, Sírvase a confirmar que se podrán proponer soluciones con puertos de 50Gbps(SFP28) para fibra óptica monomodo 10Km</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
88	5.2.2.1.1.5	31	<p>Se menciona: El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking.</p> <p>Consulta: Con el objetivo de tener una mayor pluralidad de fabricantes, Sírvase en confirmar que se podrá realizar el stacking de los switches por medio de puertos de uplink adicionales, con ello se ahorra costos en agregar módulos dedicados para los puertos de stacking del equipo.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	<p>Con la finalidad de ampliar la participación de postores, se reformula el requerimiento:</p> <p>El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking o puertos de uplinks/servicios adicionales para stacking.</p>	El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking o puertos de uplinks/servicios adicionales para stacking.
89	5.2.2.1.1.5	32	<p>Se menciona: RADIUS, TACACS, TACACS+ o equivalentes, ACL IPv4, ACL IPv6, BDPU Guard, BPDPU Filter, Root Guard o equivalente, Private VLAN o similares, DHCP Snooping, MLD Snooping.</p> <p>Consulta: Debido a que TACACS y TACACS+ (asociado al siguiente RFC 8907) tienen funcionalidades integrables con distintos fabricantes, ambos siendo estándares de la industria, Sírvase a confirmar que no se podrá cumplir esta especificación con protocolos equivalentes o propietarios.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Con el fin de permitir mayor pluralidad de postores se ha solicitado lo indicado en el presente requerimiento.	
90	5.2.2.1.1.5	32	<p>Se menciona: El switch propuesto debe soportar puertos Uplinks Modulares o Fijos con opciones de tasas de transmisión de 10Gbps y 40 Gbps.</p> <p>Consulta: Con el objetivo de garantizar una mayor velocidad en la transferencia de datos, se solicita confirmar que se podrán proponer soluciones de</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen	

			switches con uplink modulares o fijos con velocidad de transmisión de 10Gbps y 50 Gbps		correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
91	5.2.2.1.1.5	32	Se menciona: Configuración automática de QoS. Consulta: Debido a que esta característica está orientada exclusivamente al fabricante Cisco, sírvase a confirmar que esta característica sea opcional	Consulta de la empresa ITALTEL PERU S.A.C..	Sera Opcional.	Opcionalmente, configuración automática de QoS.
92	5.2.2.1.1.5	32	Se menciona: El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo. Consulta: Debido a que esta característica está orientada exclusivamente al fabricante Cisco, sírvase a confirmar que esta característica será opcional.	Consulta de la empresa ITALTEL PERU S.A.C..	Con Relación a esta etiqueta RFID que es requerida para identificación de los equipos que serán implementados en cada nodo LAN, se reformula el requerimiento para que su cumplimiento pueda ser también con código de barras o QR. El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) o QR o Código de Barra, ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo	El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) o QR o Código de Barra, ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo
93	5.2.2.1.1.6	34	Se menciona: RADIUS, TACACS, TACACS+ o equivalentes, ACL IPv4, ACL IPv6, BDPU Guard, BPDU Filter, Root Guard o equivalente, Private VLAN o similares, DHCP Snooping, MLD Snooping. Consulta: Debido a que TACACS y TACACS+ (asociado al siguiente RFC 8907) tienen funcionalidades integrables con distintos fabricantes, ambos siendo estándares de la industria, Sírvase a confirmar que no se podrá cumplir esta especificación con protocolos equivalentes o propietarios.	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Con el fin de permitir mayor pluralidad de postores se ha solicitado lo indicado en el presente requerimiento.	

94	5.2.2.1.2.1	36	Se menciona: El equipo deberá soportar por lo menos 16000 dispositivos clientes y 4096 VLANS. Consulta: Para una mayor pluralidad de fabricantes Sirvase confirmar que el equipo a ofertar soporte por lo menos 10000 dispositivos clientes.	Consulta de la empresa ITALTEL PERU S.A.C..	Se confirma.	El equipo deberá soportar por lo menos 10000 dispositivos clientes y no menos de 4000 VLANS.
95	5.2.2.1.2.1	36	Se menciona: El equipo deberá soportar por lo menos 16000 dispositivos clientes y 4096 VLANS. Consulta: Para una mayor pluralidad de fabricantes, se solicita confirmar que la cantidad de VLANs permitidas sean no menor a 4000.	Consulta de la empresa ITALTEL PERU S.A.C..	Se confirma.	El equipo deberá soportar por lo menos 10000 dispositivos clientes y no menos de 4000 VLANS.
96	5.2.2.1.2.1	36	Se menciona: Implementar barrido continuo de RF, programado bajo demanda de puntos de acceso con identificación de clientes irregulares. Consulta: Con el objetivo de una mayor pluralidad de postores, Sirvase a confirmar que el añadido 'con identificación de clientes irregulares' podrá ser opcional	Consulta de la empresa ITALTEL PERU S.A.C..	Se confirma lo indicado "con identificación de clientes irregulares" será opcional.	Implementar barrido continuo de RF, programado bajo demanda de puntos de acceso con identificación de clientes irregulares. "con identificación de cliente irregulares" será opcional.
97	5.2.2.1.2.1	37	Se menciona: Deberá soportar NETCONF (RFC 6241) o RESTCONF (RFC 8040) para proporcionar una interfaz de programabilidad estándar y permitir el acceso a parámetros de configuración. Consulta: Con el objetivo de una mayor pluralidad de postores, Sirvase a confirmar que la especificación podrá ser cumplida con RESTAPI o similares	Consulta de la empresa ITALTEL PERU S.A.C..	Para mejor entendimiento se reformula requerimiento.	Deberá soportar REST API como interfaz de programabilidad estándar y permitir el acceso a parámetros de configuración
98	5.2.2.1.2.1	37	Se menciona: Debe incluir visibilidad de las aplicaciones consumidas por los usuarios, combinando la detección y el control de aplicaciones en la red, identificando y clasificando información de Capa 4 a Capa 7 de las aplicaciones que se están utilizando en la red; que luego permitan configurar ACL por aplicación o categoría de aplicación y acelerar el ancho de banda para aplicaciones de misión crítica para priorización del tráfico y QoS; utilizando como tecnologías que pueden ser control de aplicaciones, inspección profunda de paquetes, reconocimiento de aplicaciones basado en red, o una combinación de las mismas. Consulta: Debido a que la especificación está orientada a un solo fabricante, Sirvase a confirmar que lo solicitado será considerado como opcional	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Sin embargo, con el fin de permitir pluralidad de postores el párrafo se modifica de la siguiente manera: "Debe incluir visibilidad de las aplicaciones consumidas por los usuarios, combinando la detección y el control de aplicaciones en la red, identificando y clasificando información de Capa 4 a Capa 7 de las aplicaciones que se están utilizando en la red; que luego permitan configurar ACL y/o QoS por aplicación o categoría de aplicación	Debe incluir visibilidad de las aplicaciones consumidas por los usuarios, combinando la detección y el control de aplicaciones en la red, identificando y clasificando información de Capa 4 a Capa 7 de las aplicaciones que se están utilizando en la red; que luego permitan configurar ACL y/o QoS por aplicación o categoría de aplicación

					que se están utilizando en la red; que luego permitan configurar ACL y/o QoS por aplicación o categoría de aplicación".	
99	5.2.2.1.2.1	37	Se menciona: Actualización en vivo de los Access Points Consulta: Con el objetivo de simplificar la gestión de la solución, Sírvase a confirmar que la especificación será cumplida con la solución requerida en el numeral 5.2.2.1.4 - PLATAFORMA DE GESTIÓN Y AUTENTICACION DE ACCESO A LA RED	Consulta de la empresa ITALTEL PERU S.A.C..	Se confirma parcialmente, también podrá cumplirse dicho requerimiento con la SOLUCIÓN DE ADMINISTRACION DE RED LAN	Actualización en vivo de los Access Points, también podrá cumplirse con la solución de ADMINISTRACION DE RED LAN
100	5.2.2.1.2.2	38	Se menciona: Despliegue de políticas de Calidad de Servicio (QoS) de manera automatizada en base al listado de aplicaciones críticas, no críticas y por defecto. Este despliegue será basado en las aplicaciones que son las reconocidas por la solución del fabricante y aplicaciones personalizadas que corresponden a la Entidad en base a puertos TCP o UDP o IP Consulta: Debido a que la especificación está orientada a un solo fabricante, sírvase a confirmar que lo solicitado será considerado como opcional	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Sin embargo, con el fin de permitir mayor pluralidad de postores se modificará el requerimiento de la siguiente manera: "Despliegue de políticas de Calidad de Servicio (QoS) basado en las aplicaciones que son las reconocidas por la solución del fabricante y aplicaciones personalizadas que corresponden a la Entidad en base a puertos TCP o UDP o IP"	Despliegue de políticas de Calidad de Servicio (QoS) basado en las aplicaciones que son las reconocidas por la solución del fabricante y aplicaciones personalizadas que corresponden a la Entidad en base a puertos TCP o UDP o IP"
101	5.2.2.1.3	39	Se menciona: La solución de automatización, administración y gestión de la infraestructura campus con todos sus componentes de hardware y software serán implementados en alta disponibilidad sen un entorno ON PREMISE utilizando appliances de propósito específico Consulta: Sírvase en confirmar que también se aceptarán soluciones en nube tipo SaaS para la administración y gestión de los equipos (Switching y WiFi)	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma lo solicitado, se requiere la solución en formato ON PREMISE para asegurar el tiempo de respuesta y no depender de la salida a Internet de la Entidad.	
102	5.2.2.1.3	39	Se menciona: Utilizando licenciamiento del tipo perpetuo. Consulta:	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma lo indicado, con el fin de proteger la inversión de la Entidad, el licenciamiento debe ser de tipo perpetuo.	La solución contempla el despliegue, implementación y configuración de la red inalámbrica y la red local cableada en una arquitectura de Software Defined Network con el

			Sírvase en confirmar que también se aceptaran licenciamiento bajo un esquema de suscripción garantizando el soporte y correcto funcionamiento de este.		Asimismo, para clarificar las característica y condiciones de la contratación referente al licenciamiento, la arquitectura del SDN deberá contar con el máximo nivel de licenciamiento para contar con las mejores capacidades de automatización, control y analítica.	máximo nivel de licenciamiento que ofrezca el fabricante, para contar con las mejores capacidades de automatización, control y analítica.
103	5.2.2.1.3	40	Se menciona: Verificaciones antes y después de realizar el despliegue de nuevas versiones de software en los switches. Consulta: Las verificaciones de software del sistema operativo se realiza antes de realizar el despliegue de los equipos, Sírvase en confirmar que esta funcionalidad será considerada como opcional.	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma lo solicitado, la verificación posterior a la actualización permite asegurar la confiabilidad de la solución.	
104	5.2.2.1.3	40	Se menciona: Despliegue de políticas de Calidad de Servicio (QoS). Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..	No se acoge lo solicitado, esta funcionalidad permite discernir entre los distintos tipos de equipos de la Entidad.	
105	5.2.2.1.3	40	Se menciona: El sistema de administración dispondrá de una función que centralice las configuraciones de los equipos permitiendo mantener copia de la configuración con múltiples versiones de las mismas. Deberá permitir realizar el respaldo, la restitución y la comparación de archivos de configuración Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..	Se aclara que diversos fabricantes de la industria cuentan con la capacidad de control de versiones indicada, por lo cual no se confirma lo solicitado.	
106	5.2.2.1.3	40	Se menciona: Tendrá una función que permitirá establecer una fecha u horario donde se aplicará la tarea en forma automática. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta	Consulta de la empresa ITALTEL PERU S.A.C..	Se aclara que esta funcionalidad es conocida por distintos nombres en diferentes fabricantes: cron, kron, scheduled task, entre otras. Por lo cual no se confirma lo solicitado.	

			funcionalidad será considerada como opcional dentro de la plataforma de gestión.			
107	5.2.2.1.3	40	Se menciona: Organización jerárquica de equipos en plantas, plantas en edificios y edificios en proyectos. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..	Con el fin de permitir mayor pluralidad de postores, se considerará como opcional.	Opcionalmente, Organización jerárquica de equipos en plantas, plantas en edificios y edificios en proyectos
108	5.2.2.1.3	41	Se menciona: Capacidad de generar informes de los siguientes tipos: Lista de clientes wireless o lista de tipo de dispositivo cliente Consulta: Sirvase en confirmar que la lista de clientes Wireless a exportar, será los que se encuentren activos en el dashboard	Consulta de la empresa ITALTEL PERU S.A.C..	Se confirma lo indicado.	
109	5.2.2.1.3	41	Se menciona: Información de configuración de los controladores WLAN Consulta: Sirvase en confirmar que la información de los controladores WLAN se verá la información en cada equipo.	Consulta de la empresa ITALTEL PERU S.A.C..	Se aclara que se refiere al archivo de configuración de cada controlador WLAN.	
110	5.2.2.1.3	41	Se menciona: Deberá permitir configurar para que automáticamente almacene el respaldo de las configuraciones de los equipos inalámbricos, por ejemplo, cada mes, cada semana, etc. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..	Se aclara que esto puede ser realizado a través de una tarea programada, lo cual se soporta en diversas marcas del mercado.	
111	5.2.2.1.3	42	Se menciona: Debe incluir una solución que permita el uso de algoritmos avanzados de análisis de comportamiento; para identificar patrones de tráfico, usando análisis de la información de eventos que ocurren dentro de un flujo de datos aplicando técnicas de machine learning, o plataforma de análisis de big data Telemetry que analice y muestre los datos de la red a través de algoritmos inteligentes; con el objetivo de detectar potenciales amenazas de seguridad, a través de la inclusión de hardware y software adicional que permita descifrar el tráfico para su análisis. Consulta:	Consulta de la empresa ITALTEL PERU S.A.C..	Con el fin de permitir mayor pluralidad de postores, se considerará como opcional.	Opcionalmente, debe incluir una solución que permita el uso de algoritmos avanzados de análisis de comportamiento; para identificar patrones de tráfico, usando análisis de la información de eventos que ocurren dentro de un flujo de datos aplicando técnicas de machine learning, o plataforma de análisis de big data Telemetry que analice y muestre los datos de la red a través

			Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.			de algoritmos inteligentes; con el objetivo de detectar potenciales amenazas de seguridad, a través de la inclusión de hardware y software adicional que permita descifrar el tráfico para su análisis.
112	5.2.2.1.3	42	Se menciona: Soporte de descubrimiento vía SNMP o tablas de enrutamiento o tablas ARP etc., o cualquier otro mecanismo que brinde el fabricante para automatizar este proceso. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..	Se aclara que este requerimiento puede ser cumplido usando protocolos estándares de la industria, por lo cual no se confirma lo solicitado.	
113	5.2.2.1.3	42	Se menciona: Soporte de la visualización de la configuración del servicio, la configuración y el monitoreo de la red virtual basada en topología y la consulta del estado del aprovisionamiento del servicio en tiempo real. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión	Consulta de la empresa ITALTEL PERU S.A.C..	Con el fin de permitir mayor pluralidad de postores, se considerará como opcional.	Opcionalmente, soporte de la visualización de la configuración del servicio, la configuración y el monitoreo de la red virtual basada en topología y la consulta del estado del aprovisionamiento del servicio en tiempo real.
114	5.2.2.1.3	42	Se menciona: Soporte de programación de QoS basada en usuarios y prioridades de servicio. Esto debe permitir la implementación de diferentes políticas para diferentes usuarios y aplicaciones a través de la generación de control de políticas de ancho de banda. Consulta: Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión	Consulta de la empresa ITALTEL PERU S.A.C..	Con el fin de permitir mayor pluralidad de postores, se considerará como opcional.	Opcionalmente, Soporte de programación de QoS basada en usuarios y prioridades de servicio. Esto debe permitir la implementación de diferentes políticas para diferentes usuarios y aplicaciones a través de la generación de control de políticas de ancho de banda
115	5.2.2.1.3	42	Se menciona: Soporte de monitoreo de red basado en mapas, inspección de red. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..	Se aclara que este requerimiento puede ser cumplido usando protocolos estándares de la industria, por lo cual no se confirma lo solicitado.	
116	5.2.2.1.3	42	Se menciona:		Se aclara que este requerimiento puede ser	

			<p>Soporte de visibilidad de experiencia en tiempo real del uso de aplicaciones de cada usuario en cada área.</p> <p>Consulta: Sirvase en confirmar que, para revisar la experiencia del uso de las aplicaciones, se pueda considerar un equipo adicional para que este monitoree el estado de la red inalámbrica</p>	Consulta de la empresa ITALTEL PERU S.A.C..	cumplido usando protocolos estándares de la industria, por lo cual no se confirma lo solicitado.	
117	5.2.2.1.3	42	<p>Se menciona: Soporte de seguimiento de fallas, que permita identificar con rapidez a los dispositivos defectuosos, así como analizar las causas raíz de la mala calidad.</p> <p>Consulta: Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Esta es una de las ventajas principales de la analítica, por lo cual no se confirma lo solicitado.	
118	5.2.2.1.3	42	<p>Se menciona: Capacidad de evaluar conflictos de la red inalámbrica en tiempo real.</p> <p>Consulta: Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Esta es una de las ventajas principales de la analítica, por lo cual no se confirma lo solicitado.	
119	5.2.2.1.3	42	<p>Se menciona: Capacidad de comparar las ganancias de la red inalámbrica antes y después de la calibración.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Esta es una de las ventajas principales de la analítica, por lo cual no se confirma lo solicitado.	
120	5.2.2.1.3	42	<p>Se menciona: Vistas de estadísticas de datos multidimensionales basadas en diferentes niveles y regiones</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Esta es una de las ventajas principales de la analítica, por lo cual no se confirma lo solicitado.	
121	5.2.2.1.3	43	<p>Se menciona: Permite enviar informes de salud de la red al administrador en tiempo real o periódicamente.</p> <p>Consulta: Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Esta es una de las ventajas principales de la analítica, por lo cual no se confirma lo solicitado.	

122	5.2.2.1.3	43	<p>Se menciona: El servidor debe contar con la funcionalidad de Syslog.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Si bien esta funcionalidad es estándar, se permitirá que sea opcional con el fin de permitir mayor pluralidad de postores.	El servidor debe contar opcionalmente con la funcionalidad de Syslog.
123	5.2.2.1.3	43	<p>Se menciona: Monitoreo de seguridad y verificación de la salud de la red para poder determinar si la red tiene las políticas de seguridad óptimas a nivel de configuración.</p> <p>Consulta: Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Con el fin de permitir mayor pluralidad de postores, se considerará como opcional.	Opcionalmente el Monitoreo de seguridad y verificación de la salud de la red para poder determinar si la red tiene las políticas de seguridad óptimas a nivel de configuración
124	5.2.2.1.3	43	<p>Se menciona: Permitir el monitoreo de servicios de video y voz sobre wireless.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Con el fin de permitir mayor pluralidad de postores, se considerará como opcional.	Opcionalmente permitir el monitoreo de servicios de video y voz sobre wireless
125	5.2.2.1.3	43	<p>Se menciona: Permitir visualizar la cantidad de clientes conectados, habilitar capturas en tiempo real, listar amenazas detectadas</p> <p>Consulta: Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Con el fin de permitir mayor pluralidad de postores, se considerará como opcional habilitar capturas en tiempo real y listar amenazas detectadas	Permitir visualizar la cantidad de clientes conectados, opcionalmente habilitar capturas en tiempo real y listar amenazas detectadas
126	5.2.2.1.3	43	<p>Se menciona: La solución debe de permitir realizar backups automáticos de la configuración del sistema.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Se aclara que este requerimiento puede ser cumplido usando protocolos estándares de la industria, por lo cual no se confirma lo solicitado.	
127	5.2.2.1.3	43	<p>Se menciona: Inventarios debe al menos dar información de número de serie y versión de imagen de sistema operativo.</p>		Se aclara que este requerimiento puede ser cumplido usando protocolos	

			Consulta: Sirvase en confirmar que esta información pueda ser exportada desde la página de inicio de la plataforma de gestión y no como reporte.	Consulta de la empresa ITALTEL PERU S.A.C..	estándares de la industria, por lo cual no se confirma lo solicitado.	
128	5.2.2.1.3	43	Se menciona: Permite a los usuarios importar vistas de topología y planificar ubicaciones de AP para ver la distribución de la ubicación de fallas. Consulta: Sirvase en confirmar que esta información de la distribución de la ubicación de fallas será considerada como opcional La funcionalidad de distribución de la ubicación de fallas está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..	Esta funcionalidad es cubierta por varios fabricantes de la industria, por lo cual no se confirma lo solicitado.	
129	5.2.2.1.3	43	Se menciona: Permitir correlacionar la información de la red/wifi/analíticos/control de acceso en un solo dashboard. Consulta: Sirvase en aclarar que el control de acceso se realizara a traves de la plataforma de control de Acceso (NAC)	Consulta de la empresa ITALTEL PERU S.A.C..	Con el fin de permitir mayor pluralidad de postores, se considerará como opcional a "control de acceso"	Permitir correlacionar la información de la red/wifi/analíticos y opcionalmente control de acceso, en un solo Dashboard
130	5.2.2.1.3	43	Se menciona: Permite a los usuarios importar datos de planificación de la red y comparar los datos de planificación con los datos reales de funcionamiento de la red para mostrar las diferencias entre ellos. Consulta: Sirvase en confirmar que esta información de la distribución de la ubicación de fallas, sea considerada como opcional	Consulta de la empresa ITALTEL PERU S.A.C..	Esta es una de las ventajas principales de la analítica, por lo cual no se confirma lo solicitado.	
131	5.2.2.1.3	43	Se menciona: Debe tener la capacidad de ser un servidor syslog. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..	Si bien esta funcionalidad es estándar, se permitirá que sea opcional con el fin de permitir mayor pluralidad de postores.	Opcionalmente debe tener la capacidad de ser un servidor syslog.
132	5.2.2.1.3	43	Se menciona: Debe de poder hacer backup de las configuraciones		Se aclara que este requerimiento puede ser cumplido usando protocolos	

			Consulta: Sírvese en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión	Consulta de la empresa ITALTEL PERU S.A.C..	estándares de la industria, por lo cual no se confirma lo solicitado.	
133	5.2.2.1.3	44	Se menciona: Protocolos de análisis de tiempo de respuesta de aplicaciones, análisis de tráfico de voz y video. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvese en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..	Se confirma lo solicitado, se permitirá que sea opcional con el fin de permitir mayor pluralidad de postores.	Soporte de Netflow flexible, IPFIX, o similares, y opcionalmente protocolos de análisis de tiempo de respuesta de aplicaciones, análisis de tráfico de voz y video
134	5.2.2.1.3	44	Se menciona: Los dashboard deben de ser configurables y se puede personalizar la ventana de vista de dashboard. Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvese en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de gestión.	Consulta de la empresa ITALTEL PERU S.A.C..	Se acoge lo solicitado, se permitirá que sea opcional con el fin de permitir mayor pluralidad de postores.	Opcionalmente los dashboard deben de ser configurables y se puede personalizar la ventana de vista de dashboard
135	5.2.2.1.4	45	Se menciona: Para la gestión y autenticación de acceso a la red, se debe implementar el servicio RADIUS y/o TACACS, TACACS+ o equivalentes, que incluya el licenciamiento necesario para el Sistema Operativo, el servicio RADIUS o TACACS o TACACS+ y un Servicio NTP. Consulta: Sírvese en confirmar que la funcionalidad de NTP sea considerada como opcional	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Sin embargo, con el fin de permitir mayor pluralidad de postores se aceptará NTP server o client.	Para la gestión y autenticación de acceso a la red, se debe implementar el servicio RADIUS y/o TACACS, TACACS+ o equivalentes, que incluya el licenciamiento necesario para el Sistema Operativo, el servicio RADIUS o TACACS o TACACS+ y un Servicio NTP Server o Client.
136	5.2.2.1.4	46	Se menciona: El sistema de control de acceso debe permitir integrarse al controlador SDN Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvese en confirmar que esta funcionalidad será considerada como opcional.	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Con el fin de permitir mayor pluralidad de postores, se permitirá que la PLATAFORMA DE GESTIÓN Y AUTENTICACION DE ACCESO A LA RED esté integrada en la SOLUCIÓN DE ADMINISTRACION DE RED LAN	El sistema de control de acceso debe permitir integrarse al controlador SDN. Se permitirá que la PLATAFORMA DE GESTIÓN Y AUTENTICACION DE ACCESO A LA RED esté integrada en la SOLUCIÓN DE ADMINISTRACION DE RED LAN

137	5.2.2.1.4	47	<p>Se menciona: Debe permitir vincular información a cuentas de usuario y cuentas MAC, incluyendo la dirección IP, la dirección MAC (no aplicable a cuentas MAC) y la información del dispositivo de acceso. Esta información se debe utilizar para restringir los comportamientos de acceso del usuario, por ejemplo, los usuarios solo pueden acceder a la red a través de la dirección IP vinculada a su cuenta respectiva.</p> <p>Consulta: Sirvase en confirmar que esta funcionalidad, será considerada como opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma, esta funcionalidad permite cumplir con los requisitos de autenticación que necesita la Entidad.	
138	5.2.2.1.4	48	<p>Se menciona: Debe permitir la gestión de lista negra de usuarios. Se debe poder agregar manualmente usuarios a la lista negra o configurar la función de bloqueo automático de usuarios que ingresan contraseñas incorrectas varias veces consecutivas y usuarios con direcciones IP o MAC específicas. Los usuarios en la lista negra tienen denegado el acceso a la red</p> <p>Consulta: Sirvase en confirmar que esta funcionalidad, será considerada como opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma, esta funcionalidad permite cumplir con los requisitos de seguridad que necesita la Entidad	
139	5.2.2.1.4	48	<p>Se menciona: Admite la gestión de PPSK (Clave Precompartida por Usuario). Se pueden establecer diferentes PPSK para diferentes usuarios en la misma red Wi-Fi.</p> <p>Consulta: Sirvase en confirmar que esta funcionalidad, será considerada como opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma, esta funcionalidad permite cumplir con los requisitos de seguridad inalámbrica que necesita la Entidad.	
140	5.2.2.1.4	48	<p>Se menciona: Si una regla personalizada contiene múltiples condiciones coincidentes, un terminal solo coincide con la regla cuando la puntuación total de las condiciones coincidentes en esta regla alcanza la puntuación mínima requerida.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sirvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de control de Acceso.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Se aclara que esta funcionalidad es cumplida por diversos fabricantes de la industria.	

141	5.2.2.1.4	48	<p>Se menciona: Debe utilizar inteligencia artificial para agrupar terminales no identificados después de recopilar huellas digitales de terminales.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de control de Acceso.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Se aclara que esta funcionalidad es cumplida por diversos fabricantes de la industria.	
142	5.2.2.1.4	48	<p>Se menciona: Autenticación mediante código de acceso: El usuario ingresa el código de acceso en la página del portal de autenticación. En este modo, los códigos de acceso deben ser creados y distribuidos previamente por los administradores.</p> <p>Consulta: Esta funcionalidad y/o característica está orientado al fabricante (Cisco). Para una mayor pluralidad de postores. Sírvase en confirmar que esta funcionalidad será considerada como opcional dentro de la plataforma de control de Acceso</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Se aclara que esta funcionalidad es cumplida por diversos fabricantes de la industria.	
143	5.2.2.1.4	48	<p>Se menciona: Además, el usuario puede optar por asociar un número de teléfono móvil con la cuenta durante la autenticación por SMS.</p> <p>Consulta: Sírvase en confirmar que esta funcionalidad, será considerada como opcional</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Se aclara que esta funcionalidad es cumplida por diversos fabricantes de la industria.	
144	5.2.2.1.6	52	<p>Se menciona: En el caso de Overlay distribuido: Se deberá contemplar cualquier componente de hardware adicional redundante para que permita a los usuarios de los diferentes segmentos de red creados consumir servicios que estarán ubicados en un punto común (Data Centers). Para ello se deberá hacer uso de VRF Leaking.</p> <p>Aclaración: Las configuraciones de VRF leaking están asociadas al fabricante Cisco, Sírvase en aclarar que esta configuración será opcional o reemplazado con la configuración indicada por el fabricante.</p>	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Sin embargo, para permitir mayor pluralidad de postores se considerará VRF Leaking o Route Leaking.	Se deberá contemplar cualquier componente de hardware adicional redundante para que permita a los usuarios de los diferentes segmentos de red creados consumir servicios que estarán ubicados en un punto común (Data Centers). Para ello se deberá hacer uso de VRF Leaking o Route Leaking
145	5.2.2.1.6	52	<p>Se menciona: En el caso de Overlay distribuido: Independiente del tipo de Overlay a desplegar. Se deberá realizar una integración con el NAC para poder asignar los SGT o Roles correspondientes que permitan manejar una microsegmentación.</p>		Se aclara que, con el fin de permitir mayor pluralidad de postores, se reformula el requerimiento.	Independiente del tipo de Overlay a desplegar. Se deberá realizar una integración con el NAC para poder asignar políticas basadas en roles o grupos que permitan manejar una

			Aclaración: Las configuraciones de SGT es asociada a Cisco. Sirvase en aclarar que se realizará las integraciones con el NAC de acuerdo con las soluciones brindadas por el fabricante propuesto	Consulta de la empresa ITALTEL PERU S.A.C..		microsegmentación.
146	5.2.2.1.6	52	Se menciona: Implementación de las políticas para el ingreso de operadores de red con TACACAS, TACACS+ o equivalente, para Autenticación, Autorización y Accounting. Consulta: Debido a que TACACS y TACACS+ (asociado al siguiente RFC 8907) tienen funcionalidades integrables con distintos fabricantes, ambos siendo estándares de la industria, Sirvase a confirmar que no se podrá cumplir esta especificación con protocolos equivalentes.	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Con el fin de permitir mayor pluralidad de postores se ha solicitado lo indicado en el presente requerimiento.	
147	5.2.2.1.4	45	Se menciona: Para la gestión y autenticación de acceso a la red, se debe implementar el servicio RADIUS y/o TACACS, TACACS+ o equivalentes, que incluya el licenciamiento necesario para el Sistema Operativo, el servicio RADIUS o TACACS o TACACS+ y un Servicio NTP. Consulta: Debido a que TACACS y TACACS+ (asociado al siguiente RFC 8907) tienen funcionalidades integrables con distintos fabricantes, ambos siendo estándares de la industria, Sirvase a confirmar que no se podrá cumplir esta especificación con protocolos equivalentes.	Consulta de la empresa ITALTEL PERU S.A.C..	No se confirma. Con el fin de permitir mayor pluralidad de postores se ha solicitado lo indicado en el presente requerimiento.	
148	5.2.2.1.2.1	36	Se menciona: El equipo deberá soportar por lo menos 16000 dispositivos clientes y 4096 WLANS. Consulta: Sirvase confirmar que el termino WLANS hace referencia a VLANs.	Consulta de la empresa ITALTEL PERU S.A.C..	Se confirma.	El equipo deberá soportar por lo menos 10000 dispositivos clientes y no menos de 4000 VLANS.
149	5.1	5	Se dice: PRESTACIÓN PRINCIPAL SISTEMA DE CABLEADO ESTRUCTURADO OPTIMIZACION DEL CABLEADO ESTRUCTURADO IMPLEMENTACIÓN DE 3 NUEVOS NODOS RENOVACIÓN DE EQUIPAMIENTO PASIVO EN 16 NODOS ACTUALES (CONTROL DE ACCESO, CCTV, AA DE CONFORT DE CONTINGENCIA, SISTEMA DE UPS) Y EN 2 SALAS (SALA CARRIER Y SALA BLANCA).	Consulta de la empresa ITALTEL PERU S.A.C..	Lo estipulado en la sección 5.2.1.2 y 5.2.1.3. Asimismo, podrá realizar la visita de campo para su correcto dimensionamiento.	

			Consulta: Favor de especificar cuál es el alcance del presente proyecto para las 2 salas (SALA CARRIER Y SALA BLANCA)			
149	5.3.1.4 – B	75	<p>Dice: Compresión De Video: Corriente principal: H.264 (MPEG-4 Parte 10/AVC), Subtransmisión: H.265 PEG-H Parte 2/HEVC)</p> <p>Consulta: La especificación indicada corresponde a un modelo discontinuado. Con el objetivo de poder presentar un equipo actual, se solicita se acepte la siguiente modificación:</p> <p>Debe decir: "Compresión De Video: H.264 (MPEG-4 Parte 10/AVC), Baseline perfil, Main perfil, y High perfil H.265 (MPEG-H Parte 2/HEVC) Main perfil, MJPEG"</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Se acepta modificación.	<p>Compresión De Video: H.264 (MPEG-4 Parte 10/AVC), Baseline perfil, Main perfil, y High perfil H.265 (MPEG-H Parte 2/HEVC) Main perfil, MJPEG</p>
150	5.3.1.4 – B	75	<p>Dice: Tipo H.264: Baseline perfil, Main perfil y Highperfil Tipo H.265: Main perfil, Motion JPEG</p> <p>Consulta: La especificación indicada corresponde a un modelo discontinuado. Con el objetivo de poder presentar un equipo actual, se solicita se acepte la siguiente modificación:</p> <p>Debe decir: "Tipo H.264: Baseline perfil, Main perfil, y High perfil Tipo H.265: Main perfil, MJPEG"</p>	Consulta de la empresa ITALTEL PERU S.A.C..	Se acepta modificación.	<p>Tipo H.264: Baseline perfil, Main perfil, y High perfil</p> <p>Tipo H.265: Main perfil, MJPEG"</p>
151	5.3.1.4 – B	76	<p>Dice: Seguridad: Protección por contraseña, filtrado de direcciones IP, HTTPSa, control de acceso a la red IEEE 802.1x (EAP-TLS)a, autenticación Digest, registro de acceso de usuarios, gestión centralizada de certificados, protección contra retrasos de fuerza bruta, firmware firmado, arranque seguro video firmado, pulsación de tecla segura (con certificación CC EAL4)</p> <p>Consulta:</p>		Se acepta parcialmente la modificación.	<p>Seguridad perimetral:</p> <p>- Software: Firmware firmado, protección contra retrasos de fuerza bruta, autenticación Digest y flujo de código de autorización OpenID OAuth 2.0 RFC6749 para gestión centralizada de cuentas ADFS, protección mediante contraseña, cifrado de tarjeta SD AES-XTS-Plain64 de 256 bits</p>

			<p>La especificación indicada corresponde a un modelo discontinuado. Con el objetivo de poder presentar un equipo actual, se solicita se acepte la siguiente modificación:</p> <p>Debe decir: "Seguridad perimetral: - Software: Firmware firmado, protección contra retrasos de fuerza bruta, autenticación Digest y flujo de código de autorización OpenID OAuth 2.0 RFC6749 para gestión centralizada de cuentas ADFS, protección mediante contraseña, cifrado de tarjeta SD AES-XTS-Plain64 de 256 bits - Hardware: Plataforma de ciberseguridad Axis Edge Vault Elemento seguro (CC EAL 6+), seguridad de sistema en un chip (TEE), ID de dispositivo de Axis, almacén de claves seguro, video firmado, arranque seguro, sistema de archivos cifrado (AES-XTS-Plain64 256 bits) Seguridad de red IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2), IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), X.509 Certificado PKI, firewall basado en host"</p>	Consulta de la empresa ITALTEL PERU S.A.C..		<p>- Hardware: Plataforma de ciberseguridad basada en hardware, Elemento seguro (CC EAL 6+), seguridad de sistema en un chip (TEE), ID de dispositivo, almacén de claves seguro, video firmado, arranque seguro, sistema de archivos cifrado (AES-XTS-Plain64 256 bits)</p> <p>Seguridad de red: IEEE 802.1X (EAP-TLS, PEAP-MSCHAPv2), IEEE 802.1AE (MACsec PSK/EAP-TLS), IEEE 802.1AR, HTTPS/HSTS, TLS v1.2/v1.3, Network Time Security (NTS), X.509 Certificado PKI, firewall basado en host</p>
152	General	General	<p>Consulta: Sirvase a confirmar si se enviará el detalle de los planos en autocad de los 16 nodos existentes + 02 salas (SALA CARRIER Y SALA BLANCA)</p>	Consulta de la empresa ITALTEL PERU S.A.C..	El Área usuaria de Redes, proporcionará la información disponible al contratista de la presente contratación.	
153	5.3.1.5.1.1	79	<p>Con respecto a la Estación de Monitoreo de la Solución de CCTV, se menciona lo siguiente: • Debe contar con un procesador i7 última generación.</p> <p>Consulta: Considerando que la Estación de Monitoreo propio del fabricante de la solución de CCTV, con procesador i7 ha sido discontinuado y con el objetivo de poder presentar un equipo actual, se solicita se acepte la siguiente modificación como mínimo: "• Debe contar con un procesador i3 última generación."</p>	Consulta de la empresa ITALTEL PERU S.A.C..	<p>Se aclara que, la estación de monitoreo es una estación de trabajo, para un fin específico.</p> <p>Por otro lado, con la finalidad de contar con la mejor propuesta de última generación en cuanto a sus características se reformula la redacción a lo siguiente: Debe contar con un procesador i3 o superior de última generación.</p>	Debe contar con un procesador i3 o superior de última generación.

ANEXO D

ITEM 11 DEL NUMERAL 2.8 OBSERVACIONES AL REQUERIMIENTO

N° de orden	Términos de Referencia o Especificaciones Técnicas o Requisitos de calificación		Consulta y/u Observación	Corresponde a consulta y/u observación del OEC o de las empresas invitadas en la indagación de mercado
	Numeral	Pág.		
1	5.1	8	En el cuadro de nuevas ubicaciones se menciona estos 3 nodos de comunicación (Nueva Torre piso10, Edificio Auxiliar, Radar Gambeta, Consulta Que se debe considerar en estos ambientes	Consulta de la empresa TIFA SERVICIOS Y TECNOLOGÍA DE LA INFORMACIÓN SAC.
2	5.2.1	11	En el cuadro de equipamiento que adjuntan se menciona que tienen equipamiento de telefonía IP cisco Este equipamiento también será parte de la gestión y soporte	Consulta de la empresa TIFA SERVICIOS Y TECNOLOGÍA DE LA INFORMACIÓN SAC.
3	5.2.2.1.1.1	14	Se solicita que el switch deberá contar con CPU mínimo de 2.2 Ghz Se podría considerar que el equipamiento sea de 1.6 Ghz y prestaciones mayores en RAM y SSD	Consulta de la empresa TIFA SERVICIOS Y TECNOLOGÍA DE LA INFORMACIÓN SAC.
4	5.3	54	Se solicita lo siguiente: Retiro del cableado de comunicaciones que está actualmente instalado en desuso y/o antiguo en CORPAC Lima-Callao, esto aplica solo para el caso de instalaciones de puntos nuevos de cableado, en los cuales exista cableado existente.	Consulta de la empresa GRUPO INGECORP S.A.C.

			Consulta: aparte del cable el cual está en funcionamiento existe cableado antiguo a indicado, de ser así de que cantidad, cual es la cantidad a retirar ya que esto puede impactar en los tiempos	
5	5.3.1.4	72	Se solicita la implementación de Sistema de control de Acceso. Se puede proponer equipos con mejoras tecnológicas ¿ Como por ejemplo con reconocimiento facial), aparte de los convencionales que es Biométrico, Clave o Tarjeta, se podría considerar como por ejemplo que la persona que quiere ingresar muestre su rostro ante la cámara del control de acceso y lo valide la cámara del sistema de CCTV a implementar en cada Nodo de comunicación	Consulta de la empresa TIFA SERVICIOS Y TECNOLOGÍA DE LA INFORMACIÓN SAC.
6	5	8	Dice: ALCANCE Y DESCRIPCIÓN DE LA CONTRATACIÓN 5.1 ALCANCE • Para estos nuevos nodos se deberá de considerar el cableado de fibra óptica, se muestra una figura 1 de la ubicación y conexión de cada uno de los NODOS LAN a implementar como referencia Consulta: Confirmar si los enlaces de fibra requieren de canalización y de cuantos metros serían.	Consulta de la empresa THINK NETWORKS PERU S.A.C
7	5.3	83	Dice: RENOVACIÓN DE GARANTÍA Y SOPORTE DE LA INFRAESTRUCTURA PASIVA DE CORPAC. • Adicionalmente al objeto de la contratación de equipamiento, CORPAC S.A. requiere renovar la garantía y el soporte de algunos componentes de la infraestructura pasiva implementada que tenga la garantía vigente del fabricante. Consulta: Confirmar que los componentes de administración de cableado a renovar la garantía tengan un programa de mantenimiento realizados durante los años de funcionamiento.	Consulta de la empresa THINK NETWORKS PERU S.A.C
8	5.3	84	Dice: RENOVACIÓN DE GARANTÍA Y SOPORTE DE LA INFRAESTRUCTURA PASIVA DE CORPAC. • Adicionalmente al objeto de la contratación de equipamiento, CORPAC S.A. requiere renovar la garantía y el soporte de algunos componentes de la infraestructura pasiva implementada que tenga la garantía vigente del fabricante. Consulta: Confirmar que los componentes de transformadores de aislamiento a renovar garantía tengan un programa de mantenimiento realizados durante los años de funcionamiento.	Consulta de la empresa THINK NETWORKS PERU S.A.C

9	5.3	84-85	<p>Dice: RENOVACIÓN DE GARANTÍA Y SOPORTE DE LA INFRAESTRUCTURA PASIVA DE CORPAC. Adicionalmente al objeto de la contratación de equipamiento, CORPAC S.A. requiere renovar la garantía y el soporte de algunos componentes de la infraestructura pasiva implementada que tenga la garantía vigente del fabricante.</p> <p>Consulta: Confirmar que los componentes del sistema de climatización de precisión a renovar garantía tengan un programa de mantenimiento realizados durante los años de funcionamiento</p>	Consulta de la empresa THINK NETWORKS PERU S.A.C
10	5.3	86-87	<p>Dice: RENOVACIÓN DE GARANTÍA Y SOPORTE DE LA INFRAESTRUCTURA PASIVA DE CORPAC. Adicionalmente al objeto de la contratación de equipamiento, CORPAC S.A. requiere renovar la garantía y el soporte de algunos componentes de la infraestructura pasiva implementada que tenga la garantía vigente del fabricante.</p> <p>Consulta: Confirmar que los componentes del sistema de procesamiento y control de puertas a renovar garantía tengan un programa de mantenimiento realizados durante los años de funcionamiento</p>	Consulta de la empresa THINK NETWORKS PERU S.A.C
11	5.3	86-87	<p>Dice: RENOVACIÓN DE GARANTÍA Y SOPORTE DE LA INFRAESTRUCTURA PASIVA DE CORPAC. Adicionalmente al objeto de la contratación de equipamiento, CORPAC S.A. requiere renovar la garantía y el soporte de algunos componentes de la infraestructura pasiva implementada que tenga la garantía vigente del fabricante.</p> <p>Consulta: Confirmar que los componentes del sistema de detección de incendio a renovar garantía tengan un programa de mantenimiento realizados durante los años de funcionamiento.</p>	Consulta de la empresa THINK NETWORKS PERU S.A.C
12	7	93	<p>Dice: PLAZO DE IMPLEMENTACIÓN ETAPA 1</p> <ul style="list-style-type: none"> • El plazo para la implementación de la presente contratación del Sistema de Networking (Infraestructura Activa), será de ciento cincuenta (50) días calendarios a partir del día siguiente de la fecha máxima del plazo de entrega de equipos. Este plazo incluye el suministro, instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), hasta que la solución funcione correctamente. 	Consulta de la empresa THINK NETWORKS PERU S.A.C

			<p>Observación:</p> <p>Debido a la envergadura del proyecto y la cantidad de equipos a ofertar, se solicita a la entidad que el tiempo de la etapa 1 sea de un plazo de setenta y cinco (75) días calendarios a partir del día siguiente de la fecha máxima del plazo de entrega de equipos. Este plazo incluye el suministro, instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), hasta que la solución funcione correctamente.</p>	
13	8	96	<p>Dice:</p> <p>PROFESIONAL RESIDENTE 1 PRESENCIAL (un personal por cada TURNO DE 8 HORAS totales 3)</p> <ul style="list-style-type: none"> Bachiller Universitario en Electrónica o Sistemas o Redes y Comunicaciones <p>Consulta:</p> <p>La inclusión de profesionales técnicos en el proceso ampliaría la participación de postores y personas con habilidades técnicas especializadas y experiencia práctica, por lo que se solicita a la entidad confirmar que apelando a la pluralidad de participación de postores, se aceptarán profesionales técnicos o bachiller en carreras afines como Computación e Informática y/o Informática y/o Electrónica y/o Redes y Comunicaciones de Datos y/o Ingeniería de Telemática y/o Red de Computadoras y Comunicación de Datos y/o Soporte y Mantenimiento de Equipos de Cómputo.</p>	<p>Consulta de la empresa THINK NETWORKS PERU S.A.C</p>
14	8	97	<p>Dice:</p> <p>PROFESIONAL RESIDENTE 2 PRESENCIAL (un personal por cada TURNO DE 8 HORAS total 3)</p> <ul style="list-style-type: none"> Bachiller Universitario en Electrónica o Sistemas o Redes y Comunicaciones <p>Consulta:</p> <p>La inclusión de profesionales técnicos en el proceso ampliaría la participación de postores y personas con habilidades técnicas especializadas y experiencia práctica, por lo que se solicita a la entidad confirmar que apelando a la pluralidad de participación de postores, se aceptarán profesionales técnicos o bachiller en carreras afines como Computación e Informática y/o Informática y/o Electrónica y/o Redes y Comunicaciones de Datos y/o Ingeniería de Telemática y/o Red de Computadoras y Comunicación de Datos y/o Soporte y Mantenimiento de Equipos de Cómputo.</p>	<p>Consulta de la empresa THINK NETWORKS PERU S.A.C</p>
15	5.2.2.1.1.1	14	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.1, se precisa lo siguiente:</p>	<p>Observación de la empresa IDELCOM S.A.C.</p>

			<p>(...) - El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean cómo un único switch desde una perspectiva lógica, manteniendo un único plano de control y gestión, mientras que el plano de datos o transmisión será de tipo distribuido y que garantice la alta disponibilidad en capa 2 y capa 3</p> <p>(...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>El uso de enlaces LACP, garantizando HA en capa 2 y capa 3, teniendo consideración lo siguiente:</p> <p>El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean cómo un único switch desde una perspectiva lógica para lograr agregar enlaces con LACP y garantizar HA en capa 2 y capa 3</p> <p>Todo ello, debido a que Cada fabricante tiene su procedimiento para habilitar esta funcionalidad, en tal sentido no pone en riesgo el objetivo de la contratación.</p>	
16	5.2.2.1.1.1	18	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.1, en el Apartado de Seguridad, se precisa lo siguiente:</p> <p>(...) - IEEE 802.1x suplicant(...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Que el cumplimiento de esta característica sea OPCIONAL, Teniendo en cuenta que dicha funcionalidad es aplicada en la capa de acceso, siendo una característica que defina el objetivo específico de la contratación.</p>	Observación de la empresa IDELCOM S.A.C.
17	5.2.2.1.1.2	20	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.2, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) Debe tener 32 puertos de red 40/100G (QSFP/QSFP28) como mínimo</p>	Observación de la empresa IDELCOM S.A.C.

			<p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se considere valido ofertar soluciones que se encuentren en el rango 20 puertos a más, teniendo en cuenta que con ello se cubre con más del mínimo necesario para la interconexión de nodos. Dado que dentro de uno de los objetivos de la contratación es la interconexión de como máximo de 18 nodos, resultando muy restrictivo solo solicitar 32 como mínimo.</p>	
18	5.2.2.1.1.2	20	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.2, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) Debe permitir no menos de 4096 VLAN IDs y soportar e implementar protocolo 802.1q (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>SE ACEPTEN RANGOS EN LA CANTIDAD DE VLAN IDS, no menor a 4000.</p> <p>O agregarle el conector Y/O no menos de 4094 VLAN ID y soportar e implementar protocolo 802.1q (...)</p>	Observación de la empresa IDELCOM S.A.C.
19	5.2.2.1.1.2	21	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.2, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión. (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se</p>	Consulta de la empresa IDELCOM S.A.C.

			<p>SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se acepte adicionalmente, funcionalidades como Control Plane Policing (CoPP) entre otras similares.</p>	
20	5.2.2.1.1.2	23	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) Deberá contar con mecanismo y/o función de seguridad que utilice una combinación de autenticación, criptografía y verificación de estado para asegurar que los dispositivos de la red puedan confiar en los mensajes de descubrimiento de vecinos IPv6 que se intercambian en la capa 2. (...)</p> <p>QUE, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes, en tal sentido consideramos muy restrictivo dicho requerimiento, con ello, vulnerando el principio de libre concurrencia</p>	Observación de la empresa IDELCOM S.A.C.
21	5.2.2.1.1.3	25	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES ACCESO – TIPO III, se precisa lo siguiente:</p> <p>(...) - El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal. (...)</p> <p>Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes.</p>	Observación de la empresa IDELCOM S.A.C.
22	5.2.2.1.1.3	25	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) El switch propuesto debe contar con al menos 48 puertos 10/100/1000 Base-T RJ45 con soporte PoE/PoE+, en todos sus puertos. (...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente que respecto al switch propuesto deba contar con al menos 48 puertos 100M//1G/2.5G/5G, Base-T RJ45 con soporte PoE/PoE+ en todos sus puertos, en el marco de los nuevos estándares.</p>	Consulta de la empresa IDELCOM S.A.C.

23	5.2.2.1.1.3	25	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) El switch propuesto debe contar con al menos 2 puertos 40GE de uplink. (...)</p> <p>En relación a ello, recomendamos como mejora y se acepte adicionalmente que respecto:</p> <p>PROPONER SOLUCIONES CON PUERTOS DE UPLINK A 50GE.</p>	Consulta de la empresa IDELCOM S.A.C.
24	5.2.2.1.1.3	26	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión. (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se acepte adicionalmente, funcionalidades como Control Plane Policing (CoPP) entre otras similares.</p>	Consulta de la empresa IDELCOM S.A.C.
25	5.2.2.1.1.3	26	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) El switch propuesto debe soportar puertos Uplinks Modulares o Fijos con opciones de tasas de transmisión de 10Gbps y 40 Gbps. (...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente: switches con uplink modulares o fijos con velocidad de transmisión de 10Gbps y 50 Gbps, en el marco de los nuevos estándares., y con el objetivo de garantizar una mayor velocidad en la transferencia de datos.</p>	Consulta de la empresa IDELCOM S.A.C.

26	5.2.2.1.1.3	26	<p>el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) Configuración automática de QoS. (...)</p> <p>Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes.</p>	Consulta de la empresa IDELCOM S.A.C.
27	5.2.2.1.1.3	26	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo. (...)</p> <p>Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes, considerándolo muy restrictivo dicho requerimiento, con ello, vulnerando el principio de libre competencia</p>	Consulta de la empresa IDELCOM S.A.C.
28	5.2.2.1.1.4	28	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal. (...)</p> <p>Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes, considerándolo muy restrictivo dicho requerimiento, con ello, vulnerando el principio de libre competencia</p>	Consulta de la empresa IDELCOM S.A.C.
29	5.2.2.1.1.4	28	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p>	Consulta de la empresa IDELCOM S.A.C.

			<p>(...) El switch propuesto debe contar con al menos 24 puertos 10/100/1000 Base-T RJ45 con soporte PoE/PoE+, en todos sus puertos. (...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente: 24 puertos 100M/1G/2.5G/5G, Base-T RJ45 con soporte PoE/PoE+ en todos sus puertos, en el marco de los nuevos estándares., y con el objetivo de su perdurabilidad en el tiempo y en el marco del principio de Vigencia Tecnológica.</p>	
30	5.2.2.1.1.4	28	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe contar con al menos 2 puertos 40GE de uplink. (...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente: soluciones con puertos de uplink a 50GE, en el marco de los nuevos estándares., y con el objetivo de su perdurabilidad en el tiempo y en el marco del principio de Vigencia Tecnológica.</p>	Consulta de la empresa IDELCOM S.A.C.
31	5.2.2.1.1.4	28	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) Debe incluir 2 transceivers de 40Gbps (SFP28) para fibra óptica monomodo 10Km (...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente: soluciones con puertos de 50Gbps(SFP28) para fibra óptica monomodo 10Km, en el marco de los nuevos estándares., y con el objetivo de su perdurabilidad en el tiempo y en el marco del principio de Vigencia Tecnológica.</p>	Consulta de la empresa IDELCOM S.A.C.
32	5.2.2.1.1.4	28	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking. (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se</p>	Consulta de la empresa IDELCOM S.A.C.

			<p>SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se permita adicionalmente, Utilizar puerto de uplink como puertos para stack es una tendencia que ya la tienen varios fabricantes.</p>	
33	5.2.2.1.1.4	29	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión. (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se acepte adicionalmente, funcionalidades como Control Plane Policing (CoPP) entre otras similares.</p>	Consulta de la empresa IDELCOM S.A.C.
34	5.2.2.1.1.4	29	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe soportar puertos Uplinks Modulares o Fijos con opciones de tasas de transmisión de 10Gbps y 40 Gbps. (...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente: soluciones de switches con uplink modulares o fijos con velocidad de transmisión de 10Gbps y 50 Gbps, y con el objetivo de su perdurabilidad en el tiempo y en el marco del principio de Vigencia Tecnológica.</p>	Consulta de la empresa IDELCOM S.A.C.
35	5.2.2.1.1.4	29	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) Configuración automática de QoS. (...)</p>	Consulta de la empresa IDELCOM S.A.C.

			Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes, considerándolo muy restrictivo dicho requerimiento, con ello, vulnerando el principio de libre competencia	
36	5.2.2.1.1.4	29	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo. (...)</p> <p>Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes, considerándolo muy restrictivo dicho requerimiento, con ello, vulnerando el principio de libre competencia</p>	Consulta de la empresa IDELCOM S.A.C.
37	5.2.2.1.1.5	31	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.5, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO V), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal. (...)</p> <p>Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes, considerándolo muy restrictivo dicho requerimiento, con ello, vulnerando el principio de libre competencia</p>	Consulta de la empresa IDELCOM S.A.C.
38	5.2.2.1.1.5	31	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.5, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO V), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe contar con al menos 2 puertos 40GE de uplink.(...)</p>	Consulta de la empresa IDELCOM S.A.C.

			En relación a ello, recomendamos como mejora o se acepte adicionalmente: soluciones con puertos de uplink a 50GE, y con el objetivo de su perdurabilidad en el tiempo y en el marco del principio de Vigencia Tecnológica.	
39	5.2.2.1.1.5	31	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.5, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO V), se precisa lo siguiente:</p> <p>(...) Debe incluir 2 transceivers de 40Gbps (SFP28) para fibra óptica monomodo 10Km (...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente: soluciones con puertos de 50Gbps(SFP28) para fibra óptica monomodo 10Km, y con el objetivo de su perdurabilidad en el tiempo y en el marco del principio de Vigencia Tecnológica.</p>	Consulta de la empresa IDELCOM S.A.C.
40	5.2.2.1.1.5	31	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.5, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO V), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking. (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se permita adicionalmente, Utilizar puerto de uplink como puertos para stack es una tendencia que ya la tienen varios fabricantes.</p>	Consulta de la empresa IDELCOM S.A.C.
41	8	95	<p>En relación a las características mínimas precisadas en el punto 8, en el Apartado de PERFIL DEL PERSONAL CLAVE, se precisa lo siguiente:</p> <p>(...) LÍDER DE NETWORKING LAN. Un (01) Ingeniero Electrónico o Sistemas o Telecomunicaciones, Titulado, Colegiado y habilitado, que acrediten como mínimo cinco (05) años de experiencia como arquitecto y/o líder técnico en plataformas de Networking LAN y WLAN. (...)</p> <p>Solicitamos tengan a bien aceptar adicionalmente los cargos de INGENIERO Y/O RESPONSABLE Y/O ESPECIALISTA en plataformas de Networking LAN y WLAN, toda vez que guardan relación directa con las funciones a desempeñar en el ámbito del cargo en mención, y con</p>	Consulta de la empresa IDELCOM S.A.C.

			<p>respecto al tiempo que se debe acreditar sea de (03) años de experiencia, a fin de ser congruente con los niveles de cada cargo, dado que el Jefe de Proyecto ya cuenta con (05) años.</p> <p>Todo ello, con la finalidad de promover la pluralidad de postores, y pluralidad de selección de profesionales para el equipo, todo ello, en el marco del principio de libre concurrencia.</p>	
42	8	95	<p>En relación a las características mínimas precisadas en el punto 8, en el Apartado de PERFIL DEL PERSONAL CLAVE - ESPECIALISTA EN CABLEADO ESTRUCTURADO., se precisa lo siguiente:</p> <p>(...) Certificado oficial o carta de fabricante de la solución de cableado estructurado de la plataforma a operar. (...)</p> <p>En tal sentido solicitamos que la acreditación de la Certificado oficial o carta de fabricante, se acepte el conector y/o de cualquier fabricante, puesto que la finalidad es que cuente con la acreditación y los conocimientos.</p>	Consulta de la empresa IDELCOM S.A.C.
43	8	96	<p>En relación a las características mínimas precisadas en el punto 8, en el Apartado de PERFIL DEL PERSONAL CLAVE - LÍDER DE NETWORKING LAN, se precisa lo siguiente:</p> <p>(...) El líder de networking implementador propuesto por el postor debe contar con certificaciones técnicas oficiales vigentes de nivel experto o avanzado en Enterprise o Datacom o Switching o Wireless de al menos dos (02) fabricantes reconocidos (incluyendo al fabricante de los equipos de networking propuestos). (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros postores, y con ello, vulnerando el principio de libre concurrencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Que debe con la certificación técnica vigente de nivel experto o avanzado en Enterprise o Datacom o Switching o Wireless solo del fabricante de los equipos propuestos; puesto que lo contrario evidencia un direccionamiento a un perfil en específico.</p>	Consulta de la empresa IDELCOM S.A.C.
44	8	96	<p>En relación a las características mínimas precisadas en el punto 8, en el Apartado de PERFIL DEL PERSONAL CLAVE - IMPLEMENTADOR DE NETWORKING LAN, se precisa lo siguiente:</p> <p>(...) El personal implementador propuesto por el postor debe contar con certificación técnica oficial vigente de nivel profesional en Enterprise o Switching o Datacom del fabricante propuesto, esta certificación que debe adjuntarse en copia simple en su propuesta. (...)</p>	Consulta de la empresa IDELCOM S.A.C.

			En tal sentido solicitamos que la acreditación de la certificación técnica oficial vigente de nivel profesional en Enterprise o Switching o Datacom se acepte el conector y/o de cualquier fabricante, puesto que la finalidad es que cuente con la acreditación y los conocimientos.	
45	8	96	<p>En relación a las características mínimas precisadas en el punto 8, en el Apartado de PERFIL DEL PERSONAL CLAVE - IMPLEMENTADOR DE NETWORKING WLAN, se precisa lo siguiente:</p> <p>(...) El personal implementador propuesto por el postor debe contar con certificación técnica oficial vigente de nivel profesional en Wireless del fabricante propuesto. Debe adjuntar dicha certificación en copia simple en su propuesta. (...)</p> <p>En tal sentido solicitamos que la acreditación de la certificación técnica oficial vigente de nivel profesional en Wireless, se acepte el conector y/o de cualquier fabricante, puesto que la finalidad es que cuente con la acreditación y los conocimientos.</p>	Consulta de la empresa IDELCOM S.A.C.
46	8	96	<p>En relación a las características mínimas precisadas en el punto 8, en el Apartado de PERFIL DEL PERSONAL CLAVE - PROFESIONAL RESIDENTE 1 PRESENCIAL, se precisa lo siguiente:</p> <p>(...) El personal para la operación propuesto por el postor debe tener como mínimo certificación en materia de switching y routing por parte del fabricante de los equipos de la solución; a nivel asociado, técnico, especialista o ingeniero de red (según la denominación propia del fabricante y demostrable según documentación del fabricante) y que se encuentre vigente durante toda la ejecución del servicio complementario.) (...)</p> <p>En tal sentido solicitamos que la acreditación de la en materia de switching y routing, se acepte adicionalmente el conector y/o de cualquier fabricante, puesto que la finalidad es que cuente con la acreditación y los conocimientos.</p>	Consulta de la empresa IDELCOM S.A.C.
47	7	94	<p>En relación a las características mínimas precisadas en el punto 7 exactamente en el Apartado de PLAZO DE ENTREGA, se precisa lo siguiente:</p> <p>(...)“El plazo para la Entrega de componentes del sistema de Networking (Infraestructura activa) y renovación de garantías de la infraestructura pasiva y activa de la Sede Central de CORPAC S.A. será máximo de sesenta (60) días calendarios, se contabilizará desde el día siguiente de la firma del contrato. (...)</p> <p>Solicitamos tenga a bien, consideren modificar los tiempos de entrega puesto que realmente si corresponde a una contratación sin</p>	Observación de la empresa IDELCOM S.A.C.

			direccionamiento, el plazo mínimo sería de 90 días calendario, por la envergadura y especificaciones del requerimiento, teniendo en cuenta que lo mencionado son tiempos establecidos en el mercado sujetos a la realidad.	
48	7	94	<p>Con respecto al Plazo de Implementación – ETAPA 1, se menciona lo siguiente:</p> <p>"El plazo para la implementación de la presente contratación del Sistema de Networking (Infraestructura Activa), será de ciento cincuenta (50) días calendarios a partir del día siguiente de la fecha máxima del plazo de entrega de equipos. Este plazo incluye el suministro, instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), hasta que la solución funcione correctamente."</p> <p>Se evidencia un ERROR MATERIAL en relación al plazo, existiendo divergencia entre lo mencionado en letras y lo precisado en números, en tal sentido solicito confirmar que debe ser CIENTO CINCUENTA (150).</p>	Observación de la empresa IDELCOM S.A.C.
49	5.2.2.1.1.2	20	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.5, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO V), se precisa lo siguiente:</p> <p>El switch deberá contar con CPU mínimo de 2.2 Ghz Consulta:</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre concurrencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se acepte adicionalmente, que el switch deberá contar con CPU mínimo de 1.8 GHz, sustentado en que la performance del switch no se mide por la velocidad del CPU s CPU TX en sus puerto y enlaces al CPU, sino por la velocidad de transmisión que soporta en sus puertos (throughput).</p>	Consulta de la empresa IDELCOM S.A.C.
50	5.2.2.1.1.1	16	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.1, en el Apartado de EQUIPOS DE COMUNICACIONES DE CORE (TIPO I), se precisa lo siguiente:</p> <p>(...) Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para (...)</p>	Observación de la empresa IDELCOM S.A.C.

			<p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se acepte adicionalmente, funcionalidades como Control Plane Policing (CoPP) entre otras similares.</p>	
51	5.2.2.1.1.2	20	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.1, en el Apartado de EQUIPOS DE COMUNICACIONES DE CORE (TIPO II), se precisa lo siguiente:</p> <p>(...) El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean cómo un único switch desde una perspectiva lógica, manteniendo un único plano de control y gestión, mientras que el plano de datos será de tipo distribuido y garantice la alta disponibilidad en capa 2 y capa 3. (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se acepte adicionalmente el uso de enlaces LACP, garantizando HA en capa 2 y capa 3. Considerando finalmente la siguiente especificación:</p> <p>el switch debe poseer tecnología de virtualización que permita que un par de equipos se vean cómo un único switch desde una perspectiva lógica para lograr agregar enlaces con LACP y garantizar HA en capa 2 y capa 3</p>	Consulta de la empresa IDELCOM S.A.C.
52	5.2.2.1.1.2	20	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.2, en el Apartado de EQUIPOS DE COMUNICACIONES DE CORE (TIPO II), se precisa lo siguiente:</p> <p>Debe tener 32 puertos de red 40/100G (QSFP/QSFP28) como mínimo</p> <p>Solicitamos se acepte adicionalmente soluciones que cuenten con puertos a velocidades de 50G, con la finalidad de incentivar la pluralidad de postores.</p>	Consulta de la empresa IDELCOM S.A.C.
	5.2.2.1.1.3	25	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DE 48 PUERTOS (TIPO III), se precisa lo siguiente:</p>	Consulta de la empresa IDELCOM S.A.C.

			<p>(...) Debe incluir 2 transceivers de 40Gbps (SFP28) para fibra óptica monomodo 10Km (...)</p> <p>Solicitamos se acepte adicionalmente soluciones con puertos de 50Gbps(SFP28) para fibra óptica monomodo 10Km, con la finalidad de incentivar la pluralidad de postores.</p>	
53	5.2.2.1.1.3	25	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DE 48 PUERTOS (TIPO III), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking. (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se permita adicionalmente, Utilizar puerto de uplink como puertos para stack es una tendencia que ya la tienen varios fabricantes</p>	<p>Consulta de la empresa IDELCOM S.A.C.</p>

ANEXO D.1

ABSOLUCION A LAS CONSULTAS Y/U OBSERVACIONES DEL ANEXO D

N° de orden	Términos de Referencia o Especificaciones Técnicas o Requisitos de calificación		Consulta y/u Observación	Corresponde a consulta y/u observación del OEC o de las empresas invitadas en la indagación de mercado	Análisis respecto de la consulta u observación. (Precisar si se acoge o no se acoge. En caso de no acoger sustentar los motivos)	Precisión de aquello que se incorporará en los TDR o EEETT o Requisitos de calificación, de corresponder
	Numeral	Pág.				
1	5.1	8	<p>En el cuadro de nuevas ubicaciones se menciona estos 3 nodos de comunicación (Nueva Torre piso10, Edificio Auxiliar, Radar Gambeta,</p> <p>Consulta Que se debe considerar en estos ambientes</p>	Consulta de la empresa TIFA SERVICIOS Y TECNOLOGÍA DE LA INFORMACIÓN SAC.	Se debe considerar para estos 3 ambientes el despliegue de la fibra óptica principal y contingencia, y todo lo referente para el sistema administrable del cableado en dichas ubicaciones, para albergar equipamiento LAN.	
2	5.2.1	11	<p>En el cuadro de equipamiento que adjuntan se menciona que tienen equipamiento de telefonía IP cisco</p> <p>Este equipamiento también será parte de la gestión y soporte</p>	Consulta de la empresa TIFA SERVICIOS Y TECNOLOGÍA DE LA INFORMACIÓN SAC.	<p>Dado que serán reemplazados por equipamiento de networking de la presente contratación, este nuevo equipamiento será parte de la gestión y soporte.</p> <p>En cuanto a equipamiento como el de Telefonía IP este cuenta con su propia gestión y soporte, bajo otro contrato y proveedor.</p>	

Fecha: 26/08/2024

3	5.2.2.1.1.1	14	<p>Se solicita que el switch deberá contar con CPU mínimo de 2.2 Ghz</p> <p>Se podría considerar que el equipamiento sea de 1.6 Ghz y prestaciones mayores en RAM y SSD</p>	Consulta de la empresa TIFA SERVICIOS Y TECNOLOGÍA DE LA INFORMACIÓN SAC.	Se aclara que, con el fin de tener mayor pluralidad de postores, se permitirá una frecuencia de CPU de uno o más cores de 1.4 GHz.	El switch deberá contar con CPU mínimo de 1.4 Ghz de uno o mas cores.
4	5.3	54	<p>Se solicita lo siguiente: Retiro del cableado de comunicaciones que está actualmente instalado en desuso y/o antiguo en CORPAC Lima-Callao, esto aplica solo para el caso de instalaciones de puntos nuevos de cableado, en los cuales exista cableado existente.</p> <p>Consulta: aparte del cable el cual está en funcionamiento existe cableado antiguo a indicado, de ser así de que cantidad, cual es la cantidad a retirar ya que esto puede impactar en los tiempos</p>	Consulta de la empresa GRUPO INGECORP S.A.C.	Se precisa que el presente requerimiento para el retiro solo aplica a aquellos puntos de red nuevos por implementar y que se estén en funcionamiento con cableado antiguo por reemplazar.	
5	5.3.1.4	72	<p>Se solicita la implementación de Sistema de control de Acceso.</p> <p>Se puede proponer equipos con mejoras tecnológicas ¿Como por ejemplo con reconocimiento facial), aparte de los convencionales que es Biométrico, Clave o Tarjeta, se podría considerar como por ejemplo que la persona que quiere ingresar muestre su rostro ante la cámara del control de acceso y lo Valide la cámara del sistema de CCTV a implementar en cada Nodo de comunicación</p>	Consulta de la empresa TIFA SERVICIOS Y TECNOLOGÍA DE LA INFORMACIÓN SAC.	Las especificaciones técnicas en el presente son requerimientos mínimos; el proveedor podrá proponer mejoras tecnológicas que cumplan el mínimo solicitado y las supere.	
6	5	8	<p>Dice: ALCANCE Y DESCRIPCIÓN DE LA CONTRATACIÓN 5.1 ALCANCE • Para estos nuevos nodos se deberá de considerar el cableado de fibra óptica, se muestra una figura 1 de la ubicación y conexión de cada uno de los NODOS LAN a implementar como referencia</p> <p>Consulta: Confirmar si los enlaces de fibra requieren de canalización y de cuantos metros serian.</p>	Consulta de la empresa THINK NETWORKS PERU S.A.C	<p>Las ducterías para el despliegue de la Fibra óptica outdoor son provistas por CORPAC, la canalización indoor será implementada por el proveedor para esta contratación.</p> <p>Para ello pueden realizar la visita de campo para su correcto dimensionamiento.</p>	
7	5.3	83	<p>Dice: RENOVACIÓN DE GARANTIA Y SOPORTE DE LA INFRAESTRUCTURA PASIVA DE CORPAC. • Adicionalmente al objeto de la contratación de equipamiento, CORPAC S.A. requiere renovar la garantía y el soporte de algunos componentes de la infraestructura pasiva implementada que tenga la garantía vigente del fabricante.</p> <p>Consulta: Confirmar que los componentes de administración de cableado a renovar la garantía tengan un programa de mantenimiento realizados durante los años de funcionamiento.</p>	Consulta de la empresa THINK NETWORKS PERU S.A.C	No se confirma, el proveedor debe considerar lo necesario para contar con la renovación de la garantía y/o soporte.	

8	5.3	84	<p>Dice: RENOVACIÓN DE GARANTÍA Y SOPORTE DE LA INFRAESTRUCTURA PASIVA DE CORPAC.</p> <p>• Adicionalmente al objeto de la contratación de equipamiento, CORPAC S.A. requiere renovar la garantía y el soporte de algunos componentes de la infraestructura pasiva implementada que tenga la garantía vigente del fabricante.</p> <p>Consulta: Confirmar que los componentes de transformadores de aislamiento a renovar garantía tengan un programa de mantenimiento realizados durante los años de funcionamiento.</p>	Consulta de la empresa THINK NETWORKS PERU S.A.C	No se confirma, el proveedor debe considerar lo necesario para contar con la renovación de la garantía y/o soporte.	
9	5.3	84-85	<p>Dice: RENOVACIÓN DE GARANTÍA Y SOPORTE DE LA INFRAESTRUCTURA PASIVA DE CORPAC.</p> <p>Adicionalmente al objeto de la contratación de equipamiento, CORPAC S.A. requiere renovar la garantía y el soporte de algunos componentes de la infraestructura pasiva implementada que tenga la garantía vigente del fabricante.</p> <p>Consulta: Confirmar que los componentes del sistema de climatización de precisión a renovar garantía tengan un programa de mantenimiento realizados durante los años de funcionamiento</p>	Consulta de la empresa THINK NETWORKS PERU S.A.C	No se confirma, el proveedor debe considerar lo necesario para contar con la renovación de la garantía y soporte.	
10	5.3	86-87	<p>Dice: RENOVACIÓN DE GARANTÍA Y SOPORTE DE LA INFRAESTRUCTURA PASIVA DE CORPAC.</p> <p>Adicionalmente al objeto de la contratación de equipamiento, CORPAC S.A. requiere renovar la garantía y el soporte de algunos componentes de la infraestructura pasiva implementada que tenga la garantía vigente del fabricante.</p> <p>Consulta: Confirmar que los componentes del sistema de procesamiento y control de puertas a renovar garantía tengan un programa de mantenimiento realizados durante los años de funcionamiento</p>	Consulta de la empresa THINK NETWORKS PERU S.A.C	No se confirma, el proveedor debe considerar lo necesario para contar con la renovación de la garantía y/o soporte.	
11	5.3	86-87	<p>Dice: RENOVACIÓN DE GARANTÍA Y SOPORTE DE LA INFRAESTRUCTURA PASIVA DE CORPAC.</p> <p>Adicionalmente al objeto de la contratación de equipamiento, CORPAC S.A. requiere renovar la garantía y el soporte de algunos componentes de la infraestructura pasiva implementada que tenga la garantía vigente del fabricante.</p> <p>Consulta:</p>	Consulta de la empresa THINK NETWORKS PERU S.A.C	No se confirma, el proveedor debe considerar lo necesario para contar con la renovación de la garantía y/o soporte.	

			Confirmar que los componentes del sistema de detección de incendio a renovar garantía tengan un programa de mantenimiento realizados durante los años de funcionamiento.			
12	7	93	<p>Dice: PLAZO DE IMPLEMENTACIÓN ETAPA 1</p> <ul style="list-style-type: none"> El plazo para la implementación de la presente contratación del Sistema de Networking (Infraestructura Activa), será de ciento cincuenta (50) días calendarios a partir del día siguiente de la fecha máxima del plazo de entrega de equipos. Este plazo incluye el suministro, instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), hasta que la solución funcione correctamente. <p>Observación: Debido a la envergadura del proyecto y la cantidad de equipos a ofertar, se solicita a la entidad que el tiempo de la etapa 1 sea de un plazo de setenta y cinco (75) días calendarios a partir del día siguiente de la fecha máxima del plazo de entrega de equipos. Este plazo incluye el suministro, instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), hasta que la solución funcione correctamente.</p>	Consulta de la empresa THINK NETWORKS PERU S.A.C	No se acoge la observación. Los tiempos definidos para las etapas son los que figuran en el requerimiento a necesidad de la entidad.	
13	8	96	<p>Dice: PROFESIONAL RESIDENTE 1 PRESENCIAL (un personal por cada TURNO DE 8 HORAS totales 3)</p> <ul style="list-style-type: none"> Bachiller Universitario en Electrónica o Sistemas o Redes y Comunicaciones <p>Consulta: La inclusión de profesionales técnicos en el proceso ampliaría la participación de postores y personas con habilidades técnicas especializadas y experiencia práctica, por lo que se solicita a la entidad confirmar que apelando a la pluralidad de participación de postores, se aceptarán profesionales técnicos o bachiller en carreras afines como Computación e Informática y/o Informática y/o Electrónica y/o Redes y Comunicaciones de Datos y/o Ingeniería de Telemática y/o Red de Computadoras y Comunicación de Datos y/o Soporte y Mantenimiento de Equipos de Cómputo.</p>	Consulta de la empresa THINK NETWORKS PERU S.A.C	Se acoge la consulta parcialmente, para ampliar la participación de postores; el bachiller universitario podrá ser de carreras afines como: Electrónica o Sistemas o Redes y Comunicaciones o Informática o Telecomunicaciones.	Bachiller Universitario en Electrónica o Sistemas o Redes y Comunicaciones o Informática o Telecomunicaciones.
14	8	97	<p>Dice: PROFESIONAL RESIDENTE 2 PRESENCIAL (un personal por cada TURNO DE 8 HORAS total 3)</p> <ul style="list-style-type: none"> Bachiller Universitario en Electrónica o Sistemas o Redes y Comunicaciones <p>Consulta:</p>	Consulta de la empresa THINK NETWORKS PERU S.A.C	Se acoge la consulta parcialmente, para ampliar la participación de postores; el bachiller universitario podrá ser de carreras afines como: Electrónica o Sistemas o	Bachiller Universitario en Electrónica o Sistemas o Redes y Comunicaciones o Informática o Telecomunicaciones.

			La inclusión de profesionales técnicos en el proceso ampliaría la participación de postores y personas con habilidades técnicas especializadas y experiencia práctica, por lo que se solicita a la entidad confirmar que apelando a la pluralidad de participación de postores, se aceptarán profesionales técnicos o bachiller en carreras afines como Computación e Informática y/o Informática y/o Electrónica y/o Redes y Comunicaciones de Datos y/o Ingeniería de Telemática y/o Red de Computadoras y Comunicación de Datos y/o Soporte y Mantenimiento de Equipos de Cómputo.		Redes y Comunicaciones o Informática o Telecomunicaciones.	
15	5.2.2.1.1.1	14	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.1, se precisa lo siguiente:</p> <p>(...) - El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean cómo un único switch desde una perspectiva lógica, manteniendo un único plano de control y gestión, mientras que el plano de datos o transmisión será de tipo distribuido y que garantice la alta disponibilidad en capa 2 y capa 3 (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>El uso de enlaces LACP, garantizando HA en capa 2 y capa 3, teniendo consideración lo siguiente:</p> <p>El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean cómo un único switch desde una perspectiva lógica para lograr agregar enlaces con LACP y garantizar HA en capa 2 y capa 3</p> <p>Todo ello, debido a que Cada fabricante tiene su procedimiento para habilitar esta funcionalidad, en tal sentido no pone en riesgo el objetivo de la contratación.</p>	Observación de la empresa IDELCOM S.A.C.	<p>No se confirma. Sin embargo, con el fin de permitir mayor pluralidad de postores también se aceptará para la tecnología de virtualización que el plano de control y gestión también sean distribuidos.</p>	<p>El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean cómo un único switch desde una perspectiva lógica, manteniendo un único plano de control y gestión, mientras que el plano de datos o transmisión será de tipo distribuido y que garantice la alta disponibilidad en capa 2 y capa 3. También se aceptará para la tecnología de virtualización que el plano de control y gestión también sean distribuidos.</p>
16	5.2.2.1.1.1	18	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.1, en el Apartado de Seguridad, se precisa lo siguiente:</p> <p>(...) - IEEE 802.1x suplicant(...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se</p>	Observación de la empresa IDELCOM S.A.C.	Se acoge la observación.	Opcionalmente, IEEE 802.1x suplicant

			<p>SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Que el cumplimiento de esta característica sea OPCIONAL, Teniendo en cuenta que dicha funcionalidad es aplicada en la capa de acceso, siendo una característica que defina el objetivo específico de la contratación.</p>			
17	5.2.2.1.1.2	20	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.2, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) Debe tener 32 puertos de red 40/100G (QSFP/QSFP28) como mínimo</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se considere valido ofertar soluciones que se encuentren en el rango 20 puertos a más, teniendo en cuenta que con ello se cubre con más del mínimo necesario para la interconexión de nodos. Dado que dentro de uno de los objetivos de la contratación es la interconexión de como máximo de 18 nodos, resultando muy restrictivo solo solicitar 32 como mínimo.</p>	Observación de la empresa IDELCOM S.A.C.	Es un requerimiento de la Entidad contar con un equipo de 32 puertos para crecimiento futuro. Se precisa que actualmente se tiene en porcentaje de ocupación y utilización del 59% de puertos sin implementar nuevos nodos; y sin porcentaje de crecimiento.	
18	5.2.2.1.1.2	20	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.2, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) Debe permitir no menos de 4096 VLAN IDs y soportar e implementar protocolo 802.1q (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>SE ACEPTEN RANGOS EN LA CANTIDAD DE VLAN IDS, no menor a 4000.</p> <p>O agregarle el conector Y/O no menos de 4094 VLAN ID y soportar e implementar protocolo 802.1q (...)</p>	Observación de la empresa IDELCOM S.A.C.	Se confirma que para equipo de Tipo II se aceptaran rango no menos de 4000	Debe permitir no menos de 4000 VLAN IDs y soportar e implementar protocolo 802.1q.

19	5.2.2.1.1.2	21	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.2, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión. (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se acepte adicionalmente, funcionalidades como Control Plane Policing (CoPP) entre otras similares.</p>	<p>Consulta de la empresa IDELCOM S.A.C.</p>	<p>Se confirma.</p> <p>Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.</p>	<p>Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.</p>
20	5.2.2.1.1.2	23	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) Deberá contar con mecanismo y/o función de seguridad que utilice una combinación de autenticación, criptografía y verificación de estado para asegurar que los dispositivos de la red puedan confiar en los mensajes de descubrimiento de vecinos IPv6 que se intercambian en la capa 2. (...)</p> <p>QUE, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes, en tal sentido consideramos muy restrictivo dicho requerimiento, con ello, vulnerando el principio de libre competencia</p>	<p>Observación de la empresa IDELCOM S.A.C.</p>	<p>No se confirma. El aseguramiento del vecino en IPv6 es una funcionalidad estándar de la industria.</p>	
21	5.2.2.1.1.3	25	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES ACCESO – TIPO III, se precisa lo siguiente:</p> <p>(...) - El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal. (...)</p>	<p>Observación de la empresa IDELCOM S.A.C.</p>	<p>Se reformula requerimiento de la siguiente manera:</p> <p>El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.</p>	<p>El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.</p>

			Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes.			
22	5.2.2.1.1.3	25	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) El switch propuesto debe contar con al menos 48 puertos 10/100/1000 Base-T RJ45 con soporte PoE/PoE+, en todos sus puertos. (...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente que respecto al switch propuesto deba contar con al menos 48 puertos 100M//1G/2.5G/5G, Base-T RJ45 con soporte PoE/PoE+ en todos sus puertos, en el marco de los nuevos estándares.</p>	Consulta de la empresa IDELCOM S.A.C.	<p>De la revisión en la sección 5.2.2.1.1.3 se solicita equipamiento del TIPO III.</p> <p>Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento.</p> <p>Por otro lado, de la revisión, de esta característica para que tenga congruencia el requerimiento se actualiza el soporte de PoE/PoE+/PoE++, dado que los puertos solicitados debe cumplir con el soporte y habilitado de 60W de potencia; por lo que se actualiza el requerimiento, en ese extremo</p>	<p>La Red LAN propuesta debe soportar y tener habilitados 802.11ac Wave 2, 802.11ax y 802.11be para sus aplicaciones WLAN.</p> <p>El switch propuesto debe contar con al menos 48 puertos 10/100/1000 Base-T RJ45 con soporte PoE/PoE+/PoE++, en todos sus puertos.</p>
23	5.2.2.1.1.3	25	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) El switch propuesto debe contar con al menos 2 puertos 40GE de uplink. (...)</p> <p>En relación a ello, recomendamos como mejora y se acepte adicionalmente que respecto:</p> <p>PROPONER SOLUCIONES CON PUERTOS DE UPLINK A 50GE.</p>	Consulta de la empresa IDELCOM S.A.C.	<p>Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.</p>	
24	5.2.2.1.1.3	26	En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:	Consulta de la empresa IDELCOM S.A.C.	<p>Se confirma.</p> <p>Adicionalmente, se aceptará funcionalidades como</p>	Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.

			<p>(...) Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión. (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se acepte adicionalmente, funcionalidades como Control Plane Policing (CoPP) entre otras similares.</p>		políticas de CoPP o similares o equivalentes.	
25	5.2.2.1.1.3	26	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) El switch propuesto debe soportar puertos Uplinks Modulares o Fijos con opciones de tasas de transmisión de 10Gbps y 40 Gbps. (...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente: switches con uplink modulares o fijos con velocidad de transmisión de 10Gbps y 50 Gbps, en el marco de los nuevos estándares., y con el objetivo de garantizar una mayor velocidad en la transferencia de datos.</p>	Consulta de la empresa IDELCOM S.A.C.	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
26	5.2.2.1.1.3	26	<p>el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p> <p>(...) Configuración automática de QoS. (...)</p> <p>Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes.</p>	Consulta de la empresa IDELCOM S.A.C.	Sera opcional.	Opcionalmente, configuración automática de QoS.
27	5.2.2.1.1.3	26	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DISTRIBUCIÓN – TIPO II, se precisa lo siguiente:</p>	Consulta de la empresa IDELCOM S.A.C.	Precisar que de la revisión de esta sección 5.2.2.1.1.3 corresponde a Equipos Tipo III.	El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) o QR o Código de Barra, ya sea interna o externa para la fácil identificación del equipo. Este elemento puede

			<p>(...) El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo. (...)</p> <p>Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes, considerándolo muy restrictivo dicho requerimiento, con ello, vulnerando el principio de libre concurrencia</p>		<p>Con Relación a esta etiqueta RFID que es requerida para identificación de los equipos que serán implementados en cada nodo LAN, se reformula el requerimiento para que su cumplimiento pueda ser también con código de barras o QR.</p> <p>El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) o QR o Código de Barra, ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo</p>	<p>ser externo y no necesariamente del mismo fabricante del equipo</p>
28	5.2.2.1.1.4	28	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal. (...)</p> <p>Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes, considerándolo muy restrictivo dicho requerimiento, con ello, vulnerando el principio de libre concurrencia</p>	<p>Consulta de la empresa IDELCOM S.A.C.</p>	<p>Se reformula requerimiento de la siguiente manera:</p> <p>El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.</p>	<p>El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.</p>
29	5.2.2.1.1.4	28	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe contar con al menos 24 puertos 10/100/1000 Base-T RJ45 con soporte PoE/PoE+, en todos sus puertos. (...)</p>	<p>Consulta de la empresa IDELCOM S.A.C.</p>	<p>Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento.</p> <p>Por otro lado, de la revisión, de esta característica para que tenga congruencia el requerimiento se actualiza el</p>	<p>La Red LAN propuesta debe soportar y tener habilitados 802.11ac Wave 2, 802.11ax y 802.11be para sus aplicaciones WLAN.</p> <p>El switch propuesto debe contar con al menos 24 puertos 10/100/1000 Base-T RJ45 con</p>

			En relación a ello, recomendamos como mejora o se acepte adicionalmente: 24 puertos 100M/1G/2.5G/5G, Base-T RJ45 con soporte PoE/PoE+ en todos sus puertos, en el marco de los nuevos estándares., y con el objetivo de su perdurabilidad en el tiempo y en el marco del principio de Vigencia Tecnológica.		soporte de PoE/PoE+/PoE++, dado que los puertos solicitados deben cumplir con el soporte y habilitados de 60W de potencia; por lo que se actualiza el requerimiento, en ese extremo	soporte PoE/PoE+/PoE++, en todos sus puertos.
30	5.2.2.1.1.4	28	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe contar con al menos 2 puertos 40GE de uplink. (...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente: soluciones con puertos de uplink a 50GE, en el marco de los nuevos estándares., y con el objetivo de su perdurabilidad en el tiempo y en el marco del principio de Vigencia Tecnológica.</p>	Consulta de la empresa IDELCOM S.A.C.	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
31	5.2.2.1.1.4	28	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) Debe incluir 2 transceivers de 40Gbps (SFP28) para fibra óptica monomodo 10Km (...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente: soluciones con puertos de 50Gbps(SFP28) para fibra óptica monomodo 10Km, en el marco de los nuevos estándares., y con el objetivo de su perdurabilidad en el tiempo y en el marco del principio de Vigencia Tecnológica.</p>	Consulta de la empresa IDELCOM S.A.C.	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
32	5.2.2.1.1.4	28	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking. (...)</p>	Consulta de la empresa IDELCOM S.A.C.	<p>Con la finalidad de ampliar la participación de postores, se reformula el requerimiento:</p> <p>El switch propuesto debe soportar apilamiento y la formación de stacks entre</p>	El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking o puertos de uplinks/servicios adicionales para stacking.

			<p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se permita adicionalmente, Utilizar puerto de uplink como puertos para stack es una tendencia que ya la tienen varios fabricantes.</p>		ellos utilizando puertos dedicados a Stacking o puertos de uplinks/servicios adicionales para stacking.	
33	5.2.2.1.1.4	29	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para mantener el flujo del tráfico del plano de datos, vigilando del plano de control, reforzando la seguridad en el equipo del tráfico innecesario o DoS y al priorizando al tráfico importante del plano de control y de gestión. (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se acepte adicionalmente, funcionalidades como Control Plane Policing (CoPP) entre otras similares.</p>	Consulta de la empresa IDELCOM S.A.C.	<p>Se confirma.</p> <p>Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.</p>	Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.
34	5.2.2.1.1.4	29	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe soportar puertos Uplinks Modulares o Fijos con opciones de tasas de transmisión de 10Gbps y 40 Gbps. (...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente: soluciones de switches con uplink modulares o fijos con velocidad de transmisión de 10Gbps y 50 Gbps, y con el objetivo de su perdurabilidad en el tiempo y en el marco del principio de Vigencia Tecnológica.</p>	Consulta de la empresa IDELCOM S.A.C.	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	

35	5.2.2.1.1.4	29	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) Configuración automática de QoS. (...)</p> <p>Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes, considerándolo muy restrictivo dicho requerimiento, con ello, vulnerando el principio de libre concurrencia</p>	Consulta de la empresa IDELCOM S.A.C.	Sera Opcional.	Opcionalmente, configuración automática de QoS.
36	5.2.2.1.1.4	29	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.4, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO IV), se precisa lo siguiente:</p> <p>(...) El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo. (...)</p> <p>Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por lo que el direccionamiento impide la participación de otros fabricantes, considerándolo muy restrictivo dicho requerimiento, con ello, vulnerando el principio de libre concurrencia</p>	Consulta de la empresa IDELCOM S.A.C.	<p>Con Relación a esta etiqueta RFID que es requerida para identificación de los equipos que serán implementados en cada nodo LAN, se reformula el requerimiento para que su cumplimiento pueda ser también con código de barras o QR.</p> <p>El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) o QR o Código de Barra, ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo</p>	El switch propuesto deberá incluir una etiqueta RFID (RFID Tag) o QR o Código de Barra, ya sea interna o externa para la fácil identificación del equipo. Este elemento puede ser externo y no necesariamente del mismo fabricante del equipo
37	5.2.2.1.1.5	31	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.5, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO V), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe asegurar máxima flexibilidad y aislamiento del sistema operativo principal. (...)</p> <p>Solicitamos, QUÉ, El cumplimiento de esta característica sea OPCIONAL, debido al análisis realizado en el mercado, dicha CARACTERISTICA es EXCLUSIVAMENTE DE UN FABRICANTE, por</p>	Consulta de la empresa IDELCOM S.A.C.	<p>Se reformula requerimiento de la siguiente manera:</p> <p>El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.</p>	El switch propuesto debe asegurar máxima flexibilidad del sistema operativo.

			lo que el direccionamiento impide la participación de otros fabricantes, considerándolo muy restrictivo dicho requerimiento, con ello, vulnerando el principio de libre competencia			
38	5.2.2.1.1.5	31	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.5, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO V), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe contar con al menos 2 puertos 40GE de uplink.(...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente: soluciones con puertos de uplink a 50GE, y con el objetivo de su perdurabilidad en el tiempo y en el marco del principio de Vigencia Tecnológica.</p>	Consulta de la empresa IDELCOM S.A.C.	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
39	5.2.2.1.1.5	31	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.5, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO V), se precisa lo siguiente:</p> <p>(...) Debe incluir 2 transceivers de 40Gbps (SFP28) para fibra óptica monomodo 10Km (...)</p> <p>En relación a ello, recomendamos como mejora o se acepte adicionalmente: soluciones con puertos de 50Gbps(SFP28) para fibra óptica monomodo 10Km, y con el objetivo de su perdurabilidad en el tiempo y en el marco del principio de Vigencia Tecnológica.</p>	Consulta de la empresa IDELCOM S.A.C.	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
40	5.2.2.1.1.5	31	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.5, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO V), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking. (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p>	Consulta de la empresa IDELCOM S.A.C.	<p>Con la finalidad de ampliar la participación de postores, se reformula el requerimiento:</p> <p>El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking o puertos de uplinks/servicios adicionales para stacking.</p>	El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking o puertos de uplinks/servicios adicionales para stacking.

			Se permita adicionalmente, Utilizar puerto de uplink como puertos para stack es una tendencia que ya la tienen varios fabricantes.			
41	8	95	<p>En relación a las características mínimas precisadas en el punto 8, en el Apartado de PERFIL DEL PERSONAL CLAVE, se precisa lo siguiente:</p> <p>(...) LÍDER DE NETWORKING LAN. Un (01) Ingeniero Electrónico o Sistemas o Telecomunicaciones, Titulado, Colegiado y habilitado, que acrediten como mínimo cinco (05) años de experiencia como arquitecto y/o líder técnico en plataformas de Networking LAN y WLAN. (...)</p> <p>Solicitamos tengan a bien aceptar adicionalmente los cargos de INGENIERO Y/O RESPONSABLE Y/O ESPECIALISTA en plataformas de Networking LAN y WLAN, toda vez que guardan relación directa con las funciones a desempeñar en el ámbito del cargo en mención, y con respecto al tiempo que se debe acreditar sea de (03) años de experiencia, a fin de ser congruente con los niveles de cada cargo, dado que el Jefe de Proyecto ya cuenta con (05) años.</p> <p>Todo ello, con la finalidad de promover la pluralidad de postores, y pluralidad de selección de profesionales para el equipo, todo ello, en el marco del principio de libre concurrencia.</p>	Consulta de la empresa IDELCOM S.A.C.	Se acoge parcialmente la consulta para el líder técnico; dado que principalmente se requiere expertiz por el nivel de proyecto a implementar la experiencia en años es la requerida. Con relación a la denominación en la experiencia en plataforma de Networking LAN y WLAN se realiza la actualización.	Un (01) Ingeniero Electrónico o Sistemas o Telecomunicaciones, Titulado, Colegiado y habilitado, que acrediten como mínimo cinco (05) años de experiencia como arquitecto y/o líder técnico y/o Responsable y/o Especialista y/o Ingeniero en Networking o en Plataformas de Networking LAN y WLAN.
42	8	95	<p>En relación a las características mínimas precisadas en el punto 8, en el Apartado de PERFIL DEL PERSONAL CLAVE - ESPECIALISTA EN CABLEADO ESTRUCTURADO., se precisa lo siguiente:</p> <p>(...) Certificado oficial o carta de fabricante de la solución de cableado estructurado de la plataforma a operar. (...)</p> <p>En tal sentido solicitamos que la acreditación de la Certificado oficial o carta de fabricante, se acepte el conector y/o de cualquier fabricante, puesto que la finalidad es que cuente con la acreditación y los conocimientos.</p>	Consulta de la empresa IDELCOM S.A.C.	No se confirma, dado que es una solución administrable se requiere especialista del cableado estructurado a operar; por ende, el certificado oficial o carta de fabricante de la plataforma a operar.	
43	8	96	<p>En relación a las características mínimas precisadas en el punto 8, en el Apartado de PERFIL DEL PERSONAL CLAVE - LÍDER DE NETWORKING LAN, se precisa lo siguiente:</p> <p>(...) El líder de networking implementador propuesto por el postor debe contar con certificaciones técnicas oficiales vigentes de nivel experto o avanzado en Enterprise o Datacom o Switching o Wireless de al menos dos (02) fabricantes reconocidos (incluyendo al fabricante de los equipos de networking propuestos). (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros postores, y con ello, vulnerando el principio de libre concurrencia, es por ello, es que se SOLICITA TENGA</p>	Consulta de la empresa IDELCOM S.A.C.	Dado que basado en lo acontecido en el servicio que actualmente se cuenta en CORPAC con relación a la RED LAN, se ha visto por necesario contar con el personal clave líder de networking y que cuenta con el expertiz requerido para la correcta transición desde una plataforma que viene operando en el Aeropuerto y	

			<p>A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Que debe con la certificación técnica vigente de nivel experto o avanzado en Enterprise o Datacom o Switching o Wireless solo del fabricante de los equipos propuestos; puesto que lo contrario evidencia un direccionamiento a un perfil en específico.</p>		que realice la migración en paralelo a los nuevos equipos propuestos.	
44	8	96	<p>En relación a las características mínimas precisadas en el punto 8, en el Apartado de PERFIL DEL PERSONAL CLAVE - IMPLEMENTADOR DE NETWORKING LAN, se precisa lo siguiente:</p> <p>(...) El personal implementador propuesto por el postor debe contar con certificación técnica oficial vigente de nivel profesional en Enterprise o Switching o Datacom del fabricante propuesto, esta certificación que debe adjuntarse en copia simple en su propuesta. (...)</p> <p>En tal sentido solicitamos que la acreditación de la certificación técnica oficial vigente de nivel profesional en Enterprise o Switching o Datacom se acepte el conector y/o de cualquier fabricante, puesto que la finalidad es que cuente con la acreditación y los conocimientos.</p>	Consulta de la empresa IDELCOM S.A.C.	No se acoge la consulta, el personal Implementador de Networking LAN debe contar con la acreditación respectiva del fabricante de los equipos propuestos.	
45	8	96	<p>En relación a las características mínimas precisadas en el punto 8, en el Apartado de PERFIL DEL PERSONAL CLAVE - IMPLEMENTADOR DE NETWORKING WLAN, se precisa lo siguiente:</p> <p>(...) El personal implementador propuesto por el postor debe contar con certificación técnica oficial vigente de nivel profesional en Wireless del fabricante propuesto. Debe adjuntar dicha certificación en copia simple en su propuesta. (...)</p> <p>En tal sentido solicitamos que la acreditación de la certificación técnica oficial vigente de nivel profesional en Wireless, se acepte el conector y/o de cualquier fabricante, puesto que la finalidad es que cuente con la acreditación y los conocimientos.</p>	Consulta de la empresa IDELCOM S.A.C.	No se acoge la consulta, el personal Implementador de Networking WLAN debe contar con la acreditación respectiva del fabricante de los equipos propuestos.	
46	8	96	<p>En relación a las características mínimas precisadas en el punto 8, en el Apartado de PERFIL DEL PERSONAL CLAVE - PROFESIONAL RESIDENTE 1 PRESENCIAL, se precisa lo siguiente:</p> <p>(...) El personal para la operación propuesto por el postor debe tener como mínimo certificación en materia de switching y routing por parte del fabricante de los equipos de la solución; a nivel asociado, técnico, especialista o ingeniero de red (según la denominación propia del fabricante y demostrable según documentación del fabricante) y que se encuentre vigente durante toda la ejecución del servicio complementario.) (...)</p>	Consulta de la empresa IDELCOM S.A.C.	No se acoge la consulta, el personal Profesional Residente 1 Presencial, debe contar con la acreditación respectiva del fabricante de los equipos propuestos.	

			En tal sentido solicitamos que la acreditación de la en materia de switching y routing, se acepte adicionalmente el conector y/o de cualquier fabricante, puesto que la finalidad es que cuente con la acreditación y los conocimientos.			
47	7	94	<p>En relación a las características mínimas precisadas en el punto 7 exactamente en el Apartado de PLAZO DE ENTREGA, se precisa lo siguiente:</p> <p>(...)“El plazo para la Entrega de componentes del sistema de Networking (Infraestructura activa) y renovación de garantías de la infraestructura pasiva y activa de la Sede Central de CORPAC S.A. será máximo de sesenta (60) días calendarios, se contabilizará desde el día siguiente de la firma del contrato. (...)”</p> <p>Solicitamos tenga a bien, consideren modificar los tiempos de entrega puesto que realmente si corresponde a una contratación sin direccionamiento, el plazo mínimo sería de 90 días calendario, por la envergadura y especificaciones del requerimiento, teniendo en cuenta que lo mencionado son tiempos establecidos en el mercado sujetos a la realidad.</p>	Observación de la empresa IDELCOM S.A.C.	Los plazos establecidos van acorde a la necesidad de la Entidad. En ese sentido, el plazo establecido es el requerido para la entrega de los componentes del sistema de networking (infraestructura activa) y el de renovación de las garantías de la Infraestructura pasiva.	
48	7	94	<p>Con respecto al Plazo de Implementación – ETAPA 1, se menciona lo siguiente:</p> <p>“El plazo para la implementación de la presente contratación del Sistema de Networking (Infraestructura Activa), será de ciento cincuenta (50) días calendarios a partir del día siguiente de la fecha máxima del plazo de entrega de equipos. Este plazo incluye el suministro, instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), hasta que la solución funcione correctamente.”</p> <p>Se evidencia un ERROR MATERIAL en relación al plazo, existiendo divergencia entre lo mencionado en letras y lo precisado en números, en tal sentido solicito confirmar que debe ser CIENTO CINCUENTA (150).</p>	Observación de la empresa IDELCOM S.A.C.	Efectivamente existe un error material, la Etapa 1 tiene un plazo de cincuenta días (50) calendarios.	El plazo para la implementación de la presente contratación del Sistema de Networking (Infraestructura Activa), será de cincuenta (50) días calendarios a partir del día siguiente de la fecha máxima del plazo de entrega de equipos. Este plazo incluye el suministro, instalación y configuración y todo lo relacionado al sistema de Networking (Infraestructura activa), hasta que la solución funcione correctamente.
49	5.2.2.1.1.2	20	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.5, en el Apartado de EQUIPOS DE COMUNICACIONES DE 24 PUERTOS (TIPO V), se precisa lo siguiente:</p> <p>El switch deberá contar con CPU mínimo de 2.2 Ghz Consulta:</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se</p>	Consulta de la empresa IDELCOM S.A.C.	<p>La consulta y la referencia no tienen relación. Por un lado, la sección 5.2.2.1.1.2 de la página 20 esta referido a Equipos de Tipo II; y la redacción en su consulta hace referencia a equipos de Tipo V.</p> <p>No obstante, se han realizado otras consultas</p>	

			<p>SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se acepte adicionalmente, que el switch deberá contar con CPU mínimo de 1.8 GHz, sustentado en que la performance del switch no se mide por la velocidad del CPU s CPU TX en sus puerto y enlaces al CPU, sino por la velocidad de transmisión que soporta en sus puertos (throughput).</p>		sobre este punto que han actualizado el requerimiento.	
50	5.2.2.1.1.1	16	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.1, en el Apartado de EQUIPOS DE COMUNICACIONES DE CORE (TIPO I), se precisa lo siguiente:</p> <p>(...) Debe proporcionar una manera de proteger el procesador de administración en el conmutador de cargas elevadas de paquetes (generadas por fuentes maliciosas o no maliciosas) que podrían interferir con su capacidad para (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se acepte adicionalmente, funcionalidades como Control Plane Policing (CoPP) entre otras similares.</p>	Observación de la empresa IDELCOM S.A.C.	<p>Se confirma.</p> <p>Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.</p>	Adicionalmente, se aceptará funcionalidades como políticas de CoPP o similares o equivalentes.
51	5.2.2.1.1.2	20	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.1, en el Apartado de EQUIPOS DE COMUNICACIONES DE CORE (TIPO II), se precisa lo siguiente:</p> <p>(...) El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean como un único switch desde una perspectiva lógica, manteniendo un único plano de control y gestión, mientras que el plano de datos será de tipo distribuido y garantice la alta disponibilidad en capa 2 y capa 3. (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p> <p>Se acepte adicionalmente el uso de enlaces LACP, garantizando HA en capa 2 y capa 3. Considerando finalmente la siguiente especificación:</p> <p>el switch debe poseer tecnología de virtualización que permita que un par de equipos se vean como un único switch desde una perspectiva</p>	Consulta de la empresa IDELCOM S.A.C.	<p>No se confirma. Sin embargo, con el fin de permitir mayor pluralidad de postores también se aceptará para la tecnología de virtualización que el plano de control y gestión también sean distribuidos.</p>	<p>El switch deberá contar con una tecnología de virtualización que permita que un par de equipos se vean como un único switch desde una perspectiva lógica, manteniendo un único plano de control y gestión, mientras que el plano de datos o transmisión será de tipo distribuido y que garantice la alta disponibilidad en capa 2 y capa 3. También se aceptará para la tecnología de virtualización que el plano de control y gestión también sean distribuidos.</p>

			lógica para lograr agregar enlaces con LACP y garantizar HA en capa 2 y capa 3			
52	5.2.2.1.1.2	20	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.2, en el Apartado de EQUIPOS DE COMUNICACIONES DE CORE (TIPO II), se precisa lo siguiente:</p> <p>Debe tener 32 puertos de red 40/100G (QSFP/QSFP28) como mínimo</p> <p>Solicitamos se acepte adicionalmente soluciones que cuenten con puertos a velocidades de 50G, con la finalidad de incentivar la pluralidad de postores.</p>	Consulta de la empresa IDELCOM S.A.C.	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
	5.2.2.1.1.3	25	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DE 48 PUERTOS (TIPO III), se precisa lo siguiente:</p> <p>(...) Debe incluir 2 transceivers de 40Gbps (SFP28) para fibra óptica monomodo 10Km (...)</p> <p>Solicitamos se acepte adicionalmente soluciones con puertos de 50Gbps(SFP28) para fibra óptica monomodo 10Km, con la finalidad de incentivar la pluralidad de postores.</p>	Consulta de la empresa IDELCOM S.A.C.	Cabe precisar que el requerimiento son características mínimas, los proveedores pueden ofertar mejoras al requerimiento, siempre y cuando estas sean integradas y operen correctamente con toda la solución de networking, teniendo en consideración para ello la provisión de todos los componentes para tal fin.	
53	5.2.2.1.1.3	25	<p>En relación a las características mínimas precisadas en el punto 5 del exactamente 5.2.2.1.1.3, en el Apartado de EQUIPOS DE COMUNICACIONES DE 48 PUERTOS (TIPO III), se precisa lo siguiente:</p> <p>(...) El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking. (...)</p> <p>En relación a ello, consideramos muy restrictivo dicho requerimiento, que limita la participación de otros fabricantes en el mercado, y con ello, vulnerando el principio de libre competencia, es por ello, es que se SOLICITA TENGA A BIEN y en aras de que la entidad pueda obtener mejores propuestas que:</p>	Consulta de la empresa IDELCOM S.A.C.	<p>Con la finalidad de ampliar la participación de postores, se reformula el requerimiento:</p> <p>El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking o puertos de uplinks/servicios adicionales para stacking.</p>	El switch propuesto debe soportar apilamiento y la formación de stacks entre ellos utilizando puertos dedicados a Stacking o puertos de uplinks/servicios adicionales para stacking.
			Se permita adicionalmente, Utilizar puerto de uplink como puertos para stack es una tendencia que ya la tienen varios fabricantes			

ANEXO E

ITEM 12 DEL NUMERAL 2.8 OBSERVACIONES AL REQUERIMIENTO

N° de orden	Términos de Referencia o Especificaciones Técnicas o Requisitos de calificación		Consulta u Observación	Corresponde a consulta y/u observación del OEC o de las empresas invitadas en la indagación de mercado
	Numeral	Pág.		
1	5.2.2.1.1.1	14	Tomando en cuenta que una arquitectura SDN usa procesamiento distribuido, se solicita considerar una capacidad memoria RAM de 8 GB.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
2	5.2.2.1.1.1	14	Se solicita considerar que el plano de control y gestión también sea distribuido con el fin de lograr una verdadera alta disponibilidad.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
3	5.2.2.1.1.1	14	Se solicita considerar que el transceiver para la interconexión de control sea de 10 Gbps o superior.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
4	5.2.2.1.1.1	14	Se solicita aclarar que en caso de que el mecanismo de alta disponibilidad sea virtual chassis, al reiniciarse solo uno de los equipos no se produzca un corte del servicio.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
5	5.2.2.1.1.1	15	Con el fin de utilizar terminología estándar de la industria, se solicita considerar SVI o interfaces VLAN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.

6	5.2.2.1.1.1	15	Se solicita considerar MLD v1/v2 o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.
7	5.2.2.1.1.1	15	Dado que se debe implementar SDN, se debe considerar IS-IS y IS-IS v6, por lo que solicitamos incluir dichos protocolos de enrutamiento	Consulta de la empresa REDES Y SERVICIOS S.A.C.
8	5.2.2.1.1.1	15	Con el fin de permitir mayor pluralidad de postores, se solicita considerar a RADSec como opcional	Consulta de la empresa REDES Y SERVICIOS S.A.C.
9	5.2.2.1.1.1	15	Con el fin de permitir mayor pluralidad de postores, se solicita considerar BPDU guard o similar	Consulta de la empresa REDES Y SERVICIOS S.A.C.
10	5.2.2.1.1.1	15	Con el fin de permitir mayor pluralidad de postores, se solicita considerar MLD Snooping o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.
11	5.2.2.1.1.1	16	Se solicita aclarar que los ventiladores redundantes deben estar instalados y operativos	Consulta de la empresa REDES Y SERVICIOS S.A.C.
12	5.2.2.1.1.1	17	Se solicita aclarar que los mecanismos de automatización <u>deben permitir la automatización para el aprovisionamiento de los recursos de red</u>	Consulta de la empresa REDES Y SERVICIOS S.A.C.
13	5.2.2.1.1.1	17	Con el fin de permitir mayor pluralidad de postores, se solicita considerar un <u>"Sistema operativo con capacidad de scripting mediante python"</u> .	Consulta de la empresa REDES Y SERVICIOS S.A.C.
14	5.2.2.1.1.1	18	Se solicita aclarar que se permitirá DWRR o WDRR	Consulta de la empresa REDES Y SERVICIOS S.A.C.
15	5.2.2.1.1.1	18	Se solicita aclarar que se permitirá Committed Information Rate (CIR) o Committed Access Rate (CAR).	Consulta de la empresa REDES Y SERVICIOS S.A.C.
16	5.2.2.1.1.2	19	Se solicita considerar que el plano de control y gestión también sea distribuido con el fin de lograr una verdadera alta disponibilidad.	Consulta de la empresa REDES

				Y SERVICIOS S.A.C.
17	5.2.2.1.1.2	19	Se solicita considerar que el transceiver para la interconexión de control sea de 10 Gbps o superior.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
18	5.2.2.1.1.2	19	Considerando que es una arquitectura non-blocking, se debe tener un rendimiento mínimo de 6.4 Tbps (2 x 32 puertos x 100 Gbps por puerto)	Consulta de la empresa REDES Y SERVICIOS S.A.C.
19	5.2.2.1.1.2	20	Tomando en cuenta que el rendimiento necesario para la arquitectura non-blocking debe ser 6.4 Tbps, el rendimiento mínimo debe ser de 1.2 Bpps, análogo al de los switches de core.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
20	5.2.2.1.1.2	20	Dado que según la normativa IEEE 802.1Q, el VLAN ID tiene un valor de 12 bits y los extremos superior e inferior no pueden ser utilizados, se solicita hacer el cambio al valor de 4094 VLAN IDs.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
21	5.2.2.1.1.2	20	Con el fin de utilizar terminología estándar de la industria, se solicita considerar SVI o interfaces VLAN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
22	5.2.2.1.1.2	20	Se solicita considerar MLD v1/v2 o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.
23	5.2.2.1.1.2	20	Dado que se debe implementar SDN, se debe considerar IS-IS y IS-IS v6, por lo que solicitamos incluir dichos protocolos de enrutamiento	Consulta de la empresa REDES Y SERVICIOS S.A.C.
24	5.2.2.1.1.2	21	Con el fin de permitir mayor pluralidad de postores, se solicita considerar a RADSec como opcional	Consulta de la empresa REDES Y SERVICIOS S.A.C.
25	5.2.2.1.1.2	21	Con el fin de permitir mayor pluralidad de postores, se solicita considerar BPDU guard o similar	Consulta de la empresa REDES Y SERVICIOS S.A.C.
26	5.2.2.1.1.2	21	Con el fin de permitir mayor pluralidad de postores, se solicita considerar MLD Snooping o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.

27	5.2.2.1.1.2	21	Se solicita aclarar que los ventiladores redundantes deben estar instalados y operativos	Consulta de la empresa REDES Y SERVICIOS S.A.C.
28	5.2.2.1.1.2	22	Se solicita aclarar que los mecanismos de automatización deben permitir la automatización para el aprovisionamiento de los recursos de red	Consulta de la empresa REDES Y SERVICIOS S.A.C.
29	5.2.2.1.1.2	22	Con el fin de permitir mayor pluralidad de postores, se solicita considerar un "Sistema operativo con capacidad de scripting mediante python" .	Consulta de la empresa REDES Y SERVICIOS S.A.C.
30	5.2.2.1.1.2	23	Se solicita aclarar que se permitirá DWRR o WDRR	Consulta de la empresa REDES Y SERVICIOS S.A.C.
31	5.2.2.1.1.2	23	Se solicita aclarar que se permitirá Committed Information Rate (CIR) o Committed Access Rate (CAR).	Consulta de la empresa REDES Y SERVICIOS S.A.C.
32	5.2.2.1.1.3	24	Se solicita: "El Switch deberá soportar PoE/PoE+ en todos sus puertos con la capacidad de suministrar PoE (hasta 60W por puerto)." Sin embargo, debería ser PoE/PoE+/ PoE++ .	Consulta de la empresa REDES Y SERVICIOS S.A.C.
33	5.2.2.1.1.3	24	Considerando las capacidades PoE brindadas por las fuentes de poder de diversos fabricantes, se solicita considerar una potencia de PoE de 780W como mínimo en lugar de 840W.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
34	5.2.2.1.1.3	25	Con el fin de utilizar terminología estándar de la industria, se solicita considerar SVI o interfaces VLAN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
35	5.2.2.1.1.3	25	Se solicita considerar MLD v1/v2 o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.
36	5.2.2.1.1.3	25	Dado que se debe implementar SDN, se debe considerar IS-IS y IS-IS v6, por lo que solicitamos incluir dichos protocolos de enrutamiento	Consulta de la empresa REDES Y SERVICIOS S.A.C.
37	5.2.2.1.1.3	25	Con el fin de permitir mayor pluralidad de postores, se solicita considerar a RADSec como opcional	Consulta de la empresa REDES

				Y SERVICIOS S.A.C.
38	5.2.2.1.1.3	25	Con el fin de permitir mayor pluralidad de postores, se solicita considerar BPDU guard o similar	Consulta de la empresa REDES Y SERVICIOS S.A.C.
39	5.2.2.1.1.3	25	Con el fin de permitir mayor pluralidad de postores, se solicita considerar MLD Snooping o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.
40	5.2.2.1.1.3	26	Se solicita aclarar que los ventiladores redundantes deben estar instalados y operativos.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
41	5.2.2.1.1.4	27	Se solicita: "El Switch deberá soportar PoE/PoE+ en todos sus puertos con la capacidad de suministrar PoE (hasta 60W por puerto)." Sin embargo, al igual que en la consulta anterior, debería ser PoE/PoE+/ PoE++ .	Consulta de la empresa REDES Y SERVICIOS S.A.C.
42	5.2.2.1.1.4	27	Considerando las capacidades PoE brindadas por las fuentes de poder de diversos fabricantes, se solicita considerar una potencia de PoE de 780W como mínimo en lugar de 840W.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
43	5.2.2.1.1.4	27	Con el fin de utilizar terminología estándar de la industria, se solicita considerar SVI o interfaces VLAN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
44	5.2.2.1.1.4	28	Se solicita considerar MLD v1/v2 o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.
45	5.2.2.1.1.4	28	Dado que se debe implementar SDN, se debe considerar IS-IS y IS-IS v6, por lo que solicitamos incluir dichos protocolos de enrutamiento	Consulta de la empresa REDES Y SERVICIOS S.A.C.
46	5.2.2.1.1.4	28	Con el fin de permitir mayor pluralidad de postores, se solicita considerar a RADSec como opcional	Consulta de la empresa REDES Y SERVICIOS S.A.C.
47	5.2.2.1.1.4	28	Con el fin de permitir mayor pluralidad de postores, se solicita considerar BPDU guard o similar	Consulta de la empresa REDES Y SERVICIOS S.A.C.

48	5.2.2.1.1.4	28	Con el fin de permitir mayor pluralidad de postores, se solicita considerar MLD Snooping o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.
49	5.2.2.1.1.4	29	Con el fin de permitir mayor pluralidad de postores, se solicita considerar RFID, código de barras o código QR.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
50	5.2.2.1.1.4	29	Se solicita aclarar que los ventiladores redundantes deben estar instalados y operativos.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
51	5.2.2.1.1.5	30	Tomando en cuenta las velocidades combinadas de los puertos de los distintos fabricantes de la industria, se solicita considerar 12 puertos 10/100/1000 BASE-T y 12 puertos 100M/1/2.5/5/10G BASE-T.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
52	5.2.2.1.1.5	30	Se solicita: "El Switch deberá soportar PoE/PoE+ en todos sus puertos con la capacidad de suministrar PoE (hasta 60W por puerto)." Sin embargo, debería ser PoE/PoE+/ <u>PoE++</u> .	Consulta de la empresa REDES Y SERVICIOS S.A.C.
53	5.2.2.1.1.5	30	Considerando las capacidades PoE brindadas por las fuentes de poder de diversos fabricantes, se solicita considerar una potencia de PoE de 740W como mínimo en lugar de 840W.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
54	5.2.2.1.1.5	31	Con el fin de utilizar terminología estándar de la industria, se solicita considerar SVI o interfaces VLAN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
55	5.2.2.1.1.5	31	Se solicita considerar MLD v1/v2 o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.
56	5.2.2.1.1.5	31	Dado que se debe implementar SDN, se debe considerar IS-IS y IS-IS v6, por lo que solicitamos incluir dichos protocolos de enrutamiento	Consulta de la empresa REDES Y SERVICIOS S.A.C.
57	5.2.2.1.1.5	31	Considerando los diferentes mecanismos de seguridad de los fabricantes y con el fin de permitir mayor pluralidad de postores, se solicita eliminar "incluyendo contraseñas, certificados o claves de cifrado"	Consulta de la empresa REDES Y SERVICIOS S.A.C.
58	5.2.2.1.1.5	31	Con el fin de permitir mayor pluralidad de postores, se solicita considerar a RADSec como opcional	Consulta de la empresa REDES

				Y SERVICIOS S.A.C.
59	5.2.2.1.1.5	31	Con el fin de permitir mayor pluralidad de postores, se solicita considerar BPDU guard o similar	Consulta de la empresa REDES Y SERVICIOS S.A.C.
60	5.2.2.1.1.5	31	Con el fin de permitir mayor pluralidad de postores, se solicita considerar MLD Snooping o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.
61	5.2.2.1.1.5	32	Se solicita aclarar que los ventiladores redundantes deben estar instalados y operativos.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
62	5.2.2.1.1.6	33	Considerando que los puertos de 40/100 son de uplink se solicita considerar un mínimo de 2 puertos.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
63	5.2.2.1.1.6	33	Con el fin de guardar coherencia con el resto del requerimiento y no sobredimensionar la solución, se solicita considerar una memoria flash o SSD de 2GB.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
64	5.2.2.1.1.6	34	Dada la forma de expresar las capacidades de conmutación en los distintos fabricantes, se solicita considerar un rendimiento mínimo de 1.72 Tbps.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
65	5.2.2.1.1.6	34	Con el fin de permitir mayor pluralidad de postores, se solicita considerar el rendimiento mínimo de 490 Mpps.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
66	5.2.2.1.1.6	34	Con el fin de utilizar terminología estándar de la industria, se solicita considerar SVI o interfaces VLAN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
67	5.2.2.1.1.6	34	Se indica: "El sistema operativo debe contar con mecanismos de servicio continuo con el objetivo de evitar interrupción del servicio ante operaciones de mantenimiento y actualización de software." Se solicita aclarar que esto podrá ser realizado por un mecanismo en el que el reinicio de uno de los equipos no cause el corte del servicio.	Consulta de la empresa REDES Y SERVICIOS S.A.C.

68	5.2.2.1.1.6	34	Se solicita considerar MLD v1/v2 o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.
69	5.2.2.1.1.6	34	Dado que se debe implementar SDN, se debe considerar IS-IS y IS-IS v6, por lo que solicitamos incluir dichos protocolos de enrutamiento	Consulta de la empresa REDES Y SERVICIOS S.A.C.
70	5.2.2.1.1.6	34	Se solicita considerar NetFlow o sFlow o similares.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
71	5.2.2.1.1.6	34	Se solicita considerar SPAN o similares, RSPAN o similares y ERSPAN o similares.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
72	5.2.2.1.1.6	34	Con el fin de permitir mayor pluralidad de postores, se solicita considerar BPDU guard o similar	Consulta de la empresa REDES Y SERVICIOS S.A.C.
73	5.2.2.1.1.6	34	Con el fin de permitir mayor pluralidad de postores, se solicita considerar MLD Snooping o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.
74	5.2.2.1.1.6	34	Se solicita considerar Python en lugar de phyton.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
75	5.2.2.1.1.6	35	Se solicita aclarar que los ventiladores redundantes deben estar instalados y operativos.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
76	5.2.2.1.2.1	35	No se ha indicado el estándar 802.11 be (WiFi 7).	Consulta de la empresa REDES Y SERVICIOS S.A.C.
77	5.2.2.1.2.1	35	Considerando el primer párrafo, se debe considerar un crecimiento futuro de hasta 2000 APs.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
78	5.2.2.1.2.1	36	Considerando que para una máxima inspección del tráfico este debe pasar por el controlador inalámbrico y son 120 APs, se	Consulta de la empresa REDES

			debería considerar un rendimiento mínimo de 120 Gbps para que dicho equipo no sea un cuello de botella.	Y SERVICIOS S.A.C.
79	5.2.2.1.2.1	36	Se solicita corregir el término "TLS citada" por "TLS cifrada".	Consulta de la empresa REDES Y SERVICIOS S.A.C.
80	5.2.2.1.2.1	36	Se solicita considerar Aplicar asociación dinámica de VLAN de usuario, basado en los parámetros del <u>SSID</u> o paso de autenticación	Consulta de la empresa REDES Y SERVICIOS S.A.C.
81	5.2.2.1.2.1	36	De acuerdo con el principio de vigencia tecnológica, se solicita considerar que el WPA3 debe estar soportado y habilitado.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
82	5.2.2.1.2.1	37	Se solicita considerar como opcional a: "Debe de incluir la capacidad de identificar los dispositivos inalámbricos y crear políticas de acuerdo con la identidad del dispositivo", dado que esto es propio de un sistema de control de acceso.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
83	5.2.2.1.2.2	38	Con el fin de permitir mayor pluralidad de postores, se solicita considerar el valor de ganancia 5 dBi en la banda de 5GHz.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
84	5.2.2.1.2.2	38	Considerando los valores solicitando de ganancia y para que no exista incongruencia, la potencia en dBm debe ser al menos 25 dBm en 2.4 y 5 GHz.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
85	5.2.2.1.2.2	38	El valor indicado de rendimiento de 2.9 Gbps corresponde a equipos WIFI6, considerando que se está implementando WiFi7, se sugiere considerar un valor mínimo de rendimiento de 15 Gbps.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
86	5.2.2.1.2.2	38	Tomando en cuenta que en una solución SDN el cómputo es distribuido, se solicita considerar un valor de memoria DRAM de mínimo 1024 MB.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
87	5.2.2.1.2.2	38	Se indica: "Los Access Points deben tener la capacidad de funcionar sin necesidad de un Controlador centralizado; y para ello debe funcionar con un controlador embebido." Sin embargo, la arquitectura solicitada contempla un controlador inalámbrico, por lo cual se solicita eliminar esta característica	Consulta de la empresa REDES Y SERVICIOS S.A.C.
88	5.2.2.1.2.2	38	Considerando que en WiFi 7 (802.11be) ya se tiene ancho de banda de canal de 320 MHz, se solicita considerar dicho valor adicionalmente a los de 20, 40, 80 y 160 MHz.	Consulta de la empresa REDES Y SERVICIOS S.A.C.

				Y SERVICIOS S.A.C.
89	5.2.2.1.2.2	38	Falta indicar el estándar 802.11 be (WiFi7) que figura en el resto del documento	Consulta de la empresa REDES Y SERVICIOS S.A.C.
90	5.2.2.1.2.2	38	Considerando que en WiFi 7 (802.11be) se ha optimizado la modulación, se debe considerar 4096-QAM adicionalmente a 1024-QAM.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
91	5.2.2.1.2.2	38	Considerando los diferentes mecanismos de seguridad de los fabricantes y con el fin de permitir mayor pluralidad de postores, se solicita eliminar "incluyendo contraseñas, certificados o claves de cifrado"	Consulta de la empresa REDES Y SERVICIOS S.A.C.
92	5.2.2.1.3	39	Se solicita eliminar "o El software de consola de gestión deberá ser desarrollado por el mismo fabricante de los Switches de Core ofertados.", dado que esto hace referencia a un gestor tradicional (NMS) que no es comparable con un controlador SDN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
93	5.2.2.1.3	41	Con el fin de permitir mayor pluralidad de postores, se solicitar considerar: "29. Debe incluir la clasificación de contenido web y/o aplicación por categoría". Asimismo, se solicita eliminar "y establecimiento de una reputación".	Consulta de la empresa REDES Y SERVICIOS S.A.C.
94	5.2.2.1.3	41	Se solicita considerar 1000 aplicaciones en lugar de 3000, con el fin de permitir mayor pluralidad de postores.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
95	5.2.2.1.4	46	En los atributos de usuario, se solicita considerar como opcional a one-time passwords.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
96	5.2.2.1.4	47	Considerando que EAP-MSCHAPv2 es la versión actualizada de MSCHAPv1 y MSCHAP2, se solicita considerar a MSCHAPv1 y MSCHAP2 como opcionales.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
97	5.2.2.1.4	47	Se solicita aclarar que la autenticación basada en MAC es equivalente a Machine Authentication.	Consulta de la empresa REDES Y SERVICIOS S.A.C.

98	5.2.2.1.4	47	Se solicita considerar a "Atributos extraídos del directorio activo" como opcional.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
99	B	160	Considerando que aún no se conoce el valor estimado de la contratación, se solicita que se indique el monto facturado necesario como experiencia del postor. Por ejemplo, 10,000,000.00 o un monto similar debido a la envergadura del proyecto.	Consulta de la empresa REDES Y SERVICIOS S.A.C.
100	5.2.2.1.1.4	27	Debe tener un rendimiento mínimo de 330Mpps. "Para la pluralidad de marcas sírvase aceptar un rendimiento con el stacking que sobrepasa lo requerido y así no estar sobredimensionando el equipo además nos ayudara en poder stackear los diferentes tipos de switch como 3,4 y 5 sin tener que configurar equipo por equipo sino por bloques"	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
101	5.2.2.1.1.5	30	Debe tener un rendimiento mínimo de 470Mpps. "Para la pluralidad de marcas sírvase aceptar un rendimiento con el stacking que sobrepasa lo requerido y así no estar sobredimensionando el equipo además nos ayudara en poder stackear los diferentes tipos de switch como 3,4 y 5 sin tener que configurar equipo por equipo sino por bloques".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
102	5.2.1	13	El licenciamiento de toda la solución de Networking debe ser a nombre de CORPAC y a perpetuidad; deberá contemplarse la garantía de fabricante durante 3 años contados a partir de la finalización de la implementación y a la entrega de los servicios operativos. "Sírvase aclarar cuando indica perpetuidad se hace referencia las funcionalidades de los equipo pero el licenciamiento SDN se necesita una suscripción y también registrar toda la infraestructura. En todo caso sírvase permitir con el máximo nivel de licenciamiento de al menos 5 años bajo suscripción . "	Observación de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.
103	5.2.2.1.3	39	La solución de automatización, administración y gestión de la infraestructura campus con todos sus componentes de hardware y software serán implementados en alta disponibilidad sen un entorno ON PREMISE utilizando appliances de propósito específico, la cual debe ser del mismo fabricante de los Switches de Core, Distribución, Acceso y de la solución de WLAN, con motivo de asegurar su correcta integración, utilizando	Observación de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION

		<p>licenciamiento del tipo perpetuo. La solución debe ser catalogada por el fabricante como un controlador para redes SDN o El software de consola de gestión deberá ser desarrollado por el mismo fabricante de los Switches de Core ofertados. Asimismo, se deberá incluir el sistema operativo, su licenciamiento y todo el hardware (rackeable) necesario para su puesta en operación. Podrá ser instalado en entorno virtual, el proveedor se encargará de colocar el hardware necesario y las licencias del software correspondiente (tal como hypervisor o equivalente) si la oferta es en entorno virtual.</p> <p>" Sírvase aclarar cuando indica perpetuidad se hace referencia las funcionalidades de los equipo pero el licenciamiento SDN se necesita una suscripción y también registrar toda la infraestructura. En todo caso sírvase permitir con el máximo nivel de licenciamiento de al menos 5 años bajo suscripción".</p>	Y SEGURIDAD S.A.C.
--	--	--	--------------------

ANEXO E.1

ABSOLUCION A LAS CONSULTAS Y/U OBSERVACIONES DEL ANEXO A

N° de orden	Términos de Referencia o Especificaciones Técnicas o Requisitos de calificación		Consulta u Observación	Corresponde a consulta y/u observación del OEC o de las empresas invitadas en la indagación de mercado	Análisis respecto de la consulta u observación. (Precisar si se acoge o no se acoge. En caso de no acoger sustentar los motivos))	Precisión de aquello que se incorporará en los TDR o EEETT o Requisitos de calificación, de corresponder
	Numeral	Pág.				
1	5.2.2.1.1.1	14	Tomando en cuenta que una arquitectura SDN usa procesamiento distribuido, se solicita considerar una capacidad memoria RAM de 8 GB.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	En concordancia la capacidad de conmutación del equipamiento del Tipo I; y dado que gran parte del proceso lo asume la solución de automatización, administración y gestión de la infraestructura campus de la RED LAN, se aceptarán como mínimo la capacidad de memoria RAM de 8GB, siempre y cuando no impacte en el rendimiento de los equipos.	Debe tener mínimo la capacidad de memoria RAM de 8GB siempre y cuando no impacte en el rendimiento de los equipos
2	5.2.2.1.1.1	14	Se solicita considerar que el plano de control y gestión también sea distribuido con el fin de lograr una verdadera alta disponibilidad.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Ya se está considerando: También se aceptará para la tecnología de virtualización que el plano de control y gestión también sean distribuidos	

3	5.2.2.1.1.1	14	Se solicita considerar que el transceiver para la interconexión de control sea de 10 Gbps o superior.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	Asimismo, 1 transceiver de 10Gbps o superior para interconexión del control entre Cores o en caso de que la solución tenga un plano de control distribuido en los equipos, se aceptará una solución de gestión fuera de banda para el puerto respectivo
4	5.2.2.1.1.1	14	Se solicita aclarar que en caso de que el mecanismo de alta disponibilidad sea virtual chassis, al reiniciarse solo uno de los equipos no se produzca un corte del servicio.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que en la arquitectura de tipo virtual chassis, al reiniciarse solo uno de los equipos no se producirá un corte del servicio.	o una arquitectura de tipo virtual chassis en donde todos los enlaces sean redundantes y que al reiniciarse solo uno de los equipos no se producirá un corte del servicio.
5	5.2.2.1.1.1	15	Con el fin de utilizar terminología estándar de la industria, se solicita considerar SVI o interfaces VLAN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	SVI (Switched Virtual Interface) o Interfaces VLAN
6	5.2.2.1.1.1	15	Se solicita considerar MLD v1/v2 o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	MLD v1/v2 o Multicast Querier
7	5.2.2.1.1.1	15	Dado que se debe implementar SDN, se debe considerar IS-IS y IS-IS v6, por lo que solicitamos incluir dichos protocolos de enrutamiento	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	Debe soportar e implementar los siguientes protocolos de enrutamiento dinámico: BGPv4, OSPFv2, BGPv6 o MP-BGP, OSPFv3, RIPNG, IS-IS, IS-ISv6.
8	5.2.2.1.1.1	15	Con el fin de permitir mayor pluralidad de postores, se solicita considerar a RADSec como opcional	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con el fin de permitir mayor pluralidad de postores, se considerará como opcional.	Opcionalmente RADSec o similares o equivalentes
9	5.2.2.1.1.1	15	Con el fin de permitir mayor pluralidad de postores, se solicita considerar BPDU guard o similar	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con la finalidad de ampliar la participación de postores, se reformula el requerimiento: BPDU Guard o similar o equivalente	BDPU Guard o similar o equivalente

10	5.2.2.1.1.1	15	Con el fin de permitir mayor pluralidad de postores, se solicita considerar MLD Snooping o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	MLD Snooping o Multicast Querier
11	5.2.2.1.1.1	16	Se solicita aclarar que los ventiladores redundantes deben estar instalados y operativos	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que los ventiladores redundantes deben estar instalados y operativos	El equipo deberá contar con ventiladores redundantes instalados y operativos.
12	5.2.2.1.1.1	17	Se solicita aclarar que los mecanismos de automatización deben permitir la automatización para el aprovisionamiento de los recursos de red	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que entre los mecanismos de automatización también deben permitir la automatización para el aprovisionamiento de los recursos de red.	Debe soportar e implementar mecanismos de automatización: NETCONF o RESTCONF o REST API, que permitan para exportar data y telemetría a herramientas externas; asimismo, deben permitir la automatización para el aprovisionamiento de los recursos de red.
13	5.2.2.1.1.1	17	Con el fin de permitir mayor pluralidad de postores, se solicita considerar un "Sistema operativo con capacidad de scripting mediante python" .	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con la finalidad de mayor pluralidad de postores, se considerará un sistema operativo orientado a modelos basados en programabilidad con capacidad de scripting mediante Python.	Sistema operativo orientado a modelos basados en programabilidad con capacidad de scripting mediante Python.
14	5.2.2.1.1.1	18	Se solicita aclarar que se permitirá DWRR o WDRR	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	DWRR o WDRR
15	5.2.2.1.1.1	18	Se solicita aclarar que se permitirá Committed Information Rate (CIR) o Committed Access Rate (CAR).	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	Committed Information Rate (CIR) o Committed Access Rate (CAR).
16	5.2.2.1.1.2	19	Se solicita considerar que el plano de control y gestión también sea distribuido con el fin de lograr una verdadera alta disponibilidad.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Ya se está considerando: También se aceptará para la tecnología de virtualización que el plano de control y gestión también sean distribuidos.	

17	5.2.2.1.1.2	19	Se solicita considerar que el transceiver para la interconexión de control sea de 10 Gbps o superior.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	1 transceiver de 10Gbps (QSFP) o superior
18	5.2.2.1.1.2	19	Considerando que es una arquitectura non-blocking, se debe tener un rendimiento mínimo de 6.4 Tbps (2 x 32 puertos x 100 Gbps por puerto)	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma.	Debe ser non-blocking. Tener mínimo un rendimiento de 6.4Tbps
19	5.2.2.1.1.2	20	Tomando en cuenta que el rendimiento necesario para la arquitectura non-blocking debe ser 6.4 Tbps, el rendimiento mínimo debe ser de 1.2 Bpps, análogo al de los switches de core.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma.	Debe tener un rendimiento mínimo de 1.2Bpps
20	5.2.2.1.1.2	20	Dado que según la normativa IEEE 802.1Q, el VLAN ID tiene un valor de 12 bits y los extremos superior e inferior no pueden ser utilizados, se solicita hacer el cambio al valor de 4094 VLAN IDs.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que se solicita 4000 VLAN IDs	
21	5.2.2.1.1.2	20	Con el fin de utilizar terminología estándar de la industria, se solicita considerar SVI o interfaces VLAN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	SVI (Switched Virtual Interface) o Interfaces VLAN
22	5.2.2.1.1.2	20	Se solicita considerar MLD v1/v2 o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	MLD v1/v2 o Multicast Querier
23	5.2.2.1.1.2	20	Dado que se debe implementar SDN, se debe considerar IS-IS y IS-IS v6, por lo que solicitamos incluir dichos protocolos de enrutamiento	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	Debe soportar e implementar los siguientes protocolos de enrutamiento dinámico: BGPv4, OSPFv2, BGPv6 o MP-BGP, OSPFv3, RIPNG, IS-IS, IS-ISv6.
24	5.2.2.1.1.2	21	Con el fin de permitir mayor pluralidad de postores, se solicita considerar a RADSec como opcional	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con el fin de permitir mayor pluralidad de postores, se considerará como opcional.	Opcionalmente RADSec o similares o equivalentes
25	5.2.2.1.1.2	21	Con el fin de permitir mayor pluralidad de postores, se solicita considerar BPDU guard o similar	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con la finalidad de ampliar la participación de postores, se reformula el requerimiento: BPDU Guard o similar o equivalente	BPDU Guard o similar o equivalente

26	5.2.2.1.1.2	21	Con el fin de permitir mayor pluralidad de postores, se solicita considerar MLD Snooping o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	MLD Snooping o Multicast Querier
27	5.2.2.1.1.2	21	Se solicita aclarar que los ventiladores redundantes deben estar instalados y operativos	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que los ventiladores redundantes deben estar instalados y operativos	El equipo deberá contar con ventiladores redundantes instalados y operativos.
28	5.2.2.1.1.2	22	Se solicita aclarar que los mecanismos de automatización deben permitir la automatización para el aprovisionamiento de los recursos de red	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que entre los mecanismos de automatización también deben permitir la automatización para el aprovisionamiento de los recursos de red.	Debe soportar e implementar mecanismos de automatización: NETCONF o RESTCONF o REST API, que permitan para exportar data y telemetría a herramientas externas; asimismo, deben permitir la automatización para el aprovisionamiento de los recursos de red.
29	5.2.2.1.1.2	22	Con el fin de permitir mayor pluralidad de postores, se solicita considerar un "Sistema operativo con capacidad de scripting mediante python" .	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con la finalidad de mayor pluralidad de postores, se considerará un sistema operativo orientado a modelos basados en programabilidad con capacidad de scripting mediante Python.	Sistema operativo orientado a modelos basados en programabilidad con capacidad de scripting mediante Python.
30	5.2.2.1.1.2	23	Se solicita aclarar que se permitirá DWRR o WDRR	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	DWRR o WDRR
31	5.2.2.1.1.2	23	Se solicita aclarar que se permitirá Committed Information Rate (CIR) o Committed Access Rate (CAR).	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	Committed Information Rate (CIR) o Committed Access Rate (CAR).
32	5.2.2.1.1.3	24	Se solicita: "El Switch deberá soportar PoE/PoE+ en todos sus puertos con la capacidad de suministrar PoE (hasta 60W por puerto)." Sin embargo, debería ser PoE/PoE+/ PoE++ .	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	El Switch deberá soportar PoE/PoE+/PoE++ en todos sus puertos con la capacidad de suministrar PoE (hasta 60W por puerto).

33	5.2.2.1.1.3	24	Considerando las capacidades PoE brindadas por las fuentes de poder de diversos fabricantes, se solicita considerar una potencia de PoE de 780W como mínimo en lugar de 840W.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Tomando en cuenta las potencias brindadas por los switches de diversos fabricantes con la capacidad PoE++, se confirma la consulta.	Ante la caída de una de las fuentes el switch debe seguir proveyendo 780W de PoE como mínimo.
34	5.2.2.1.1.3	25	Con el fin de utilizar terminología estándar de la industria, se solicita considerar SVI o interfaces VLAN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	SVI (Switched Virtual Interface) o Interfaces VLAN
35	5.2.2.1.1.3	25	Se solicita considerar MLD v1/v2 o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	MLD v1/v2 o Multicast Querier
36	5.2.2.1.1.3	25	Dado que se debe implementar SDN, se debe considerar IS-IS y IS-IS v6, por lo que solicitamos incluir dichos protocolos de enrutamiento	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	Debe soportar e implementar los siguientes protocolos de enrutamiento dinámico: BGPv4, OSPFv2, BGPv6 o MP-BGP, OSPFv3, RIPNG, IS-IS, IS-ISv6.
37	5.2.2.1.1.3	25	Con el fin de permitir mayor pluralidad de postores, se solicita considerar a RADSec como opcional	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con el fin de permitir mayor pluralidad de postores, se considerará como opcional.	Opcionalmente RADSec o similares o equivalentes
38	5.2.2.1.1.3	25	Con el fin de permitir mayor pluralidad de postores, se solicita considerar BDPDU guard o similar	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con la finalidad de ampliar la participación de postores, se reformula el requerimiento: BDPDU Guard o similar o equivalente	BDPDU Guard o similar o equivalente
39	5.2.2.1.1.3	25	Con el fin de permitir mayor pluralidad de postores, se solicita considerar MLD Snooping o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	MLD Snooping o Multicast Querier
40	5.2.2.1.1.3	26	Se solicita aclarar que los ventiladores redundantes deben estar instalados y operativos.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que los ventiladores redundantes e intercambiables en caliente (Hotswappable) deben estar instalados y operativos.	Debe incluir ventiladores redundantes e intercambiables en caliente (Hotswappable) y estar instalados y operativos.
41	5.2.2.1.1.4	27	Se solicita: "El Switch deberá soportar PoE/PoE+ en todos sus puertos con la capacidad de suministrar PoE (hasta 60W por	Consulta de la empresa REDES	Se confirma	El Switch deberá soportar PoE/PoE+/PoE++ en todos sus puertos

			puerto). Sin embargo, al igual que en la consulta anterior, debería ser PoE/PoE+/PoE++.	Y SERVICIOS S.A.C.		con la capacidad de suministrar PoE (hasta 60W por puerto).
42	5.2.2.1.1.4	27	Considerando las capacidades PoE brindadas por las fuentes de poder de diversos fabricantes, se solicita considerar una potencia de PoE de 780W como mínimo en lugar de 840W.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Tomando en cuenta las potencias brindadas por los switches de diversos fabricantes con la capacidad PoE++, se confirma la consulta.	Ante la caída de una de las fuentes el switch debe seguir proveyendo 780W de PoE como mínimo.
43	5.2.2.1.1.4	27	Con el fin de utilizar terminología estándar de la industria, se solicita considerar SVI o interfaces VLAN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	SVI (Switched Virtual Interface) o Interfaces VLAN
44	5.2.2.1.1.4	28	Se solicita considerar MLD v1/v2 o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	MLD v1/v2 o Multicast Querier
45	5.2.2.1.1.4	28	Dado que se debe implementar SDN, se debe considerar IS-IS y IS-IS v6, por lo que solicitamos incluir dichos protocolos de enrutamiento	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	Debe soportar e implementar los siguientes protocolos de enrutamiento dinámico: BGPv4, OSPFv2, BGPv6 o MP-BGP, OSPFv3, RIPNG, IS-IS, IS-ISv6.
46	5.2.2.1.1.4	28	Con el fin de permitir mayor pluralidad de postores, se solicita considerar a RADSec como opcional	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con el fin de permitir mayor pluralidad de postores, se considerará como opcional.	Opcionalmente RADSec o similares o equivalentes
47	5.2.2.1.1.4	28	Con el fin de permitir mayor pluralidad de postores, se solicita considerar BPDU guard o similar	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con la finalidad de ampliar la participación de postores, se reformula el requerimiento: BPDU Guard o similar o equivalente	BPDU Guard o similar o equivalente
48	5.2.2.1.1.4	28	Con el fin de permitir mayor pluralidad de postores, se solicita considerar MLD Snooping o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	MLD Snooping o Multicast Querier
49	5.2.2.1.1.4	29	Con el fin de permitir mayor pluralidad de postores, se solicita considerar RFID, código de barras o código QR.	Consulta de la empresa REDES	En la ET ya se encuentra considerado RFID (RFID Tag) o QR o código de barra.	

				Y SERVICIOS S.A.C.		
50	5.2.2.1.1.4	29	Se solicita aclarar que los ventiladores redundantes deben estar instalados y operativos.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que los ventiladores redundantes e intercambiables en caliente (Hotswappable) deben estar instalados y operativos.	Debe incluir ventiladores redundantes e intercambiables en caliente (Hotswappable) y estar instalados y operativos.
51	5.2.2.1.1.5	30	Tomando en cuenta las velocidades combinadas de los puertos de los distintos fabricantes de la industria, se solicita considerar 12 puertos 10/100/1000 BASE-T y 12 puertos 100M/1/2.5/5/10G BASE-T.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que, considerando las velocidades de los switches actuales, se aceptará lo siguiente: 24 puertos 10/100/1000/2500/5000 Base-T RJ45 o 12 puertos 10/100/1000 BASE-T RJ-45 y 12 puertos 100M/1/2.5/5/10G BASE-T RJ-45	24 puertos 10/100/1000/2500/5000 Base-T RJ45 o 12 puertos 10/100/1000 BASE-T RJ-45 y 12 puertos 100M/1/2.5/5/10G BASE-T RJ-45
52	5.2.2.1.1.5	30	Se solicita: "El Switch deberá soportar PoE/PoE+ en todos sus puertos con la capacidad de suministrar PoE (hasta 60W por puerto)." Sin embargo, debería ser PoE/PoE+/PoE++.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	El Switch deberá soportar PoE/PoE+/PoE++ en todos sus puertos con la capacidad de suministrar PoE (hasta 60W por puerto).
53	5.2.2.1.1.5	30	Considerando las capacidades PoE brindadas por las fuentes de poder de diversos fabricantes, se solicita considerar una potencia de PoE de 740W como mínimo en lugar de 840W.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Tomando en consideración las potencias brindadas por diversos fabricantes con la capacidad de PoE++ del tipo multigigabit, se confirma la consulta.	Ante la caída de una de las fuentes el switch debe seguir proveyendo 740W de PoE como mínimo.
54	5.2.2.1.1.5	31	Con el fin de utilizar terminología estándar de la industria, se solicita considerar SVI o interfaces VLAN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	SVI (Switched Virtual Interface) o Interfaces VLAN
55	5.2.2.1.1.5	31	Se solicita considerar MLD v1/v2 o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	MLD v1/v2 o Multicast Querier
56	5.2.2.1.1.5	31	Dado que se debe implementar SDN, se debe considerar IS-IS y IS-IS v6, por lo que solicitamos incluir dichos protocolos de	Consulta de la empresa REDES	Se confirma	Debe soportar e implementar los siguientes protocolos de

			enrutamiento	Y SERVICIOS S.A.C.		enrutamiento dinámico: BGPv4, OSPFv2, BGPv6 o MP-BGP, OSPFv3, RIPNG, IS-IS, IS-ISv6.
57	5.2.2.1.1.5	31	Considerando los diferentes mecanismos de seguridad de los fabricantes y con el fin de permitir mayor pluralidad de postores, se solicita eliminar "incluyendo contraseñas, certificados o claves de cifrado"	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con la finalidad de mayor pluralidad se reformula el requerimiento: Debe incluir un componente en hardware o software que permita verificar la legitimidad del hardware y software de forma segura, para asegurar la integridad y autenticidad del hardware y software.	Debe incluir un componente en hardware o software que permita verificar la legitimidad del hardware y software de forma segura, para asegurar la integridad y autenticidad del hardware y software.
58	5.2.2.1.1.5	31	Con el fin de permitir mayor pluralidad de postores, se solicita considerar a RADSec como opcional	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con el fin de permitir mayor pluralidad de postores, se considerará como opcional.	Opcionalmente RADSec o similares o equivalentes
59	5.2.2.1.1.5	31	Con el fin de permitir mayor pluralidad de postores, se solicita considerar BPDU guard o similar	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con la finalidad de ampliar la participación de postores, se reformula el requerimiento: BPDU Guard o similar o equivalente	BDPU Guard o similar o equivalente
60	5.2.2.1.1.5	31	Con el fin de permitir mayor pluralidad de postores, se solicita considerar MLD Snooping o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	MLD Snooping o Multicast Querier
61	5.2.2.1.1.5	32	Se solicita aclarar que los ventiladores redundantes deben estar instalados y operativos.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que los ventiladores redundantes e intercambiables en caliente (Hotswappable) deben estar instalados y operativos.	Debe incluir ventiladores redundantes e intercambiables en caliente (Hotswappable) y estar instalados y operativos.
62	5.2.2.1.1.6	33	Considerando que los puertos de 40/100 son de uplink se solicita considerar un mínimo de 2 puertos.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Al ser puerto de uplink, se confirma consulta	Debe incluir un mínimo de 2 puertos de 40/100 Gbps

63	5.2.2.1.1.6	33	Con el fin de guardar coherencia con el resto del requerimiento y no sobredimensionar la solución, se solicita considerar una memoria flash o SSD de 2GB.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	Debe tener mínimo una memoria Flash de 2GB o SSD de 2GB
64	5.2.2.1.1.6	34	Dada la forma de expresar las capacidades de conmutación en los distintos fabricantes, se solicita considerar un rendimiento mínimo de 1.72 Tbps.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con la finalidad de mayor pluralidad se reformula el requerimiento: Tener mínimo un rendimiento de 1.72 Tbps	Tener mínimo un rendimiento de 1.72 Tbps
65	5.2.2.1.1.6	34	Con el fin de permitir mayor pluralidad de postores, se solicita considerar el rendimiento mínimo de 490 Mpps.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con la finalidad de mayor pluralidad se reformula el requerimiento: Tener mínimo un rendimiento de 490 Mpps	Tener mínimo un rendimiento de 490 Mpps
66	5.2.2.1.1.6	34	Con el fin de utilizar terminología estándar de la industria, se solicita considerar SVI o interfaces VLAN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	SVI (Switched Virtual Interface) o Interfaces VLAN
67	5.2.2.1.1.6	34	Se indica: "El sistema operativo debe contar con mecanismos de servicio continuo con el objetivo de evitar interrupción del servicio ante operaciones de mantenimiento y actualización de software." Se solicita aclarar que esto podrá ser realizado por un mecanismo en el que el reinicio de uno de los equipos no cause el corte del servicio.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que evitar interrupción del servicio, incluye que: Cuando estén en operación de pares como un único dispositivo lógico, ante la caída o reinicio del equipo si se actualiza o entra en mantenimiento; no debe causar corte del servicio, las cuales se presentan por lo general en operaciones de mantenimiento y actualización de software. Por lo tanto, el reinicio de uno de los equipos no debe cause el corte del servicio.	
68	5.2.2.1.1.6	34	Se solicita considerar MLD v1/v2 o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	MLD v1/v2 o Multicast Querier

69	5.2.2.1.1.6	34	Dado que se debe implementar SDN, se debe considerar IS-IS y IS-IS v6, por lo que solicitamos incluir dichos protocolos de enrutamiento	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	Debe soportar e implementar los siguientes protocolos de enrutamiento dinámico: BGPv4, OSPFv2, BGPv6 o MP-BGP, OSPFv3, RIPNG, IS-IS, IS-ISv6.
70	5.2.2.1.1.6	34	Se solicita considerar NetFlow o sFlow o similares.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	NetFlow o sFlow o similares
71	5.2.2.1.1.6	34	Se solicita considerar SPAN o similares, RSPAN o similares y ERSPAN o similares.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	SPAN o similares, RSPAN o similares y ERSPAN o similares.
72	5.2.2.1.1.6	34	Con el fin de permitir mayor pluralidad de postores, se solicita considerar BPDU guard o similar	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con la finalidad de ampliar la participación de postores, se reformula el requerimiento: BPDU Guard o similar o equivalente	BDPU Guard o similar o equivalente
73	5.2.2.1.1.6	34	Con el fin de permitir mayor pluralidad de postores, se solicita considerar MLD Snooping o multicast querier	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	MLD Snooping o Multicast Querier
74	5.2.2.1.1.6	34	Se solicita considerar Python en lugar de phyton.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	Python
75	5.2.2.1.1.6	35	Se solicita aclarar que los ventiladores redundantes deben estar instalados y operativos.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que los ventiladores redundantes e intercambiables en caliente (Hotswappable) deben estar instalados y operativos.	Debe incluir ventiladores redundantes e intercambiables en caliente (Hotswappable) y estar instalados y operativos.
76	5.2.2.1.2.1	35	No se ha indicado el estándar 802.11 be (WiFi 7).	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con relación a los Equipos de Controlador/Gateway de Wirelless, deben permitir la convivencia de los estándares 802.11 a/b/g/n/ac/ax/be.	La red inalámbrica debe de poder permitir la convivencia de estándares 802.11a/b/g/n/ac/ax/be

						Debe incluir e implementar los siguientes estándares: IEEE 802.11a/b/g/n/ac/ax/be
77	5.2.2.1.2.1	35	Considerando el primer párrafo, se debe considerar un crecimiento futuro de hasta 2000 APs.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	El soporte de 2000 APs es requisito mínimo, para en un futuro poder gestionar centralizadamente los APs de diversas sedes.	
78	5.2.2.1.2.1	36	Considerando que para una máxima inspección del tráfico este debe pasar por el controlador inalámbrico y son 120 APs, se debería considerar un rendimiento mínimo de 120 Gbps para que dicho equipo no sea un cuello de botella.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Realizando el cálculo promedio aceptable, se considerará un rendimiento no menor de 80 Gbps.	Deberá manejar un rendimiento no menor a 80 Gbps
79	5.2.2.1.2.1	36	Se solicita corregir el término "TLS citada" por "TLS cifrada".	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se confirma	TLS cifrada
80	5.2.2.1.2.1	36	Se solicita considerar Aplicar asociación dinámica de VLAN de usuario, basado en los parámetros del <u>SSID</u> o paso de autenticación	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Considerando los diversos mecanismos de asociación dinámica de VLANs, se acepta lo solicitado.	Aplicar asociación dinámica de VLAN de usuario, basado en los parámetros del SSID o paso de autenticación
81	5.2.2.1.2.1	36	De acuerdo con el principio de vigencia tecnológica, se solicita considerar que el WPA3 debe estar soportado y habilitado.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Considerando el Principio de Vigencia Tecnológica, se aclara que el WPA3 debe estar soportado y habilitado.	Preparado para soportar y debe tener habilitado WPA3.
82	5.2.2.1.2.1	37	Se solicita considerar como opcional a: "Debe de incluir la capacidad de identificar los dispositivos inalámbricos y crear políticas de acuerdo con la identidad del dispositivo", dado que esto es propio de un sistema de control de acceso.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Considerando que la identificación de dispositivos inalámbricos es propia de un NAC; se acepta lo solicitado.	Opcionalmente, debe de incluir la capacidad de identificar los dispositivos inalámbricos y crear políticas de acuerdo con la identidad del dispositivo (Android, iPhone, Etc.)
83	5.2.2.1.2.2	38	Con el fin de permitir mayor pluralidad de postores, se solicita considerar el valor de ganancia 5 dBi en la banda de 5GHz.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que lo solicitado no impacta en el rendimiento de la solución, por lo cual es aceptado.	y en 5GHz de 5 dBi como mínimo
84	5.2.2.1.2.2	38	Considerando los valores solicitando de ganancia y para que no exista incongruencia, la potencia en dBm debe ser al menos 25 dBm en 2.4 y 5 GHz.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Tomando en cuenta los valores de las diferentes potencias brindadas por los APs de diversos fabricantes de la	Debe tener como mínimo 23dBm en 2.4GHz y 24dBm en 5GHz.

				Y SERVICIOS S.A.C.	industria, la potencia en dBm debe ser al menos 23 dBm en 2.4Ghz y 24 dBm en 5Ghz.	
85	5.2.2.1.2.2	38	El valor indicado de rendimiento de 2.9 Gbps corresponde a equipos WIFI6, considerando que se está implementando WIFI7, se sugiere considerar un valor mínimo de rendimiento de 15 Gbps.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se precisa que el valor de rendimiento para los APs es el mínimo, los proveedores pueden ofertar mejoras al requerimiento sin costo adicional.	
86	5.2.2.1.2.2	38	Tomando en cuenta que en una solución SDN el cómputo es distribuido, se solicita considerar un valor de memoria DRAM de mínimo 1024 MB.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Considerando el cómputo distribuido de una solución SDN, se acepta lo solicitado.	Debe tener una memoria DRAM de mínimo 1024 MB
87	5.2.2.1.2.2	38	Se indica: "Los Access Points deben tener la capacidad de funcionar sin necesidad de un Controlador centralizado; y para ello debe funcionar con un controlador embebido." Sin embargo, la arquitectura solicitada contempla un controlador inalámbrico, por lo cual se solicita eliminar esta característica	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Tomando en consideración que el controlador embebido es propia de una solución del tipo small Business, la característica indicada será opcional.	Los Access Points deben tener la capacidad de funcionar sin necesidad de un Controlador centralizado; y para ello debe funcionar con un controlador embebido <u>(opcional)</u> .
88	5.2.2.1.2.2	38	Considerando que en WiFi 7 (802.11be) ya se tiene ancho de banda de canal de 320 MHz, se solicita considerar dicho valor adicionalmente a los de 20, 40, 80 y 160 MHz.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se precisa que los anchos de banda son los mínimos, los proveedores pueden ofertar mejoras al requerimiento sin costo adicional.	
89	5.2.2.1.2.2	38	Falta indicar el estándar 802.11 be (WiFi7) que figura en el resto del documento	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se precisa que lo especificado son los requisitos mínimos, los proveedores pueden ofertar mejoras al requerimiento sin costo adicional.	
90	5.2.2.1.2.2	38	Considerando que en WiFi 7 (802.11be) se ha optimizado la modulación, se debe considerar 4096-QAM adicionalmente a 1024-QAM.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se precisa que lo especificado son los requisitos mínimos, los proveedores pueden ofertar mejoras al requerimiento sin costo adicional.	
91	5.2.2.1.2.2	38	Considerando los diferentes mecanismos de seguridad de los fabricantes y con el fin de permitir mayor pluralidad de postores,	Consulta de la empresa REDES	Con la finalidad de mayor pluralidad se reformula el requerimiento:	Debe incluir un componente en hardware o software que permita verificar la

			se solicita eliminar "incluyendo contraseñas, certificados o claves de cifrado"	Y SERVICIOS S.A.C.	Debe incluir un componente en hardware o software que permita verificar la legitimidad del hardware y software de forma segura, para asegurar la integridad y autenticidad del hardware y software.	legitimidad del hardware y software de forma segura, para asegurar la integridad y autenticidad del hardware y software.
92	5.2.2.1.3	39	Se solicita eliminar "o El software de consola de gestión deberá ser desarrollado por el mismo fabricante de los Switches de Core ofertados.", dado que esto hace referencia a un gestor tradicional (NMS) que no es comparable con un controlador SDN.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	No se confirma, no se está solicitando un NMS, lo que requiere la entidad es la solución similar o equivalente para la automatización de la red, el aprovisionamiento y administración de la infraestructura de red de campus sea esta LAN y WLAN.	
93	5.2.2.1.3	41	Con el fin de permitir mayor pluralidad de postores, se solicitar considerar: "29. Debe incluir la clasificación de contenido web y/o aplicación por categoría". Asimismo, se solicita eliminar "y establecimiento de una reputación".	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con el fin de permitir mayor pluralidad de postores, se acepta lo requerido.	29. Debe incluir la clasificación de contenido web y/o aplicación por categoría.
94	5.2.2.1.3	41	Se solicita considerar 1000 aplicaciones en lugar de 3000, con el fin de permitir mayor pluralidad de postores.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Lo indicado ya es parte de las especificaciones técnicas.	
95	5.2.2.1.4	46	En los atributos de usuario, se solicita considerar como opcional a one-time passwords.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con el fin de permitir mayor pluralidad de postores, se acepta lo requerido.	Atributos de usuario: usuario, clave y certificados, (one-time passwords es opcional).
96	5.2.2.1.4	47	Considerando que EAP-MSCHAPv2 es la versión actualizada de MSCHAPv1 y MSCHAP2, se solicita considerar a MSCHAPv1 y MSCHAP2 como opcionales.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Considerando el Principio de Vigencia Tecnológica, se acepta lo solicitado.	Opcionalmente MSCHAPv1 o MSCHAPv2.
97	5.2.2.1.4	47	Se solicita aclarar que la autenticación basada en MAC es equivalente a Machine Authentication.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Se aclara que son equivalentes	Machine Authentication o <u>MAC</u> o equivalente.

98	5.2.2.1.4	47	Se solicita considerar a "Atributos extraídos del directorio activo" como opcional.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	Con el fin de permitir mayor pluralidad de postores, se acepta lo requerido.	Atributos extraídos del directorio activo (opcional)
99	B	160	Considerando que aún no se conoce el valor estimado de la contratación, se solicita que se indique el monto facturado necesario como experiencia del postor. Por ejemplo, 10,000,000.00 o un monto similar debido a la envergadura del proyecto.	Consulta de la empresa REDES Y SERVICIOS S.A.C.	No Aplica en esta etapa.	
100	5.2.2.1.1.4	27	Debe tener un rendimiento mínimo de 330Mpps. "Para la pluralidad de marcas sírvase aceptar un rendimiento con el stacking que sobrepasa lo requerido y así no estar sobredimensionando el equipo además nos ayudara en poder stackear los diferentes tipos de switch como 3,4 y 5 sin tener que configurar equipo por equipo sino por bloques"	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se aclara que lo solicitado es mínimo, con el fin de tener el rendimiento adecuado de la solución, por lo cual podrá entregarse equipos de mayores capacidades en beneficio de la Entidad, sin costo adicional.	
101	5.2.2.1.1.5	30	Debe tener un rendimiento mínimo de 470Mpps. "Para la pluralidad de marcas sírvase aceptar un rendimiento con el stacking que sobrepasa lo requerido y así no estar sobredimensionando el equipo además nos ayudara en poder stackear los diferentes tipos de switch como 3,4 y 5 sin tener que configurar equipo por equipo sino por bloques".	Consulta de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se precisa que en el presente requerimiento para equipos de Tipo V el rendimiento mínimo figura como 440Mpps con el fin de permitir mayor pluralidad de postores. Por otro lado, se podrá entregar equipos con mayores capacidades en beneficio de la Entidad, sin costo adicional.	
102	5.2.1	13	El licenciamiento de toda la solución de Networking debe ser a nombre de CORPAC y a perpetuidad; deberá contemplarse la garantía de fabricante durante 3 años contados a partir de la finalización de la implementación y a la entrega de los servicios operativos. "Sírvase aclarar cuando indica perpetuidad se hace referencia las funcionalidades de los equipo pero el licenciamiento SDN se necesita una suscripción y también registrar toda la infraestructura. En todo caso sírvase permitir con el máximo nivel de licenciamiento de al menos 5 años bajo suscripción . "	Observación de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se aclara que el todo el licenciamiento del equipamiento deberá ser perpetuo y sólo se permitirá como suscripción durante el tiempo de la prestación accesoria a las actualizaciones y soporte del licenciamiento.	

103	5.2.2.1.3	39	<p>La solución de automatización, administración y gestión de la infraestructura campus con todos sus componentes de hardware y software serán implementados en alta disponibilidad sen un entorno ON PREMISE utilizando appliances de propósito específico, la cual debe ser del mismo fabricante de los Switches de Core, Distribución, Acceso y de la solución de WLAN, con motivo de asegurar su correcta integración, utilizando licenciamiento del tipo perpetuo. La solución debe ser catalogada por el fabricante como un controlador para redes SDN o El software de consola de gestión deberá ser desarrollado por el mismo fabricante de los Switches de Core ofertados. Asimismo, se deberá incluir el sistema operativo, su licenciamiento y todo el hardware (rackeable) necesario para su puesta en operación. Podrá ser instalado en entorno virtual, el proveedor se encargará de colocar el hardware necesario y las licencias del software correspondiente (tal como hypervisor o equivalente) si la oferta es en entorno virtual.</p> <p>" Sírvase aclarar cuando indica perpetuidad se hace referencia las funcionalidades de los equipo pero el licenciamiento SDN se necesita una suscripción y también registrar toda la infraestructura. En todo caso sírvase permitir con el máximo nivel de licenciamiento de al menos 5 años bajo suscripción".</p>	Observación de la empresa PLATAFORMA TECNOLÓGICA EN COMUNICACION Y SEGURIDAD S.A.C.	Se aclara que el todo el licenciamiento del equipamiento deberá ser perpetuo y sólo se permitirá como suscripción durante el tiempo de la prestación accesorio a las actualizaciones y soporte del licenciamiento.	
-----	-----------	----	---	---	--	--