Anexo Técnico No. 1

Ficha de Especificaciones y requerimientos técnicos mínimos para Switches AP & NAC – Lote 1

Se debe suscribir el presente Anexo Técnico, sin alterar o suprimir ninguna de las características e ítems relacionados en el mismo, el cual contempla la totalidad de las especificaciones técnicas mínimas para la ejecución y cumplimiento de la necesidad técnica identificada por parte de la entidad, como parte del proceso de estudio de mercado que adelanta la SUPERSERVICIOS. Se deberá entregar el soporte y garantía de los componentes, así como entregar el licenciamiento, documentación y/o demás soportes descritos en este documento en los términos, condiciones y de conformidad con las especificaciones técnicas descritas al respecto por cada ítem.	
ÍTEM	**LICENCIAMIENTO**
A	**CARACTERÍSTICAS GENERALES**
1	Renovar el servicio de suscripción para el licenciamiento en Aruba central de los siguientes modelos de dispositivos: ● **Switches:** Aruba 8325, Aruba 6300M, Aruba 2930M, Aruba 2930F, HP 5140. ● **Access Points:** AP-505-RW, AP-515-RW ● **NAC:** C1000, C2010
2	Mantener las mismas funcionalidades con las que cuenta actualmente la entidad tanto en los equipos como en el licenciamiento en Aruba central.
3	Renovar el servicio de suscripción del licenciamiento a Aruba central de los Switches y Access Points hasta el 22 de noviembre del 2026.
4	Renovar el soporte y garantía de los Switches, Access Point y los Network Access Control - NAC C1000 y C2010 a partir de la fecha de vencimiento (Que para el caso del presente proceso será hasta el 22 de noviembre del 2026).
B	**SOPORTE Y GARANTÍA**
5	Asistir a la entidad en todas las peticiones de soporte que se presenten relacionadas con la operación y funcionamiento de los equipos en un esquema 7x24 (los siete (7) días de la semana las veinticuatro (24) horas del día), hasta el final de garantía que para el presente proceso será hasta el día 22 de noviembre de 2026; por lo que el contratista debe realizar las actividades de gestión técnica, soporte y atención a fallas, de manera coordinada con el supervisor del contrato para los Switches, Access Points y Network Access Control.
6	Los equipos deben quedar operativos con las características solicitadas en las especificaciones técnicas, por lo que la SUPERSERVICIOS no deberá adquirir licenciamiento adicional para cumplir con los requerimientos del presente anexo técnico, los demás documentos que hacen parte integral del proceso, y del contrato que se derive del proceso de selección.
7	El contratista deberá entregar una carta de compromiso al supervisor del contrato que se derive del proceso de selección, en la cual se comprometa a prestar el servicio de soporte mediante un equipo humano certificado por el fabricante de la plataforma existente de Switches, Access Points y los Network Access Control, hasta el 22 de noviembre del 2026.
8	El contratista deberá atender y resolver cualquier incidente (solicitud de servicio donde se describe indisponibilidad de uno o varios servicios) reportado por parte de la SUPERSERVICIOS, de los Switches, Access Points y los Network Access Control, tanto en el hardware como en el software, en un esquema de atención 7x24x6, (Atención siete (7) días de la semana, las veinticuatro (24) horas del

	día, con tiempo de atención en sitio de seis (6) horas calendario después de reportado el caso, en el término dentro del cual se debe brindar atención y diagnóstico previo a brindar una solución al incidente presentado) en los medios definidos de común acuerdo por el contratista y supervisor del contrato en la matriz de escalamiento, dentro de los que se encuentran (telefónico, email, acceso remoto o presencial en caso de que la SUPERSERVICIOS así lo requiera). Este soporte deberá ser suministrado por personal especializado del contratista y certificado por el fabricante. Deberá contar con atención en la ubicación donde se encuentre el equipo con dicho cubrimiento. El contratista deberá contactar al fabricante en los casos que sea requerido para que brinde atención del incidente, dentro del rango de tiempo asignado de seis (6) horas calendario para el diagnóstico y dentro de las veinticuatro (24) horas calendario para brindar la solución al incidente, hasta el final de garantía que para el presente proceso será hasta el día 22 de noviembre de 2026.
9	El contratista deberá atender y resolver cualquier requerimiento (solicitud de servicio que no genere indisponibilidad) sobre los Switches, Access Points y los Network Access Control,, tanto en el hardware como en el software, en un esquema de atención 5x8x12 en los medios definidos de común acuerdo por el contratista y supervisor del contrato en la matriz de escalamiento, dentro de los que se encuentran (telefónico, email, acceso remoto o presencial en caso de que la SUPERSERVICIOS así lo requiera). Este soporte deberá ser suministrado por personal especializado del contratista y certificado por el fabricante. El contratista deberá contactar al fabricante en los casos que sea requerido para que brinde atención del requerimiento, dentro del rango de tiempo asignado de ocho (8) horas calendario para el diagnóstico y cuarenta y ocho (48) horas calendario para brindar la solución al requerimiento, hasta el día 22 de noviembre de 2026.
	El servicio de soporte debe incluir atención de incidentes y requerimientos a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario continuo, de acuerdo con la matriz de escalamiento definida de común acuerdo entre el contratista y la SUPERSERVICIOS para la solución, la cual debe ser entregada al supervisor del contrato dentro de los dos (2) días siguientes a la suscripción de la respectiva acta de inicio del contrato que se derive del proceso de selección.
	El contratista deberá incluir la garantía del fabricante de los Switches, Access Points y los Network Access Control,, la cual deberá ser entregada por parte del contratista a la entidad dentro de los tres (3) días siguientes al acta de inicio del contrato. El período de cobertura de la garantía será por el mismo período de soporte de operación y funcionamiento de los Switches, Access Point y los Network Access Control,en alta disponibilidad Aruba ClearPass, hasta el final de garantía que para el presente proceso será hasta el día 22 de noviembre de 2026.
	Durante el tiempo de vigencia del soporte y garantía (que para el caso en concreto será por el término desde la firma del acta de inicio hasta el día 22 de noviembre de 2026), sin costo adicional para la SUPERSERVICIOS, el contratista debe llevar a cabo las actualizaciones de nuevas versiones de software liberados, parches de la solución y un (1) mantenimiento preventivo; este último será definido por la entidad de común acuerdo con el contratista, lo anterior siguiendo los procedimientos de calidad de la entidad
	Si para la solución de los requerimientos de servicios técnicos enmarcados en las actividades de mantenimiento preventivo de los Switches, Access Points y los Network Access Control, el contratista requiere la intervención del fabricante o de un tercero (personal certificado); el contratista debe garantizar a través de su gestión, el acompañamiento y participación de manera presencial durante el desarrollo de las actividades de solución. En todo caso el contratista será el directamente responsable de la solución del problema y de mantener debidamente informado al supervisor del contrato.
	El contratista, durante la ejecución del contrato y todo el término de soporte y garantía, al momento de finalizar cada actividad requerida (requerimiento e incidente) deberá entregar un informe con su respectiva orden de servicio al supervisor del contrato, de todas las actividades realizadas por el personal incluyendo:

- Horario de ingreso y salida a las instalaciones de la SUPERSERVICIOS.
- Actividades realizadas por cada especialista, recomendaciones, procedimientos aplicados, relación de cambio de partes si da lugar, aplicación de mejores prácticas, pendientes, recomendaciones y toda la documentación relevante para mantener la gestión de los Switches, Access Points y los Network Access Control.
- Relación de los tickets escalados al fabricante, descripción y seguimientos a las actividades realizadas hasta la solución del incidente.

ÍTEM	DISPOSITIVOS					
A.	LISTADO PARA LICENCIAMIENTO EN ARUBA CENTRAL					
	TIPO	MODELO	SERIAL	MAC	SEDE	CIUDAD
1	Access Point	AP-505-RW	CNKNKPP3NC	D0:D3:E0:CC:60:8C	Principal	Bogotá
2	Access Point	AP-505-RW	CNKNKPP3N6	D0:D3:E0:CC:5E:34	Principal	Bogotá
3	Access Point	AP-515-RW	CNKJKD528X	24:62:CE:CA:2F:A4	Principal	Bogotá
4	Access Point	AP-515-RW	CNKJKD529B	24:62:CE:CA:24:DC	Principal	Bogotá
5	Access Point	AP-515-RW	CNKJKD52B3	24:62:CE:CA:21:DC	Principal	Bogotá
6	Access Point	AP-515-RW	CNKJKD520G	24:62:CE:CA:1A:D0	Principal	Bogotá
7	Access Point	AP-515-RW	CNKJKD51K9	24:62:CE:CA:26:38	Principal	Bogotá
8	Access Point	AP-515-RW	CNKJKD528W	24:62:CE:CA:22:8A	Principal	Bogotá
9	Access Point	AP-515-RW	CNKJKD529V	24:62:CE:CA:26:DE	Principal	Bogotá
10	Access Point	AP-515-RW	CNKJKD529Y	24:62:CE:CA:28:84	Principal	Bogotá
11	Access Point	AP-515-RW	CNKJKD52B2	24:62:CE:CA:21:B4	Principal	Bogotá
12	Access Point	AP-515-RW	CNKJKD529W	24:62:CE:CA:1C:C2	Principal	Bogotá
13	Access Point	AP-515-RW	CNKJKD52B4	24:62:CE:CA:2B:C2	Principal	Bogotá
14	Access Point	AP-515-RW	CNKJKD52B0	24:62:CE:CA:21:E0	Principal	Bogotá
15	Access Point	AP-515-RW	CNKJKD528R	24:62:CE:CA:2B:44	Principal	Bogotá
16	Access Point	AP-515-RW	CNKJKD51J1	24:62:CE:CA:2B:58	Principal	Bogotá
17	Access Point	AP-515-RW	CNKJKD528S	24:62:CE:CA:1E:4A	Principal	Bogotá
18	Access Point	AP-515-RW	CNKKKD59BG	24:62:CE:CA:E9:0A	Principal	Bogotá
19	Access Point	AP-505-RW	CNKNKPP3LR	D0:D3:E0:CC:5A:68	Civis	Bogotá
20	Access Point	AP-515-RW	CNKKKD59FG	24:62:CE:CA:DE:CA	Civis	Bogotá
21	Access Point	AP-515-RW	CNKKKD59GM	24:62:CE:CA:DD:4A	Civis	Bogotá
22	Access Point	AP-515-RW	CNKKKD59FP	24:62:CE:CA:F2:26	Civis	Bogotá
23	Access Point	AP-515-RW	CNKKKD59H6	24:62:CE:CA:F5:E6	Civis	Bogotá
24	Access Point	AP-505-RW	CNKNKPP3JX	D0:D3:E0:CC:5E:A0	Territorial Occidente	Medellín
25	Access Point	AP-515-RW	CNPYLBMGGL	20:9C:B4:C5:32:60	Civis	Bogotá
26	Access Point	AP-515-RW	CNP5KD545B	B0:1F:8C:C9:9A:24	Civis	Bogotá
27	Access Point	AP-515-RW	CNP5KD545D	B0:1F:8C:C9:C4:B8	Civis	Bogotá
28	Access Point	AP-515-RW	PHR8KD51R1	50:E4:E0:C3:13:0C	Civis	Bogotá
29	Access Point	AP-515-RW	CNP5KD545H	B0:1F:8C:C9:B8:86	Civis	Bogotá

30	Access Point	AP-515-RW	CNP5KD545K	B0:1F:8C:C9:AD:88	Civis	Bogotá
31	Access Point	AP-505-RW	CNKNKPP3NG	D0:D3:E0:CC:6A:30	Territorial Noroccidente	Barranquilla
32	Access Point	AP-505-RW	CNKNKPP3NF	D0:D3:E0:CC:57:32	Territorial Noroccidente	Barranquilla
33	Access Point	AP-505-RW	CNKNKPP3NJ	D0:D3:E0:CC:54:8A	Territorial Oriente	Bucaramanga
34	Access Point	AP-505-RW	CNKNKPP3NP	D0:D3:E0:CC:6E:3C	Territorial Oriente	Bucaramanga
35	Access Point	AP-515-RW	CNKJKD51LD	24:62:CE:CA:1C:AA	Principal	Bogotá
36	Access Point	AP-505-RW	CNKNKPP49D	D0:D3:E0:CC:73:8E	Territorial Occidente	Medellín
37	Access Point	AP-505-RW	CNKNKPP45L	D0:D3:E0:CC:6F:D8	Territorial Occidente	Medellín
38	Access Point	AP-515-RW	CNHJKD5CXS	F4:2E:7F:C7:9F:78	Principal	Bogotá
39	Access Point	AP-505-RW	CNKNKPP3T2	D0:D3:E0:CC:54:0E	Territorial Suroccidente	Cali
40	Access Point	AP-505-RW	CNKNKPP3PD	D0:D3:E0:CC:5A:1E	Territorial Suroccidente	Cali
41	Access Point	AP-515-RW	CNLWKD58YB	CC:88:C7:C3:2E:EC	Civis	Bogotá
42	Switch	6300	SG04KN00YV	B8:D4:E7:BA:BA:00	Civis	Bogotá
43	Switch	6300	SG07KMY0WZ	64:E8:81:CC:B3:80	Civis	Bogotá
44	Switch	6300	SG04KN00TP	B8:D4:E7:B5:67:C0	Civis	Bogotá
45	Switch	6300	SG04KN00Z7	B8:D4:E7:B9:7E:80	Civis	Bogotá
46	Switch	6300	SG04KN00YR	B8:D4:E7:B9:3C:40	Civis	Bogotá
47	Switch	2930M	SG05JQN4F3	B8:D4:E7:BD:68:00	Territorial Noroccidente	Barranquilla
48	Switch	2930M	SG05JQN4FZ	B8:D4:E7:BD:C8:00	Territorial Noroccidente	Barranquilla
49	Switch	2930M	SG05JQN4FM	B8:D4:E7:BD:F3:C0	Territorial Noroccidente	Barranquilla
50	Switch	2930M	SG05JQN5C8	B8:D4:E7:B9:73:00	Territorial Oriente	Bucaramanga
51	Switch	2930M	SG05JQN5CD	B8:D4:E7:B9:C1:40	Territorial Oriente	Bucaramanga
52	Switch	2930M	SG05JQN5CB	B8:D4:E7:B9:D0:C0	Territorial Oriente	Bucaramanga
53	Switch	6300	SG04KN00ZJ	B8:D4:E7:B9:3D:40	Principal	Bogotá
54	Switch	2930M	SG05JQN5BN	B8:D4:E7:A4:9B:00	Territorial Occidente	Medellín
55	Switch	2930M	SG05JQN4GH	B8:D4:E7:BD:E5:00	Territorial Occidente	Medellín
56	Switch	6300	SG03KN2014	10:4F:58:FE:C1:C0	Principal	Bogotá
57	Switch	6300	SG03KN203B	B8:D4:E7:06:13:80	Principal	Bogotá
58	Switch	6300	SG03KN203G	B8:D4:E7:06:F1:C0	Principal	Bogotá

59	Switch	8325	TW05KM0060	B8:D4:E7:D3:B1:00	Principal	Bogotá
60	Switch	8325	TW05KM00CD	B8:D4:E7:D3:46:00	Principal	Bogotá
61	Switch	6300	SG07KMY0NZ	64:E8:81:BD:9B:80	Principal	Bogotá
62	Switch	6300	SG04KN01F0	B8:D4:E7:BB:F3:00	Principal	Bogotá
63	Switch	6300	SG04KN00RH	B8:D4:E7:B5:CA:C0	Principal	Bogotá
64	Switch	6300	SG04KN01F1	B8:D4:E7:BC:5C:80	Principal	Bogotá
65	Switch	6300	SG07KMY0X7	64:E8:81:CC:F3:40	Principal	Bogotá
66	Switch	6300	SG04KN018W	B8:D4:E7:BB:63:00	Principal	Bogotá
67	Switch	6300	SG07KMY0NY	64:E8:81:BD:DB:C0	Principal	Bogotá
68	Switch	6300	SG04KN00TL	B8:D4:E7:B5:A2:00	Principal	Bogotá
69	Switch	6300	SG04KN00RD	B8:D4:E7:B5:3B:C0	Principal	Bogotá
70	Switch	6300	SG07KMY0X5	64:E8:81:CC:83:C0	Principal	Bogotá
71	Switch	6300	SG04KN01D3	B8:D4:E7:BD:AC:00	Principal	Bogotá
72	Switch	6300	SG04KN00RR	B8:D4:E7:B5:4B:80	Principal	Bogotá
73	Switch	6300	SG04KN00TK	B8:D4:E7:B5:E4:C0	Principal	Bogotá
74	Switch	6300	SG04KN00ZB	B8:D4:E7:B5:6F:80	Principal	Bogotá
75	Switch	6300	SG04KN00R9	B8:D4:E7:B9:99:00	Principal	Bogotá
76	Switch	6300	SG07KMY0X2	64:E8:81:CC:A2:00	Principal	Bogotá
77	Switch	6300	SG04KN01DD	B8:D4:E7:BA:EF:C0	Principal	Bogotá
78	Switch	6300	SG04KN00TN	B8:D4:E7:B5:63:00	Principal	Bogotá
79	Switch	2930M	SG05JQN5BW	B8:D4:E7:A4:7B:C0	Territorial Suroccidente	Cali
80	Switch	2930M	SG05JQN5C6	B8:D4:E7:A4:9B:40	Territorial Suroccidente	Cali
81	Switch	2930M	SG05JQN5C4	B8:D4:E7:B9:83:C0	Territorial Suroccidente	Cali
82	Switch	6300	SG04KN00SR	B8:D4:E7:B5:DA:40	Civis	Bogotá
83	Switch	2930F	TW9BHKX3DG	10:4F:58:22:F7:40	Principal	Bogotá
84	Switch	5140	CN27LCY0BN	54:77:8A:6E:58:90	Civis	Bogotá
85	Switch	5140	CN27LCY0CP	54:77:8A:6E:65:90	Civis	Bogotá
86	Switch	5140	CN27LCY0B0	54:77:8A:6E:50:70	Civis	Bogotá
87	Switch	5140	CN27LCY0BD	54:77:8A:6E:55:50	Civis	Bogotá

B	**LISTADO PARA LICENCIAMIENTO EN ARUBA CLEARPASS.**					
	TIPO	***MODELO***	***SERIAL***	***UBICACIÓN***	***SEDE***	***TIPO***
88	Clearpass	C1000	USHTHYK002	Principal	Bogotá	Clearpass
89	Clearpass	C2010	2M2209024P	Principal	Bogotá	Clearpass

C	**LICENCIAMIENTO ARUBA CENTRAL**					
	SERIAL	***No. PARTE***	***DESCRIPCIÓN***	***CANTIDAD***	***SERIAL***	***NO. PARTE***
90	PRSW2250552669	N/A	IMC Dig	1	PRSW2250552669	N/A
91	PRSW2250552668	N/A	IMC Basic	1	PRSW2250552668	N/A

92	PA5A5UYADAD3D6	JY926AAE	Aruba Central DM 1 Token 3y Sub E-STU	80	PA5A5UYADAD3D6	JY926AAE

NOTA: Mediante el diligenciamiento y firma de este Anexo Técnico por parte del Representante Legal del proponente interesado, el mismo se compromete a proveer el servicio y a entregar los bienes, equipos y demás, descritos en este documento en los términos, condiciones y de conformidad con las especificaciones técnicas descritas al respecto por cada ítem, y en observancia de las obligaciones contractuales y el plazo previsto en el mismo, una vez se dé inicio a la ejecución del proyecto.

En mi calidad de Representante Legal, en forma voluntaria e irrevocable, mediante la suscripción y firma del presente documento, manifiesto CONOCER y ACEPTAR, de manera uniforme y sin modificación alguna, la totalidad de las especificaciones técnicas, obligaciones y condiciones planteadas por la SUPERSERVICIOS a través del pliego de condiciones y las contenidas en esta ***Ficha de Especificaciones y requerimientos técnicos mínimos para Switches AP & NAC – Lote 1***, la cual contempla la totalidad de las especificaciones técnicas mínimas para la ejecución y cumplimiento del **Lote 1** descrito en el ítem **3.1.1. ALCANCE** de los Estudios Previos.

EN CONSECUENCIA, ME COMPROMETO A DARLES ESTRICTO CUMPLIMIENTO.

NOMBRE O RAZÓN SOCIAL DEL OFERENTE: _____

NOMBRE DEL REPRESENTANTE LEGAL: _____

FIRMA DEL REPRESENTANTE LEGAL: _____

C.C. DEL REPRESENTANTE LEGAL: _____

Anexo Técnico No. 2

Ficha de Especificaciones y requerimientos técnicos mínimos para Appliances DDI Lote 2

Se debe suscribir el presente Anexo Técnico, sin alterar o suprimir ninguna de las características e ítems relacionados en el mismo, el cual contempla la totalidad de las especificaciones técnicas mínimas para la ejecución y cumplimiento de la necesidad técnica identificada por parte de la entidad, como parte del proceso de estudio de mercado que adelanta la Superservicios.

Se deberá entregar el soporte y garantía de los componentes, así como entregar el licenciamiento, documentación y/o demás soportes descritos en este documento en los términos, condiciones y de conformidad con las especificaciones técnicas descritas al respecto por cada ítem.

ÍTEM	APPLIANCE DDI (DHCP - Protocolo de configuración dinámica de Host; DNS - Sistema de nombres de Dominio; e, IPAM - Administración de direcciones IP) y NTP - Protocolo de Tiempo de Red.
A.	**Descripción del Requerimiento**
1	Renovación de suscripción por (1) un año para appliances físicos SOLIDserver 1170 debe incluir suscripción del software DNS guardian.
2	Renovación del licenciamiento de los servicios DHCP, DNS, NTP e IPAM.
3	Los equipos deben conservar todas las funcionalidades actuales.
B.	**Características Generales**
4	La entidad solicita la renovación de la licencia para los appliances físicos SOLIDserver 1170 con el que actualmente cuenta la entidad, esta licencia debe contar con suscripción del software DNS guardian la cual permita habilitar las funcionalidades y actualizaciones durante el tiempo de vigencia del servicio adquirido por término de un (1) año.
5	El equipo SOLIDserver 1170 es una appliance de alto rendimiento diseñada para la gestión centralizada de servicios de red críticos como DNS, DHCP, NTP e IPAM.
6	Rendimiento optimizado para entornos empresariales medianos a grandes, con hasta 250 dominios DNS y 5 millones de consultas DNS por día.
7	Procesador multi-core con arquitectura x86 de 64 bits y soporte de virtualización para alta eficiencia operativa.
8	Almacenamiento robusto en SSD, con RAID y protección integrada para asegurar alta disponibilidad de los servicios.
9	Interfaces de red múltiples, incluyendo puertos Ethernet de 1 GbE y 10 GbE para una conectividad flexible.
10	Alta seguridad, con soporte para DNSSEC, ACLs, autenticación RADIUS/TACACS+, y funciones de hardening.
11	Soporte completo de IPv4 e IPv6, así como herramientas avanzadas para planificación, asignación y supervisión de direcciones IP (IPAM).
12	Administración centralizada y basada en roles, con interfaz web intuitiva y opciones de automatización.

13	Compatibilidad con entornos híbridos y multi-cloud, facilitando la integración con plataformas externas mediante APIs RESTful.
C.	**Funciones del licenciamiento**
14	**Servicios de red integrados** ● Activación de funciones DNS, DHCP, NTP e IPAM (gestión de direcciones IP). ● Soporte para IPv4 e IPv6 de forma simultánea.
15	**Gestión centralizada y automatizada** ● La licencia habilita una interfaz unificada para gestionar múltiples servicios desde un único punto. ● Incluye capacidades de automatización, planificación y descubrimiento de red.
16	**Seguridad avanzada** Protección contra amenazas DNS mediante funcionalidades como: ● **DNS Guardian**: detección de tráfico malicioso, protección contra DDoS, y filtrado de reputación. ● **DNSSEC**: firma digital para garantizar integridad y autenticidad de respuestas DNS.
17	**Alta disponibilidad y recuperación** ● Soporte para failover automático, sincronización de datos entre nodos y balanceo de carga (opcional según licencia).
18	**Soporte técnico y mantenimiento** ● Acceso a soporte técnico 5X8, según el nivel de licencia. ● Actualizaciones de software, parches de seguridad y mejoras funcionales incluidas.
19	**Escalabilidad por volumen** ● Funciones activadas en función del volumen de usuarios, cantidad de dominios, o consultas DNS. ● Se puede escalar desde redes pequeñas hasta ambientes distribuidos o multi-sede.
20	**Integración y APIs** ● Acceso a APIs RESTful para integración con plataformas de terceros, herramientas de automatización o gestión multi-cloud.
D.	**Soporte**

21	Durante el período de garantía, el contratista deberá atender y resolver todas las peticiones de soporte que se presenten relacionadas con la operación y funcionamiento de los dispositivos y/o servicios existentes de la solución completa DDI. Tanto en el software como en el hardware, en un esquema de atención 7x24x2 (siete (7) días a la semana, veinticuatro (24) horas al día y dos (2) horas para la atención), en los medios definidos de común acuerdo por el contratista y supervisor del contrato en la matriz de escalamiento, dentro de los que se encuentran telefónico, email, acceso remoto o presencial en caso de que la SUPERSERVICIOS así lo requiera con atención en sitio (en horario continuo). Por el término de un (1) año contado a partir de las fechas de renovación del licenciamiento, soporte y garantía. Por lo que el contratista debe realizar las actividades de gestión técnica, soporte y atención a fallas, de manera coordinada con el supervisor del contrato.
22	Todos los componentes de la solución completa DDI con que cuenta la entidad, deben quedar operativos con las características solicitadas en las especificaciones técnicas de este Anexo Técnico No. 1, que hace parte integral de este documento, por lo cual la SUPERSERVICIOS no deberá adquirir licenciamiento adicional para cumplir con los requerimientos descritos en este proceso de selección, en el pliego de condiciones, las adendas que se lleguen a expedir, en el presente anexo técnico, en los demás documentos que hacen parte integral de este proceso, y en el contrato que se derive del presente proceso de selección.
23	Debe entregar carta de compromiso al momento de la entrega de los documentos de renovación y adquisición del licenciamiento, soporte y garantía de los componentes de la solución completa DDI al supervisor del contrato, en la cual se compromete a prestar el servicio de soporte por un equipo humano certificado por el fabricante de la plataforma instalada, por el término de un(1) año contado a partir de las fechas de renovación del licenciamiento, soporte y garantía conforme a lo dispuesto en este Anexo Técnico No. 1. que hace parte integral de este documento.
24	Debe atender y resolver cualquier requerimiento (solicitud de servicio que no genere indisponibilidad) sobre los componentes de la solución completa de DDI (DHCP, DNS, NTP e IPAM), relacionados en el Anexo Técnico N°1 que hace parte integral de este documento, tanto en el software como en el hardware, en un esquema de atención 5x8 (cinco (5) días a la semana, ocho (8) horas al día) en los medios definidos de común acuerdo por el contratista y supervisor del contrato en la matriz de escalamiento, dentro de los que se encuentran telefónico, email, acceso remoto o presencial en caso de que la SUPERSERVICIOS así lo requiera con atención en sitio. El soporte a requerimientos deberá ser suministrado por personal especializado del contratista y certificado por el fabricante. El contratista deberá contactar al fabricante en los casos que sea requerido para que brinde atención del requerimiento, dentro del rango de tiempo asignado de ocho (8) horas hábiles para el diagnóstico y cuarenta (40) horas calendario para brindar la solución al requerimiento, por el término de un (1) año que para el caso será para los componentes de la solución completa de DDI (DHCP, DNS, NTP e IPAM) contado a partir de las fechas de renovación del licenciamiento, soporte y garantía, conforme lo dispuesto en este Anexo Técnico No. 1. PARÁGRAFO: En el caso que el proveedor requiera más tiempo para dar la solución al requerimiento en aquellos casos en que se necesite apoyo con asistencia del fabricante, se deberá sustentar al supervisor del contrato y proponer dentro de los tiempos establecidos por la entidad para brindar solución al requerimiento la(s) medida(s) de contingencia ante el(los) requerimiento(s) reportado(s).

25	Durante el tiempo de vigencia del soporte y garantía del contrato para el licenciamiento y soporte adquirido para los los componentes de la solución completa de DDI (DHCP, DNS, NTP e IPAM), el contratista debe llevar a cabo las actualizaciones de nuevas versiones de software o firmware liberados y estables por el fabricante de manera oportuna y debe realizar un (1) mantenimiento preventivo físico y lógico, este último será definido por la entidad de común acuerdo con el contratista, sin costo adicional para la Superservicios. **PARÁGRAFO 1:** El contratista en común acuerdo con la entidad programará la fecha y hora para las actualizaciones de firmware y software en los momentos que se lleguen a solicitar por la entidad durante la vigencia de la garantía y soporte. **PARÁGRAFO 2:** El contratista dispondrá del recurso técnico para realizar los backup de configuraciones y data de los dispositivos previo a la elaboración de las actividades de actualización de los componentes de seguridad de la entidad.
26	Si para la solución de los requerimientos de servicios técnicos enmarcados en las actividades de mantenimiento preventivo sobre los componentes de la solución de DDI, el contratista requiere la intervención del fabricante o de un tercero (personal certificado); el contratista debe garantizar a través de su gestión, el acompañamiento y participación de manera presencial durante el desarrollo de las actividades de solución. En todo caso el contratista será el directamente responsable de la solución del problema y de mantener debidamente informado al supervisor del contrato
27	El contratista, durante la ejecución del contrato y todo el término de soporte, al momento de finalizar cada actividad requerida (requerimiento e incidente) deberá entregar un informe con su respectiva orden de servicio al supervisor del contrato, de todas las actividades realizadas por el personal incluyendo: ● Horario de ingreso y salida a las instalaciones de la SUPERSERVICIOS. ● Actividades realizadas por cada especialista, recomendaciones, procedimientos aplicados, relación de cambio de partes si da lugar, aplicación de mejores prácticas, pendientes, recomendaciones y toda la documentación relevante para mantener la gestión sobre los componentes de la infraestructura de seguridad. ● Relación de los tickets escalados al fabricante, descripción y seguimientos a las actividades realizadas hasta la solución del incidente.

NOTA: Mediante el diligenciamiento y firma de este Anexo Técnico por parte del Representante Legal del proponente interesado, el mismo se compromete a proveer el servicio y a entregar los bienes, equipos y demás, descritos en este documento en los términos, condiciones y de conformidad con las especificaciones técnicas descritas al respecto por cada ítem, y en observancia de las obligaciones contractuales y el plazo previsto en el mismo, una vez se dé inicio a la ejecución del proyecto.

En mi calidad de Representante Legal, en forma voluntaria e irrevocable, mediante la suscripción y firma del presente documento, manifiesto CONOCER y ACEPTAR, de manera uniforme y sin modificación alguna, la totalidad de las especificaciones técnicas, obligaciones y condiciones planteadas por la SUPERSERVICIOS a través del pliego de condiciones y las contenidas en esta ***Ficha de Especificaciones y requerimientos técnicos mínimos para Appliances DDI Lote 2***, la cual contempla la totalidad de las

especificaciones técnicas mínimas para la ejecución y cumplimiento del Lote 2 descrito en el ítem **3.1.1. ALCANCE** de los Estudios Previos.

EN CONSECUENCIA, ME COMPROMETO A DARLES ESTRICTO CUMPLIMIENTO.

NOMBRE O RAZÓN SOCIAL DEL OFERENTE: _____

NOMBRE DEL REPRESENTANTE LEGAL: _____

FIRMA DEL REPRESENTANTE LEGAL: _____

C.C. DEL REPRESENTANTE LEGAL: _____

Anexo Técnico No. 3

Ficha de Especificaciones y requerimientos técnicos mínimos para WAAP & CDN – Lote 3

Se debe suscribir el presente Anexo Técnico, sin alterar o suprimir ninguna de las características e ítems relacionados en el mismo, el cual contempla la totalidad de las especificaciones técnicas mínimas para la ejecución y cumplimiento de la necesidad técnica identificada por parte de la entidad, como parte del proceso de estudio de mercado que adelanta la Superservicios. *Se deberá entregar el soporte y garantía de los componentes, así como entregar el licenciamiento, documentación y/o demás soportes descritos en este documento en los términos, condiciones y de conformidad con las especificaciones técnicas descritas al respecto por cada ítem.*
Adquisición, implementación y soporte de una solución del servicio Content Delivery Network (CDN), Web Application APIs Protection (WAAP) y Anti-DDoS (DDoS) en la nube, que permita afrontar las amenazas de disponibilidad, integridad, confidencialidad de la información y mitigar los posibles riesgos asociados.
ALCANCE
La solución ofertada debe estar en el cuadrante de líderes y visionarios de Gartner para Web Application Firewall en los dos últimos reportes publicados (2024 y 2025).
Se requiere que la solución ofertada sea una solución en la completamente en nube tipo SaaS, sin necesidad de instalar hardware ni software en la infraestructura de la Superservicios
Proveer el servicio de protección de ataque distribuido de denegación de servicio (DDoS-Distributed Denial of Service) y servicio firewall de aplicaciones web (WAAP – protección de aplicaciones web y APIs) para veinticuatro (24) sitios web de la entidad. Los sitios adicionales se cobrarán por el valor unitario de cada sitio
La solución debe permitir implementar controles basados en políticas internas hacia los servidores web de la entidad.
En caso de ser requerido la solución debe incluir la funcionalidad de balanceo de carga entre servidores web (debe soportar múltiples métodos de balanceo), soportar balanceo / distribución de tráfico y enrutar el contenido hacia distintos servidores web
La solución debe contar con sus respectivas actualizaciones periódicas a nivel de firmas de seguridad durante el periodo contratado.
La solución debe soportar protección de tráfico sobre IPV4 e IPV6 para los sitios web.
La solución deberá actuar como un reverse proxy entre el navegador del usuario final y el servidor del website de la Superservicios
La solución debe soportar la funcionalidad de activar HTTP/2 sin ningún costo adicional, incluso si los servidores Web de la entidad no lo soportan HTTP/2. Con esto se busca tener mejor desempeño y seguridad en las aplicaciones web.

La solución debe ofrecer CDN propietario de la misma marca, de manera tal que los sitios web sean más rápidos y ayude a bajar el consumo de ancho de banda. El CDN debe ofrecer: ● Una cantidad mínima a 40 datacenter distribuidos en los 5 continentes para reducir el número de saltos de los paquetes (ida y vuelta), con esto, cada visitante tendrá el sitio cercano a ser local. ● Caché: de objetos estáticos, dinámicos y de todo el sitio. ● Balanceo de carga entre los servidores web ● Failover de servidores web ● Failover automático de datacenter
La solución debe tener un SLA de 99.999%.
La solución debe permitir evidenciar los ataques a los sitios web 7X24X365 e inclusive durante la ejecución del contrato.
La solución debe permitir acceso en línea y en tiempo real del monitoreo, las políticas y reglas configuradas desde una única interfaz gráfica.
La solución debe estar en capacidad de evitar cualquier otro ataque externo que provenga de nuevos desarrollos, tecnologías emergentes, técnicas, BOTs e inventivas para los ataques que afecten los servicios web de la entidad
La solución debe ofrecer un tiempo mínimo de 2 min o inferior para la propagación de reglas cuando se crean o modifican.
La solución debe permitir creación y modificación de reglas de protección.
La nube de la solución debe ofrecer mitigación contra ataques DDoS de cualquier tipo mínimo 10 Gbps con SLAs máximo a 10 segundos o inferior.
La solución debe garantizar como mínimo: ● Mecanismos de detección basado en firmas. ● Mecanismos de detección basado en comportamiento ● Mecanismos ante ataques de DDoS en capa 4 y capa 7 para tráfico cifrado y no cifrado. ● Mecanismos para detectar y bloquear tráfico Bot ● Mecanismos para mitigar ataques de fuerza bruta, buffer overflow, manipulación de cookies y web scraping. ● Mecanismos para proporcionar los controles de protección contra riesgos de seguridad indicados por OWASP. ● Mecanismos de control métodos para peticiones HTTP y HTTPS ● Mecanismos de protección contra el escaneo de puerto y entorno.

- Mecanismos de protección contra problemas de protocolo y codificación.
- Mecanismos de protección contra inyección de encabezado, contrabando de solicitud y división de respuesta.
- Mecanismos de protección contra archivos (RFI)
- Mecanismos de protección contra ejecución remota de código.
- Mecanismos de protección contra ataques de inyección de PHP.
- Mecanismos de protección contra secuencias de comandos de sitios cruzados XSS.
- Mecanismos de protección contra ataques de inyección de SQL.
- Mecanismos de protección contra ataques de fijación de sesión.
- Mecanismos de protección contra troyanos de puerta trasera.
- Mecanismos de protección contra manipulación de ID y parámetros ocultos.
- Mecanismos de protección contra ataques de fuerza bruta.
- Mecanismos de protección contra falsificación de peticiones en sitios cruzados (CSRF)
- Mecanismos de protección para ataques de desbordamiento de búfer.

GENERALES

- Actualización automática del WAF, cuando se encuentran problemas de seguridad que afecten a los usuarios, se aplican reglas de WAF para proteger las páginas Web.
- La solución debe permitir la entrega de contenido y seguridad en Internet deberá estar soportada por una plataforma de nube de cómputo distribuido ubicado en al menos cuarenta (40) datacenters distribuidos alrededor del mundo.
- Independientemente de la capacidad de ancho de banda y/o cantidad de transferencia incluida en el servicio, éste no debe ser interrumpido en caso de que el ancho de banda, la cantidad de peticiones, visitantes, páginas vistas o cantidad de transferencia lleguen a su límite contractual.
- La plataforma de nube de cómputo distribuido deberá ofrecer un Nivel de Servicio del 99.999% de disponibilidad, anexar documentación de fábrica que sustente el requerimiento.
- La plataforma de nube de cómputo distribuido deberá detectar la ubicación de red de un visitante y atender sus peticiones desde el punto de red más próximo y óptimo al usuario final.
- La solución debe ofrecer un tiempo menor a dos (2) minutos para la propagación de reglas cuando estas se creen o modifiquen.
- La solución de Firewall Aplicativo Web deberá incluir el servicio de actualización de reglas y amenazas sin necesidad de que éstas sean actualizadas o mantenidas por personal de la SUPERSERVICIOS.

- La solución debe ofrecer integración con DevSecOps con el apoyo del contratista.
- En caso de requerirse, creación de API para purgado de Caché de los sitios.
- Disponer del equipo humano que sea requerido y especializado en la marca para garantizar el servicio CDN, Anti-DDoS Web y WAAP en la nube, durante un (1) año contado a partir de la suscripción del acta de inicio del contrato, las veinticuatro (24) horas del día por los siete (7) días de la semana.

ENTREGA DE CONTENIDO WEB

- La solución debe hacer distribución completa de los sitios web de la Superservicios, por medio de los protocolos HTTP y HTTPS.
- La solución deberá llevar a cabo la distribución del contenido sin necesidad de cambiar de proveedor de hospedaje web y sin necesidad de replicar el contenido de los sitios web de la Superservicios y/o las bases de datos hacia infraestructuras ajenas a la organización.
- La solución deberá llevar a cabo la distribución de contenido de los sitios web de la Superservicios en modelo de servicio, sin necesidad de instalar hardware ni software en la infraestructura de la Superservicios ni modificar código de aplicaciones.
- La petición hacía los sitios web de la Superservicios deben llevarse mediante conexiones HTTP y HTTPS persistentes.
- Redirección de HTTP a HTTPS en la solución.

ACELERACIÓN DE SITIOS WEB

- La solución debe acelerar el tiempo de descarga de los sitios web de CLIENTE.
- La solución debe ofrecer CDN, WAF y AntiDDoS de la misma marca.
- La solución debe llevar a cabo la compresión de datos al distribuir los contenidos cuando éstos se traten de archivos de texto simple.
- La solución debe optimizar el protocolo TCP para acelerar el tiempo de descarga por medio del protocolo HTTP y HTTPS.
- La solución debe identificar la procedencia de la región en el mundo donde es solicitado el contenido del sitio WEB de EL CLIENTE.
- La solución debe ser capaz de hacer cacheo de contenido dinámico NO personalizado.

Nota: El CDN puede ser de la misma marca u OEM de otro fabricante.

PROTECCIÓN-DDoS

La solución de PROTECCIÓN-DDoS, debe brindar protección contra ataques de denegación de servicio, bloqueando como mínimos los siguientes ataques, para los sitios web:

- TCP SYN+ACK

- TCP FIN
- TCP RESET
- TCP ACK
- TCP ACK + PSH
- TCP Fragment
- UDP
- ICMP
- IGMP
- HTTP Flood
- Brute Force
- Connection Flood
- Slowloris
- Spoofing
- DNS flood
- Mixed SYN + UDP o ICMP + UDP flood
- Ping de la muerte
- Smurf
- Reflected ICMP y UDP
- Teardrop
- Ataques DDoS de Día Cero
- Attacks targeting Apache, Windows o vulnerabilidades OpenBSD
- Attacks hacia Servidores DNS
- Protección DDoS del comportamiento de la capa de red
- Ataques Slow rate
- Network Challenge Response

Control de sobrecarga de conexiones sobre los servidores.

Controles heurísticos en capa 7, Reconocimiento de anomalías.

Excesivas conexiones TCP por destino.
Prevención de escaneo Dark Address
Mitigación contra ataques DDoS en max. 10 segundos.
PROTECCIÓN WAPP
La solución de WAF debe brindar controles de protección a los sitios web sobre cualquier puerto TCP como 80 (HTTP), 443 (HTTPS) o 8080, entre otros, distribuido en la plataforma de nube de cómputo, contra todos los ataques/amenazas identificados en el OWASP top 10 más reciente, incluyendo, más no limitándose a ataques de tipo: ● SQL INJECTION ● CROSS SITE SCRIPTING ● CROSS-SITE REQUEST FORGERY ● BOTNET MALICIOSAS ● MOTOR DE BÚSQUEDAS MALICIOSAS ● ACCESO ILEGAL A RECURSOS ● EJECUCIÓN MALICIOSA DE ARCHIVOS ● FALSIFICACIÓN DE PETICIONES EN SITIOS CRUZADOS (CSRF) ● PÉRDIDA DE AUTENTICACIÓN Y GESTIÓN DE SESIONES ● REMOTE FILE INCLUSION ● LOCAL FILE INCLUSION ● OS COMMANDS ● TROYANOS Y VIRUS ● EXPLOIT ● FUGAS DE INFORMACIÓN ● FIRMAS PERSONALIZADAS ● GET FLOODS ● COMMAND INJECTION ● PREDICTABLE RESOURCE LOCATION ● IMPROPER OUTPUT HANDLING ● DIRECTORY INDEXING

● SESSION HIJACKING ● HTTP PROTOCOL MANIPULATION ● XML AND WEB SERVICES ATTACKS ● Habilitar SNI.
Con esto la herramienta debe ser capaz de proteger de las siguientes amenazas: Browser Exploit Against SSL /TLS, Brute Force Login, Malicious Robots, Man in the Middle, Cross Site request forgery, DDoS, HTTP Header Overflow Attack, Clickjacking, Cookie Tampering, Credit Card Theft, Server information leakage, Malformed XML.
La solución debe proveer como mínimo un ancho de banda para la protección de Aplicaciones Web de 170 Mbps para 24 sitios WEB de la entidad sin importar picos momentáneos de un ancho de banda mayor.
La solución de Firewall de Aplicativo Web debe estar en capacidad de hacer inspección del tráfico SSL del cliente, con el fin de hacer una mejor detección de amenazas que estén viajando sobre protocolos seguros.
Protección contra Bad BOTS
Administración de Good BOTS
Control de Acceso: Listas blancas y negras basadas en geolocación, IP y firmas de cliente
Creación de Políticas de seguridad personalizadas
Soporta TLS.

Certificados digitales propios sin costo o importación de los propios del cliente. Estos certificados deben ser públicos y válidos en internet, no autofirmados.
Chequeo de SOAP, JSON
CDN
Optimización de contenido mediante compresión, modificación de contenido, entre otros
Caché de contenido estático como imágenes, contenido CSS y archivos JavaScript
Refrescamiento asíncrono de caché una vez expira
Rehúso de sesiones para optimización de manejo de sesiones en el servidor Web
Caché de contenido dinámico
Purgado automático y manual de chache. También lo permite mediante API
Optimización avanzada de imágenes mediante compresión y renderización progresiva
TCP pre-pooling: permite la apertura de múltiples sesiones TCP para aceleración de la comunicación con el origen
ACUERDOS DE NIVEL DE SERVICIO
SLA 99.999%
INFORMES
La solución debe generar informes semanales de comportamiento del servicio, el cual deberá estar avalado por el supervisor delegado por la entidad, para ser enviado al correo electrónico que suministre el supervisor delegado por la Entidad.
La herramienta debe permitir la consulta de los logs del servicio ofrecido en un rango de hasta de 90 días, de tal manera que se identifiquen las amenazas o incidentes detallados del ataque detectado.
La solución debe ser capaz de enviar las alertas por correos electrónicos que suministre el supervisor delegado por la entidad cuando se detecte un ataque.
Estadísticas de tráfico en tiempo real
Monitoreo de eventos de seguridad
La herramienta debe poder enviar logs al SIEM que tiene la entidad (FortiSIEM).
MONITOREO
Suministrar al supervisor delegado por la Entidad la URL que permita el ingreso seguro a la herramienta para ejercer control y seguimiento del servicio requerido. El acceso debe poder permitir doble factor de autenticación al menos uno de los siguientes métodos: Email, SMS o Google Authenticator.
Suministrar, sin costo adicional para la Entidad, todas las herramientas necesarias para garantizar a la Unidad de Gestión un óptimo monitoreo del servicio.
GENERALIDADES

Se requiere que la solución tenga los siguientes módulos/funcionalidades activas: ● Tráfico Limpio ● Protección DDoS Web (L3, L4, L7) ● CDN ● Cache ● GSLB ● WAF ● Protección de API ● Control por reputación de IPs ● Clasificación de clientes ● Administración y detección de comportamiento de BOTs ● Detección de Apropiación/robo de cuentas (ATO) ● CAPTCHAs (ilimitados) ● Detección de protección del lado del cliente ● Sala de Espera/Fila virtual ● Inteligencia artificial/Analítica dedicada de uso único y específico para Aplicaciones Web ● Retención de eventos de 90 días en la solución. Estos módulos mencionados deben ofrecerse como un “Single Stack”, es decir, módulos o funcionalidades propias, dentro de la misma infraestructura y desarrolladas por el mismo fabricante; libre de integraciones.
El servicio WAF debe permitir crear listas blancas y negras por IP, por excepciones particulares, por el contenido de URL (por ejemplo, un de Cross Site Scripting válido), por tipo/nombre de BOT, etc.
La solución debe estar en capacidad de analizar y clasificar el tráfico entrante hacia las aplicaciones web. Así mismo tendrá la capacidad de identificar BOTs buenos, BOTs malos, BOTs sospechosos, tipo de navegador del usuario, entre otros.
Garantizar a la Superservicios que en caso de un eventual cambio del direccionamiento público o la implementación de un hosting de alguno de los sitios contratados durante la ejecución del contrato, no afectará la prestación del servicio objeto del presente proceso. (Se requiere previo aviso por parte de la entidad)
La solución debe descubrir la totalidad de las API y los end points produciendo swager en forma automática para ser controlado por el api del waf.
En caso de un ataque y/o para evitar estos, la solución debe contemplar el uso de tecnología CAPTCHA, como alternativa principal de ingreso a los sitios a cubrir en los cuales la entidad lo tenga o lo requiera.
La solución deberá contar con un módulo para la protección de Accesos a áreas administrativas o restringidas para el monitoreo del servicio
Administración Web de la solución basada en roles para los diferentes usuarios para ingresar al servicio, accesible sólo para personal de la Superservicios.
La solución deberá soportar al menos los siguientes métodos para doble factor de autenticación, para ingresar al servicio de WAF: ● E mail. ● SMS. ● Google Authenticator o similar. ● Llamadas a celular.
Asistir a la Entidad en todas las peticiones de soporte que se presenten relacionadas con la operación y funcionamiento de la solución en el tiempo 7 días de la semana las 24 horas del día y los 365 días del año.

REGLAS DE FIREWALL DE APLICACIONES
El servicio WAAP debe permitir crear reglas de firewall de aplicativo web personalizadas con las siguientes posibles acciones: ● Alerta ● Bloqueo de solicitud ● Bloqueo de Sesión ● Bloqueo de IP ● Bloquear País ● Solicitar soporte de cookie ● Solicitar soporte de script java ● Solicitar soporte de CAPTCHA ● Listas blancas ● Listas negras Estas reglas deben permitir filtrar tráfico con base en parámetros como: ● HTTP Header ● HTTP Method ● Post Data ● URL ● Número en sesión ● Tipo de cliente
La solución debe permitir la creación de reglas de firewall para protección WEB.
La solución debe tener opción para protección de autenticación en login para la autenticación del monitoreo del servicio de nube.
El servicio debe tener la opción de configurar la caché WEB de contenido estático, dinámico y todo el sitio por URL específica. Así mismo debe permitir deshabilitar el Cache para URLs particulares.
Debe tener protección contra backdoors.
Debe proteger contra RFI (Remote File Inclusion).
ANALITICA Y OPTIMIZACION DE SITIOS PERSONALIZADA
El contratista deberá proveer un servicio que le permita a la entidad tomar medidas para optimización en los sitios Web, es decir, el servicio debe informar el estado y lo que ocurra sobre cualquier recurso de las aplicaciones web de la entidad, sin importar el tipo de recurso ni haber sido advertido o informado previamente por la entidad. Esto es, errores emitidos por la aplicación web, por el cliente, tamaños de cada recurso, así como los tiempos de carga de cada uno de ellos. El servicio debe tener la capacidad de enviar reportes periódicos programables al menos diaria, semanal y mensualmente.
El contratista deberá proveer a la entidad información relevante sobre los sitios web tal que permita conocer desde qué ciudad y país de dicha ciudad se envían Requests hacia los sitios web de la entidad, así como también el navegador, cliente y aplicaciones usadas sin limitarse a cantidad de Requests, visitas, conexiones,

sesiones ni ciudades.
La analítica debe reportar las IP más transaccionales debe reportar el nivel de seguridad SSL debe reportar el Datacenter al cual se redireccionan las solicitudes hacia la aplicación.

NOTA: Mediante el diligenciamiento y firma de este Anexo Técnico por parte del Representante Legal del proponente interesado, el mismo se compromete a proveer el servicio y a entregar los bienes y demás, descritos en este documento en los términos, condiciones y de conformidad con las especificaciones técnicas descritas al respecto por cada ítem, y en observancia de las obligaciones contractuales y el plazo previsto en el mismo, una vez se dé inicio a la ejecución del proyecto.

En mi calidad de Representante Legal, en forma voluntaria e irrevocable, mediante la suscripción y firma del presente documento, manifiesto CONOCER y ACEPTAR, de manera uniforme y sin modificación alguna, la totalidad de las especificaciones técnicas, obligaciones y condiciones planteadas por la SUPERSERVICIOS a través del pliego de condiciones y las contenidas en esta ***Ficha de Especificaciones y requerimientos técnicos mínimos para WAAP & CDN – Lote 3***, la cual contempla la totalidad de las especificaciones técnicas mínimas requeridas para el Lote 3 descrito en el ítem **3.1.1. ALCANCE** de los Estudios Previos.

EN CONSECUENCIA, ME COMPROMETO A DARLES ESTRICTO CUMPLIMIENTO.

NOMBRE O RAZÓN SOCIAL DEL OFERENTE: _____

NOMBRE DEL REPRESENTANTE LEGAL: _____

FIRMA DEL REPRESENTANTE LEGAL: _____

C.C. DEL REPRESENTANTE LEGAL: _____

Anexo Técnico No. 4

Ficha de Especificaciones y requerimientos técnicos mínimos para Solución de Seguridad – Lote 4

Se debe suscribir el presente Anexo Técnico, sin alterar o suprimir ninguna de las características e ítems relacionados en el mismo, el cual contempla la totalidad de las especificaciones técnicas mínimas para la ejecución y cumplimiento de la necesidad técnica identificada por parte de la entidad, como parte del proceso de estudio de mercado que adelanta la SUPERSERVICIOS.

Se deberá entregar el soporte y garantía de los componentes, así como entregar el licenciamiento, documentación y/o demás soportes descritos en este documento en los términos, condiciones y de conformidad con las especificaciones técnicas descritas al respecto por cada ítem.

LICENCIAMIENTO, GARANTÍA Y SOPORTE DE LOS COMPONENTES DE LA SOLUCIÓN DE SEGURIDAD DE LA ENTIDAD

DISPOSITIVOS Y SERVICIOS CON SUS RESPECTIVOS SERIALES

El proveedor deberá considerar los seriales de los dispositivos y servicios a los cuales se requiere la renovar el licenciamiento:

DISPOSITIVO	SERIAL
Fortigate – 601E	**FG6H1E5819902474, FG6H1E5819902508**
FortiSandBox - 2000E	**FSA2KET618000092**
FortiSIEM - 2000F	**FSM2KFT319000029**
FortiAnalyzer - 300G	**FAZ3HGTA23000432**
Fortimail – Cloud	**FEVM04M000193815**
FortiEDR - Cloud	**FEDR00TM23000503**

EQUIPO	FECHA DE FINALIZACIÓN	FECHA DE INICIO PROXIMA LICENCIA
FortiAnalyzer 300G	17/12/2025	18/12/2025
FortiEDR	17/12/2025	18/12/2025
FortiMail Cloud	10/12/2025	11/12/2025
FortiGate 601E	17/12/2025	18/12/2025
FortiGate 601E	17/12/2025	18/12/2025
FortiSandbox 2000E	17/12/2025	18/12/2025
FortiSIEM 2000F	17/12/2025	18/12/2025

RENOVACIÓN DEL LICENCIAMIENTO, SOPORTE Y GARANTÍA DE FABRICANTE, CON UPGRADE DE HARDWARE PARA SOLUCIÓN DE FIREWALL PERIMETRAL

Realizar la renovación del licenciamiento, suscripciones de seguridad, funcionalidades y soporte de fábrica para los dispositivos Firewall de nueva Generación con los que cuenta la entidad, la cual corresponde a la plataforma FORTIGATE 601E con los siguientes seriales:

DISPOSITIVO	**SERIAL**
Fortigate – 601E	**FG6H1E5819902474, FG6H1E5819902508**

Se deberá suministrar los Upgrades de hardware requeridos para que la solución soporte las siguientes características de desempeño

- Desempeño de Firewall: 11.5 Gbps
- Desempeño de Protección de Amenazas: 10.5 Gbps
- Desempeño de IPS: 14 Gbps
- Desempeño Throughput paquetes por segundo: 105 Mpps
- Desempeño en sesiones Concurrentes: 8 Million

Características de hardware:

- 4x 25G SFP28 slots, 4x 10GE SFP+ slots, 18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 8x GE SFP slots, SPU NP7 and CP9 hardware accelerated, 480GB onboard SSD storage, dual AC power supplies

Se deberá suministrar todos los componentes necesarios a nivel de conectividad (SFP) para el funcionamiento de las interfaces en 10GB hasta 25GB.

Realizar un Assessment de seguridad sobre la solución renovada, así mismo, la optimización en las configuraciones (Integraciones de seguridad entre Firewall, VPN SSL, VPN Site to Site, Configuración Perfiles de Seguridad, Integración con SIEM y FortiAnalyzer y FortiSASE así como sistemas de autenticación de tipo LDAP y NAC), y puesta en producción

renovar el licenciamiento, soporte y la garantía de fabricante, por el término de un (1) año, contado a partir de la entrega de los certificados de renovación de licenciamiento, soporte y garantía y de entrega de los equipos objeto del upgrade.

RENOVACIÓN DE LICENCIAMIENTO SANDBOX, SIEM, ANALYZER, FORTIMAIL Y ENDPOINT

Realizar la renovación de la licencia, garantía y soporte de un (1) dispositivo Sandbox (*Appliance*) – FortiSandbox 2000E, con que cuenta actualmente la entidad, contado a partir de la fecha de activación, por el término de un (1) año. Con el propósito de mantener las funcionalidades actuales del dispositivo, a partir de la fecha de vencimiento, documentado en el portal de licenciamiento del fabricante para la cuenta de la SUPERSERVICIOS, se debe adicionar un (1) licenciamiento de Windows 11 con Ofimática, para adicionar a las máquinas virtuales usadas para el escaneo de vulnerabilidades.

Realizar un Assessment de seguridad sobre la solución renovada, así mismo, la optimización en las configuraciones (Integraciones de seguridad con los firewall de Perímetro con que cuenta la entidad On-Premise y Cloud, así como pruebas funcionales con las máquinas virtuales en windows 11).

PARÁGRAFO: El contratista deberá entregar a la SUPERSERVICIOS la certificación del fabricante donde indique de manera clara el período de activación de las mismas, junto con el certificado de activación del licenciamiento, de conformidad con las fechas establecidas en este ítem.
Realizar la renovación de las trescientas (300) licencias, garantía y soporte en un esquema 7x24 (siete (7) días a la semana, veinticuatro (24) horas al día) de un (1) dispositivo SIEM (*Appliance*) FortiSIEM 2000F, con que cuenta actualmente la entidad contado a partir de la fecha de activación, por el término de un (1) año. Con el propósito de mantener las funcionalidades actuales del dispositivo, a partir de la fecha de vencimiento, documentado en el portal de licenciamiento del fabricante para la cuenta de la SUPERSERVICIOS. Realizar un Assessment de seguridad sobre la solución renovada, así mismo, la optimización en las configuraciones (Integraciones de seguridad con la infraestructura tecnológica con que cuenta la Superservicios, análisis de reglas, reportes,automatizaciones y tableros de control)
Realizar la renovación de la licencia, garantía y soporte del dispositivo Analizador de tráfico (*Appliance*) FortiAnalyzer 300G, con que cuenta actualmente la entidad contado a partir de la fecha de activación, por el término de un (1) año. Con el propósito de mantener las funcionalidades actuales del dispositivo, a partir de la fecha de vencimiento, documentado en el portal de licenciamiento del fabricante para la cuenta de la SUPERSERVICIOS. Realizar un Assessment de seguridad sobre la solución renovada, así mismo, la optimización en las configuraciones (Integraciones de seguridad con los firewall de Perímetro con que cuenta la entidad On-Premise, analisi y optimizaciones de reportes y alertas)
Realizar la renovación de los mil ochocientas (1800) buzones que incluyan garantía y soporte del Software como Servicio (SaaS) de FortiMail Cloud, con que cuenta actualmente la entidad contado a partir de la fecha de activación, conservando las mismas características, por el término de un (1) año. Con el propósito de mantener las funcionalidades actuales del servicio a partir de la fecha de vencimiento, documentado en el portal de licenciamiento del fabricante para la cuenta de la SUPERSERVICIOS. Se debe adquirir doscientos (200) nuevos buzones que incluyan garantía y soporte del Software como Servicio (SaaS) de FortiMail Cloud, con que cuenta actualmente la entidad. Con el objetivo de mantener la disponibilidad del servicio ante el ingreso de nuevos colaboradores (funcionarios - contratistas) en la entidad. Realizar un Assessment de seguridad sobre la solución renovada, así mismo, la optimización en las configuraciones (Análisis y optimizaciones de los módulos de seguridad integrados al FortiMail Cloud) **PARÁGRAFO:** El contratista deberá entregar a la SUPERSERVICIOS la certificación del fabricante donde indique de manera clara el período de activación de las mismas, junto con el certificado de activación del licenciamiento, de conformidad con las fechas establecidas en este ítem.
Realizar el upgrade de las mil setecientas (1700) licencias, garantía y soporte en un esquema 7x24 (siete (7) días a la semana, veinticuatro (24) horas al día) de Software como Servicio (SaaS) de la solución EDR, FortiEDR, con que cuenta actualmente la entidad a XDR, FortiXDR, contado a partir de la fecha de activación, por el término de un (1) año. Lo anterior, con el propósito de mejorar las funcionalidades actuales del servicio, a partir de la fecha de vencimiento, documentado en el portal de licenciamiento del fabricante para la cuenta de la SUPERSERVICIOS. **PARÁGRAFO:** El contratista deberá entregar a la SUPERSERVICIOS la certificación del fabricante donde indique de manera clara el período de activación de las mismas, junto con el certificado de activación del licenciamiento, de conformidad con las fechas establecidas en este ítem.

GARANTÍA
Se debe contemplar garantía, repuestos y mano de obra por cada uno de los dispositivos que conforman la solución de seguridad, con que cuenta actualmente la entidad, por el término de un (1) año, a partir de la fecha de vencimiento de la garantía actual. 1. Dos (2) dispositivos Firewall Fortigate nuevos entregados en el upgrade de hardware, por el término de un (1) año, contado a partir de la fecha de activación. 2. Un (1) dispositivo Sandbox – FortiSandbox 2000E, por el término de un (1) año, contado a partir de la fecha de activación. 3. Un (1) dispositivo SIEM – FortiSIEM 2000F, por el término de un (1) año, contado a partir de la fecha de activación. 4. Un (1) dispositivo Reporteador – FortiAnalyzer 300G, por el término de un (1) año, contado a partir de la fecha de activación.
1. Se debe contemplar la continuidad del servicio 7X24 por cada uno de las herramientas Cloud que conforman la solución de seguridad, con que cuenta actualmente la entidad, por el término de un (1) año, a partir de la fecha de vencimiento de la garantía actual. 2. Una (1) Servicio de protección de correo electrónico - **FortiMail CLOUD**, por el término de un (1) año contado a partir de la fecha de activación. 3. Una (1) Servicio XDR - **FortiXDR Cloud**, por el término de un (1) año contado a partir de la fecha de activación.
Durante el periodo de garantía debe atender y resolver cualquier solicitud de servicio y/o incidente y/o asistencia técnica donde se describa la indisponibilidad de uno o varios dispositivos y/o servicios existentes de la solución completa de seguridad de la entidad (Firewall Fortigate, FortiSandbox, FortiSIEM y FortiAnalyzer). Tanto en el software como en el hardware, en un esquema de atención 7x24x6 (siete (7) días a la semana, veinticuatro (24) horas al día y seis (6) horas para la atención). En los medios definidos de común acuerdo por el contratista y supervisor del contrato en la matriz de escalamiento, dentro de los que se encuentran telefónico, email, acceso remoto o presencial en caso de que la SUPERSERVICIOS así lo requiera con atención en sitio (en horario continuo).
Durante el periodo de garantía debe atender y resolver cualquier solicitud de servicio y/o incidente y/o asistencia técnica donde se describa la indisponibilidad de uno o varios dispositivos y/o servicios existentes de la solución completa de seguridad de la entidad (FortiMail y FortiXDR). Tanto en el software como en el hardware, en un esquema de atención 7x24x2 (siete (7) días a la semana, veinticuatro (24) horas al día y dos (2) horas para la atención). En los medios definidos de común acuerdo por el contratista y supervisor del contrato en la matriz de escalamiento, dentro de los que se encuentran telefónico, email, acceso remoto o presencial en caso de que la SUPERSERVICIOS así lo requiera con atención en sitio (en horario continuo).
La atención durante el periodo de garantía debe ser en los medios definidos de común acuerdo por el contratista y supervisor del contrato en la matriz de escalamiento, dentro de los que se encuentran telefónico, email, acceso remoto o presencial en caso de que la SUPERSERVICIOS así lo requiera con atención en sitio (en horario continuo).
Durante el periodo de garantía para los servicios de atención de solicitudes de servicio y/o incidentes y/o asistencia técnica de uno o varios dispositivos y/o servicios existentes de la solución completa de seguridad de la entidad (Firewall Fortigate, FortiMail, FortiSandbox, FortiSIEM, FortiAnalyzer y FortiXDR) debe ser brindada por personal especializado del contratista y certificado por el fabricante. El contratista debe contactar al fabricante en los casos que sea requerido para que brinde apoyo a atención de solicitudes de servicio y/o incidentes y asistencia técnica.

PARÁGRAFO: En el caso que el proveedor requiera más tiempo para dar la solución al incidente en aquellos casos en que se necesite apoyo con asistencia del fabricante, se deberá sustentar al supervisor del contrato y proponer dentro de los tiempos establecidos por la entidad para brindar solución al requerimiento la(s) medida(s) de contingencia ante el(los) requerimiento(s) reportado(s).
La garantía ofrecida deberá ser a través del fabricante y deberá cubrir cualquier defecto de fabricación o mal funcionamiento y/o reemplazo del equipo en caso de ser necesario, dicha garantía y soporte de la solución será por el término de un (1) año contado a partir de las fechas de renovación del licenciamiento, soporte y garantía de la solución completa de seguridad de la entidad (Firewall Fortigate, FortiMail, FortiSandbox, FortiSIEM, FortiAnalyzer y FortiXDR), contado a partir de la fecha de activación.
SOPORTE
Apoyar a la entidad en todas las peticiones de soporte que se presenten relacionadas con la operación y funcionamiento de uno o varios dispositivos y/o servicios existentes de la solución completa de seguridad de la entidad (Firewall Fortigate, FortiSandbox, FortiSIEM y FortiAnalyzer). Tanto en el software como en el hardware, en un esquema de atención 7x24x6 (siete (7) días a la semana, veinticuatro (24) horas al día y seis (6) horas para la atención), en los medios definidos de común acuerdo por el contratista y supervisor del contrato en la matriz de escalamiento, dentro de los que se encuentran telefónico, email, acceso remoto o presencial en caso de que la SUPERSERVICIOS así lo requiera con atención en sitio (en horario continuo). Por el término de un (1) año contado a partir de las fechas de renovación del licenciamiento, soporte y garantía. Por lo que el contratista debe realizar las actividades de gestión técnica, soporte y atención a fallas, de manera coordinada con el supervisor del contrato.
Apoyar a la entidad en todas las peticiones de soporte que se presenten relacionadas con la operación y funcionamiento de uno o varios dispositivos y/o servicios existentes de la solución completa de seguridad de la entidad (FortiMail y FortiXDR). Tanto en el software como en el hardware, en un esquema de atención 7x24x2 (siete (7) días a la semana, veinticuatro (24) horas al día y dos (2) horas para la atención), en los medios definidos de común acuerdo por el contratista y supervisor del contrato en la matriz de escalamiento, dentro de los que se encuentran telefónico, email, acceso remoto o presencial en caso de que la SUPERSERVICIOS así lo requiera con atención en sitio (en horario continuo). Por el término de un (1) año contado a partir de las fechas de renovación del licenciamiento, soporte y garantía. Por lo que el contratista debe realizar las actividades de gestión técnica, soporte y atención a fallas, de manera coordinada con el supervisor del contrato.
Todos los componentes de la solución completa de seguridad con que cuenta la entidad, deben quedar operativos con las características solicitadas en las especificaciones técnicas de este ***Anexo No. 4 Ficha Técnica Solución de Seguridad – Lote 4 – Requerimientos técnicos mínimos***, que hace parte integral de este documento del licenciamiento Firewall Fortigate, FortiSandbox, FortiSIEM, FortiAnalyzer, FortiMail, y FortiXDR, por lo cual la SUPERSERVICIOS no deberá adquirir licenciamiento adicional para cumplir con los requerimientos descritos en este proceso de selección, en el pliego de condiciones, las adendas que se lleguen a expedir, en el presente anexo técnico, en los demás documentos que hacen parte integral de este proceso, y en el contrato que se derive del presente proceso de selección.
Debe entregar carta de compromiso al momento de la entrega de los documentos de renovación y adquisición del licenciamiento, soporte y garantía de los componentes de la solución completa de seguridad al supervisor del contrato, en la cual se compromete a prestar el servicio de soporte por un equipo humano certificado por el fabricante de la plataforma instalada, por el término de un(1) año contado a partir de las fechas de renovación del licenciamiento, soporte y garantía conforme a lo dispuesto en este ***Anexo No. 4 Ficha Técnica Solución de Seguridad – Lote 4 – Requerimientos técnicos mínimos***. que hace parte integral de este documento.
Debe atender y resolver cualquier requerimiento (solicitud de servicio que no genere indisponibilidad) sobre los componentes de la solución completa de seguridad de la entidad (Firewall Fortigate, FortiSandbox,

FortiSIEM, FortiAnalyzer, FortiMail, y FortiXDR). relacionados en el ***Anexo No. 4 Ficha Técnica Solución de Seguridad – Lote 4 – Requerimientos técnicos mínimos*** que hace parte integral de este documento, tanto en el software como en el hardware, en un esquema de atención 5x8 (cinco (5) días a la semana, ocho (8) horas al día) en los medios definidos de común acuerdo por el contratista y supervisor del contrato en la matriz de escalamiento, dentro de los que se encuentran telefónico, email, acceso remoto o presencial en caso de que la SUPERSERVICIOS así lo requiera con atención en sitio. El soporte a requerimientos deberá ser suministrado por personal especializado del contratista y certificado por el fabricante. El contratista deberá contactar al fabricante en los casos que sea requerido para que brinde atención del requerimiento, dentro del rango de tiempo asignado de ocho (8) horas hábiles para el diagnóstico y cuarenta (40) horas calendario para brindar la solución al requerimiento, por el término de un (1) año que para el caso será para los componentes de la solución completa de seguridad de la entidad (Firewall Fortigate, FortiSandbox, FortiSIEM, FortiAnalyzer, FortiMail, y FortiXDR) contado a partir de la fecha de activación, conforme lo dispuesto en este ***Anexo No. 4 Ficha Técnica Solución de Seguridad – Lote 4 – Requerimientos técnicos mínimos***. **PARÁGRAFO:** En el caso que el proveedor requiera más tiempo para dar la solución al incidente en aquellos casos en que se necesite apoyo con asistencia del fabricante, se deberá sustentar al supervisor del contrato y proponer dentro de los tiempos establecidos por la entidad para brindar solución al requerimiento la(s) medida(s) de contingencia ante el(los) requerimiento(s) reportado(s).
Durante el tiempo de vigencia del soporte y garantía del contrato para el licenciamiento y soporte adquirido para los componentes de la solución completa de seguridad de la entidad (Firewall Fortigate, FortiSandbox, FortiSIEM, FortiAnalyzer, FortiMail, y FortiXDR), el contratista debe llevar a cabo las actualizaciones de nuevas versiones de software o firmware liberados y estables por el fabricante de manera oportuna y debe realizar un (1) mantenimiento preventivo físico y lógico, este último será definido por la entidad de común acuerdo con el contratista, sin costo adicional para la Superservicios. **PARÁGRAFO 1:** El contratista en común acuerdo con la entidad programará la fecha y hora para las actualizaciones de firmware y software en los momentos que se lleguen a solicitar por la entidad durante la vigencia de la garantía y soporte. **PARÁGRAFO 2:** El contratista dispondrá del recurso técnico para realizar los backup de configuraciones y data de los dispositivos previo a la elaboración de las actividades de actualización de los componentes de seguridad de la entidad.
Si para la solución de los requerimientos de servicios técnicos enmarcados en las actividades de mantenimiento preventivo sobre los componentes de la solución de seguridad, el contratista requiere la intervención del fabricante o de un tercero (personal certificado); el contratista debe garantizar a través de su gestión, el acompañamiento y participación de manera presencial durante el desarrollo de las actividades de solución. En todo caso el contratista será el directamente responsable de la solución del problema y de mantener debidamente informado al supervisor del contrato.
El contratista, durante la ejecución del contrato y todo el término de soporte, al momento de finalizar cada actividad requerida (requerimiento e incidente) deberá entregar un informe con su respectiva orden de servicio al supervisor del contrato, de todas las actividades realizadas por el personal incluyendo: ● Horario de ingreso y salida a las instalaciones de la SUPERSERVICIOS. ● Actividades realizadas por cada especialista, recomendaciones, procedimientos aplicados, relación de cambio de partes si da lugar, aplicación de mejores prácticas, pendientes, recomendaciones y toda la documentación relevante para mantener la gestión sobre los componentes de la infraestructura de seguridad. ● Relación de los tickets escalados al fabricante, descripción y seguimientos a las actividades realizadas hasta la solución del incidente.

CERTIFICACIONES REQUERIDAS

El oferente debe presentar las especialidades técnicas del fabricante dentro de la cuales son obligatorias (Cloud Security, Operational Technology, SASE, SD-WAN, Secure Networking Firewall, Security Operations, Zero Trust Network Access), de igual forma el oferente debe estar categorizado como Engage Tech Support Partner.

ISO27001: El oferente debe presentar junto con su propuesta el certificado ISO 27001 versión 2013 o 2022 (SGSI) y este debe de tener al menos un (1) año de vigencia, lo anterior con el fin de garantizar que se cumplen con los estándares de seguridad de la información.

En caso de uniones temporales y/o consorcios cada uno de los integrantes debe aportar las certificaciones de los puntos anteriores por individual, no se aceptan propuestas donde solo uno de los integrantes del consorcio cumpla con el requerimiento, lo anterior con el fin de evitar figuras de apalancamiento entre los proveedores los cuales pueden ocasionar pérdida en la calidad de los servicios profesionales solicitados.

EQUIPO MÍNIMO DE TRABAJO REQUERIDO

Equipo	Título / Certificaciones / Cursos	Experiencia Profesional Específica
Un (01 Ingeniero Gerente de Proyecto	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones, industrial o carreras afines. ● Posgrado en Gerencia de Proyectos y/o Certificación PMP. ● Certificación ITIL Foundation v3 o superior. ● Certificación ITIL Service Offerings and Agreements.	Experiencia mínima 5 proyectos gerenciando y/o coordinando proyectos de TI y/o Seguridad Informática. Tarjeta Profesional con expedición mínima de diez (10) años
Un (01) Ingeniero Líder Técnico	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. ● Especialización o maestría en Seguridad de la Información o informática. ● Certificación vigente en SCRUM Foundations Professional (SFPC).	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo de tres (3) años como líder o coordinador o gerente de servicio de TI. Certificaciones de Experiencia específica de mínimo años (4) años en implementación o administración en plataformas de seguridad.

	● Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018. ● Certificación vigente en AUDITOR LÍDER en la norma ISO/IEC 27001:2022. ● Certificación vigente en LÍDER GESTOR CIBERSEGURIDAD en la norma ISO/IEC 27032:2023. ● Certificación vigente en Especialista en Soluciones de Fortinet Certified Solution Specialist Security Operations (FCSS Security Operations) y Fortinet Certified Solution Specialist Network Security (FCSS Network Security).	La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
Un (01) Ingeniero Implementador	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. ● Especialización y/o maestría en Seguridad de la Información o informática. ● Certificación vigente en AUDITOR LÍDER en la norma ISO/IEC 27001:2022. ● Certificación vigente en Profesional de Seguridad de Redes de Fortinet (FCP Network Security).	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo de cuatro (4) años en implementación, soporte y/o monitoreo de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
Un (01) Ingeniero de afinamiento y soporte	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. ● Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018. ● Certificación vigente en Profesional de Seguridad de Redes de Fortinet (FCP Network Security).	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo de cuatro (4) años en implementación, soporte y monitoreo de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
Nota 1: El personal requerido debe ser propio del oferente, no se aceptan figuras de tercerización de servicios y/o prestación de servicios, para ello se deben enviar las hojas de vida, junto con el contrato de vinculación laboral en conjunto con la oferta.		

Nota 2: No se aceptan cargos mixtos, es decir, solo podrá aplicar una persona por rol.

NOTA: Mediante el diligenciamiento y firma de este Anexo Técnico por parte del Representante Legal del proponente interesado, el mismo se compromete a proveer el servicio, entregar los bienes, poner a disposición de la Entidad el recurso humano indicado con el perfil señalado y demás, descritos en este documento en los términos, condiciones y de conformidad con las especificaciones técnicas descritas al respecto por cada ítem, y en observancia de las obligaciones contractuales y el plazo previsto en el mismo, una vez se dé inicio a la ejecución del proyecto.

NOTA 2: En caso de resultar favorecedor el proponente se compromete a que dentro de los tres (03) días hábiles siguientes a la firma del acta de inicio deberá entregar a la Entidad los documentos requeridos y enlistados en este Anexo Técnico por cada uno de los perfiles solicitados por la entidad y aceptados por el proponente mediante la firma y diligenciamiento de este Anexo Técnico, para aprobación de la SUPERSERVICIOS. Y adicionalmente, se compromete a mantener un perfil idóneo conforme lo indicado en este Anexo durante todo el periodo de ejecución del contrato y su respectivo período de soporte.

En mi calidad de Representante Legal, en forma voluntaria e irrevocable, mediante la suscripción y firma del presente documento, manifiesto CONOCER y ACEPTAR, de manera uniforme y sin modificación alguna, la totalidad de las especificaciones técnicas, obligaciones y condiciones planteadas por la SUPERSERVICIOS a través del pliego de condiciones y las contenidas en esta ***Ficha de Especificaciones y requerimientos técnicos mínimos para Solución de Seguridad – Lote 4*** , la cual contempla la totalidad de las especificaciones técnicas mínimas requeridas para el Lote 4 descrito en el ítem **3.1.1. ALCANCE** de los Estudios Previos.

EN CONSECUENCIA, ME COMPROMETO A DARLES ESTRICTO CUMPLIMIENTO.

NOMBRE O RAZÓN SOCIAL DEL OFERENTE: _____

NOMBRE DEL REPRESENTANTE LEGAL: _____

FIRMA DEL REPRESENTANTE LEGAL: _____

C.C. DEL REPRESENTANTE LEGAL: _____

Anexo Técnico No. 5

Ficha de Especificaciones y requerimientos técnicos mínimos para Herramienta de monitoreo de red – Lote 5

Se debe suscribir el presente Anexo Técnico, sin alterar o suprimir ninguna de las características e ítems relacionados en el mismo, el cual contempla la totalidad de las especificaciones técnicas mínimas para la ejecución y cumplimiento de la necesidad técnica identificada por parte de la entidad, como parte del proceso de estudio de mercado que adelanta la SUPERSERVICIOS.

Se deberá entregar el soporte y garantía de los componentes, así como entregar el licenciamiento, documentación y/o demás soportes descritos en este documento en los términos, condiciones y de conformidad con las especificaciones técnicas descritas al respecto por cada ítem.

ÍTEM	*PRODUCTO*	*DESCRIPCIÓN*	*CANTIDAD*
1	PAESSLER PRTG NETWORK MONITOR - Number of sensors: 10000 (XL1: PRTG 10000) - Subscription period: 3 Years	Suscripción de la herramienta en nube para la herramienta de software PRTG Network Monitor XL1:PRTG 10000 SENSORES en la modalidad de 10000 sensores. Por el término de treinta y seis (36) meses	1

- Entregar a la SUPERSERVICIOS dentro de los cinco (5) días hábiles siguientes a la suscripción del acta de inicio, el documento o certificación en el cual se evidencie la activación de la suscripción del Lote 5, PRTG Network Monitor XL1:PRTG 10.000 sensores, que para el caso será por el término de treinta y seis (36) meses, a partir de dicha activación.

- Suministrar el usuario y contraseña para descargar los instaladores del producto y sus productos relacionados, manteniéndola activada a favor de la Entidad, por el término de treinta y seis (36) meses.

- Realizar las actualizaciones necesarias de la suscripción de la licencia de PRTG Network Monitor XL1:PRTG 10.000 sensores, en su última versión estable y disponible, durante la totalidad del término de la suscripción contratada.

NOTA 1: Se debe suscribir el presente Anexo Técnico, sin alterar o suprimir ninguna de las características e ítems relacionados en el mismo, el cual contempla la totalidad de las especificaciones técnicas mínimas para la ejecución y cumplimiento de la necesidad técnica identificada por parte de la entidad, como parte del proceso de estudio de mercado que adelanta la Superservicios.

NOTA 2: Se deberá entregar el soporte y garantía de los componentes, así como entregar el licenciamiento, documentación y/o demás soportes descritos en este documento en los términos, condiciones y de conformidad con las especificaciones técnicas descritas al respecto por cada ítem.

NOTA3: Mediante el diligenciamiento y firma de este Anexo Técnico por parte del Representante Legal del proponente interesado, el mismo se compromete a proveer el servicio y a entregar los bienes y demás, descritos en este documento en los términos, condiciones y de conformidad con las especificaciones técnicas descritas al respecto por cada ítem, y en observancia de las obligaciones contractuales y el plazo previsto en el mismo, una vez se dé inicio a la ejecución del proyecto.

En mi calidad de Representante Legal, en forma voluntaria e irrevocable, mediante la suscripción y firma del presente documento, manifiesto CONOCER y ACEPTAR, de manera uniforme y sin modificación alguna, la totalidad de las especificaciones técnicas, obligaciones y condiciones planteadas por la SUPERSERVICIOS a través del pliego de condiciones y las contenidas en este ***Ficha de Especificaciones y requerimientos técnicos mínimos para Herramienta de monitoreo de red – Lote 5***, la cual contempla la totalidad de las especificaciones técnicas mínimas requeridas para el Lote 5 descrito en el ítem **3.1.1. ALCANCE** de los Estudios Previos.

EN CONSECUENCIA, ME COMPROMETO A DARLES ESTRICTO CUMPLIMIENTO.

NOMBRE O RAZÓN SOCIAL DEL OFERENTE: _____

NOMBRE DEL REPRESENTANTE LEGAL: _____

FIRMA DEL REPRESENTANTE LEGAL: _____

C.C. DEL REPRESENTANTE LEGAL: _____

Anexo Técnico No. 6

Ficha de Especificaciones y requerimientos técnicos mínimos para copias de respaldo – Lote 6

ÍTEM	RENOVACIÓN DE LA SOLUCIÓN ACTUAL DE BACKUP	CANTIDAD
		1
A.	**ALCANCE**	
1	Adquisición de una solución de Backup moderna para respaldo y recuperación para la información, servicios y aplicaciones de la SUPERSERVICIOS, con licenciamiento para (240) servidores Virtuales en Vmware y (10) Servidores físicos con licenciamiento avanzado para el software de back up con características de ciberseguridad, replicación y recuperación instantánea, inmutabilidad, mas soporte y garantía un (1) año. Para la correcta implementación de la solución de respaldo y recuperación de datos, se requerirán servicios profesionales especializados que incluyan la instalación, configuración, integración, pruebas y puesta en marcha de la solución de respaldo así como la integración con la solución de almacenamiento actual Exagrid. Estos servicios deben garantizar que la solución se integre adecuadamente con la infraestructura tecnológica de la Entidad, que se configuren políticas de respaldo, retención y replicación acordes a las necesidades Entidad, y que se entregue capacitación y transferencia al personal que administra la solución. Asimismo, se espera el acompañamiento durante la puesta en producción y la entrega de la documentación técnica correspondiente a la implementación. **1. Objeto de la Adquisición** Adquisición de una solución de Backup moderna para respaldo y recuperación de la información, servicios y aplicaciones de la SUPERSERVICIOS. La solución deberá incluir: ● **Licenciamiento:** Para **doscientos cuarenta (240) servidores virtuales** en VMware y **diez (10) servidores físicos**. ● **Características Avanzadas:** El licenciamiento debe incluir funcionalidades de **ciberseguridad, replicación, recuperación instantánea e inmutabilidad**. ● **Soporte y Garantía:** Se requiere soporte y garantía por un período de **un (1) año**. **2. Servicios Profesionales Requeridos** Para la correcta implementación, se necesitarán servicios profesionales especializados que garanticen la integración adecuada con la infraestructura tecnológica de la Entidad. Estos	

servicios deben incluir:

- **Instalación y Configuración:** Instalación, configuración, integración, pruebas y puesta en marcha completa de la solución de respaldo.
- **Integración:** Integración específica con la solución de almacenamiento actual **Exagrid**.
- **Políticas:** Configuración de políticas de respaldo, retención y replicación acordes a las necesidades de la Entidad.
- **Capacitación:** Entrega de capacitación y transferencia de conocimiento al personal que administrará la solución.
- **Acompañamiento:** Soporte durante la fase de puesta en producción.
- **Documentación:** Entrega de toda la documentación técnica correspondiente a la implementación.

3. Requerimientos Técnicos del Software

El software de respaldo debe cumplir con todas las especificaciones técnicas y funcionales detalladas a continuación, sin incurrir en costos o licencias adicionales para su implementación.

3.1. Administración y Licenciamiento

- **Instalación:** Debe ser instalado y configurado para alta disponibilidad en el servidor que la Entidad disponga.
- **Consola de Administración:** La solución debe operar con una consola de administración unificada que funcione **On-Premise o en la Nube**, según designe la Entidad.
- **Interfaz de Usuario:** Debe contar con una interfaz gráfica (GUI) y una interfaz de línea de comandos (CLI), ambas disponibles en **español o inglés**.
- **Licenciamiento:** Cubrir **240 servidores virtuales** en VMware y **10 servidores físicos**.
- **Soporte y Vigencia:** La solución debe contar con soporte **7x24** durante la vigencia de la suscripción. El soporte de Nivel I será con el oferente y el de Nivel II con el fabricante. El licenciamiento y la garantía deben tener una vigencia mínima de **doce (12) meses**.

3.2. Compatibilidad e Integración

- **Sistemas Operativos:** Soportar Windows Server (2008, 2012, 2016, 2019, 2022, 2025) y distribuciones de Linux (Centos 7-8, Ubuntu 20.04-24.04, AlmaLinux, Rocky Linux, Red Hat, entre otros).
- **Hipervisores:** Ser compatible con VMware, Nutanix Acropolis Hypervisor (AHV), Hyper-V, y permitir copias de seguridad en versiones actuales y futuras de estos.
- **Bases de Datos:** Permitir respaldo y recuperación granular de motores como MS SQL Server, PostgreSQL, MariaDB y Oracle.
- **Integración con Oracle:** Soportar la integración con Oracle Recovery Manager (RMAN) para respaldo y recuperación. Debe ser compatible con Oracle Database (11gR2, 12c, 18c, 19c, 21c), Oracle RAC y discos ASM.
- **Almacenamiento:** Integrarse con plataformas SAN, NAS y repositorios de almacenamiento hiperconvergentes o tipo *scale-out*. Debe ser compatible con la inmutabilidad de dispositivos de deduplicación como EMC Data Domain, HPE StoreOnce y **ExaGrid**.

- **Contenedores:** Soportar el respaldo y restauración de servicios en contenedores (On-premise y/o en la nube) que funcionen en plataformas como **Openshift** o similares. Debe permitir la migración de aplicaciones entre distribuciones de Kubernetes y proveedores de nube.
- **Automatización:** Soportar PowerShell SDK y API para ser consumida por otras herramientas de la Entidad.

3.3. Funcionalidades de Respaldo y Recuperación

- **Tipos de respaldo:** Soportar copias de seguridad **full, incremental, diferencial e incremental inverso**.
- **Alcance:** Permitir respaldar y restaurar máquinas virtuales completas, bases de datos, *file servers* y servidores físicos.
- **Automatización:** Permitir la configuración de tareas o *jobs* automáticos y programación múltiple para backup y replicación, así como la generación de copias por demanda.
- **Recuperación Granular:** Permitir la restauración de un solo archivo, un elemento de aplicación o una base de datos desde disco o cinta, sin usar productos de terceros.
- **Recuperación de Oracle:** Admitir la recuperación granular de bases de datos Oracle desde la consola del software, hacia un servidor y ubicación diferentes al de origen.
- **Archivos en Uso:** Contar con tecnología para respaldar archivos que se encuentren abiertos y en uso.
- **Recuperación Instantánea:** Incluir funcionalidades de copias instantáneas (*snapshots*) y recuperación ante desastres. Para VMware, debe ser capaz de detectar y eliminar *snapshots* huérfanos automáticamente.
- **Migración:** Proporcionar tecnología para la migración de máquinas virtuales VMware entre clústeres y centros de datos.

3.4. Seguridad y Ciber Resiliencia

- **Autenticación Multifactor (MFA):** Incluir mecanismos de MFA para prevenir acciones no autorizadas como eliminación de respaldos o cambios de permisos.
- **Control de Acceso:** Permitir el control de acceso basado en roles y la delegación granular de tareas de respaldo y restauración.
- **Inmutabilidad:** Ofrecer configuración de retención e inmutabilidad para proteger los backups contra eliminación o modificación no autorizada (ej. ransomware), tanto en repositorios locales como en almacenamiento de objetos en la nube.
- **Cifrado:** Contar con cifrado de extremo a extremo (End-to-End) para los archivos de respaldo usando el estándar **AES de 256 bits**, de forma independiente a la plataforma de almacenamiento.
- **Análisis de Amenazas:** Verificar la consistencia de los backups y escanear en busca de malware y ransomware (en tránsito y en reposo) mediante firmas, reglas heurísticas, YARA o Inteligencia Artificial, sin requerir un entorno aislado.
- **Detección de anomalías:** Detectar factores de riesgo de ransomware, como cambios anómalos en la cantidad de archivos de las máquinas virtuales.
- **Escaneo de Virus:** Permitir el escaneo de datos de producción en busca de virus antes o durante la verificación del respaldo.

3.5. Optimización y Eficiencia

- **Deduplicación:** Ofrecer deduplicación de datos en el almacenamiento, incluso si no se

	aplica en el origen. Utilizar deduplicación global para optimizar el uso del ancho de banda. ● **Compresión:** Contar con niveles de compresión para optimizar el espacio de almacenamiento. ● **Replicación Avanzada:** Permitir la replicación nativa entre el centro de datos principal y el alterno. Incluir tecnologías como deduplicación, copias instantáneas y protección continua de datos (CDP) para recuperación a cualquier punto en el tiempo. **3.6. Monitoreo, Informes y Gestión** ● **Operación Centralizada:** Permitir un control completo y centralizado de la protección de datos en repositorios de disco y almacenamiento en la nube. ● **Catálogo Central:** Ofrecer un catálogo central de copias de seguridad. ● **Indexación y Búsqueda:** Permitir la indexación de copias de seguridad (no autocontenida) para una fácil búsqueda de archivos por metadatos. ● **Dashboard:** Contar con un *dashboard* con *widgets* para monitorear la infraestructura de respaldo. ● **Alertas:** Consolidar alertas y proporcionar notificaciones proactivas sobre trabajos fallidos y otros problemas potenciales. ● **Informes:** Generar informes centralizados y por demanda sobre: ○ Salud y estado de la infraestructura. ○ Estado de los trabajos de respaldo (duración, resultado). ○ Operaciones de recuperación para fines de auditoría. ○ Máquinas virtuales no protegidas. ○ Cambios en políticas de respaldo para auditoría. ○ Estadísticas de consumo (CPU, RAM, disco, IOPS, latencias). ● **Planificación de Capacidad:** Pronosticar la utilización del espacio de almacenamiento de respaldo. **3.7. Requisitos de Mercado y Políticas** ● **Posicionamiento en el Mercado:** La solución debe estar ubicada en la sección de **líderes del cuadrante de Gartner** para soluciones de backup y recuperación empresarial durante los años **2024 y 2025**. ● **Políticas de Retención:** Permitir la configuración de políticas de retención flexibles, incluyendo modelos como "corto plazo", "incrementales hacia adelante", "incrementales inversas" y el modelo "full + incremental para siempre".
2	*Soporte y garantía de los equipos enunciados debe ser hasta el día 27 de noviembre de 2026.* * Cuatro (4) Exagrid EX40000E-SEC * Un (1) Exagrid EX52000E

	<table><tr><th>Product Serial Number</th><th>Internal Mo...</th></tr><tr><td>EX-CT422042800430</td><td>052TS20</td></tr><tr><td>EX-AVTA203603608</td><td>040TS15</td></tr><tr><td>EX-AVTA203303529</td><td>040TS15</td></tr><tr><td>EX-AVTA192302004</td><td>040TS15</td></tr><tr><td>EX-AVTA192301989</td><td>040TS15</td></tr></table>
B.	**SOPORTE**
1	El soporte debe cubrir las actualizaciones de firmware, al menos una (1) vez al año durante el término de soporte.
3	El contratista debe garantizar el suministro de repuestos sin costo adicional el término de soporte.
4	Cubrir las actualizaciones de Firmware necesarias y que hayan sido liberadas por el fabricante. Cuando estas sean recomendadas para mitigar fallas de seguridad inminentes y no dentro de las actualizaciones normales de fabrica.
6	Realizar los mantenimientos preventivos y correctivos a todos los equipos que conforman el objeto de este proceso de selección
7	El licenciamiento de la solución de Backup debe contar con soporte por 1 año y los Appliances EXAGRID deben contar con soporte de fábrica hasta el veintisiete (27) de noviembre de 2026. y los Appliances EXAGRID deben contar con soporte de fábrica hasta el veintisiete (27) noviembre de 2026. Con servicio de garantía en partes, con mano de obra incluida y con atención en la ubicación donde se encuentre el equipo con dicho cubrimiento Debe contar con atención de **5x8x4** (Atención cinco (5) días de la semana, las ocho (8) horas del día y tiempo de atención en forma remota, pero de ser necesario manos remotas, debe ser prestado por el contratista en sitio, cuatro (4) horas hábiles después de reportado el caso y realizado un diagnóstico previo). El contratista deberá allegar la garantía del fabricante donde se especifique el período de cobertura de la misma.
8	Durante el periodo de soporte, el contratista se compromete a dar el soporte al software y reparar los equipos y dejarlos en perfecto estado de funcionamiento en un tiempo máximo de ocho (8) horas contadas a partir de la fecha y hora de haber realizado el reporte de la falla en los medios definidos por el contratista y supervisor del contrato.
9	Cuando se presente fallas generales o particulares en los equipos, el contratista deberá dar soporte en sitio con personal certificado en un tiempo no mayor a cuatro (4) horas hábiles, contadas a partir de la fecha y hora de haber realizado el reporte de la falla en los medios definidos por el contratista y supervisor del contrato si así lo requiere y no es posible dar la solución de forma remota.

C.	HARDWARE
10	Asistir a la Entidad en todas las peticiones de soporte que se presenten relacionadas con la operación y funcionamiento de la solución en el tiempo de **5x8x4** (Atención cinco (5) días de la semana, las ocho (8) horas del día y tiempo de atención en forma remota pero de ser necesario manos remotas, debe ser prestado por el contratista en sitio, cuatro (4) horas hábiles después de reportado el caso y realizado un diagnóstico previo); por lo que el contratista debe realizar las actividades de gestión técnica, soporte y atención a fallas, de manera coordinada para los componentes o servicios de la solución que se renovará.
11	Durante el tiempo de soporte, el soporte de la solución debe ser prestado por el Fabricante con el equipo humano certificado por el mismo en acompañamiento de personal con experiencia en la solución por parte del contratista en la plataforma con la que cuenta la entidad.
12	El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario hábil. (De acuerdo con la matriz de escalamiento definida por el fabricante)
13	El fabricante debe incluir la garantía de reemplazo de unidades completas, componentes, tarjetas, cables, accesorios o partes en la modalidad **5x8x4** durante el periodo de soporte definido para toda la solución, que para el caso será hasta el día 27 de noviembre 2026.
14	Se deberá incluir dentro de la renovación del soporte el reemplazo de unidades completas, componentes, tarjetas, cables, accesorios o partes durante el periodo de soporte definido,que para el caso será hasta el día 27 de noviembre de 2026.
15	Si para la solución de los requerimientos de servicios técnicos enmarcados en las actividades de mantenimiento preventivo, el contratista requiere la intervención de la casa fabricante de los equipos o de un tercero (personal certificado); el contratista debe garantizar a través de su gestión, el acompañamiento y participación de manera presencial durante el desarrollo de las actividades de solución. **NOTA: En todo caso el contratista será directamente responsable de la solución del problema y de mantener debidamente informado al supervisor del contrato.**
16	El contratista al finalizar una actividad requerida debe entregar un informe con su respectiva orden de servicio, al supervisor del contrato, de todas las actividades realizadas por el personal incluyendo: - Horario de ingreso y salida a las instalaciones de la SSPD. - Actividades realizadas por cada especialista, recomendaciones, aplicación de mejores prácticas, y toda la documentación relevante para mantener la gestión del sistema ofertado.

ÍTEM	SERVICIOS DE INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO	CANTIDAD
		1

A.	SERVICIOS DE INSTALACIÓN
1	El contratista debe realizar la planeación de cada una de las actividades con el fin de disminuir los tiempos de afectación del servicio, lo cual puede ejecutarse en horarios hábiles o no-hábiles por lo cual el contratista, durante la ejecución de la implementación de la ampliación, debe contemplar lo anterior dentro de sus costos al momento de realizar su propuesta.
2	El contratista debe verificar la necesidad de la elaboración o generación de nuevas políticas de copias de respaldo según los lineamientos de la SUPERSERVICIOS objeto de esta contratación.
3	Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante.
4	Pruebas sobre la solución de copias de respaldo del servicio de renovación de soporte contratado.
5	Como parte de las pruebas a realizar, el contratista debe revisar la consistencia de una muestra aleatoria de los copias de respaldo, tanto las que se realizan en el GRID principal, como a las que les realiza la replicación hacía el GRID Secundario en sitio alterno.
6	Hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la solución de copias de respaldo, propiedad de la SUPERSERVICIOS, así como la solución integral de copias de seguridad, en forma escrita.
B.	**ALCANCE DE LOS SERVICIOS**
7	Se debe realizar el proceso de instalación, upgrade o implementación y puesta a punto del software y solución de backup de ser necesario.
8	Revisión de arquitectura y software instalados en donde al menos se revisen los siguientes puntos: a. Versiones actuales de los servidores a respaldar en el nodo (*Appliance*) parte de la actual solución integral de copias de respaldo de la entidad para replicación de información en sitio alterno. b. Esquema de Red. c. Tiempos de transferencia. d. Tazas de restauración.
9	Se debe realizar la verificación de las políticas de copias de respaldo de los clientes (servidores) de la entidad que hacen parte de la toma de copias y replicación, verificando que se utilicen de manera óptima los espacios de los nodos (*Appliances*)
10	El contratista debe realizar las pruebas de funcionalidad del producto, medición de tiempos de respuesta de las copias de respaldo, las recuperaciones y utilización de espacio en disco y tasas de deduplicación; de acuerdo con los lineamientos del supervisor del contrato.

C.	**PROTOCOLO DE PRUEBAS**
11	Posterior a la firma del acta de inicio, dentro de los cinco (5) días hábiles siguientes, el contratista debe presentar al supervisor del contrato el formato de protocolo de pruebas (documento de pruebas) para la respectiva aprobación por parte de la SUPERSERVICIOS.
12	El contratista debe realizar pruebas durante un tiempo de siete (7) días a cada uno de los elementos, equipos y sistemas ofrecidos; término contado a partir de la aceptación del protocolo de pruebas. **Nota: Las pruebas deben ser ejecutadas antes del vencimiento del tiempo para la realización del servicio posventa (soporte y mantenimiento).**
13	Las pruebas funcionales efectuadas deberán verificar el desempeño de los elementos, equipos y sistemas, para garantizar que cumplen con todos los requerimientos funcionales y técnicos de las características técnicas de los componentes de la solución de copias de respaldo propiedad de la SUPERSERVICIOS.
D.	**MONITOREO**
14	El fabricante debe reportar a la SUPERSERVICIOS, cualquier alarma que se genere en las plataformas monitoreadas por medio de la funcionalidad "call home" o similar, a través de correo electrónico o cualquier otro medio, para esto la entidad entregará al contratista una matriz de acuerdo a cada elemento monitoreado donde se establecerá el responsable y contacto para el reporte.

NOTA: Mediante el diligenciamiento y firma de este Anexo Técnico por parte del Representante Legal del proponente interesado, el mismo se compromete a proveer el servicio y a entregar los bienes y demás, descritos en este documento en los términos, condiciones y de conformidad con las especificaciones técnicas descritas al respecto por cada ítem, y en observancia de las obligaciones contractuales y el plazo previsto en el mismo, una vez se dé inicio a la ejecución del proyecto.

En mi calidad de Representante Legal, en forma voluntaria e irrevocable, mediante la suscripción y firma del presente documento, manifiesto CONOCER y ACEPTAR, de manera uniforme y sin modificación alguna, la totalidad de las especificaciones técnicas, obligaciones y condiciones planteadas por la SUPERSERVICIOS a través del pliego de condiciones y las contenidas en esta ***Ficha de Especificaciones y requerimientos técnicos mínimos para copias de respaldo – Lote 6***, la cual contempla la totalidad de

las especificaciones técnicas mínimas requeridas para el Lote 3 descrito en el ítem **3.1.1. ALCANCE** de los Estudios Previos.

EN CONSECUENCIA, ME COMPROMETO A DARLES ESTRICTO CUMPLIMIENTO.

NOMBRE O RAZÓN SOCIAL DEL OFERENTE: _____

NOMBRE DEL REPRESENTANTE LEGAL: _____

FIRMA DEL REPRESENTANTE LEGAL: _____

C.C. DEL REPRESENTANTE LEGAL: _____