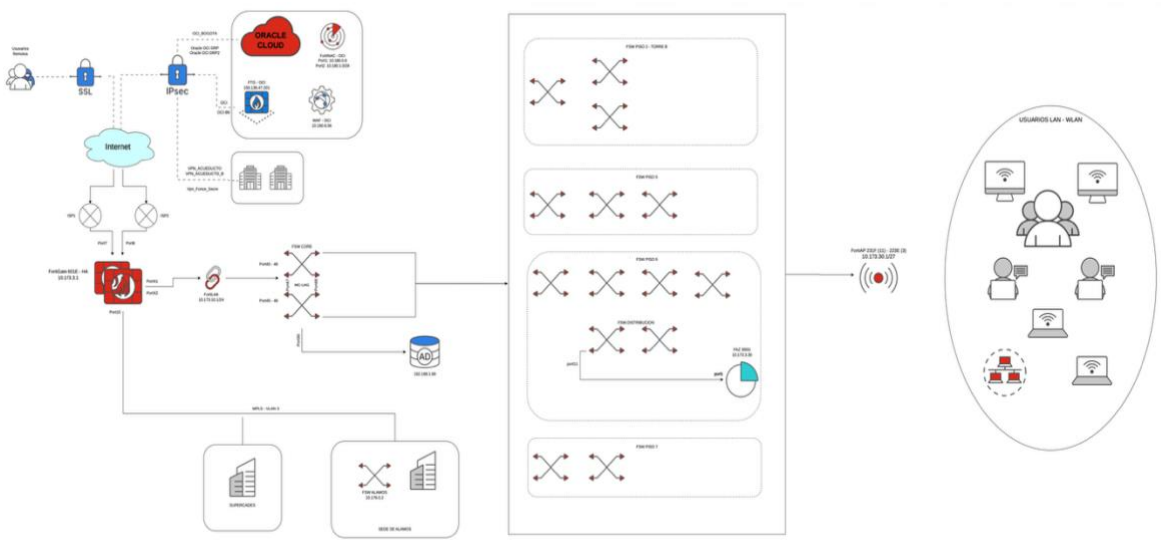
ANEXO No. 1
FICHA TÉCNICA

OIS-193-CONTRATAR LA ADQUISICIÓN Y RENOVACIÓN DEL LICENCIAMIENTO, SOPORTE DE FÁBRICA FORTINET Y BOLSA DE HORAS PARA LA ADMINISTRACIÓN Y SOPORTE DE LA INFRAESTRUCTURA DE SEGURIDAD DEL FONDO DE PRESTACIONES ECONÓMICAS, CESANTÍAS Y PENSIONES - FONCEP.

ÍTEM	RENOVACIÓN DEL LICENCIAMIENTO DE LOS COMPONENTES DE SEGURIDAD
A.	**DESCRIPCIÓN**
1.	Actualmente el FONCEP cuenta con la siguiente arquitectura de conectividad: **Topología General**  El proveedor deberá considerar los dispositivos y servicios asociados a estos sobre los cuales se requiera la renovar el licenciamiento. Así mismo 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 contado a partir de la entrega, activación recibo a satisfacción de los siguientes servicios:

COMPONENTE 1 <<SEGURIDAD PERIMETRAL>>

Ítem	Descripción	Marca	Ubicación	Referencia	Serial	Unidad	Cantidad
1	FIREWALL	FORTINET	Firewall Sede Principal	FortiGate 601E	FG6H1ETB20902580	Unidad	1
2	FIREWALL	FORTINET	Firewall Sede Principal	FortiGate 601E	FG6H1ETB20902550	Unidad	1
3	AP	FORTINET	FortiAP Sede Principal	FAP223E	FP223E5520000571	Unidad	1
4	AP	FORTINET	FortiAP Sede Principal	FAP223E	FP223E5520000581	Unidad	1
5	AP	FORTINET	FortiAP Sede Principal	FAP223E	FP223E5521002288	Unidad	1
6	AP	FORTINET	FortiAP Sede Principal	FAP431F	FP431FTF21005346	Unidad	1
7	WAF	FORTINET	WAF Cloud Oracle OCI	FortiWEB VM04	FVVM04TM23000596	Unidad	1
8	ADMINISTRADOR DE REGISTROS	FORTINET	FortiAnalyzer	FortiAnalyzer 300G	FAZ3HGTA23000478	Unidad	1
9	FortiGate VM - Virtual Appliance	FORTINET	FortiGate Nube	FortiGate VM08	FGVM8VTM24003253	Unidad	1
10	FORTINAC VM	FORTINET	FORTINAC	FORTINAC VM	FNVXCATM25003491	Unidad	1

Para los componentes FortiGate 601E (x2) y FortiAnalyzer 300G se deberá incluir el licenciamiento ENTERPRISE:

- Enterprise Protection (IPS, AI-based Inline Malware Prevention, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium)

- Enterprise Protection (FortiCare Premium plus Indicators of Compromise Service, Security Automation Service, and FortiGuard Outbreak Service)

Realizar los correctivos lógicos y de configuración que se requieran sobre otros equipos de conectividad con que cuenta la entidad:

Ítem	Descripción	Marca	Ubicación	Referencia	Serial	Unidad	Cantidad
1	AP	FORTINET	FortiAP Sede Principal	FORTIAP 431F	FP431F22006012	Unidad	1
2	AP	FORTINET	FortiAP Sede Principal	FORTIAP 431F	FP431FTF22006010	Unidad	1
3	AP	FORTINET	FortiAP Sede Principal	FORTIAP 431F	FP431FTF22003627	Unidad	1
4	AP	FORTINET	FortiAP Sede Principal	FORTIAP 431F	FP431FTF22002111	Unidad	1
5	AP	FORTINET	FortiAP Sede Principal	FORTIAP 431F	FP431FTF2309A460	Unidad	1
6	AP	FORTINET	FortiAP Sede Principal	FORTIAP 431F	FP431FTF2309A45M	Unidad	1
7	AP	FORTINET	FortiAP Sede Principal	FORTIAP 431F	FP431FTF2309A45Q	Unidad	1
8	AP	FORTINET	FortiAP Sede Principal	FORTIAP 431F	FP431FTF2309A453	Unidad	1
9	AP	FORTINET	FortiAP Sede Principal	FORTIAP 431F	FP431FTF2309A44Y	Unidad	1
10	AP	FORTINET	FortiAP Sede Principal	FORTIAP 431F	FP431FTF2309A454	Unidad	1

Una vez efectuados los correctivos lógicos y de configuración, se efectuará un monitoreo mensual por parte de la supervisión sobre el funcionamiento de los AP, del cual se dejará constancia en el informe de supervisión y el informe mensual del contratista, en caso de que se presenten fallas, el contratista deberá revisar y ajustar nuevamente los correctivos y la configuración aplicada.

De igual forma, se relacionan a continuación los equipos de conectividad de la entidad, sobre los cuales se requiere contemplar garantía, repuestos y mano de obra, además de soporte para la administración y configuración técnica:

COMPONENTE 2 <<SWITCHES>>

Ítem	Descripción	Marca	Ubicación	Referencia	Serial	Unidad	Cantidad
1	Switch Core	FORTINET	Firewall Sede Principal	FortiSwitch 1048E	FS1E48T4 23001195	Unidad	1
2	Switch Core	FORTINET	Firewall Sede Principal	FortiSwitch 1048E	FS1E48T4 23001693	Unidad	1
3	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 23056706	Unidad	1
4	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 23056808	Unidad	1
5	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 23058498	Unidad	1
6	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 23058533	Unidad	1
7	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 25017450	Unidad	1
8	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFT2 3003667	Unidad	1
9	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 23059011	Unidad	1
10	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 24047795	Unidad	1
11	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 23059147	Unidad	1
12	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 23059926	Unidad	1
13	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 23060242	Unidad	1
14	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 23060244	Unidad	1
15	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 23060268	Unidad	1

	16	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 23077284	Unidad	1
	17	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 23036080	Unidad	1
	18	Switch Acceso	FORTINET	Firewall Sede Principal	FortiSwitch 148F FPOE	S148FFTF 23035164	Unidad	1

Durante la reunión de inicio, el FONCEP hará entrega al proponente adjudicatario y/o futuro contratista del documento de arquitectura de red de la entidad y el manual de políticas de seguridad configurado actualmente.

ITEM	SERVICIOS REQUERIDOS
B.	**DESCRIPCIÓN**
1.	Configurar, afinar y revisar los reportes / logs de las plataformas mencionadas anteriormente, mantener actualizados los niveles de Firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante.
2.	Se deben incluir en la oferta mínimo dos (02) actividades de mantenimiento preventivo y/o correctivo y/o afinamiento con el fin de minimizar problemas y mantener los sistemas actualizados, estas actividades deberán ser con previa aprobación del responsable TI de la entidad.
3.	Prestar el servicio de soporte, en un esquema 7*24*365 a partir de la firma del acta de inicio del contrato, el cual deberá prestarse de forma telefónica, remoto, por correo electrónico, en sitio o a través de una página web, según se requiera, dependiendo del caso reportado. De igual modo proporcionar procedimiento de detección de incidentes que se encuentren dentro del alcance del contrato.
4.	Presentar, dentro de los diez (10) días hábiles siguientes a la suscripción del acta de inicio, documento del procedimiento implementado para la radicación de los casos de soporte tecnológico requeridos por la entidad y los ANS establecidos, acorde con los requerimientos definidos en la presente ficha técnica.
5.	Actualizar la documentación técnica de seguridad perimetral actualmente establecida en el FONCEP, incluyendo los cambios en configuración efectuados durante la ejecución del contrato, sobre los equipos de seguridad y conectividad de la entidad, teniendo en cuenta esta actividad de documentación.
6.	El licenciamiento renovado debe contemplar garantía partes o totalidad del dispositivo por parte del fabricante, por cada uno de los dispositivos que conforman la solución de seguridad de cada una de las plataformas con las cuales cuenta actualmente la entidad, mencionadas en la presente ficha y en el pliego de condiciones, por el término de un (1) año contado a partir de la entrega, activación y recibo a satisfacción. **NOTA: <u>Todas las plataformas deben quedar con su respectivo licenciamiento hasta el 15 de julio de 2027.</u>**
7.	El contratista deberá entregar al FONCEP la garantía donde se indique de manera clara el período de cobertura de la misma, junto con el certificado de activación del licenciamiento donde se indique la fecha de finalización (contada a partir de la entrega, activación y recibo a satisfacción), de conformidad con las fechas establecidas en este ítem.
8.	La garantía deberá ser ofrecida a través del fabricante y debe cubrir cualquier defecto de fabricación o mal funcionamiento y reemplazo del equipo en caso de ser necesario. Dicha

<table>
<tr><td></td><td>garantía, será por el término de un (1) año contado a partir de la fecha de entrega y activación de la renovación de licenciamientos y la activación de la nueva licencia.</td></tr>
<tr><td>9.</td><td>El contratista debe proveer un licenciamiento para realizar políticas de control de acceso sobre la red LAN y WLAN de la entidad, con la finalidad de robustecer los controles de seguridad de los usuarios que realizan la conexión a la infraestructura interna. Esta licencia deberá tener capacidad de registrar 1.000 puntos concurrentes y debe estar soportada y garantizada por el fabricante por un término de 12 meses a partir de la activación de las licencias.

La plataforma de control de acceso debe garantizar la integración nativa con las soluciones de seguridad y de red con las que cuenta la entidad.</td></tr>
<tr><td>10.</td><td>La plataforma de control de acceso debe permitir distintos niveles de operación (visibilidad, Control, respuesta)</td></tr>
<tr><td>11.</td><td>La plataforma de control de acceso debe contar con un proceso continuo de detección y categorización de dispositivos, que permita detectar y controlar dispositivos desconocidos o no autorizados de manera automática, sin requerir de agentes instalados en los dispositivos.</td></tr>
<tr><td>12.</td><td>La entidad proveerá los recursos de cómputo necesarios para la implementación de la plataforma de control de acceso. El contratista suministrará usuario de consulta para acceso a la plataforma de control, realizando la correspondiente transferencia de conocimiento para su empleo.</td></tr>
<tr><td>13.</td><td>Para la implementación de acciones correctivas el contratista debe realizar la parametrización y ajustes necesarios a la infraestructura de ciber seguridad y de seguridad de la información con que cuenta FONCEP.</td></tr>
<tr><td>14.</td><td>Acompañar el proceso de implementación del protocolo de comunicaciones IPv6 a nivel de los switches de comunicaciones del Foncep .</td></tr>
<tr><td>15.</td><td>El soporte y atención a casos deberá contemplar:

• El servicio de soporte y administración debe incluir atención de incidentes sobre las plataformas mencionadas.
• Consultas a través de llamadas telefónicas, correo electrónico.
• Sesiones remotas y atención en sitio (En caso de requerirse) en horario Hábil y No Hábil.
• Todo con respecto a las plataformas y objeto del presente contrato.

<table>
<tr><th colspan="2">PRIORIDAD</th><th>DESCRIPCION</th></tr>
<tr><td>1</td><td>CRITICA</td><td>La producción está parada o severamente impactada de manera que no se puede continuar trabajando. La operación es de misión crítica para la entidad y/o está en situación de emergencia.</td></tr>
<tr><td>2</td><td>ALTA</td><td>Experimenta perdida del servicio, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera restringida.</td></tr>
<tr><td>3</td><td>MEDIA</td><td>Experimenta una pérdida de servicio menor, el impacto es un inconveniente.</td></tr>
<tr><td>4</td><td>BAJA</td><td>No impacta la operación del programa, no se experimenta perdida del servicio y no se impide la operación de los sistemas.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><th colspan="2">PRIORIDAD</th><th>DESCRIPCION</th></tr>
<tr><td>1</td><td>CRITICA</td><td>De manera remota (2) horas de atención y (3) horas de traslado a sitio.</td></tr>
<tr><td>2</td><td>ALTA</td><td>De manera remota (3) horas de atención y (4) horas de traslado a sitio.</td></tr>
<tr><td>3</td><td>MEDIA</td><td>De manera remota (8) horas y de ser necesario traslado a sitio</td></tr>
<tr><td>4</td><td>BAJA</td><td>De manera remota (24) horas y de ser necesario traslado a sitio</td></tr>
</table>
</td></tr>
<tr><td>16.</td><td>El contratista deberá realizar y documentar entre otras, las siguientes actividades previa coordinación con el supervisor del contrato en desarrollo:

• Revisar la consistencia de los Backups realizados a las plataformas. Hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma, en forma escrita.
• Configurar, afinar y revisar los reportes / logs de las plataformas.
• Mantener actualizados los niveles de Firmware de los componentes mencionados de acuerdo con las últimas versiones estables liberadas por el fabricante.
• El contratista deberá garantizar la realización de un mínimo de tres (3) horas mensuales de capacitación durante toda la vigencia del contrato, en relación con los temas objeto del mismo y asociados a las soluciones Fortinet. Estas actividades de formación tendrán carácter adicional y no serán imputables ni descontables de la bolsa de horas definida en el ítem 3 de la presente ficha técnica.
Las capacitaciones deberán estar orientadas al fortalecimiento de capacidades técnicas y operativas del personal designado por la entidad, incluyendo, entre otros, aspectos de administración, operación, mejores prácticas, actualización tecnológica y resolución de incidentes sobre la plataforma implementada. El contratista deberá garantizar que dichas sesiones sean impartidas por personal idóneo y certificado, así como suministrar los soportes, materiales y evidencias de ejecución correspondientes.</td></tr>
<tr><td>17.</td><td>ENTREGABLES

El contratista deberá entregar los siguientes informes:

1. Un (1) informe de las actividades adelantadas, dentro de las que se encuentran:

– La renovación de las licencias, garantía y soporte de las plataformas.
– La activación del licenciamiento adquirido y del servicio de actualización de licencias y soporte técnico por un (1) año el cual deberá corresponder hasta el 15 de julio de 2027).
– La instalación y configuración del equipo actualizado de FortiAnalyzer.

2. El contratista deberá realizar una visita mensual, de la cual se generará un informe técnico detallado que evidencie el estado, funcionamiento y desempeño de los componentes de seguridad perimetral, incluyendo la identificación de posibles fallas, riesgos y recomendaciones de mejora.
3. Procedimiento para la radicación de solicitudes de soporte e incidencias tecnológicas de la plataforma tecnológica del FONCEP.</td></tr>
</table>

	4. Usuario de acceso a la consola de monitoreo para consulta, acta de transferencia de conocimiento y manual de uso. **5.** El contratista deberá entregar un informe detallado en el cual se evidencie el estado de la consola (Firewall), funcionamiento, posibles fallas o fallas reportadas y recomendaciones. **6.** Presentar previo al desarrollo de cada actividad, un documento con la propuesta de horas de consumo asociado, que deberá ser aprobado por el supervisor del contrato. **7.** Reporte mensual de actividades en el cual se detalle la relación de la cantidad de los requerimientos y/o solicitudes atendidas, las horas consumidas, el detalle de las actividades desarrolladas y los documentos técnicos actualizados, el cual será el soporte de pago por parte del supervisor del contrato designado por el FONCEP. **8.** Un (1) informe de Assessment, que incluya el resultado de las siguientes actividades: – Relación de los equipos de seguridad informática del FONCEP. – Los cambios de configuraciones efectuadas sobre los equipos, tendientes a mantener la solución (hardware, software y configuraciones) en correcto funcionamiento con un esquema de respaldo periódico de la configuración, de acuerdo con la política de seguridad establecida en el FONCEP. – La Arquitectura de la solución de seguridad informática actualizada en el FONCEP, incluyendo los diagramas topológicos y planos editables bajo formatos de VISIO o Architect o PowerPoint, o cualquier formato estándar de diagramación de arquitectura editable, así como diagramas de ingeniería de detalle donde se indique como mínimo (Configuración de puertos, integraciones de plataformas e integración con aplicaciones de la entidad). – El contratista deberá realizar la actualización permanente y documentación integral de la topología general de la infraestructura tecnológica de la entidad, garantizando su consistencia, trazabilidad y alineación con la arquitectura vigente. Como producto final, deberá entregar, al término del contrato, la documentación completa, detallada y debidamente validada, incluyendo diagramas, inventarios, interconexiones, configuraciones relevantes y demás elementos que permitan la adecuada comprensión, gestión y continuidad operativa de la plataforma tecnológica. – El contratista deberá diseñar, programar y ejecutar jornadas de capacitación dirigidas a los funcionarios y/o contratistas de FONCEP, sobre los componentes, herramientas y procesos asociados al objeto contractual, de conformidad con las características y lineamientos definidos en presente ficha técnica. Estas actividades no generarán costos adicionales para FONCEP ni serán objeto de facturación independiente. Como soporte, el contratista deberá elaborar y entregar las actas de capacitación debidamente suscritas, incluyendo listado de asistencia, contenidos impartidos, evidencias de ejecución, evaluación de apropiación del conocimiento y

	recomendaciones, garantizando la trazabilidad y la transferencia efectiva del conocimiento – Recomendaciones del fabricante y mejores prácticas del mercado.
ITEM	**CERTIFICACIONES REQUERIDAS**
C.	**ACREDITACIÓN DISTRIBUIDOR AUTORIZADO**
1.	El oferente debe allegar certificación con la oferta en la que acredite ser canal (Partner) certificado con nivel de membresía NSE8 o su equivalente actual Fortinet Certified EXPERT. Este documento debe ser expedido por el fabricante con fecha no mayor a treinta (30) días calendario a la fecha de cierre del presente proceso y la misma deberá ser dirigida a FONCEP. Ahora bien, teniendo en cuenta que la presente certificación dentro del mercado es de amplia utilización y aceptación en idioma distinto al castellano, el proponente podrá aportar este documento en su lengua original, acompañado de una traducción simple al castellano para su acreditación. En caso de proponentes plurales, cada integrante deberá presentar esta certificación.”
D.	**CERTIFICACIONES VIGENTES NSE.**
1.	El proponente deberá aportar con la oferta las certificaciones vigentes que se enuncian a continuación, las cuales, deben ser expedidas por el fabricante con una expedición no mayor de treinta (30) días calendario antes del cierre del proceso, así: NSE4 y/o NSE5 y/o NSE6 o su equivalente actual Fortinet Certified Professional, NSE7 o su equivalente actual Fortinet Certified Solution Specialist. Dichas certificaciones, demostrarán que el proponente cuenta con experiencia en administración y gestión de plataformas de seguridad Fortinet. Ahora bien, teniendo en cuenta que las presentes certificaciones dentro del mercado son de amplia utilización y aceptación en idioma distinto al castellano, el proponente podrá aportar estos documentos en su lengua original, acompañados de una traducción simple al castellano para su acreditación. En caso de proponentes plurales, al menos uno de los integrantes deberá presentar estas certificaciones.
ITEM	**COMPONENTE 3 ADQUIRIR EL SOPORTE Y ADMINISTRACIÓN DE LOS EQUIPOS Y SOFTWARE DE SEGURIDAD PERIMETRAL DE LOS SERVICIOS TECNOLÓGICOS DEL FONCEP.**
E.	**DESCRIPCIÓN**
1.	El contratista debe incluir dentro del servicio especializado correspondiente a mínimo **120 horas** para las siguientes actividades relacionadas con la administración de la seguridad perimetral del FONCEP: - Afinamiento de las políticas de seguridad - Afinamiento de las redes en IPv4 e IPv6 - Afinamiento de las redes LAN y WLAN - Afinamiento de los reportes y/o notificaciones de eventos o incidentes dentro de las plataformas de seguridad. - Apoyo proactivo y reactivo en sesiones con proveedores para el robustecimiento de infraestructura tecnológico del FONCEP.

<table>
<tr><td></td><td>
- Sesiones de transferencia de conocimiento a nuevos casos de uso sobre las plataformas de seguridad.
- Validación de estadísticas de comportamiento de tráfico, usuarios, métricas y demás sobre la herramienta FortiAnalyzer.
- Backups sobre la configuración de las herramientas de seguridad perimetral.
- Capacitación no certificada virtual a funcionarios del FONCEP sobre temas relacionados con la seguridad de la información.
- Actividades de apoyo y administración sobre las herramientas de seguridad perimetral de la entidad.
</td></tr>
<tr><td>2.</td><td>En el caso de nuevas configuraciones o mejoras de las configuraciones actuales definidas por la entidad, el contratista deberá participar activamente en el proceso de cambios, observando objetivamente si hay lugar al hecho del cambio o en caso contrario si hay una propuesta que conduzca a una mejora representativa del ambiente actual.</td></tr>
<tr><td>3.</td><td>El contratista deberá hacer uso de la herramienta FortiAnalyzer para la presentación de informes bajo demanda o programados a requerir por la entidad, con la finalidad de dar visibilidad y objetividad a los procesos de seguridad de la información del FONCEP.</td></tr>
<tr><td>4.</td><td>
Presentar a la suscripción del contrato y previo a la firma del acta de inicio, las Hojas de Vida propuestas para el equipo de trabajo asociado al presente contrato, de acuerdo con las siguientes especificaciones del equipo técnico requerido para la ejecución del contrato:

EQUIPO MÍNIMO DE TRABAJO

El proponente adjudicatario deberá contar con un equipo mínimo de trabajo para la ejecución del contrato, con el fin de garantizar un adecuado servicio al Fondo de Prestaciones Económicas, Cesantías y Pensiones - FONCEP. Para efectos de la verificación de las hojas de vida, el contratista deberá presentar, con la suscripción del contrato y previo a la firma del acta de inicio la documentación que acredite el cumplimiento de los requisitos exigidos para el equipo de trabajo.

<table>
<tr><th>ROL</th><th>CANTIDAD</th><th>REQUISITOS MÍNIMOS</th></tr>
<tr><td>Gerente de Proyecto</td><td>UNO (1)</td><td>Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. Tarjeta Profesional con expedición mínimo de ocho (8) años.

• Posgrado en Gerencia de Proyectos y/o Certificación PMP.
• Certificación Itil Foundation v3 o superior

Experiencia mínima en cuatro (4) proyectos gerenciando y/o coordinando proyectos de TI y/o Seguridad Informática.

La experiencia se cuenta a partir de la expedición de la tarjeta profesional.</td></tr>
</table>
</td></tr>
</table>

	Líder Técnico	UNO (1)	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. • Especialización o maestría en Seguridad de la Información o informática o ciberseguridad. • Certificación vigente como especialista en Network Security, emitida por el fabricante. • Certificación vigente de Auditor interno ISO 20000-1 • Certificación vigente de Auditor Líder ISO/EIC 27001:2022 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. La experiencia se cuenta a partir de la expedición de la tarjeta profesional
	Administrador de Plataforma 5X8	UNO (1)	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. • Especialización o maestría en Seguridad de la Información ó informática ó Ciberseguridad. • Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018. • Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 27001:2022. • Certificación vigente como profesional de Network Security, emitida por el fabricante. • Certificación vigente como especialista en Network Security, emitida por el fabricante. Experiencia general de cuatro (4) años en proyectos de TI, de los cuales mínimo de tres (3) años en implementación, soporte y/o administración y/o monitoreo de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
	Ingeniero Soporte 7x24	UNO (1)	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. • Certificación vigente como profesional Network Security, emitida por el fabricante. Experiencia general de tres (3) años en proyectos de TI, de los cuales mínimo de un (1) año en actividades de soporte y/o administración y/o monitoreo de soluciones de

			seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.

Nota 1: En los casos de diagnóstico, soporte, solución de incidencias, el profesional que aborde o sea el encargado de brindar la solución, deberá ser personal idóneo, con la suficiente experticia y certificado de acuerdo con los perfiles exigidos en la presente ficha y demás documentos del proceso; dicha condición será analizada y validada al momento de la aprobación y pago de las horas de soporte y deberá guardar plena relación con el documento de propuesta de consumo de horas asociado. No se permitirá la rotación del recurso sin previa autorización por parte de la Supervisión del Contrato.

Nota 2: El proponente adjudicatario y/o futuro contratista deberá contar con el repositorio interno de conocimiento que refleje el diagnóstico e historial de atención de casos de la entidad, de tal forma que se agilice la atención de nuevas incidencias similares o de la misma naturaleza, sin que el diagnóstico implique un consumo mayor de horas. Dicha situación será analizada en la presentación del informe de atención de cada evento y al momento de autorizar el pago por concepto de consumo de horas por parte de la Supervisión del Contrato.

CONOCEMOS, CUMPLIMOS, ACEPTAMOS Y NOS COMPROMETEMOS A MANTENER Y CUMPLIR CON TODAS LAS CONDICIONES Y REQUERIMIENTOS MÍNIMOS OBLIGATORIOS ESTABLECIDOS EN ESTE DOCUMENTO, LOS CUALES SE ENTENDERÁN COMO OFERTA TÉCNICA MÍNIMA.

NOMBRE DEL PROPONENTE _____
NOMBRE Y FIRMA DEL REPRESENTANTE LEGAL _____
IDENTIFICACIÓN C.C._____
TELÉFONO(S)_____
DIRECCIÓN_____
CORREO ELECTRÓNICO _____
CIUDAD_____