ANEXO No. 2 ESPECIFICACIONES TÉCNICAS

<table>
<tr><th>ÍTEM</th><th>ESPECIFICACIONES TECNICAS</th><th>CUMPLE</th><th>NO CUMPLE</th></tr>
<tr><td>1</td><td>MANTENIMIENTO PREVENTIVO Y CORRECTIVO PLATAFORMA TECNOLÓGICA DIPOL NIVEL CENTRAL, REGIONAL Y MANTENIMIENTO DE LOS SERVIDORES QUE CONFORMAN LA INFRAESTRUCTURA HIPERCONVERGENTE</td><td></td><td></td></tr>
<tr><td>1.1</td><td>Con el fin de garantizar la disponibilidad de la infraestructura, el contratista deberá prestar a todo costo, el servicio preventivo (mantenimiento preventivo exceptuando la limpieza del equipamiento tecnológico con compresor de aire) y corregir fallas que se presenten a partir de la firma del contrato y tres meses posterior a la vigencia del mismo (mantenimiento correctivo) tanto en los equipos físicos (hardware) como el software (firmware, drivers, actualizaciones y aplicación de parches) con cobertura total de cada uno de sus repuestos y elementos que componen el o los equipos o solución tecnológica (fibras, cables de poder, patch cord, switch, etc,.) relacionados a continuación:

Hardware:

<table>
<tr><th>ítem</th><th>Dispositivo</th><th>Serie</th></tr>
<tr><td>1</td><td colspan="2">Centro de Procesamiento de Datos principal de la DIPOL
(Avenida Boyacá No. 142ª – 55)</td></tr>
<tr><td>1.1</td><td>Servidor HP Proliant DL380 G6</td><td>USE940N9C9</td></tr>
<tr><td>1.2</td><td>Servidor DELL PowerEdge R820</td><td>6N4YHX1</td></tr>
<tr><td>1.3</td><td>Servidor Lenovo SR590</td><td>J3021MLL</td></tr>
<tr><td>1.4</td><td>Servidor Lenovo SR590</td><td>J3021MLM</td></tr>
<tr><td>1.5</td><td>Servidor DELL R760XS</td><td>GGV8L84</td></tr>
<tr><td>1.6</td><td>Servidor HP Proliant DL180 G10</td><td>2M213004M</td></tr>
<tr><td>1.7</td><td>Servidor HP Proliant DL360P G8</td><td>MXQ449029S</td></tr>
<tr><td>1.8</td><td>Servidor HP Proliant DL360P G8</td><td>MXQ449029Q</td></tr>
<tr><td>1.9</td><td>Servidor HP Proliant DL120 G9</td><td>2M2637017S</td></tr>
<tr><td>1.10</td><td>Servidor HP Proliant DL380 G5</td><td>2UX83101AF</td></tr>
<tr><td>1.11</td><td>Servidor HP Proliant DL360e G8</td><td>MXQ449029R</td></tr>
<tr><td>1.12</td><td>Servidor HP Proliant DL360e G8</td><td>MXQ449029N</td></tr>
<tr><td>1.13</td><td>Servidor HP Proliant DL360e G8</td><td>MXQ449029P</td></tr>
<tr><td>1.14</td><td>Servidor HP Proliant DL360e G8</td><td>MXQ41702V3</td></tr>
<tr><td>1.15</td><td>Servidor HP Proliant ML150 G6</td><td>USE008N31P</td></tr>
<tr><td>1.16</td><td>Servidor IBM Power 720</td><td>06949BR</td></tr>
<tr><td>1.17</td><td>Servidor IBM System X3650 M5</td><td>E2VZ070</td></tr>
<tr><td>1.18</td><td>Servidor IBM System X3550</td><td>KQKKA35</td></tr>
<tr><td>1.19</td><td>IBM System Storage DS4800 controller</td><td>78A009Z</td></tr>
<tr><td>1.20</td><td>IBM System Storage DS4800 enclosure</td><td>78K0X14</td></tr>
<tr><td>1.21</td><td>IBM System Storage DS4800 enclosure</td><td>136871W</td></tr>
<tr><td>1.22</td><td>IBM System Storage DS4800 enclosure</td><td>136872B</td></tr>
<tr><td>1.23</td><td>Servidor Cisco UCS C240 M5</td><td>WZP22120CA6</td></tr>
<tr><td>1.24</td><td>Servidor Cisco UCS C240 M5</td><td>WZP221115A6</td></tr>
<tr><td>1.25</td><td>Servidor Cisco UCS C220 M3</td><td>FCH1717V1S9</td></tr>
<tr><td>1.26</td><td>Servidor Cisco UCS C220 M3</td><td>FCH1717V1TH</td></tr>
<tr><td>1.27</td><td>Storage IBM Storwize V7000 Controller</td><td>78N20CX</td></tr>
<tr><td>1.28</td><td>Storage IBM Storwize V7000 Enclosure</td><td>78N20DZ</td></tr>
<tr><td>1.29</td><td>Storage IBM Storwize V7000 Enclosure</td><td>78N228L</td></tr>
<tr><td>1.30</td><td>Storage IBM Storwize V7000 Enclosure</td><td>78N20F7</td></tr>
<tr><td>1.31</td><td>Storage IBM Storwize V7000 Enclosure</td><td>78N20DN</td></tr>
<tr><td>1.32</td><td>Storage IBM Storwize V7000 Enclosure</td><td>78N20FG</td></tr>
<tr><td>1.33</td><td>Tape Library IBM TS4300 L8</td><td>78-005BK</td></tr>
<tr><td>1.34</td><td>Tape Library IBM TS4300 L8</td><td>78-004CZ</td></tr>
<tr><td>1.35</td><td>Tape Library IBM TS4300 L8</td><td>78-004D7</td></tr>
<tr><td>1.36</td><td>Tape Library IBM TS4300 L8</td><td>78-004CX</td></tr>
<tr><td>1.37</td><td>Tape Library IBM TS4300 L8</td><td>78-004D9</td></tr>
<tr><td>1.38</td><td>Switch SAN FC IBM TYPE 2005-B5K</td><td>105104P</td></tr>
<tr><td>1.39</td><td>Switch SAN FC IBM TYPE 2005-B5K</td><td>105104B</td></tr>
<tr><td>1.40</td><td>Switch SAN FC HP</td><td>USB606502K</td></tr>
</table>
</td><td></td><td></td></tr>
</table>

		1.41	Switch SAN FC HP	USB606S026			
		1.42	Switch SAN BROCADE 300	0742025-140ALJ005			
		1.43	Switch SAN BROCADE 300	0742025-140ALJ00Z			
		1.44	Switch SAN BROCADE 300	0741025-1508ALJ021			
		1.45	Servidor SUN Oracle X4-2	1518NML0C3			
		1.46	Servidor SUN Oracle X4-2	1518NML0C2			
		1.47	Servidor SUN Oracle X4-2	1518NML0C4			
		1.48	Servidor Oracle SPARC T-5	AK00208348			
		1.49	Servidor Oracle SPARC T-5	AK00208347			
		1.50	ZFS Storage Oracle ZS3-2	1518NM204N			
		1.51	ZFS Storage Oracle ZS3-2	1418NM200T			
		1.52	ZFS Storage Oracle ZS3-2	1418NM200P			
		1.53	Storage Oracle DE2-24C	1518NMT0BB			
		1.54	Storage Oracle DE2-24P	1439NM400J			
		1.55	Storage Oracle DE2-24P	1418NM401F			
		1.56	Servidor Lenovo SR530	J1005L78			
		1.57	Servidor Lenovo SR530	J1005L79			
		1.58	HP StoreEasy 3850 Gateway System	4C363203WY			
		1.59	HP StoreEasy 3850 Gateway Sngl Node	USE6327Y4M			
		1.60	HP StoreEasy 3850 Gateway Sngl Node	USE6327Y4P			
		1.61	HPE MSA 2040 ES SAN DC SFF Storage	2S6625B466			
		1.62	HPE D27000 Disk Enclosure	7CE612P25S			
		1.63	HPE MSA 2040 ES LFF Disk Enclosure	2S6626D163			
		1.64	HPE MSA 2040 ES LFF Disk Enclosure	2S6626D165			
		1.65	HPE MSA 2040 ES LFF Disk Enclosure	2S6626D166			
		1.66	HPE MSA 2040 ES LFF Disk Enclosure	2S6626D184			
		1.67	HPE MSA 2040 ES LFF Disk Enclosure	2S6626D185			
		1.68	HPE MSA 2040 ES LFF Disk Enclosure	2S6626D162			
		1.69	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RP1			
		1.70	Servidor Lenovo ThinkAgile VX7520 Appliance	J10087GX			
		1.71	Servidor Lenovo ThinkAgile VX7520 Appliance	J100875G			
		1.72	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RR5			
		1.73	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RR4			
		1.74	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RP3			
		1.75	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RP2			
		1.76	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RP4			
		1.77	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RP5			
		1.78	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RR6			
		1.79	Servidor Lenovo ThinkSystem SR590 (Veeam Backup)	J1015GPD			
		2	Centro de Procesamiento de Datos Alterno				
		2.1	Servidor Lenovo SR650	J10050CZ			
		2.2	Servidor Lenovo VX5520 (ThinkAgile) – Type 7Y94	J1015AEB			
		2.3	Servidor Lenovo VX5520 (ThinkAgile) – Type 7Y94	J1015AEA			
		2.4	Servidor Lenovo VX5520 (ThinkAgile) – Type 7Y94	J1015AEC			
		2.5	Servidor Lenovo VX5520 (ThinkAgile) – Type 7Y94	J1015GN7			
		2.6	Servidor Lenovo VX5520 (ThinkAgile) – Type 7Y94	J1015GN6			
		2.7	Servidor Lenovo VX5520 (ThinkAgile) – Type 7Y94	J1015GN5			
		3	Complejo policial del Sur Enrique Santos Castillo (Transversal 33 No. 47 a 35 Sur, Bogotá Fátima)				
		3.1	Servidor Dell PowerEdge R720	5NBK3Y1			
		3.2	Servidor HUAWEI 2288H V5	2102311XBJ10J8000080			
		4	Centro de Procesamiento de Datos AOPEI (Avenida Boyacá No. 142a – 55)				
		4.1	Servidor IBM System X3650 M4	KQ0Z5WA			
		4.2	Servidor IBM System X3650 M4	KQ9W6A3			
		4.3	Servidor IBM System X3650 M4	KQ9W6AZ			
		4.4	Servidor IBM System X3650 M4	KQ0Z5UZ			
		4.5	Storage IBM DS3512 controller	13D1862			
		4.6	Storage IBM DS3512 enclosure	13D16Y4			
		4.7	Storage IBM DS3512 enclosure	13D17PZ			
		4.8	Storage IBM DS3512 enclosure	13D17R3			
		4.9	Storage IBM DS3512 enclosure	13D17PV			
		4.10	Storage IBM DS3512 enclosure	13D1873			
		4.11	Storage Ultrastor RS16FS enclosure Fred C	D0099031763			
		4.12	Storage Ultrastor RS16FS enclosure Fred C	D0106032839			
		4.13	Storage Ultrastor RS16FS enclosure Fred C	D0111033748			
		4.14	Servidor Digital Intelligence Fred C	N0099031762			
		4.15	Switch SAN FC IBM	10311TD			
		4.16	Switch SAN FC IBM	10311VH			
		4.17	Storage DELL PowerVault NX3200	FTNVGX1			
		4.18	Storage DELL PowerVault NX3200 enclosure	1HPJQD2			
		4.19	SAN Store Wize V3700 controller	7881710			
		4.20	SAN Store Wize V3700 enclosure	7874829			

	4.21	SAN Store Wize V3700 enclosure	7874087		
	4.22	SAN Store Wize V3700 enclosure	78C0715		
	4.23	Servidor IBM Storwize V5000	781MB44		
	5	Centro Operacional de Fusión de Inteligencia (COFIN Villavicencio)			
	5.1	Storage DELL PowerVault NX3200	FDT3K02		
	6	Centro Operacional de Fusión de Inteligencia (COFIN Neiva)			
	6.1	Storage DELL PowerVault NX3200	34W6CZ1		
	7	Centro Operacional de Fusión de Inteligencia (COFIN Envigado)			
	7.1	Storage DELL PowerVault NX3200	8SX0DZ1		
	8	Centro Operacional de Fusión de Inteligencia (COFIN Popayán)			
	8.1	Storage DELL PowerVault NX3200	FDS4K02		
	9	Centro Operacional de Fusión de Inteligencia (COFIN Bucaramanga)			
	9.1	Storage DELL PowerVault NX3200	FDT0K02		
	10	Centro Operacional de Fusión de Inteligencia (COFIN Arauca)			
	10.1	Storage DELL PowerEdge R750xs	2200PZ3		
	11	Centro Operacional de Fusión de Inteligencia (COFIN Montería)			
	11.1	Storage DELL PowerEdge R750xs	1200PZ3		
	12	Regional de Inteligencia No. 1 (BOGOTÁ)			
	12.1	Servidor HP Proliant ML 310e G8	USE420YH0L		
	12.2	Servidor HP Proliant ML 310e G8	MX244800C6		
	13	Regional de Inteligencia No. 2 (NEIVA)			
	13.1	Servidor HP Proliant ML 310e G8	MX244800BP		
	13.2	Servidor HP Proliant ML 110	USE040N0A0		
	14	Regional de Inteligencia No. 3 (PEREIRA)			
	14.1	Servidor HP Proliant ML 310e G8	MX244800BV		
	14.2	Servidor HP Proliant ML 350	USE839NAMQ		
	15	Regional de Inteligencia No. 4 (POPAYÁN)			
	15.1	Servidor HP Proliant ML 310e G8	BRC3243DPH		
	15.2	Servidor HP Proliant ML 310e G8	MX244800BH		
	15.3	NAS Lenovo PX400D	1S70CJ9001LAMG008M3X		
	16	Regional de Inteligencia No. 5 (CUCUTÁ)			
	16.1	Servidor HP Proliant ML 310e G8	MX244800BD		
	16.2	Servidor HP Proliant ML 110	USE040N0A3		
	17	Regional de Inteligencia No. 6 (MEDELLÍN)			
	17.1	Servidor Servidor HP Proliant ML 110 G6	USE040N0AR		
	17.2	Servidor HP Proliant ML 310e G8	MX244800BT		
	17.3	Servidor Lenovo Think system ST550	J10026N3		
	18	Regional de Inteligencia No. 7 (VILLAVICENCIO)			
	18.1	Servidor HP Proliant ML 310e G8	MX244800BW		
	19	Regional de Inteligencia No. 8 (BARRANQUILLA)			
	19.1	Servidor HP Proliant ML 310e G8	MX244800BF		

Software:

S.O Windows Server
S.O Windows Storage Server
S.O Linux (diferentes distribuciones)
S.O AIX
IBM Tivoli Storage Manager (TSM)
IBM Spectrum Protect
General Parallel File System (GPFS)
Software de administración de switches FC
IBM System Storage, series DS4000, V3700, V7000
DELL System Storage
Storage Management Utility
IBM Hardware Management Console (HMC)
SAMBA
VMWARE VSPHERE
VMWARE VSAN
VEEAM
VEEAM ONE
System Center Configuration Manager

<table>
<tr><th>2</th><th colspan="3">REQUERIMIENTOS GENERALES DE LOS SERVICIOS SOLICITADOS</th></tr>
<tr><td>2.1</td><td colspan="3">El contratista prestará en sitio los servicios de mantenimiento y soporte técnico con personal certificado y con experiencia certificable mínima de tres (3) años en infraestructuras equivalentes, verificable mediante hojas de vida, certificaciones o contratos ejecutados (ítem 6.3), con acompañamiento de un funcionario que la DIPOL designe para tal efecto, así:

En la ciudad de Bogotá D.C,

▪ Centro de Procesamiento de Datos del Grupo de Tecnologías de la Información y las Comunicaciones de la DIPOL (Avenida Boyacá No. 142 a – 55)
▪ Centro de Procesamiento de Datos del Área de Operaciones de Inteligencia de la DIPOL (Avenida Boyacá No. 142 a – 55)
▪ Centro de Procesamiento de Datos alterno de la DIPOL
▪ Escuela de Poligrafía de la Policía Nacional (Transversal 33 No. 47 a 35 Sur, Fátima)
▪ Sede de las ocho Regionales de Inteligencia Policial, así:

<table>
<tr><th>REGIONAL DE INTELIGENCIA POLICIAL (RIPOL)</th><th>CIUDAD</th><th>DIRECCIÓN</th></tr>
<tr><td>RIPOL 1</td><td>Bogotá D.C</td><td>Calle 17 # 65B-99</td></tr>
<tr><td>RIPOL 2</td><td>Neiva</td><td>Calle 21 Sur # 235 zona industrial Canaima</td></tr>
<tr><td>RIPOL 3
COFIN 2</td><td>Pereira</td><td>Avenida Las Américas 46-35 (Instalaciones Comando Metropolitana de Pereira)</td></tr>
<tr><td>RIPOL 4</td><td>Popayán</td><td>Avenida Panamericana 1N-75 barrio Villa Paula (Instalaciones Metropolitana de Policía de Popayán)</td></tr>
<tr><td>RIPOL 5</td><td>Cúcuta</td><td>Calle 22N # 2-03 Urbanización Tasajero (Instalaciones Región de Policía No. 5)</td></tr>
<tr><td>RIPOL 6</td><td>Medellín</td><td>Calle 111 # 64C-350 barrio Boyacá Las Brisas (Instalaciones del Centro de Instrucción Policial Carlos Holguín)</td></tr>
<tr><td>RIPOL 7</td><td>Villavicencio</td><td>Calle 44 # 35-96 barrio El Triunfo (Instalaciones Inspección</td></tr>
<tr><td>RIPOL 8</td><td>Barranquilla</td><td>Carrera 43 # 47-53 (Instalaciones Comando de Policía Metropolitana)</td></tr>
</table>
</td></tr>
<tr><td>2.2</td><td colspan="3">El contratista deberá elaborar el plan de trabajo detallado (EDT) para los servicios de soporte contratado y que incluya los mantenimientos preventivos, las actualizaciones de firmware, de sistema operativo y demás herramientas incluidas en el presente proceso. Este documento deberá ser concertado y entregado al supervisor del contrato en los primeros quince (15) días calendario siguientes a la aprobación de la garantía única.</td></tr>
</table>

<table>
<tr><td>2.3</td><td>El contratista deberá garantizar a la DIPOL la disponibilidad permanente de los siguientes medios de contacto:

- Número de teléfono móvil de un contacto directo en la empresa para atención de casos que requieran prioridad.
- Número telefónico general de la compañía para el reporte de incidencias.
- Correo electrónico de soporte para atender los requerimientos.</td><td></td><td></td></tr>
<tr><td>2.4</td><td>El contratista deberá implementar y cumplir un esquema formal de gestión de incidentes basado en niveles de severidad y acuerdos de nivel de servicio (SLA), aplicable a toda la infraestructura y servicios cubiertos por el contrato. Dicho esquema deberá permitir la atención priorizada de eventos, garantizar la continuidad operativa y facilitar la supervisión y control contractual.

Clasificación de severidades:

Los incidentes deberán clasificarse en las siguientes categorías, de acuerdo con su impacto operativo y nivel de afectación:

Severidad Crítica (P1): Incidentes que generen indisponibilidad total de servicios misión crítica, afectación grave a la continuidad del negocio, riesgo alto para la seguridad de la información o interrupción de servicios esenciales de autenticación, almacenamiento, respaldo o virtualización.

Severidad Alta (P2): Incidentes que provoquen degradación significativa del servicio, afectación parcial de componentes críticos o riesgo de escalamiento a una condición crítica, sin indisponibilidad total.

Severidad Media/Baja (P3): Solicitudes de soporte, ajustes menores, actividades de mantenimiento no urgente o requerimientos informativos que no afecten la operación.

Acuerdos de nivel de servicio (SLA)

El contratista deberá cumplir, como mínimo, con los siguientes niveles de servicio, los cuales serán exigibles contractualmente:

<table>
<tr><th>Severidad</th><th>Tiempo máximo de respuesta</th><th>Tiempo máximo de atención en sitio</th><th>Tiempo máximo de restauración</th></tr>
<tr><td>P1 – Crítica</td><td>≤ 15 minutos</td><td>Bogotá D.C.: ≤ 2 horas
Regionales: ≤ 12 horas</td><td>≤ 24 horas</td></tr>
<tr><td>P2 – Alta</td><td>≤ 30 minutos</td><td>≤ 24 horas</td><td>≤ 48 horas</td></tr>
<tr><td>P3 – Media/Baja</td><td>≤ 8 horas</td><td>Según programación acordada</td><td>Según programación</td></tr>
</table>
</td><td></td><td></td></tr>
<tr><td>2.5</td><td>Los problemas técnicos deberán ser atendidos de forma presencial en el sitio de la incidencia, ofreciendo soporte técnico especializado para los componentes de hardware y software contemplados en el contrato. El objetivo será restablecer la</td><td></td><td></td></tr>
</table>

	operatividad del sistema afectado, cumpliendo estrictamente con los tiempos de respuesta y resolución definidos en este documento		
2.6	El contratista deberá prestar asistencia técnica 7/24 (siete días por veinticuatro horas) durante la vigencia del contrato		
2.7	El contratista deberá mantener un stock de repuestos durante la ejecución del contrato, que incluya discos duros compatibles con los servidores y sistemas de almacenamiento, memorias, drives de librerías, fuentes de poder, ventiladores, placas motherboard de los servidores y switches SAN especificados en los pliegos. La DIPOL se reserva el derecho de verificar dicho stock.		
2.8	El oferente deberá garantizar un stock de discos duros para los sistemas de almacenamiento descritos en el ítem 1.1, de manera que, en caso de falla simultánea de discos en un mismo arreglo, puedan ser reemplazados conforme a los niveles de servicio establecidos en este pliego. Además, deberá anexar una certificación firmada en la que se comprometa a mantener dicho stock durante la vigencia del contrato. El stock deberá permitir la reposición inmediata de al menos dos (2) discos por tipo y tecnología instalada en cada sistema crítico, o su equivalente funcional.		
2.9	Las refacciones, discos o equipos que deban ser reemplazados deberán ser nuevos, originales y con características iguales o superiores a las especificadas. En caso de que los productos originales ya no se encuentren en fabricación, podrán ser remanufacturados, siempre que cumplan con las características mínimas requeridas o superiores.		
2.10	El contratista garantizará la disponibilidad de la infraestructura mediante la revisión y aplicación de parches, así como la actualización de drivers, firmware y/o microcódigo a los equipos descritos en el numeral 1.1. Al inicio de la ejecución del contrato, deberá presentar un informe detallado sobre el nivel actual de parches, firmware y/o microcódigo de dichos equipos, indicando la fuente de información utilizada para su validación. Este informe deberá ser entregado al supervisor del contrato para su revisión y aprobación.		
2.11	Las actualizaciones de drivers, firmware y/o microcódigo, así como la aplicación de parches, podrán realizarse previa coordinación con el supervisor del contrato. Para los equipos descritos en el numeral 1.1 que requieran actualizaciones o parches, conforme al informe del numeral 2.10, el contratista deberá presentar un plan de trabajo detallado, que incluya los procedimientos a seguir, los requisitos para la instalación o aplicación, el tiempo de ejecución, las tareas de pre-instalación y post-instalación, la contingencia en caso de fallos, y el cronograma o minutograma. El contratista garantizará que las actividades de actualización no afecten la disponibilidad del servicio de datos de los equipos mencionados en el numeral 1.1.		
2.12	El contratista deberá proporcionar la actualización de licencias del software Lenovo xClarity Pro para los servidores Lenovo ThinkAgile VX7520 mencionados en el ítem 1.1.		
2.13	El contratista deberá garantizar el funcionamiento del hardware de las plataformas hiperconvergentes configuradas en los servidores Lenovo ThinkAgile, así como gestionar y resolver las alertas que indiquen posibles fallas en sus componentes.		
2.14	El contratista deberá suministrar el licenciamiento del software Veeam Backup y Veeam One por un periodo de un año, realizando su correcta instalación y garantizando su funcionamiento a partir del vencimiento del licenciamiento actual		

	con el que cuenta la entidad. Este licenciamiento deberá estar a nombre de la Dirección de Inteligencia Policial.		
3	**MANTENIMIENTOS**		
3.1	**Mantenimientos preventivos y correctivos:** Los mantenimientos correctivos deberán realizarse según sea necesario para resolver de manera oportuna los incidentes reportados. Se llevarán a cabo dos (2) mantenimientos durante la vigencia del contrato, con un plan de trabajo de al menos ocho (8) horas por sesión en sitio, en las instalaciones descritas en el ítem 2.1 del anexo de requerimientos técnicos mínimos. Las actividades incluyen, pero no se limitan a: - Verificación y aseguramiento de conexiones de red (tomas, cables, conectores). - Verificación y aseguramiento de conexiones internas de equipos (cables, conectores, tarjetas). - Limpieza y reemplazo de unidades de DVD, CD-ROM y Tape Backup, si es necesario. - Eliminación de polvo de componentes internos (uso de herramientas adecuadas para no activar sistemas de detección). - Limpieza, ajuste y lubricación de ventiladores y reemplazo, si es necesario. - Limpieza y ajuste de fuentes de poder y reemplazo, si es necesario. - Lubricación de partes mecánicas. - Verificación y ajuste de tamaño de sistemas de archivos del sistema operativo. - Revisión de archivos de logs del sistema operativo. - Eliminación de archivos temporales, si es necesario. - Reinstalación o reconfiguración del sistema operativo y herramientas de software en los servidores, cuando sea requerido. - Actualización de drivers o firmware de dispositivos de hardware. - Aplicación de parches a sistemas operativos Windows Server, Linux, AIX, VMware, entre otros instalados en los servidores descritos en el ítem 1.1. - Liberación de cartuchos atascados en las librerías de cintas. - Revisión de configuración de alias, zonas y puertos físicos de conexión en los ‘SAN Switch’, incluyendo desconexión y retiro de fibras no conectadas a los host systems. - Revisión y configuración de los componentes de hardware y software del file server Linux. - Revisión periódica de componentes físicos y lógicos de los Subsystem Storage.		
3.2	**Asistencia en configuraciones y proyectos relacionados:** El contratista deberá asistir a la DIPOL en la ejecución de configuraciones, incluyendo las actividades descritas a continuación. Las tareas se abordarán como proyectos según su complejidad, con la documentación y planificación necesaria para cada una. - Configuración de la capacidad de los FS de TSM y Spectrum Protect, en ambientes de producción y contingencia, previa revisión de la estructura y distribución de archivos del sistema operativo.		

	- Soporte para soluciones de backup Tivoli Storage Manager (TSM) y Spectrum Protect, incluyendo actualizaciones de versiones, parches de sistema operativo, instalación de agentes y configuración de tareas de backup. - Migración del servidor de Spectrum Protect a un servidor blade IBM Power7, y ejecución de las configuraciones necesarias para el funcionamiento de la plataforma de backup. - Pruebas de recuperación de backups generados por TSM y Spectrum Protect. - Migración de data activa entre cintas magnéticas LTO, incluyendo configuraciones necesarias en librerías y herramientas de backup, garantizando la integridad de los archivos migrados. - Verificación de la salud de las controladoras de dominio, estado de replicación, roles FSMO, resolución de nombres, relaciones de confianza y sincronización de hora mediante NTP. - Hardening a los servidores Windows que indique el supervisor del contrato, realizando las configuraciones locales y desde el dominio que sean necesarias, previa validación de los riesgos y aprobación del supervisor - Revisión y creación de políticas GPO en el directorio activo, según las necesidades de la DIPOL. - Asistencia en la solución de errores en NIC Teaming de las controladoras de dominio y en la unificación de dominios entre el nivel central y unidades desconcentradas. - Eliminación y creación de arreglos en sistemas SAN, optimizando el rendimiento y capacidad de almacenamiento. - Organización de conexiones fibre channel en los SAN Switch, y migración de conexiones entre los Switch FC en el Centro de Procesamiento de Datos. - Asistencia en la configuración de IPv6 en servidores físicos y virtuales, revisión y reconfiguración del DHCP en actualizaciones de Windows Server. - Instalación, configuración y ejecución de controles de cambio en los sistemas operativos, y actualización de parches. - Configuración de sincronización de archivos mediante DFS entre servidores de producción y contingencia, asegurando su correcta sincronización. - Solución de errores en System Center y base de datos, y asistencia en la configuración de reglas para el despliegue de software y actualizaciones de Windows. - Revisión y corrección de la entidad certificadora del Active Directory, y asistencia en la generación y despliegue de nuevos certificados. - Asistencia en el diligenciamiento del inventario de equipos servidores, conforme a las directrices del Ministerio de la Información y las Comunicaciones. - Revisión y optimización de la configuración del clúster de conmutación por error del servidor de archivos, con pruebas de la configuración de alta disponibilidad (HA).		
3.3	Durante la vigencia del contrato, el contratista será responsable de ejecutar los mantenimientos preventivos y correctivos, asumiendo todos los costos relacionados con el traslado de equipos, refacciones, instalaciones, configuraciones, personal técnico en sitio y demás recursos necesarios para solucionar las fallas reportadas o potenciales. Estos mantenimientos deberán ser realizados por personal profesional certificado, con experiencia comprobada y la capacidad necesaria para llevar a cabo las tareas sobre los equipos descritos en el numeral 1.1. El supervisor del contrato podrá solicitar las certificaciones,		

	diplomas y demás documentos pertinentes para verificar la idoneidad del personal asignado. En caso de que el ingeniero no cumpla con los requisitos establecidos, el contratista deberá reemplazarlo. El personal propuesto deberá ser el mismo a lo largo del proyecto, y cualquier cambio deberá ser comunicado por escrito, garantizando que el nuevo profesional cumpla con los requisitos exigidos.		
3.4	**Actualización sistema operativo y nivel funcional del dominio** El contratista deberá planear, ejecutar y documentar la actualización de la versión del sistema operativo de las controladoras de dominio y el incremento del nivel funcional del dominio al último nivel estable soportado por el fabricante, bajo un enfoque de proyecto técnico integral. Dicha actividad deberá desarrollarse conforme a buenas prácticas, lineamientos del fabricante y estándares de seguridad de la información, contemplando como mínimo: análisis previo del estado del dominio, verificación de compatibilidad, identificación y mitigación de riesgos, definición de controles previos y posteriores, ejecución controlada por fases, planes de contingencia y estrategias de reversión (rollback) plenamente documentadas. El proceso deberá garantizar la continuidad del servicio, la integridad de la información, la no afectación de los servicios de autenticación, autorización y directorio, y deberá culminar con la entrega de un informe técnico que evidencie la correcta ejecución, validación y estabilización de la plataforma.		
3.5	El contratista deberá proporcionar acompañamiento al personal del Grupo de Tecnologías de la Información y las Comunicaciones de la DIPOL para el traslado o movimiento de cualquier dispositivo de hardware dentro de los Centros de Procesamiento de Datos de producción y contingencia.		
3.6	El contratista deberá garantizar la disponibilidad de la infraestructura de hardware mediante herramientas de monitoreo que generen alertas sobre fallas de hardware, degradación de servicios o eventos críticos, las cuales deberán ser atendidas conforme a los SLA definidos.		
3.7	Cuando se realice el reemplazo de discos duros de los servidores y/o sistemas de almacenamiento, la DIPOL, de acuerdo con sus protocolos de seguridad de la información, procederá a destruirlos. Por lo tanto, estos no serán entregados al contratista.		
3.8	Después de cada visita de mantenimiento preventivo o correctivo, el contratista deberá entregar un informe que incluya, como mínimo, la siguiente información: Datos del equipo atendido Fecha y hora de la atención Duración de la visita Actividades realizadas durante la intervención Información del técnico que atendió el caso		
3.9	El contratista deberá evaluar y documentar el estado técnico y funcional de los equipos tecnológicos que sean objeto de intervención en el marco del contrato, incluyendo servidores, sistemas de almacenamiento, librerías y demás componentes de la infraestructura tecnológica definida por la entidad. Como resultado de esta evaluación, deberá elaborar informes técnicos periódicos en los que se identifique el estado operativo de los equipos, la condición de sus componentes críticos, la vigencia del soporte del fabricante y la proyección estimada de vida útil remanente, con base en criterios técnicos y buenas prácticas aplicables. Cuando del análisis se evidencie obsolescencia tecnológica, agotamiento de la vida útil o riesgos relevantes para la continuidad del servicio, el contratista deberá formular recomendaciones técnicas debidamente sustentadas orientadas al reemplazo, renovación o actualización de los equipos afectados. Los informes servirán como insumo para la planeación tecnológica, la gestión del riesgo y la toma de decisiones institucionales, en los términos y formatos que defina la entidad.		
4	**TRANSFERENCIA DE CONOCIMIENTO**		

4.1	El contratista deberá proporcionar transferencia de conocimiento al personal operador del Centro de Procesamiento de Datos de la DIPOL en relación con las siguientes herramientas: Windows Server, Spectrum Protect, Active Directory y VMware. La transferencia deberá cubrir, entre otros aspectos, los conceptos teóricos fundamentales sobre el funcionamiento de estas herramientas, así como los comandos, rutinas y configuraciones necesarias para su correcta administración.		
4.2	El contratista deberá proporcionar, sin costo adicional para la DIPOL, formación a cuatro (4) funcionarios en el curso CompTIA Server+ (SK0-005). La formación deberá ser impartida por personal certificado en el curso y llevarse a cabo en un centro de instrucción autorizado, que cuente con los medios tecnológicos, laboratorios y las herramientas necesarias para asegurar el éxito de la actividad académica.		
5	**GARANTÍA TÉCNICA**		
5.1	El contratista proporcionará soporte durante los tres (3) meses siguientes a la fecha de finalización del contrato. Durante este período, atenderá incidentes que afecten la plataforma tecnológica de la DIPOL y pongan en riesgo la infraestructura crítica de TI, poniendo a disposición el personal calificado y los recursos necesarios para su resolución, conforme al alcance del contrato		
5.2	Si es necesario, el contratista escalará a la casa fabricante las necesidades de soporte especializado para resolver fallos en los sistemas de la DIPOL incluidos en este contrato		
5.3	La atención y resolución de incidentes se realizará conforme a los niveles de severidad y SLA definidos en el numeral 2.4 del presente documento.		
5.4	Si es necesario retirar equipos, dispositivos o componentes de la DIPOL para su reparación en las instalaciones del contratista, este asumirá los costos y riesgos del traslado. Además, deberá proporcionar un equipo de características similares en calidad de préstamo durante el tiempo necesario para resolver el inconveniente. En caso de que se requiera realizar pruebas en un ambiente controlado, el contratista podrá utilizar su centro de cómputo de Datos, siempre que se garantice la seguridad del equipo y/o dispositivo de la DIPOL.		
5.5	El contratista otorgará una garantía de hasta un (1) año, contados a partir de la finalización del contrato, sobre las piezas o componentes reemplazados durante su ejecución.		
5.6	El servicio se considerará correctamente prestado cuando el componente intervenido opere sin alertas críticas, sin eventos de error registrados en los logs del sistema y supere las pruebas de validación funcional definidas por el fabricante o por la entidad, evidenciadas mediante registros técnicos y acta de conformidad del supervisor.		
6	**CERTIFICACIONES**		
6.1	**NIVEL DE EDUCACION O NIVEL ACADEMICO** Con el fin de garantizar la idoneidad técnica, la adecuada ejecución de las actividades contratadas y la mitigación de riesgos operativos sobre la infraestructura tecnológica de la Dirección de Inteligencia Policial, el contratista deberá disponer de personal profesional con formación académica y experiencia certificable en tecnologías de la información y las comunicaciones. En consecuencia, el proponente deberá asignar como mínimo tres (3) profesionales en ingeniería de sistemas, ingeniería de telecomunicaciones o áreas afines, quienes deberán acreditar formación académica y certificaciones técnicas vigentes, expedidas por fabricantes, correspondientes a las certificaciones que se relacionan a continuación, las cuales deberán ser		

	acreditadas de manera individual o conjunta (como se detalla en la nota 1) por los profesionales propuestos, conforme a lo exigido en el presente proceso. • Lenovo Data Center Technical Sales • IBM Certified Administration Spectrum Protect • IBM Certified Administration Tivoli Storage Manager • Microsoft® Certified Solutions Expert • Microsoft Certified Technology Specialist • VTSP-HCI (Hyper-Converged Infrastructure) • VSP-HCI (Hyper-Converged Infrastructure) • VMware Certified Professional – Data Center Virtualization • VMware vSphere Foundations • Veeam Certified Engineer (MCE) Nota 1. Un mismo profesional podrá acreditar una o varias de las certificaciones exigidas. El oferente podrá distribuir las certificaciones entre los profesionales propuestos y, de ser necesario, presentar un número superior a tres (3) profesionales, siempre que, en conjunto, se acrediten la totalidad de las certificaciones técnicas exigidas para este proceso y se cuente, como mínimo, con tres (3) profesionales. En todo caso, cada profesional propuesto deberá acreditar al menos una (1) de las certificaciones exigidas; no se aceptarán profesionales sin certificación. Nota 2. No se aceptarán certificaciones de asistencia, participación o capacitación sin evaluación formal de competencias. Nota 3. El oferente deberá adjuntar en su propuesta copia legible del acta de grado o diploma expedido por institución de educación superior reconocida por el Ministerio de Educación Nacional, por cada profesional propuesto. Nota 4. En el caso de profesionales extranjeros, se deberá presentar certificación de homologación del título profesional expedida por el Ministerio de Educación Nacional de Colombia, conforme a la normatividad vigente. Nota 5. Las certificaciones técnicas exigidas deberán encontrarse vigentes a la fecha de cierre del proceso de selección. Será responsabilidad exclusiva del oferente acreditar su vigencia mediante los soportes documentales correspondientes. Nota 6. El supervisor del contrato podrá solicitar la sustitución del personal que no acredite las competencias técnicas exigidas o cuyo desempeño no resulte satisfactorio durante la ejecución del contrato. Nota 7. En caso de que el fabricante haya modificado la denominación de alguna de las certificaciones exigidas, el oferente podrá allegar la certificación vigente que la sustituya, siempre que demuestre de manera objetiva y verificable que corresponde a la actualización o equivalencia directa de la certificación originalmente solicitada.		
6.2	**EXPERIENCIA DEL PROPONENTE:** Con el fin de garantizar la calidad de los servicios a contratar y evitar incumplimientos en la ejecución del futuro contrato, se requiere acreditar experiencia en proyectos similares al objeto del presente estudio previo, según los códigos de clasificación de los bienes, obras o servicios (UNSPSC) en las clasificaciones 81112300 y/o 81111800 y/o 83112200, para lo cual el oferente deberá acreditar contratos realizados por valor igual o superior a 399.8		

	S.M.M.L.V, de procesos adelantados con empresas públicas o privadas. Lo anterior se verificará mediante la presentación del Registro Único de Proponentes (RUP).		
6.3	**EXPERIENCIA DEL PERSONAL:** Es fundamental para la Dirección de Inteligencia Policial que todo el personal profesional asignado al equipo de trabajo cuente con idoneidad y experiencia general y específica, que asegure la calidad de las actividades a realizar sobre la infraestructura tecnológica descrita en el pliego de condiciones técnicas. En consecuencia, el proponente deberá acreditar que, durante los años 2023, 2024 y/o 2025, los profesionales incluidos en su oferta participaron en proyectos en los cuales realizaron actividades de instalación, implementación y/o configuración sobre uno o varios de los sistemas detallados a continuación. La experiencia de los profesionales podrá ser distribuida y acumulada entre los integrantes del equipo de trabajo para cumplir con el total de los sistemas exigidos, sin perjuicio de que cada profesional deba acreditar experiencia certificada en al menos uno (1) de los sistemas relacionados. - IBM Spectrum Protect - IBM Tivoli Storage Manager - Servidores Power - Storage IBM - Storage HP - Linux Red Hat - Windows Server - Lenovo Xclarity Pro - Lenovo ThinkAgile Appliance - Replica de datos con Veeam Backup Nota: Las certificaciones de experiencia deberán ser emitidas por las empresas en las que los profesionales propuestos en la oferta hayan participado en proyectos de instalación, implementación y/o configuración sobre los sistemas mencionados anteriormente. Las certificaciones deberán contener información legible sobre el funcionario, incluyendo un concepto sobre su desempeño durante la ejecución de las actividades contratadas.		
6.4	**CERTIFICACIONES DEL OFERENTE:** Con el fin de garantizar la correcta ejecución del contrato, mitigar riesgos asociados a la inexperiencia técnica y asegurar la continuidad operativa de la plataforma tecnológica de la Dirección de Inteligencia Policial, la DIPOL exige que el oferente acredite capacidad formal de soporte, escalamiento y relacionamiento directo con los fabricantes de las tecnologías que soportan la infraestructura institucional. Para tal efecto, el oferente deberá acreditar mínimo tres (3) membresías o certificaciones vigentes, expedidas por los fabricantes de las tecnologías objeto del contrato que se indican a continuación, siendo obligatorio que una (1) de estas corresponda a la membresía con BROADCOM, en el nivel mínimo Select, en razón a que los sistemas de información más críticos de la entidad operan		

	sobre la plataforma de virtualización VMware, actualmente administrada por dicho fabricante. Las dos (2) restantes deberán corresponder a cualquiera de las siguientes: • **LENOVO:** Membresía Silver o superior • **IBM:** Membresía Silver o superior • **VEEAM:** Membresía Silver o superior • **DELL: Membresia GOLD o superior** Nota 1: La exigencia de estas acreditaciones se fundamenta en la necesidad institucional de asegurar la idoneidad técnica, la experiencia y el respaldo del fabricante del proveedor, como medida de mitigación de riesgos operativos durante la ejecución del contrato. Nota 2. En caso de que el fabricante haya modificado la denominación de alguna de las certificaciones exigidas, el oferente podrá allegar la certificación vigente que la sustituya, siempre que demuestre de manera objetiva y verificable que corresponde a la actualización o equivalencia directa de la certificación originalmente solicitada.		
6.5	El contratista deberá allegar certificado de autenticidad de las licencias incluidas en el presente proceso, en cumplimiento a lo establecido en la circular conjunta de la Procuraduría General de la Nación y la Unidad Administrativa Especial Dirección Nacional de Derecho Autor, frente a la celebración de contratos de software o licenciamiento		
7	**CONFIDENCIALIDAD Y SEGURIDAD**		
7.1	En virtud del presente contrato, el contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del presente contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo. El contratista deberá firmar un compromiso de reserva.		
7.2	Si la DIPOL considera pertinente someter a estudio de seguridad y confidencialidad al personal que realiza la prestación del servicio, el contratista permitirá y facilitará todos los medios que la entidad le requiera para este fin.		
7.3	El personal que realice la instalación y configuración de equipos y sistemas, deberá cumplir con un estudio de confiabilidad realizado por la Dirección de Inteligencia de la Policía Nacional, en cualquier momento durante la vigencia del contrato. En el evento de no aprobar dicho estudio algunas de las personas vinculadas a este proyecto, el contratista deberá realizar el cambio de estas personas por otras que también deberán cumplir con el estudio de confiabilidad requerido.		
8	**CAPACIDAD OPERATIVA**		
8.1	Con el fin de garantizar la calidad de los servicios a contratar y evitar posibles incumplimientos en la ejecución del contrato, se requiere que las firmas participantes en el proceso de selección cuenten con un número mínimo de personal profesional e idóneo en los sistemas, aplicaciones y plataformas que conforman la infraestructura tecnológica de la DIPOL, tal como se detalla en el anexo de especificaciones técnicas de este proceso. Este aspecto es crucial para la correcta ejecución de los mantenimientos preventivos, la resolución oportuna y eficaz de incidentes a nivel físico y lógico, y para prevenir riesgos sobre la disponibilidad e integridad de los activos de información del organismo. Además, los oferentes deberán demostrar su capacidad para: • Adquirir en el mercado, tanto nacional como internacional, los componentes de hardware necesarios para el reemplazo de equipos. • Contar con medios logísticos y administrativos adecuados para movilizar personal y refacciones a los sitios donde se encuentren los equipos descritos		

	en el proceso, incluidas las ocho Regionales de Inteligencia, según se indica en el ítem 2.1 del anexo de especificaciones técnicas mínimas requeridas. • Gestionar ante las casas fabricantes la solución de problemas complejos que no puedan ser resueltos con sus propios recursos. Por lo anterior, los oferentes deberán anexar en su propuesta una certificación de capacidad operativa, emitida por el representante legal o quien haga sus veces.		
9	**CLAUSULAS AMBIENTALES**		
9.1	Desarrollar y cumplir, durante la vigencia y ejecución del objeto del contrato, con las buenas prácticas ambientales con relación al ahorro y uso eficiente del agua y la energía, así como el manejo integral de residuos (no peligrosos y peligrosos), establecidas por la Dirección y el marco del mantenimiento del Sistema de Gestión Ambiental en las Instalaciones del Contratante; que contribuyan al cumplimiento de la política ambiental y objetivos ambientales institucionales.		
9.2	Cumplir con la normatividad ambiental vigente nacional para reducir los aspectos e impactos ambientales asociados a la actividad y aplicación de buenas prácticas ambientales.		
9.3	El contratista deberá garantizar que los materiales de los empaques y/o embalajes estén constituidos con un porcentaje de material reciclable o provenir de una fuente sustentable no se permite el embalaje en componentes de ICOPOR.		
9.4	El contratista deberá realizar adecuada disposición final de los residuos generados entregando al supervisor del contrato el certificado de disposición final, en caso de ser residuos peligrosos deberá entregar el manifiesto de recolección y licencia ambiental de la empresa que realizo la disposición final.		
10	**CLAUSULAS SEGURIDAD Y SALUD EN EL TRABAJO**		
10.1	El oferente deberá entregar en la oferta el documento firmado por el representante legal el cual indique el número de trabajadores permanentes, el nivel de riesgo de su principal actividad económica y asimismo anexar la calificación de los estándares mínimos del Sistema de Gestión de Seguridad y Salud en el Trabajo de la vigencia anterior, lo anterior como consideración a la Resolución 0312 del 13 de febrero del 2019 del Ministerio de Trabajo “Por la cual se definen los Estándares Mínimos del Sistema de Gestión de SST”, en cumplimiento al art. 1 la presente Resolución tiene por objeto establecer los Estándares Mínimos del SG-SST para las personas naturales y jurídicas señaladas en el art. 2 aplica a los empleadores públicos y privados, a los contratantes del personal bajo modalidad de contrato civil, comercial o administrativo, a los trabajadores dependientes e independientes, a las organizaciones de economía solidaria y del sector cooperativo a las agremiaciones u asociaciones que afilian trabajadores independientes al sistema de seguridad social integral, a las empresas de servicios temporales, a los estudiantes afiliados al Sistema General de Riesgos Laborales y los trabajadores en misión; a las administradoras de riesgos laborales; a la Policía Nacional en lo que corresponde a su personal no uniformado y al personal civil de las Fuerzas Militares; quienes deben implementar los Estándares Mínimos del Sistema de Gestión de SST en el marco del Sistema de Garantía de Calidad del Sistema General de Riesgos Laborales.		
10.2	El contratista deberá entregar al supervisor del contrato los documentos que evidencien objetivamente, la afiliación a la Seguridad Social Integral del personal que ejecutará el objeto contractual, (E.P.S., A.F.P., A.R.L., C.C.F.), obligándose a mantener dicha afiliación, durante la totalidad del tiempo necesario para la ejecución de la actividad contratada.		
10.3	El contratista deberá anexar la matriz de Elementos de Protección Personal de acuerdo con la actividad a desarrollar y garantizar el uso de los mismos durante el desarrollo de las tareas planteadas en la ejecución del contrato.		

10.4	En caso de presentarse un accidente de trabajo dentro de las instalaciones de la Dirección de Inteligencia, le corresponde al contratista realizar el respectivo reporte e investigación dentro del tiempo reglamentario, presentará una copia de la documentación al supervisor del contrato, con el fin de que este haga llegar la copia al Grupo de Seguridad y Salud en el Trabajo de la Dirección de Inteligencia Policial, según lo establecido en la Resolución 1401 del 14/05/2007 del Ministerio de Trabajo y Protección Social "Por la cual se reglamenta la investigación de incidentes y accidentes de trabajo" o cualquiera que la modifique, reemplace o sustituya.		
10.5	El contratista correrá con los gastos médicos, de hospitalización y procedimientos médicos a que haya a lugar, en caso de que uno de sus funcionarios sufra un accidente laboral durante la ejecución del presente contrato.		
10.6	El contratista deberá dar cumplimiento a lo establecido en el Decreto 1072 del 26 de mayo del 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo", Resolución 0312 del 13 de febrero del 2019 del Ministerio de Trabajo "Por la cual se definen los Estándares Mínimos del Sistema de Gestión de SST" y Resolución 02232 del 01/08/20025 "Por el cual se actualiza política y los objetivos del Sistema de Gestión de Seguridad y Salud en el Trabajo en la Policía Nacional".		
10.7	En caso de presentarse una emergencia dentro de las instalaciones durante el desarrollo del objeto contractual, el contratista deberá garantizar que el personal bajo su mando, atienda las recomendaciones durante la activación del plan de emergencia de las instalaciones policiales.		
10.8	En caso de que se desarrolle en la Dirección de Inteligencia Policial una auditoría del SG-SST durante la ejecución del contrato, el contratista deberá suministrar al supervisor del contrato la documentación requerida del objeto contractual.		
10.9	El contratista garantizará que el personal que ingrese a las instalaciones se encuentre con la debida identificación de la empresa.		

PROPONENTE_____

Declaramos bajo nuestra responsabilidad personal, y comprometiendo la responsabilidad institucional de las personas jurídicas que representamos, que cumplimos en su totalidad con las especificaciones técnicas de verificación y de obligatorio cumplimiento que diligenciamos en la casilla de cumple.

FIRMA,
Representante Legal

ANEXO No. 8 FICHA TÉCNICA

FICHA TÉCNICA DE PRODUCTO

DENOMINACIÓN DE BIEN O SERVICIO

MANTENIMIENTO

DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO

MANTENIMIENTO PREVENTIVO Y CORRECTIVO PLATAFORMA TECNOLÓGICA DIPOL NIVEL CENTRAL, REGIONAL Y MANTENIMIENTO DE LOS SERVIDORES QUE CONFORMAN LA INFRAESTRUCTURA HIPERCONVERGENTE

UNIDAD DE MEDIDA

Unidad

DESCRIPCIÓN GENERAL

<table>
<tr><th>ÍTEM</th><th>ESPECIFICACIONES TECNICAS</th></tr>
<tr><td>1</td><td>MANTENIMIENTO PREVENTIVO Y CORRECTIVO PLATAFORMA TECNOLÓGICA DIPOL NIVEL CENTRAL, REGIONAL Y MANTENIMIENTO DE LOS SERVIDORES QUE CONFORMAN LA INFRAESTRUCTURA HIPERCONVERGENTE</td></tr>
<tr><td>1.1</td><td>Con el fin de garantizar la disponibilidad de la infraestructura, el contratista deberá prestar a todo costo, el servicio preventivo (mantenimiento preventivo exceptuando la limpieza del equipamiento tecnológico con compresor de aire) y corregir fallas que se presenten a partir de la firma del contrato y tres meses posterior a la vigencia del mismo (mantenimiento correctivo) tanto en los equipos físicos (hardware) como el software (firmware, drivers, actualizaciones y aplicación de parches) con cobertura total de cada uno de sus repuestos y elementos que componen el o los equipos o solución tecnológica (fibras, cables de poder, patch cord, switch, etc,.) relacionados a continuación:

Hardware:

<table>
<tr><th>ítem</th><th>Dispositivo</th><th>Serie</th></tr>
<tr><td>1</td><td colspan="2">Centro de Procesamiento de Datos principal de la DIPOL
(Avenida Boyacá No. 142ª – 55)</td></tr>
<tr><td>1.1</td><td>Servidor HP Proliant DL380 G6</td><td>USE940N9C9</td></tr>
<tr><td>1.2</td><td>Servidor DELL PowerEdge R820</td><td>6N4YHX1</td></tr>
<tr><td>1.3</td><td>Servidor Lenovo SR590</td><td>J3021MLL</td></tr>
<tr><td>1.4</td><td>Servidor Lenovo SR590</td><td>J3021MLM</td></tr>
<tr><td>1.5</td><td>Servidor DELL R760XS</td><td>GGV8L84</td></tr>
<tr><td>1.6</td><td>Servidor HP Proliant DL180 G10</td><td>2M213004M</td></tr>
<tr><td>1.7</td><td>Servidor HP Proliant DL360P G8</td><td>MXQ449029S</td></tr>
<tr><td>1.8</td><td>Servidor HP Proliant DL360P G8</td><td>MXQ449029Q</td></tr>
<tr><td>1.9</td><td>Servidor HP Proliant DL120 G9</td><td>2M2637017S</td></tr>
<tr><td>1.10</td><td>Servidor HP Proliant DL380 G5</td><td>2UX83101AF</td></tr>
</table>
</td></tr>
</table>

			1.11	Servidor HP Proliant DL360e G8	MXQ449029R		
			1.12	Servidor HP Proliant DL360e G8	MXQ449029N		
			1.13	Servidor HP Proliant DL360e G8	MXQ449029P		
			1.14	Servidor HP Proliant DL360e G8	MXQ41702V3		
			1.15	Servidor HP Proliant ML150 G6	USE008N31P		
			1.16	Servidor IBM Power 720	06949BR		
			1.17	Servidor IBM System X3650 M5	E2VZ070		
			1.18	Servidor IBM System X3550	KQKKA35		
			1.19	IBM System Storage DS4800 controller	78A009Z		
			1.20	IBM System Storage DS4800 enclosure	78K0X14		
			1.21	IBM System Storage DS4800 enclosure	136871W		
			1.22	IBM System Storage DS4800 enclosure	136872B		
			1.23	Servidor Cisco UCS C240 M5	WZP22120CA6		
			1.24	Servidor Cisco UCS C240 M5	WZP221115A6		
			1.25	Servidor Cisco UCS C220 M3	FCH1717V1S9		
			1.26	Servidor Cisco UCS C220 M3	FCH1717V1TH		
			1.27	Storage IBM Storwize V7000 Controller	78N20CX		
			1.28	Storage IBM Storwize V7000 Enclosure	78N20DZ		
			1.29	Storage IBM Storwize V7000 Enclosure	78N228L		
			1.30	Storage IBM Storwize V7000 Enclosure	78N20F7		
			1.31	Storage IBM Storwize V7000 Enclosure	78N20DN		
			1.32	Storage IBM Storwize V7000 Enclosure	78N20FG		
			1.33	Tape Library IBM TS4300 L8	78-005BK		
			1.34	Tape Library IBM TS4300 L8	78-004CZ		
			1.35	Tape Library IBM TS4300 L8	78-004D7		
			1.36	Tape Library IBM TS4300 L8	78-004CX		
			1.37	Tape Library IBM TS4300 L8	78-004D9		
			1.38	Switch SAN FC IBM TYPE 2005-B5K	105104P		
			1.39	Switch SAN FC IBM TYPE 2005-B5K	105104B		
			1.40	Switch SAN FC HP	USB606502K		
			1.41	Switch SAN FC HP	USB606S026		
			1.42	Switch SAN BROCADE 300	0742025-140ALJ005		
			1.43	Switch SAN BROCADE 300	0742025-140ALJ00Z		
			1.44	Switch SAN BROCADE 300	0741025-1508ALJ021		
			1.45	Servidor SUN Oracle X4-2	1518NML0C3		
			1.46	Servidor SUN Oracle X4-2	1518NML0C2		
			1.47	Servidor SUN Oracle X4-2	1518NML0C4		
			1.48	Servidor Oracle SPARC T-5	AK00208348		
			1.49	Servidor Oracle SPARC T-5	AK00208347		
			1.50	ZFS Storage Oracle ZS3-2	1518NM204N		
			1.51	ZFS Storage Oracle ZS3-2	1418NM200T		
			1.52	ZFS Storage Oracle ZS3-2	1418NM200P		
			1.53	Storage Oracle DE2-24C	1518NMT0BB		
			1.54	Storage Oracle DE2-24P	1439NM400J		
			1.55	Storage Oracle DE2-24P	1418NM401F		
			1.56	Servidor Lenovo SR530	J1005L78		
			1.57	Servidor Lenovo SR530	J1005L79		
			1.58	HP StoreEasy 3850 Gateway System	4C363203WY		
			1.59	HP StoreEasy 3850 Gateway Sngl Node	USE6327Y4M		

			1.60	HP StoreEasy 3850 Gateway Sngl Node	USE6327Y4P			
			1.61	HPE MSA 2040 ES SAN DC SFF Storage	2S6625B466			
			1.62	HPE D27000 Disk Enclosure	7CE612P25S			
			1.63	HPE MSA 2040 ES LFF Disk Enclosure	2S6626D163			
			1.64	HPE MSA 2040 ES LFF Disk Enclosure	2S6626D165			
			1.65	HPE MSA 2040 ES LFF Disk Enclosure	2S6626D166			
			1.66	HPE MSA 2040 ES LFF Disk Enclosure	2S6626D184			
			1.67	HPE MSA 2040 ES LFF Disk Enclosure	2S6626D185			
			1.68	HPE MSA 2040 ES LFF Disk Enclosure	2S6626D162			
			1.69	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RP1			
			1.70	Servidor Lenovo ThinkAgile VX7520 Appliance	J10087GX			
			1.71	Servidor Lenovo ThinkAgile VX7520 Appliance	J100875G			
			1.72	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RR5			
			1.73	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RR4			
			1.74	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RP3			
			1.75	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RP2			
			1.76	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RP4			
			1.77	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RP5			
			1.78	Servidor Lenovo ThinkAgile VX7520 Appliance	J1007RR6			
			1.79	Servidor Lenovo ThinkSystem SR590 (Veeam Backup)	J1015GPD			
			2	Centro de Procesamiento de Datos Alterno				
			2.1	Servidor Lenovo SR650	J10050CZ			
			2.2	Servidor Lenovo VX5520 (ThinkAgile) – Type 7Y94	J1015AEB			
			2.3	Servidor Lenovo VX5520 (ThinkAgile) – Type 7Y94	J1015AEA			
			2.4	Servidor Lenovo VX5520 (ThinkAgile) – Type 7Y94	J1015AEC			
			2.5	Servidor Lenovo VX5520 (ThinkAgile) – Type 7Y94	J1015GN7			
			2.6	Servidor Lenovo VX5520 (ThinkAgile) – Type 7Y94	J1015GN6			
			2.7	Servidor Lenovo VX5520 (ThinkAgile) – Type 7Y94	J1015GN5			
			3	Complejo policial del Sur Enrique Santos Castillo (Transversal 33 No. 47 a 35 Sur, Bogotá Fátima)				
			3.1	Servidor Dell PowerEdge R720	5NBK3Y1			
			3.2	Servidor HUAWEI 2288H V5	2102311XBJ10J8000080			
			4	Centro de Procesamiento de Datos AOPEI (Avenida Boyacá No. 142a – 55)				
			4.1	Servidor IBM System X3650 M4	KQ0Z5WA			
			4.2	Servidor IBM System X3650 M4	KQ9W6A3			
			4.3	Servidor IBM System X3650 M4	KQ9W6AZ			
			4.4	Servidor IBM System X3650 M4	KQ0Z5UZ			
			4.5	Storage IBM DS3512 controller	13D1862			
			4.6	Storage IBM DS3512 enclosure	13D16Y4			
			4.7	Storage IBM DS3512 enclosure	13D17PZ			
			4.8	Storage IBM DS3512 enclosure	13D17R3			
			4.9	Storage IBM DS3512 enclosure	13D17PV			
			4.10	Storage IBM DS3512 enclosure	13D1873			
			4.11	Storage Ultrastor RS16FS enclosure Fred C	D0099031763			
			4.12	Storage Ultrastor RS16FS enclosure Fred C	D0106032839			
			4.13	Storage Ultrastor RS16FS enclosure Fred C	D0111033748			
			4.14	Servidor Digital Intelligence Fred C	N0099031762			
			4.15	Switch SAN FC IBM	10311TD			
			4.16	Switch SAN FC IBM	10311VH			

4.17	Storage DELL PowerVault NX3200	FTNVGX1
4.18	Storage DELL PowerVault NX3200 enclosure	1HPJQD2
4.19	SAN Store Wize V3700 controller	7881710
4.20	SAN Store Wize V3700 enclosure	7874829
4.21	SAN Store Wize V3700 enclosure	7874087
4.22	SAN Store Wize V3700 enclosure	78C0715
4.23	Servidor IBM Storwize V5000	781MB44
5	Centro Operacional de Fusión de Inteligencia (COFIN Villavicencio)	
5.1	Storage DELL PowerVault NX3200	FDT3K02
6	Centro Operacional de Fusión de Inteligencia (COFIN Neiva)	
6.1	Storage DELL PowerVault NX3200	34W6CZ1
7	Centro Operacional de Fusión de Inteligencia (COFIN Envigado)	
7.1	Storage DELL PowerVault NX3200	8SX0DZ1
8	Centro Operacional de Fusión de Inteligencia (COFIN Popayán)	
8.1	Storage DELL PowerVault NX3200	FDS4K02
9	Centro Operacional de Fusión de Inteligencia (COFIN Bucaramanga)	
9.1	Storage DELL PowerVault NX3200	FDT0K02
10	Centro Operacional de Fusión de Inteligencia (COFIN Arauca)	
10.1	Storage DELL PowerEdge R750xs	2200PZ3
11	Centro Operacional de Fusión de Inteligencia (COFIN Montería)	
11.1	Storage DELL PowerEdge R750xs	1200PZ3
12	Regional de Inteligencia No. 1 (BOGOTÁ)	
12.1	Servidor HP Proliant ML 310e G8	USE420YH0L
12.2	Servidor HP Proliant ML 310e G8	MX244800C6
13	Regional de Inteligencia No. 2 (NEIVA)	
13.1	Servidor HP Proliant ML 310e G8	MX244800BP
13.2	Servidor HP Proliant ML 110	USE040N0A0
14	Regional de Inteligencia No. 3 (PEREIRA)	
14.1	Servidor HP Proliant ML 310e G8	MX244800BV
14.2	Servidor HP Proliant ML 350	USE839NAMQ
15	Regional de Inteligencia No. 4 (POPAYÁN)	
15.1	Servidor HP Proliant ML 310e G8	BRC3243DPH
15.2	Servidor HP Proliant ML 310e G8	MX244800BH
15.3	NAS Lenovo PX400D	1S70CJ9001LAMG008M3X
16	Regional de Inteligencia No. 5 (CUCUTÁ)	
16.1	Servidor HP Proliant ML 310e G8	MX244800BD
16.2	Servidor HP Proliant ML 110	USE040N0A3
17	Regional de Inteligencia No. 6 (MEDELLÍN)	
17.1	Servidor Servidor HP Proliant ML 110 G6	USE040N0AR
17.2	Servidor HP Proliant ML 310e G8	MX244800BT
17.3	Servidor Lenovo Think system ST550	J10026N3
18	Regional de Inteligencia No. 7 (VILLAVICENCIO)	
18.1	Servidor HP Proliant ML 310e G8	MX244800BW
19	Regional de Inteligencia No. 8 (BARRANQUILLA)	
19.1	Servidor HP Proliant ML 310e G8	MX244800BF

Software:

S.O Windows Server

	S.O Windows Storage Server S.O Linux (diferentes distribuciones) S.O AIX IBM Tivoli Storage Manager (TSM) IBM Spectrum Protect General Parallel File System (GPFS) Software de administración de switches FC IBM System Storage, series DS4000, V3700, V7000 DELL System Storage Storage Management Utility IBM Hardware Management Console (HMC) SAMBA VMWARE VSPHERE VMWARE VSAN VEEAM VEEAM ONE System Center Configuration Manager
2	**REQUERIMIENTOS GENERALES DE LOS SERVICIOS SOLICITADOS**
2.1	El contratista prestará en sitio los servicios de mantenimiento y soporte técnico con personal certificado y con experiencia certificable mínima de tres (3) años en infraestructuras equivalentes, verificable mediante hojas de vida, certificaciones o contratos ejecutados (ítem 6.3), con acompañamiento de un funcionario que la DIPOL designe para tal efecto, así: En la ciudad de Bogotá D.C, ▪ Centro de Procesamiento de Datos del Grupo de Tecnologías de la Información y las Comunicaciones de la DIPOL (Avenida Boyacá No. 142 a – 55) ▪ Centro de Procesamiento de Datos del Área de Operaciones de Inteligencia de la DIPOL (Avenida Boyacá No. 142 a – 55) ▪ Centro de Procesamiento de Datos alterno de la DIPOL ▪ Escuela de Poligrafía de la Policía Nacional (Transversal 33 No. 47 a 35 Sur, Fátima) ▪ Sede de las ocho Regionales de Inteligencia Policial, así:

REGIONAL DE INTELIGENCIA POLICIAL (RIPOL)	CIUDAD	DIRECCIÓN
RIPOL 1	Bogotá D.C	Calle 17 # 65B-99
RIPOL 2	Neiva	Calle 21 Sur # 235 zona industrial Canaima
RIPOL 3	Pereira	Avenida Las Américas 46-35 (Instalaciones Comando Metropolitana de Pereira)
RIPOL 4	Popayán	Avenida Panamericana 1N-75 barrio Villa Paula (Instalaciones Metropolitana de Policía de Popayán)
RIPOL 5	Cúcuta	Calle 22N # 2-03 Urbanización Tasajero (Instalaciones Región de Policía No. 5)
RIPOL 6	Medellín	Calle 111 # 64C-350 barrio Boyacá Las Brisas (Instalaciones del Centro de Instrucción Policial Carlos Holguín)
RIPOL 7	Villavicencio	Calle 44 # 35-96 barrio El Triunfo (Instalaciones Inspección
RIPOL 8	Barranquilla	Carrera 43 # 47-53 (Instalaciones Comando de Policía Metropolitana)

2.2	El contratista deberá elaborar el plan de trabajo detallado (EDT) para los servicios de soporte contratado y que incluya los mantenimientos preventivos, las actualizaciones de firmware, de sistema operativo y demás herramientas incluidas en el presente proceso. Este documento deberá ser concertado y entregado al supervisor del contrato en los primeros quince (15) días calendario siguientes a la aprobación de la garantía única.
2.3	El contratista deberá garantizar a la DIPOL la disponibilidad permanente de los siguientes medios de contacto: - Número de teléfono móvil de un contacto directo en la empresa para atención de casos que requieran prioridad. - Número telefónico general de la compañía para el reporte de incidencias. - Correo electrónico de soporte para atender los requerimientos.
2.4	El contratista deberá implementar y cumplir un esquema formal de gestión de incidentes basado en niveles de severidad y acuerdos de nivel de servicio (SLA), aplicable a toda la infraestructura y servicios cubiertos por el contrato. Dicho esquema deberá permitir la atención priorizada de eventos, garantizar la continuidad operativa y facilitar la supervisión y control contractual. **Clasificación de severidades:** Los incidentes deberán clasificarse en las siguientes categorías, de acuerdo con su impacto operativo y nivel de afectación: **Severidad Crítica (P1)**: Incidentes que generen indisponibilidad total de servicios misión crítica, afectación grave a la continuidad del negocio, riesgo alto para la seguridad de la información o interrupción de servicios esenciales de autenticación, almacenamiento, respaldo o virtualización. **Severidad Alta (P2)**: Incidentes que provoquen degradación significativa del servicio, afectación parcial de componentes críticos o riesgo de escalamiento a una condición crítica, sin indisponibilidad total. **Severidad Media/Baja (P3)**: Solicitudes de soporte, ajustes menores, actividades de mantenimiento no urgente o requerimientos informativos que no afecten la operación. **Acuerdos de nivel de servicio (SLA)** El contratista deberá cumplir, como mínimo, con los siguientes niveles de servicio, los cuales serán exigibles contractualmente:
2.5	Los problemas técnicos deberán ser atendidos de forma presencial en el sitio de la incidencia, ofreciendo soporte técnico especializado para los componentes de hardware y software contemplados en el contrato. El objetivo será restablecer la operatividad del sistema afectado, cumpliendo estrictamente con los tiempos de respuesta y resolución definidos en este documento

Severidad	Tiempo máximo de respuesta	Tiempo máximo de atención en sitio	Tiempo máximo de restauración
P1 – Crítica	≤ 15 minutos	Bogotá D.C.: ≤ 2 horas Regionales: ≤ 12 horas	≤ 24 horas
P2 – Alta	≤ 30 minutos	≤ 24 horas	≤ 48 horas
P3 – Media/Baja	≤ 8 horas	Según programación acordada	Según programación

2.6	El contratista deberá prestar asistencia técnica 7/24 (siete días por veinticuatro horas) durante la vigencia del contrato
2.7	El contratista deberá mantener un stock de repuestos durante la ejecución del contrato, que incluya discos duros compatibles con los servidores y sistemas de almacenamiento, memorias, drives de librerías, fuentes de poder, ventiladores, placas motherboard de los servidores y switches SAN especificados en los pliegos. La DIPOL se reserva el derecho de verificar dicho stock.
2.8	El oferente deberá garantizar un stock de discos duros para los sistemas de almacenamiento descritos en el ítem 1.1, de manera que, en caso de falla simultánea de discos en un mismo arreglo, puedan ser reemplazados conforme a los niveles de servicio establecidos en este pliego. Además, deberá anexar una certificación firmada en la que se comprometa a mantener dicho stock durante la vigencia del contrato. El stock deberá permitir la reposición inmediata de al menos dos (2) discos por tipo y tecnología instalada en cada sistema crítico, o su equivalente funcional.
2.9	Las refacciones, discos o equipos que deban ser reemplazados deberán ser nuevos, originales y con características iguales o superiores a las especificadas. En caso de que los productos originales ya no se encuentren en fabricación, podrán ser remanufacturados, siempre que cumplan con las características mínimas requeridas o superiores.
2.10	El contratista garantizará la disponibilidad de la infraestructura mediante la revisión y aplicación de parches, así como la actualización de drivers, firmware y/o microcódigo a los equipos descritos en el numeral 1.1. Al inicio de la ejecución del contrato, deberá presentar un informe detallado sobre el nivel actual de parches, firmware y/o microcódigo de dichos equipos, indicando la fuente de información utilizada para su validación. Este informe deberá ser entregado al supervisor del contrato para su revisión y aprobación.
2.11	Las actualizaciones de drivers, firmware y/o microcódigo, así como la aplicación de parches, podrán realizarse previa coordinación con el supervisor del contrato. Para los equipos descritos en el numeral 1.1 que requieran actualizaciones o parches, conforme al informe del numeral 2.10, el contratista deberá presentar un plan de trabajo detallado, que incluya los procedimientos a seguir, los requisitos para la instalación o aplicación, el tiempo de ejecución, las tareas de pre-instalación y post-instalación, la contingencia en caso de fallos, y el cronograma o minutograma. El contratista garantizará que las actividades de actualización no afecten la disponibilidad del servicio de datos de los equipos mencionados en el numeral 1.1.
2.12	El contratista deberá proporcionar la actualización de licencias del software Lenovo xClarity Pro para los servidores Lenovo ThinkAgile VX7520 mencionados en el ítem 1.1.
2.13	El contratista deberá garantizar el funcionamiento del hardware de las plataformas hiperconvergentes configuradas en los servidores Lenovo ThinkAgile, así como gestionar y resolver las alertas que indiquen posibles fallas en sus componentes.
2.14	El contratista deberá suministrar el licenciamiento del software Veeam Backup y Veeam One por un periodo de un año, realizando su correcta instalación y garantizando su funcionamiento a partir del vencimiento del licenciamiento actual con el que cuenta la entidad. Este licenciamiento deberá estar a nombre de la Dirección de Inteligencia Policial.
3	**MANTENIMIENTOS**
3.1	**Mantenimientos preventivos y correctivos:** Los mantenimientos correctivos deberán realizarse según sea necesario para resolver de manera oportuna los incidentes reportados. Se llevarán a cabo dos (2) mantenimientos durante la vigencia del contrato, con un plan de trabajo de al menos ocho (8) horas por sesión en sitio, en las instalaciones descritas en el ítem 2.1 del anexo de requerimientos técnicos mínimos. Las actividades incluyen, pero no se limitan a: - Verificación y aseguramiento de conexiones de red (tomas, cables, conectores).

		- Verificación y aseguramiento de conexiones internas de equipos (cables, conectores, tarjetas). - Limpieza y reemplazo de unidades de DVD, CD-ROM y Tape Backup, si es necesario. - Eliminación de polvo de componentes internos (uso de herramientas adecuadas para no activar sistemas de detección). - Limpieza, ajuste y lubricación de ventiladores y reemplazo, si es necesario. - Limpieza y ajuste de fuentes de poder y reemplazo, si es necesario. - Lubricación de partes mecánicas. - Verificación y ajuste de tamaño de sistemas de archivos del sistema operativo. - Revisión de archivos de logs del sistema operativo. - Eliminación de archivos temporales, si es necesario. - Reinstalación o reconfiguración del sistema operativo y herramientas de software en los servidores, cuando sea requerido. - Actualización de drivers o firmware de dispositivos de hardware. - Aplicación de parches a sistemas operativos Windows Server, Linux, AIX, VMware, entre otros instalados en los servidores descritos en el ítem 1.1. - Liberación de cartuchos atascados en las librerías de cintas. - Revisión de configuración de alias, zonas y puertos físicos de conexión en los 'SAN Switch', incluyendo desconexión y retiro de fibras no conectadas a los host systems. - Revisión y configuración de los componentes de hardware y software del file server Linux. - Revisión periódica de componentes físicos y lógicos de los Subsystem Storage.	
	3.2	**Asistencia en configuraciones y proyectos relacionados:** El contratista deberá asistir a la DIPOL en la ejecución de configuraciones, incluyendo las actividades descritas a continuación. Las tareas se abordarán como proyectos según su complejidad, con la documentación y planificación necesaria para cada una. - Configuración de la capacidad de los FS de TSM y Spectrum Protect, en ambientes de producción y contingencia, previa revisión de la estructura y distribución de archivos del sistema operativo. - Soporte para soluciones de backup Tivoli Storage Manager (TSM) y Spectrum Protect, incluyendo actualizaciones de versiones, parches de sistema operativo, instalación de agentes y configuración de tareas de backup. - Migración del servidor de Spectrum Protect a un servidor blade IBM Power7, y ejecución de las configuraciones necesarias para el funcionamiento de la plataforma de backup. - Pruebas de recuperación de backups generados por TSM y Spectrum Protect. - Migración de data activa entre cintas magnéticas LTO, incluyendo configuraciones necesarias en librerías y herramientas de backup, garantizando la integridad de los archivos migrados. - Verificación de la salud de las controladoras de dominio, estado de replicación, roles FSMO, resolución de nombres, relaciones de confianza y sincronización de hora mediante NTP. - Hardening a los servidores Windows que indique el supervisor del contrato, realizando las configuraciones locales y desde el dominio que sean necesarias, previa validación de los riesgos y aprobación del supervisor - Revisión y creación de políticas GPO en el directorio activo, según las necesidades de la DIPOL. - Asistencia en la solución de errores en NIC Teaming de las controladoras de dominio y en la unificación de dominios entre el nivel central y unidades desconcentradas. - Eliminación y creación de arreglos en sistemas SAN, optimizando el rendimiento y capacidad de almacenamiento. - Organización de conexiones fibre channel en los SAN Switch, y migración de conexiones entre los Switch FC en el Centro de Procesamiento de Datos. - Asistencia en la configuración de IPv6 en servidores físicos y virtuales, revisión y reconfiguración del DHCP en actualizaciones de Windows Server.	

	- Instalación, configuración y ejecución de controles de cambio en los sistemas operativos, y actualización de parches. - Configuración de sincronización de archivos mediante DFS entre servidores de producción y contingencia, asegurando su correcta sincronización. - Solución de errores en System Center y base de datos, y asistencia en la configuración de reglas para el despliegue de software y actualizaciones de Windows. - Revisión y corrección de la entidad certificadora del Active Directory, y asistencia en la generación y despliegue de nuevos certificados. - Asistencia en el diligenciamiento del inventario de equipos servidores, conforme a las directrices del Ministerio de la Información y las Comunicaciones. - Revisión y optimización de la configuración del clúster de conmutación por error del servidor de archivos, con pruebas de la configuración de alta disponibilidad (HA).
3.3	Durante la vigencia del contrato, el contratista será responsable de ejecutar los mantenimientos preventivos y correctivos, asumiendo todos los costos relacionados con el traslado de equipos, refacciones, instalaciones, configuraciones, personal técnico en sitio y demás recursos necesarios para solucionar las fallas reportadas o potenciales. Estos mantenimientos deberán ser realizados por personal profesional certificado, con experiencia comprobada y la capacidad necesaria para llevar a cabo las tareas sobre los equipos descritos en el numeral 1.1. El supervisor del contrato podrá solicitar las certificaciones, diplomas y demás documentos pertinentes para verificar la idoneidad del personal asignado. En caso de que el ingeniero no cumpla con los requisitos establecidos, el contratista deberá reemplazarlo. El personal propuesto deberá ser el mismo a lo largo del proyecto, y cualquier cambio deberá ser comunicado por escrito, garantizando que el nuevo profesional cumpla con los requisitos exigidos.
3.4	**Actualización sistema operativo y nivel funcional del dominio** El contratista deberá planear, ejecutar y documentar la actualización de la versión del sistema operativo de las controladoras de dominio y el incremento del nivel funcional del dominio al último nivel estable soportado por el fabricante, bajo un enfoque de proyecto técnico integral. Dicha actividad deberá desarrollarse conforme a buenas prácticas, lineamientos del fabricante y estándares de seguridad de la información, contemplando como mínimo: análisis previo del estado del dominio, verificación de compatibilidad, identificación y mitigación de riesgos, definición de controles previos y posteriores, ejecución controlada por fases, planes de contingencia y estrategias de reversión (rollback) plenamente documentadas. El proceso deberá garantizar la continuidad del servicio, la integridad de la información, la no afectación de los servicios de autenticación, autorización y directorio, y deberá culminar con la entrega de un informe técnico que evidencie la correcta ejecución, validación y estabilización de la plataforma.
3.5	El contratista deberá proporcionar acompañamiento al personal del Grupo de Tecnologías de la Información y las Comunicaciones de la DIPOL para el traslado o movimiento de cualquier dispositivo de hardware dentro de los Centros de Procesamiento de Datos de producción y contingencia.
3.6	El contratista deberá garantizar la disponibilidad de la infraestructura de hardware mediante herramientas de monitoreo que generen alertas sobre fallas de hardware, degradación de servicios o eventos críticos, las cuales deberán ser atendidas conforme a los SLA definidos.
3.7	Cuando se realice el reemplazo de discos duros de los servidores y/o sistemas de almacenamiento, la DIPOL, de acuerdo con sus protocolos de seguridad de la información, procederá a destruirlos. Por lo tanto, estos no serán entregados al contratista.
3.8	Después de cada visita de mantenimiento preventivo o correctivo, el contratista deberá entregar un informe que incluya, como mínimo, la siguiente información: Datos del equipo atendido Fecha y hora de la atención Duración de la visita Actividades realizadas durante la intervención

	Información del técnico que atendió el caso
3.9	El contratista deberá evaluar y documentar el estado técnico y funcional de los equipos tecnológicos que sean objeto de intervención en el marco del contrato, incluyendo servidores, sistemas de almacenamiento, librerías y demás componentes de la infraestructura tecnológica definida por la entidad. Como resultado de esta evaluación, deberá elaborar informes técnicos periódicos en los que se identifique el estado operativo de los equipos, la condición de sus componentes críticos, la vigencia del soporte del fabricante y la proyección estimada de vida útil remanente, con base en criterios técnicos y buenas prácticas aplicables. Cuando del análisis se evidencie obsolescencia tecnológica, agotamiento de la vida útil o riesgos relevantes para la continuidad del servicio, el contratista deberá formular recomendaciones técnicas debidamente sustentadas orientadas al reemplazo, renovación o actualización de los equipos afectados. Los informes servirán como insumo para la planeación tecnológica, la gestión del riesgo y la toma de decisiones institucionales, en los términos y formatos que defina la entidad.
4	**TRANSFERENCIA DE CONOCIMIENTO**
4.1	El contratista deberá proporcionar transferencia de conocimiento al personal operador del Centro de Procesamiento de Datos de la DIPOL en relación con las siguientes herramientas: Windows Server, Spectrum Protect, Active Directory y VMware. La transferencia deberá cubrir, entre otros aspectos, los conceptos teóricos fundamentales sobre el funcionamiento de estas herramientas, así como los comandos, rutinas y configuraciones necesarias para su correcta administración.
4.2	El contratista deberá proporcionar, sin costo adicional para la DIPOL, formación a cuatro (4) funcionarios en el curso CompTIA Server+ (SK0-005). La formación deberá ser impartida por personal certificado en el curso y llevarse a cabo en un centro de instrucción autorizado, que cuente con los medios tecnológicos, laboratorios y las herramientas necesarias para asegurar el éxito de la actividad académica.
5	**GARANTÍA TÉCNICA**
5.1	El contratista proporcionará soporte durante los tres (3) meses siguientes a la fecha de finalización del contrato. Durante este período, atenderá incidentes que afecten la plataforma tecnológica de la DIPOL y pongan en riesgo la infraestructura crítica de TI, poniendo a disposición el personal calificado y los recursos necesarios para su resolución, conforme al alcance del contrato
5.2	Si es necesario, el contratista escalará a la casa fabricante las necesidades de soporte especializado para resolver fallos en los sistemas de la DIPOL incluidos en este contrato
5.3	La atención y resolución de incidentes se realizará conforme a los niveles de severidad y SLA definidos en el numeral 2.4 del presente documento.
5.4	Si es necesario retirar equipos, dispositivos o componentes de la DIPOL para su reparación en las instalaciones del contratista, este asumirá los costos y riesgos del traslado. Además, deberá proporcionar un equipo de características similares en calidad de préstamo durante el tiempo necesario para resolver el inconveniente. En caso de que se requiera realizar pruebas en un ambiente controlado, el contratista podrá utilizar su centro de cómputo de Datos, siempre que se garantice la seguridad del equipo y/o dispositivo de la DIPOL.
5.5	El contratista otorgará una garantía de hasta un (1) año, contados a partir de la finalización del contrato, sobre las piezas o componentes reemplazados durante su ejecución.
5.6	El servicio se considerará correctamente prestado cuando el componente intervenido opere sin alertas críticas, sin eventos de error registrados en los logs del sistema y supere las pruebas de validación funcional definidas por el fabricante o por la entidad, evidenciadas mediante registros técnicos y acta de conformidad del supervisor.
6	**CERTIFICACIONES**

	6.1	**NIVEL DE EDUCACION O NIVEL ACADEMICO** Con el fin de garantizar la idoneidad técnica, la adecuada ejecución de las actividades contratadas y la mitigación de riesgos operativos sobre la infraestructura tecnológica de la Dirección de Inteligencia Policial, el contratista deberá disponer de personal profesional con formación académica y experiencia certificable en tecnologías de la información y las comunicaciones. En consecuencia, el proponente deberá asignar como mínimo tres (3) profesionales en ingeniería de sistemas, ingeniería de telecomunicaciones o áreas afines, quienes deberán acreditar formación académica y certificaciones técnicas vigentes, expedidas por fabricantes, correspondientes a las certificaciones que se relacionan a continuación, las cuales deberán ser acreditadas de manera individual o conjunta (como se detalla en la nota 1) por los profesionales propuestos, conforme a lo exigido en el presente proceso. • Lenovo Data Center Technical Sales • IBM Certified Administration Spectrum Protect • IBM Certified Administration Tivoli Storage Manager • Microsoft® Certified Solutions Expert • Microsoft Certified Technology Specialist • VTSP-HCI (Hyper-Converged Infrastructure) • VSP-HCI (Hyper-Converged Infrastructure) • VMware Certified Professional – Data Center Virtualization • VMware vSphere Foundations • Veeam Certified Engineer (MCE) Nota 1. Un mismo profesional podrá acreditar una o varias de las certificaciones exigidas. El oferente podrá distribuir las certificaciones entre los profesionales propuestos y, de ser necesario, presentar un número superior a tres (3) profesionales, siempre que, en conjunto, se acrediten la totalidad de las certificaciones técnicas exigidas para este proceso y se cuente, como mínimo, con tres (3) profesionales. En todo caso, cada profesional propuesto deberá acreditar al menos una (1) de las certificaciones exigidas; no se aceptarán profesionales sin certificación. Nota 2. No se aceptarán certificaciones de asistencia, participación o capacitación sin evaluación formal de competencias. Nota 3. El oferente deberá adjuntar en su propuesta copia legible del acta de grado o diploma expedido por institución de educación superior reconocida por el Ministerio de Educación Nacional, por cada profesional propuesto. Nota 4. En el caso de profesionales extranjeros, se deberá presentar certificación de homologación del título profesional expedida por el Ministerio de Educación Nacional de Colombia, conforme a la normatividad vigente. Nota 5. Las certificaciones técnicas exigidas deberán encontrarse vigentes a la fecha de cierre del proceso de selección. Será responsabilidad exclusiva del oferente acreditar su vigencia mediante los soportes documentales correspondientes. Nota 6. El supervisor del contrato podrá solicitar la sustitución del personal que no acredite las competencias técnicas exigidas o cuyo desempeño no resulte satisfactorio durante la ejecución del contrato. Nota 7. En caso de que el fabricante haya modificado la denominación de alguna de las certificaciones exigidas, el oferente podrá allegar la certificación vigente que la sustituya, siempre que demuestre de manera objetiva y verificable que corresponde a la actualización o equivalencia directa de la certificación originalmente solicitada.	

6.2	**EXPERIENCIA DEL PROPONENTE:** Con el fin de garantizar la calidad de los servicios a contratar y evitar incumplimientos en la ejecución del futuro contrato, se requiere acreditar experiencia en proyectos similares al objeto del presente estudio previo, según los códigos de clasificación de los bienes, obras o servicios (UNSPSC) en las clasificaciones 81112300 y/o 81111800 y/o 83112200, para lo cual el oferente deberá acreditar contratos realizados por valor igual o superior a 399.8 S.M.M.L.V, de procesos adelantados con empresas públicas o privadas. Lo anterior se verificará mediante la presentación del Registro Único de Proponentes (RUP).
6.3	**EXPERIENCIA DEL PERSONAL:** Es fundamental para la Dirección de Inteligencia Policial que todo el personal profesional asignado al equipo de trabajo cuente con idoneidad y experiencia general y específica, que asegure la calidad de las actividades a realizar sobre la infraestructura tecnológica descrita en el pliego de condiciones técnicas. En consecuencia, el proponente deberá acreditar que, durante los años 2023, 2024 y/o 2025, los profesionales incluidos en su oferta participaron en proyectos en los cuales realizaron actividades de instalación, implementación y/o configuración sobre uno o varios de los sistemas detallados a continuación. La experiencia de los profesionales podrá ser distribuida y acumulada entre los integrantes del equipo de trabajo para cumplir con el total de los sistemas exigidos, sin perjuicio de que cada profesional deba acreditar experiencia certificada en al menos uno (1) de los sistemas relacionados. - IBM Spectrum Protect - IBM Tivoli Storage Manager - Servidores Power - Storage IBM - Storage HP - Linux Red Hat - Windows Server - Lenovo Xclarity Pro - Lenovo ThinkAgile Appliance - Replica de datos con Veeam Backup Nota: Las certificaciones de experiencia deberán ser emitidas por las empresas en las que los profesionales propuestos en la oferta hayan participado en proyectos de instalación, implementación y/o configuración sobre los sistemas mencionados anteriormente. Las certificaciones deberán contener información legible sobre el funcionario, incluyendo un concepto sobre su desempeño durante la ejecución de las actividades contratadas.
6.4	**CERTIFICACIONES DEL OFERENTE:** Con el fin de garantizar la correcta ejecución del contrato, mitigar riesgos asociados a la inexperiencia técnica y asegurar la continuidad operativa de la plataforma tecnológica de la Dirección de Inteligencia Policial, la DIPOL exige que el oferente acredite capacidad formal de soporte, escalamiento y relacionamiento directo con los fabricantes de las tecnologías que soportan la infraestructura institucional. Para tal efecto, el oferente deberá acreditar mínimo tres (3) membresías o certificaciones vigentes, expedidas por los fabricantes de las tecnologías objeto del contrato que se indican a continuación, siendo obligatorio que una (1) de estas corresponda a la membresía con BROADCOM, en el nivel mínimo Select, en razón a que los sistemas de información más críticos de la entidad operan sobre la plataforma de virtualización VMware, actualmente administrada por dicho fabricante. Las dos (2) restantes deberán corresponder a cualquiera de las siguientes:

	• **LENOVO:** Membresía Silver o superior • **IBM:** Membresía Silver o superior • **VEEAM:** Membresía Silver o superior • **DELL: Membresia GOLD o superior** Nota 1: La exigencia de estas acreditaciones se fundamenta en la necesidad institucional de asegurar la idoneidad técnica, la experiencia y el respaldo del fabricante del proveedor, como medida de mitigación de riesgos operativos durante la ejecución del contrato. Nota 2. En caso de que el fabricante haya modificado la denominación de alguna de las certificaciones exigidas, el oferente podrá allegar la certificación vigente que la sustituya, siempre que demuestre de manera objetiva y verificable que corresponde a la actualización o equivalencia directa de la certificación originalmente solicitada.
6.5	El contratista deberá allegar certificado de autenticidad de las licencias incluidas en el presente proceso, en cumplimiento a lo establecido en la circular conjunta de la Procuraduría General de la Nación y la Unidad Administrativa Especial Dirección Nacional de Derecho Autor, frente a la celebración de contratos de software o licenciamiento
7	**CONFIDENCIALIDAD Y SEGURIDAD**
7.1	En virtud del presente contrato, el contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del presente contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo. El contratista deberá firmar un compromiso de reserva.
7.2	Si la DIPOL considera pertinente someter a estudio de seguridad y confidencialidad al personal que realiza la prestación del servicio, el contratista permitirá y facilitará todos los medios que la entidad le requiera para este fin.
7.3	El personal que realice la instalación y configuración de equipos y sistemas, deberá cumplir con un estudio de confiabilidad realizado por la Dirección de Inteligencia de la Policía Nacional, en cualquier momento durante la vigencia del contrato. En el evento de no aprobar dicho estudio algunas de las personas vinculadas a este proyecto, el contratista deberá realizar el cambio de estas personas por otras que también deberán cumplir con el estudio de confiabilidad requerido.
8	**CAPACIDAD OPERATIVA**
8.1	Con el fin de garantizar la calidad de los servicios a contratar y evitar posibles incumplimientos en la ejecución del contrato, se requiere que las firmas participantes en el proceso de selección cuenten con un número mínimo de personal profesional e idóneo en los sistemas, aplicaciones y plataformas que conforman la infraestructura tecnológica de la DIPOL, tal como se detalla en el anexo de especificaciones técnicas de este proceso. Este aspecto es crucial para la correcta ejecución de los mantenimientos preventivos, la resolución oportuna y eficaz de incidentes a nivel físico y lógico, y para prevenir riesgos sobre la disponibilidad e integridad de los activos de información del organismo. Además, los oferentes deberán demostrar su capacidad para: • Adquirir en el mercado, tanto nacional como internacional, los componentes de hardware necesarios para el reemplazo de equipos. • Contar con medios logísticos y administrativos adecuados para movilizar personal y refacciones a los sitios donde se encuentren los equipos descritos en el proceso, incluidas las ocho Regionales de Inteligencia, según se indica en el ítem 2.1 del anexo de especificaciones técnicas mínimas requeridas. • Gestionar ante las casas fabricantes la solución de problemas complejos que no puedan ser resueltos con sus propios recursos. Por lo anterior, los oferentes deberán anexar en su propuesta una certificación de capacidad operativa, emitida por el representante legal o quien haga sus veces.

ELABORACION DE ESTUDIOS PREVIOS PARA CONTRATOS	
ESPECIFICACIONES TÉCNICAS MÍNIMAS	**POLICÍA NACIONAL**