FICHA TÉCNICA INTEGRAL PARA DESCRIPCIÓN DE NECESIDADES CONTRACTUALES

OBJETO:	Adquirir la renovación y actualización de los componentes de hardware y software asociados a las plataformas de seguridad perimetral, protección de Antivirus y solución de copias de seguridad (backup) de la Superintendencia de Transporte.
ALCANCE:	El objeto de la presente contratación comprende la adquisición y renovación de las soluciones tecnológicas de ciberseguridad y de copias de respaldo de la información de la Superintendencia de Transporte, con el fin de garantizar la protección integral y continua de la infraestructura tecnológica institucional, así como la continuidad operativa, la disponibilidad, integridad y recuperación oportuna de la información institucional. Esta contratación se estructura en tres componentes: **COMPONENTE No. 1 – Soluciones de Seguridad Perimetral:** • El Upgrade y/o adquisición por obsolescencia de un (1) firewall de nueva generación (NGFW, como mínimo, las capacidades técnicas descritas en el ítem 1 del Componente No. 1 de la presente ficha técnica. • La renovación por un (1) año del licenciamiento y soporte del fabricante de la solución FortiWeb, serial FWBVMSTM25000368. • La renovación por un (1) año del licenciamiento y soporte del fabricante de la solución FortiAnalyzer, serial FAZ3HGTA25000031. • La renovación por un (1) año del licenciamiento y soporte del fabricante de la solución FortiAuthenticator, serial FAC-VMTM25001799. **COMPONENTE No. 2 – Solución antivirus:** • La suscripción de la licencia para un total de 591 equipos de cómputo asignados a funcionarios y contratistas, asegurando la protección de los endpoint contra amenazas informáticas y ataques dirigidos, así como la administración centralizada mediante una consola unificada. • La suscripción de 70 licencias de antivirus para la protección de los servidores físicos y virtuales alojados en el Datacenter principal de la entidad, incluyendo aquellos que operan en entornos híbridos con nubes públicas, garantizando visibilidad, control, prevención de exploits, bloqueo de ataques de red y protección antimalware sin afectación al rendimiento. • La provisión de soporte técnico y afinamiento, incluyendo al menos una visita técnica mensual para la actualización de licencias, ajustes en configuraciones, administración del software y acompañamiento en sitio cuando sea necesario, a fin de mantener el óptimo funcionamiento y la efectividad de las soluciones antivirus implementadas.

	• La inclusión de todas las actualizaciones, mejoras y parches necesarios para mantener la vigencia y robustez del software contra las amenazas emergentes durante la vigencia contractual. • Prevención de malware basada en Machine Learning e Inteligencia Artificial: Componente de seguridad que permita prevenir y bloquear en tiempo real la ejecución de malware, ransomware y código malicioso mediante técnicas de Machine Learning e Inteligencia Artificial, proporcionando protección frente a amenazas conocidas, variantes desconocidas y ataques de día cero (Zero-Day), antes de que afecten los sistemas y la información institucional. • Protección avanzada en tiempo real pos-ejecución: Componente de seguridad que permita detectar y bloquear comportamientos maliciosos, ransomware y actividades sospechosas que logren evadir las capas iniciales de prevención, mediante análisis de comportamiento en tiempo real, evitando el cifrado de archivos, la exfiltración de información y otras acciones maliciosas, sin afectar la continuidad operativa de los sistemas protegidos. • Consola de administración y monitoreo centralizado: Componente que permita la gestión unificada de los equipos de usuario y servidores protegidos, incluyendo la administración de políticas de seguridad, despliegue y actualización de agentes, monitoreo en tiempo real, generación de alertas, visualización de eventos, gestión de incidencias, elaboración de reportes e indicadores de seguridad, así como el control centralizado de licencias y funcionalidades de la solución implementada. **COMPONENTE No. 3 – Solución de Copias de Respaldo:** • La renovación del soporte de fábrica de las licencias Veeam Availability Suite Enterprise Plus para 120 instancias, con actualizaciones de versionamiento y soporte 7x24. Con esta contratación, la Superintendencia de Transporte busca asegurar la continuidad operativa de sus servicios tecnológicos, el cumplimiento de las políticas y normativas de seguridad de la información, la protección efectiva de los activos digitales institucionales contra incidentes de seguridad informática y la recuperación oportuna de la información, contribuyendo así a la estabilidad de las operaciones misionales.
CLASIFICADOR DE BIENES Y SERVICIOS:	

Clasificación UNSPSC	Segmento	Familia	Clase
43222500	Difusión de Tecnologías de Información y Telecomunicaciones	Equipos o plataformas y accesorios de	Equipo de seguridad de red

		redes multimedia o de voz y datos	
81111800	Servicios basados en ingeniería, investigación y tecnología	Servicios Informáticos	Servicios de sistemas y administración de componentes
43233200	Tecnología de la información y la comunicación	Software	Software de seguridad y protección
43222600	Difusión de Tecnologías de Información y Telecomunicaciones	Equipos de datos o redes de comunicación	Equipo de servicio de red
43231500	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software funcional específico de la empresa
81111900	Servicios basados en ingeniería, investigación y tecnología	Servicios informáticos	Sistemas de recuperación de información
81112100	Servicios basados en ingeniería, investigación y tecnología	Servicios informáticos	Servicios de internet
81112500	Servicios basados en ingeniería, investigación y tecnología	Servicios informáticos	Mantenimiento y soporte de software
43212000	Difusión de Tecnologías de Información y Telecomunicaciones	Equipo informático y accesorios	Accesorios de pantallas de computador

Conforme a lo establecido en el Decreto 1082 de 2015 (artículo 2.2.1.1.1.4.1), los servicios y bienes adquiridos por la Superintendencia de Transporte- en adelante SUPERTRANSPORTE, se encuentran enmarcados en las clasificaciones UNSPSC, conforme el Plan Anual de Adquisiciones.

1. COMPETENCIA, DESCRIPCIÓN DE LA NECESIDAD QUE SE PRETENDE SATISFACER CON EL PROCESO DE CONTRATACIÓN Y JUSTIFICACIÓN TÉCNICA

1.1 COMPETENCIA:

Que, de acuerdo con el artículo 2 de la Constitución Política son fines esenciales del Estado colombiano, servir a la comunidad, garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución, asegurar la convivencia pacífica y la vigencia de un orden justo. Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares

Que, la Superintendencia de Transporte, es un organismo de naturaleza pública creada por la Ley 1ª de 1991, modificada por la Ley 1753 del 2015, y Ley 1955 de 2019, dotándola de personería jurídica a la Superintendencia de Transporte, la cual, para todos sus efectos, tendrá el régimen presupuestal y financiero aplicable a los establecimientos públicos.

Que, en virtud del Decreto 2409 de 2018, la Superintendencia de Transporte es un organismo descentralizado del orden nacional, de carácter técnico, con personería jurídica, autonomía administrativa, financiera y presupuestal, adscrita al Ministerio de Transporte que tiene por objeto, ejercer las funciones de vigilancia, inspección, y control que le corresponden al Presidente de la República como suprema autoridad administrativa en materia de tránsito, transporte y su infraestructura de conformidad con la ley y la delegación establecida en el citado decreto.

Que, en la estructura de la Superintendencia de Transporte, se ubica la Oficina de Tecnologías de la Información y las Comunicaciones, a quien le corresponde liderar la gestión estratégica de TI, definiendo las políticas, planes, objetivos y metas en gestión de tecnologías que faciliten el cumplimiento de la misión institucional y el apoyo a las demás dependencias de la entidad en la implementación de soluciones que permitan el fortalecimiento de la Gestión institucional, encaminando los proyectos de TI al cumplimiento de los lineamientos del Gobierno Nacional y definidos por el MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (MINTIC).

Que, lo anterior, de acuerdo con lo definido en el artículo 11 del Decreto No. 2409 de 2018, en el que se establecen las funciones de la Oficina de Tecnologías de la Información y las Comunicaciones de la Superintendencia de Transporte, la cual tiene entre otras: "1. Liderar la gestión estratégica de tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado. (…) 3. Desarrollar los lineamientos en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de la entidad y/o sector en beneficio de la prestación efectiva de sus servicios y que a su vez faciliten la gobernabilidad y gestión de las Tecnologías de la Información y las Comunicaciones TIC. Así mismo, velar por el cumplimiento y actualización de las políticas y estándares en esta materia. (…) 9. Liderar los procesos de adquisición de bienes y servicios de tecnología, mediante la definición de criterios de optimización y métodos que direccionen la toma de decisiones de inversión en tecnologías de la información buscando el beneficio económico y de los servicios de la entidad. (…) 10. Adelantar acciones

que faciliten la coordinación y articulación entre entidades del sector y del Estado en materia de integración e interoperabilidad de información y servicios, creando sinergias y optimizando los recursos para coadyuvar en la prestación de mejores servicios al ciudadano. (…) 17. Propender y facilitar el uso y apropiación de las tecnologías, los sistemas de información y los servicios digitales por parte de los servidores públicos, los ciudadanos y los grupos de interés a quienes están dirigidos". En concordancia con lo anterior la Superintendencia de Transporte, dentro de las metas para el cuatrienio 2023-2026, según su Plan Estratégico Institucional, competen a la Oficina de Tecnologías de la Información y las Comunicaciones de la Superintendencia de Transporte, las siguientes:

✓ Unificar los sistemas misionales de información de la Entidad.
✓ Transformar Digitalmente a la Supertransporte a través de la Política de Gobierno Digital.

En línea con la Meta Institucional "Transformar Digitalmente a la Supertransporte a través de la Política de Gobierno Digital", la Oficina de Tecnologías de la Información y las Comunicaciones ha dispuesto en el Plan Estratégico de Tecnologías de la Información - PETI, las Políticas y Estándares para la Gestión de la Gobernabilidad de TI, confiriendo especial importancia a la Gestión de Infraestructura, así:



Así mismo, la Superintendencia de Transporte, como una entidad técnica de vigilancia, inspección y control, debe propender por el cumplimiento de la política de negocio TI en el cual debe velar por la infraestructura tecnológica, con miras a lograr la renovación y actualización de los componentes de hardware y software asociados a las plataformas de seguridad perimetral, protección de endpoints y solución de copias de seguridad (backup) de la Superintendencia de Transporte, que contribuyen al normal desarrollo de las actividades misionales de la Oficina de Tecnologías y Comunicaciones TIC, de acuerdo con las funciones descritas en el Decreto 2409 de 2018 y en concordancia con lo estipulado en la Política de Gobierno Digital por medio del componente de Servicios Ciudadanos Digitales cuyos propósitos son: 1. Habilitar y mejorar la provisión de servicios digitales de confianza y calidad. 2. Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de la información. 3. Tomar decisiones basadas en datos a partir del aumento en el uso y aprovechamiento de la información. 4. Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto. 5.

Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales, a través del aprovechamiento de las TIC.

1.2 DESCRIPCIÓN DE LA NECESIDAD

La infraestructura tecnológica de la Superintendencia de Transporte cuenta con componentes críticos para la seguridad de la información y la continuidad de los servicios tecnológicos, entre los que se incluyen firewalls perimetrales, herramientas de autenticación, análisis y monitoreo de eventos de seguridad, puntos de acceso, soluciones de protección antivirus y de seguridad de (Endpoint Protection y Server Protection), así como herramientas de respaldo, recuperación y restauración de la información (Backup). Estas soluciones requieren procesos de renovación, actualización y mantenimiento que permitan conservar su eficacia, disponibilidad y capacidad de respuesta frente a las amenazas y los riesgos emergentes del entorno digital.

La unificación de las necesidades de renovación y actualización de las plataformas de seguridad perimetral, protección de endpoints y copias de seguridad (backup) resulta conveniente al permitir una gestión integral de la seguridad de la información, optimizar recursos, reducir cargas administrativas y centralizar el licenciamiento, soporte técnico y mantenimiento. Asimismo, facilita la coordinación de las soluciones, fortalece la protección de los activos de información y contribuye a garantizar la continuidad operativa de la infraestructura tecnológica de la Superintendencia de Transporte.

COMPONENTE No. 1 - SOLUCIÓN DE SEGURIDAD PERIMETRAL

La entidad cuenta con las siguientes soluciones de ciberseguridad del fabricante Fortinet, cuyo licenciamiento y soporte requieren renovación por un (1) año. La función de cada solución se describe conforme a la documentación oficial del fabricante:

Solución	Función según el fabricante	Serial
FortiWeb	Firewall de aplicaciones web (WAF) que protege las aplicaciones web y las API frente a amenazas conocidas y de día cero.	FWBVMSTM25000368
FortiAnalyzer	Plataforma de registro, análisis y reporte centralizado de eventos de seguridad, que ofrece un repositorio unificado de datos, visibilidad completa y automatización para la detección y respuesta.	FAZ3HGTA25000031
FortiAuthenticator	Solución de gestión de identidades y acceso (IAM) que provee servicios de autenticación RADIUS y TACACS+, autenticación multifactor, inicio de sesión único (SSO) y servicios de autoridad certificadora.	FAC-VMTM25001799

La renovación de estas soluciones permite mantener vigentes el soporte del fabricante y las actualizaciones durante la vigencia contractual, garantizando la continuidad de la protección de las aplicaciones web, la trazabilidad de los eventos de seguridad y el control de acceso de los usuarios de la entidad.

La entidad requiere adquirir un (1) firewall de nueva generación (NGFW), debido a que el equipo actual de marca Fortigate Fortigate-501E presenta obsolescencia tecnología, lo cual es vital reemplazar dicho equipo para la protección de su perímetro de red, con capacidades de prevención de intrusiones, control de aplicaciones, inspección de tráfico cifrado y redes privadas virtuales (VPN), que cumpla como mínimo las especificaciones técnicas descritas en el numeral 2.1 Componente 1 de la ficha técnica.

COMPONENTE No. 2 - SOLUCIÓN DE ANTIVIRUS.

La falta de una solución antivirus vigente y centralizada incrementa la exposición de la Entidad a malware, ransomware y otras amenazas cibernéticas, poniendo en riesgo la confidencialidad, integridad y disponibilidad, para lo cual resulta indispensable contar con soluciones de antivirus actualizadas y robustas que protejan tanto los endpoints, es decir, los equipos de cómputo de usuarios finales como funcionarios y contratistas, como los servidores que alojan los sistemas de información de la entidad. En este sentido, la suscripción de la licencia del antivirus se configura como una medida estratégica para garantizar la defensa integral contra amenazas informáticas, resguardando la confidencialidad, integridad y disponibilidad de la información conforme al estándar internacional ISO/IEC 27001 y a la norma colombiana NTC ISO/IEC 27001. Por eso, es de vital importancia que el oferente adjudicatario cuente con la certificación ISO 27001 vigente, para garantizar que esté alineado con la política de seguridad de la entidad.

Para este componente se requieren 591 licencias de antivirus para endpoint y 70 licencias de antivirus para servidores, por un año (ítem 2.2) de la ficha técnica.

Así mismo, aunque el software antivirus es estable y suele recibir soporte remoto, es necesario contemplar un acompañamiento técnico presencial mensual que permita la actualización de licencias, ajustes de configuración y asesoramiento en el sitio. Este soporte asegura que las herramientas de protección se mantengan optimizadas y adaptadas a las condiciones específicas de la infraestructura tecnológica de la Superintendencia.

Ahora bien, dado que la mayoría de los riesgos de seguridad de la información provienen de ataques externos o incidentes internos que pueden comprometer la confidencialidad y funcionalidad de los sistemas, es indispensable renovar las licencias antivirus, incluyendo la actualización y soporte técnico. Esta suscripción garantizará la protección continua de los equipos y servidores, incluyendo los nuevos dispositivos portátiles y All in One adquiridos durante el primer semestre de 2025. Se mantiene la cantidad de licencias, ya que, aunque se incorporen nuevos equipos, se procederá a la baja de un número equivalente de dispositivos obsoletos. Además, fortalecerá la gestión de seguridad conforme a los más altos estándares internacionales.

En ese orden de ideas, y con el propósito de garantizar la seguridad y el correcto funcionamiento de la infraestructura tecnológica que soporta las operaciones de la Superintendencia de Transporte, resulta indispensable contar con herramientas especializadas, como los antivirus. Estos se renuevan tanto para

los computadores como para los servidores de la entidad, y se gestionan para proteger las aplicaciones y sistemas operativos contra amenazas informáticas. La adquisición de licencias para productos y servicios como el antivirus es fundamental para minimizar riesgos, asegurar la continuidad operativa y contribuir al eficiente cumplimiento de las funciones misionales de la Oficina de Tecnologías de la Información y las Comunicaciones.

COMPONENTE No. 3 - SOLUCIÓN DE COPIAS DE RESPALDO

Para garantizar la disponibilidad de la información, es esencial fortalecer y mejorar la infraestructura tecnológica que la soporta. Por ello, es necesario renovar y adquirir licencias de productos y servicios del sistema de copias de respaldo de la información. Esto permitirá asegurar la operación tecnológica, garantizar la continuidad del cumplimiento de su misión y mitigar posibles fallas. Además, es indispensable contar con dispositivos de almacenamiento robustos que aseguren la integridad y confidencialidad de la información, ofreciendo las mejores características de desempeño, seguridad, redundancia, disponibilidad y eficiencia.

Si bien es cierto que la Supertransporte está asegurando la operación de la infraestructura tecnológica con la renovación y adquisición de licenciamiento de copias de respaldo, esta es tan solo una parte de toda la infraestructura actual, la cual protege las copias de respaldo de los sistemas de información tanto de los servidores de aplicaciones como los servidores de bases de datos de la entidad. En este orden de ideas, también se precisa que en el año 2022, bajo el contrato 331, se adelantó un proceso para la ampliación de este almacenamiento (hiperconvergencia), que permitió aumentar y generó la necesidad de respaldar nuevos sistemas de información.

La agrupación de los tres componentes en un mismo proceso de contratación responde a que las soluciones hacen parte de la protección de la información de la entidad, se encuentran a cargo de la misma dependencia (Oficina de Tecnologías de la Información y las Comunicaciones) y comparten la misma vigencia de licenciamiento y soporte de doce (12) meses, lo que permite una gestión, seguimiento y supervisión unificados del contrato.

Actualmente, la Entidad cuenta con plataformas de seguridad perimetral de la marca **FORTINET**, que soportan los mecanismos de protección y control de la infraestructura tecnológica, así como una solución de copias de seguridad (backup) de **VEEAM**, cuya operación se encuentra integrada con la infraestructura tecnológica de almacenamiento y procesamiento de las marcas **HUAWEI e IBM**.

En este contexto, la renovación, actualización, ampliación o adquisición de componentes de hardware, software, licenciamiento y servicios de soporte debe garantizar la compatibilidad e integración con las plataformas existentes, preservar las configuraciones, políticas de seguridad y esquemas de administración actualmente establecidos, así como mantener la continuidad de los servicios tecnológicos y la disponibilidad, integridad y confidencialidad de la información institucional.

La sustitución de estas tecnologías por soluciones de fabricantes diferentes podría implicar riesgos técnicos y operativos asociados a procesos de migración, integración y adaptación, tales como interrupciones en los servicios, pérdida o indisponibilidad de información, incompatibilidades tecnológicas, generación de nuevas vulnerabilidades de seguridad, afectación de los esquemas de respaldo y recuperación, así como costos adicionales de implementación, capacitación, administración y soporte.

La renovación con el mismo fabricante responde a criterios de continuidad operativa, compatibilidad tecnológica, eficiencia administrativa y protección de la inversión pública, toda vez que la sustitución de la solución actualmente implementada implicaría adelantar procesos de evaluación, adquisición, migración, configuración, parametrización y transferencia de conocimiento, generando posibles costos adicionales, reprocesos y riesgos de indisponibilidad o afectación de los servicios de respaldo y recuperación de información.

El presente proceso de contratación es fundamental para asegurar la continuidad de los servicios tecnológicos y optimizar el rendimiento de diversos componentes de la infraestructura tecnológica. Además, contribuye a garantizar la seguridad y confiabilidad de los sistemas de información, así como a maximizar la eficiencia y la productividad de la entidad.

La necesidad aquí descrita se encuentra contemplada dentro del Plan Anual de Adquisiciones de la Entidad para la presente vigencia y será ejecutada con recursos de funcionamiento. Dado que estos recursos están destinados a mejorar la infraestructura tecnológica de la entidad, su asignación a las soluciones de ciberseguridad y de copias de respaldo responde a la necesidad estratégica de garantizar la continuidad del servicio y la protección de la información como activo esencial.

En este contexto, resulta prioritario garantizar la continuidad operativa de las plataformas mediante la renovación y actualización del licenciamiento, las garantías y los servicios de soporte técnico asociados, así como la actualización de los componentes de hardware y software que lo requieran. Estas acciones permitirán fortalecer la protección frente a amenazas provenientes de la red, el software, el hardware, las aplicaciones y las actividades de los usuarios, reduciendo la exposición a vulnerabilidades y los riesgos derivados de la obsolescencia tecnológica, el vencimiento de licencias y la falta de soporte del fabricante.

2. ESPECIFICACIONES TÉCNICAS DEL BIEN O SERVICIO A CONTRATAR

2.1 COMPONENTE No. 1 – SOLUCION DE SEGURIDAD PERIMETRAL

<table>
<tr><th>No.</th><th>DESCRIPCIÓN</th><th>CANTIDAD</th></tr>
<tr><td>1</td><td>Sustitución tecnología del firewall Fortigate-501E, soporte y Garantía por mínimo 12 meses

El Upgrade y/o adquisición por obsolescencia de un (1) firewall de nueva generación (NGFW, que contenga como mínimo las capacidades técnicas descritas en el numeral

Dentro de la renovación o sustitución se debe obtener un equipo con las capacidades superiores al actual incluye migración, implementación, actualizaciones, mantenimientos correctivos ante fallas daños de los equipos, servicios profesionales para configuraciones y endurecimiento de seguridad cuando sea requerido por la entidad.

Requerimiento mínimo con licenciamiento.

<table>
<tr><th>Categoría</th><th>Especificación</th><th>Requerido</th></tr>
<tr><td>Interfaces y Módulos</td><td>Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ Slots</td><td>4</td></tr>
</table>
</td><td>1</td></tr>
</table>

			Hardware Accelerated 10 GE SFP+ / GE SFP Slots	4	
			Hardware Accelerated GE SFP Slots	16	
			Hardware Accelerated GE RJ45 Slots	8	
			2.5 GE / GE HA Port	1	
			USB Ports	2	
			RJ45 Console Port	1	
			Included Transceivers	2x SFP SX	
		Rendimiento- Enterprise Traffic Mix	IPS Throughput	38 Gbps	
			NGFW Rendimiento- Throughput	29 Gbps	
			Threat Protection Throughput	26 Gbps	
		Rendimiento y Capacidad del Sistema	IPv4 Firewall Throughput(1518 / 512 / 64 Gbps byte, UDP)	164 / 163 / 145	
			IPv6 Firewall Throughput (1518 / 512 / 86 Gbps byte, UDP)	164 / 163 / 145	
			Firewall Latency (64 byte, UDP)	3.87	
			Firewall Throughput (Packet per Rendimient Second)	217.5 Mpps	
			Concurrent Sessions (TCP)	28 Million	
			New Sessions/Second (TCP)	700000	
			Firewall Policies	30000	
			IPsec VPN Throughput (512 byte)	55 Gbps	
			Concurrent SSL- VPN Users (Recommended Maximum, Tunnel Mode)	10000	
2	**Renovación soporte y Garantía x 12 meses FortiAnalyzer- 300G** Serial FAZ3HGTA25000031 (Coterm End Date:2026-03-17) Dentro del soporte incluye actualizaciones, templates reportes, mantenimientos correctivos ante fallas daños de los equipos y servicios profesionales de configuraciones cuando sea requerido y reemplazo de equipos si fuera necesario, debe incluirse la licencia de indicadores de compromiso y automatización.				**1**
3	**Renovación soporte y Garantía x 12 meses del fortiweb VM04** Serial FWBVMSTM25000368 (Coterm End Date:2026- 03-17) Dentro de la renovación debe incluir migración, implementación, actualizaciones, mantenimientos correctivos ante fallas y servicios profesionales de configuraciones cuando sea requerido para parametrizaciones.				**1**
4	**Renovación soporte y Garantía x 12 meses del FortiAuthenticator VM**				**1**

	Serial FAC-VMTM25001799 (Coterm End Date:2026-03-16) Dentro de la renovación debe incluir actualizaciones, mantenimientos correctivos ante fallas y servicios profesionales de configuraciones cuando sea requerido.	
5	**Especificaciones de la renovación de las soluciones Fortinet** ✓ La vigencia de la renovación será de un (1) año, contado a partir de la fecha de vencimiento del licenciamiento actual de cada solución, de forma que no existan periodos sin cobertura. ✓ La renovación debe quedar registrada a nombre de la Superintendencia de Transporte en el portal de soporte del fabricante, asociada a cada número de serie. ✓ El oferente deberá estar en alguno el los dos más altos niveles de membresía para garantizar que cuenta con la capacidad de ingeniería para este proyecto para lo cual deberá entregar una carta del fabricante certificando esta capacidad, deberá tener una vigencia no mayor a 30 días y deberá estar dirigida a la entidad. ✓ Durante la vigencia de la renovación, la entidad debe contar con acceso al soporte técnico del fabricante y a las actualizaciones de software liberadas por este para cada solución	

2.2 COMPONENTE No. 2 - SOLUCION DE ANTIVIRUS.

No.	DESCRIPCIÓN	CANTIDAD
1	**Suscripción de licenciamiento para protección de estaciones de trabajo (Endpoint Protection).** La suscripción de la licencia para un total de **591 equipos de cómputo** asignados a funcionarios y contratistas, asegurando la protección de los endpoint contra amenazas informáticas y ataques dirigidos, así como la administración centralizada mediante una consola unificada. La solución deberá incluir servicio de actualización automática para los clientes y gestión manual y/o programada desde la consola de administración; actualización a la última versión estable del software antivirus, bibliotecas de definiciones, mejoras y correcciones sin costo adicional; actualización centralizada de firmas, motores de búsqueda, parches y actualizaciones extraordinarias; generación de reportes de amenazas y acciones ejecutadas; actualización automática de políticas de prevención, vacunas y patrones de seguridad; servicio proactivo para la implementación de políticas de prevención ante nuevas amenazas; capacidad de cifrado de información confidencial; compatibilidad con sistemas operativos Windows, Windows Server y distribuciones Linux soportadas por el fabricante; prevención de malware basada en Machine Learning e Inteligencia Artificial para la detección y bloqueo de amenazas conocidas, desconocidas y ataques de día cero (Zero-Day); protección avanzada en tiempo real pos-ejecución para la detección de ransomware, actividades sospechosas, cifrado no autorizado de archivos y otros comportamientos maliciosos mediante análisis de comportamiento.	591
2	**Suscripción de licenciamiento para protección de servidores.** La suscripción de **70 licencias de antivirus para servidores físicos y virtuales**	70

	alojados en el Datacenter principal de la Entidad, incluyendo ambientes híbridos y servicios en nube pública, garantizando visibilidad, control, prevención de exploits, bloqueo de ataques de red, protección antimalware, capacidades de detección avanzada mediante Machine Learning e Inteligencia Artificial, protección contra ransomware y monitoreo centralizado sin afectación al rendimiento de los sistemas.	
3	**Consola de administración y monitoreo centralizado.** La solución deberá incluir una consola de administración que constituya el único punto de administración y control de todos los componentes de seguridad implementados. La consola deberá permitir la administración centralizada de licencias, equipos, grupos, usuarios y políticas de seguridad; despliegue e instalación remota de agentes; actualización remota de componentes; escaneos programados y bajo demanda; generación de reportes; monitoreo en tiempo real; notificaciones automáticas; correlación y visualización de eventos; gestión de incidencias; seguimiento de amenazas detectadas mediante Machine Learning e Inteligencia Artificial; monitoreo de eventos de ransomware, indicadores de compromiso (IoC), ataques de día cero y actividades sospechosas; implementación centralizada de políticas de seguridad, bloqueo de puertos, carpetas compartidas y dispositivos; comunicación bidireccional por eventos entre agentes y consola; visualización del estado de protección de estaciones y servidores; auditoría de acciones administrativas; y control centralizado de actualizaciones de toda la solución.	1
4	**Integración con la infraestructura de seguridad de la Entidad.** El agente de endpoint y la consola de administración deberán integrarse de forma nativa o por API con el firewall perimetral de la Entidad, compartiendo telemetría de los equipos como usuario, dirección MAC, sistema operativo, versión del agente y vulnerabilidades detectadas. La solución deberá permitir la agrupación dinámica de activos bajo esquemas de confianza cero (Zero Trust), el envío de registros y eventos de host hacia la plataforma de registro y análisis centralizado de eventos de seguridad de la Entidad, así como la ejecución de acciones de respuesta automatizada, incluyendo cuarentena o aislamiento de equipos comprometidos ante la detección de indicadores de compromiso (IoC).	1
5	**Soporte técnico especializado y acompañamiento.** La provisión de soporte técnico y afinamiento de la solución, incluyendo como mínimo una visita técnica mensual para revisión de la operación, actualización de licencias, administración de la solución, ajustes de configuración, optimización de políticas de seguridad y acompañamiento especializado en sitio o remoto cuando sea requerido, garantizando el correcto funcionamiento de la plataforma durante toda la vigencia contractual.	1
6	**Actualizaciones, mantenimiento y protección continua**. La inclusión de todas las actualizaciones, mejoras, nuevas versiones, bibliotecas de firmas, así como motores de análisis, patrones de malware, políticas de prevención, vacunas, parches de seguridad o componentes similares, necesarios para mantener la vigencia tecnológica, efectividad y robustez de la solución frente a amenazas emergentes durante un período de doce (12) meses, sin costos adicionales para la Entidad.	1
7	**Licenciamiento, documentación y certificaciones.** Aplicación de las licencias antivirus, realización de las actualizaciones y revisiones respectivas, y entrega del documento físico o digital donde conste el derecho de uso de las licencias. El proveedor deberá entregar ficha técnica, manuales de operación y mantenimiento, documentación de la solución y procedimientos de disposición final. El oferente deberá acreditar el más alto nivel de membresía o partnership otorgado por el	1

	fabricante mediante certificación vigente expedida con una antelación no mayor a treinta (30) días y dirigida a la Entidad. Debe contar con certificación ISO 27001 vigente o su equivalente, en concordancia con los requisitos de seguridad de la información de la Entidad. (Dicho requisito debe presentarse al momento de firmar el acta de inicio)	

2.3 SOLUCION DE COPIAS DE SEGURIDAD "BACKUP".

No.	DESCRIPCIÓN	CANTIDAD
1	Renovación de soporte de fábrica de las Licencias Veeam Availability Suite Enterprise Plus (includes Backup & Replication Enterprise Plus + Veeam ONE) con numero de parte P-VASPLS-VS-PP000- 00 BASIC SUPPORT-ID:#02299979 a un (1) año, para 120 instancias, y actualizaciones de versionamiento de la herramienta veeam backup.	1
2	Prestación de soporte técnico y reemplazo de partes físicas para el equipo de Unidad de cintas - 3 drives - MARCA: IBM -REFERENCIA: TS4300 Tape Library con 3 drives LTO8 SERIAL N°: 78014ZC.	1
3	Prestación de soporte técnico y reemplazo de partes físicas para el equipo Appliance de discos duros -MARCA: HUAWEI REFERENCIA: 2288H V5 SERIAL N°: 2102311XBJ10J8000081 Por periodo de 1 año.	1
4	Adquisición o espacio de nube con capacidad de 30 teras con las siguientes características: Espacio en nube con protección LRS (Local Redundancy Storage). - Aprovisionamiento y configuración de Jobs de sincronización. - Opción de restauración y copias en medio físico. - La comunicación debe ofrecer de cifrado. - Conexion VPN Site-to-Site o similares. - Configuración copias mensuales. - Sin costos adicionales por descarga o egreso. - Almacenamiento para ser usado como copia secundaria. - Opción de inmutabilidad. - Opción de protocolo S3, ReFS o XFS. Compatible con Veeam – versión actual que tiene la entidad	1
5	La entrega del almacenamiento en nube, la activación de la renovación del licenciamiento Veeam Backup y el soporte de los equipos físicos de la solución de backups, junto con la entrega del documento físico o digital donde conste el derecho de uso de estos, previendo que la entidad no quede desamparada en los licenciamientos	1

Nota 1: Las licencias de Veeam, adquisición de espacio en nube y soporte para los equipos IBM y HUAWEI tienen una duración de doce (12) meses, durante los cuales se recibirá soporte y actualizaciones.

2.4 SOPORTE Y MANTENIMIENTO (aplica para los componentes 1, 2 y 3)

No.	SERVICIO
2.4.1.	Se requiere soporte especializado por un (1) año, a partir de la fecha de acta de inicio

	del contrato. - La atención de incidentes debe realizarse un máximo de 4 horas en un esquema 7*24*365 - En caso de requerir cambio de partes del contratista debe garantizar el reemplazo en un máximo de 24 horas una vez identificada la falla. - El servicio de soporte debe incluir atención de incidentes sobre la plataforma ofertada. - Consultas a través de llamadas telefónicas, correo electrónico. Sesiones remotas y atención en sitio (En caso de requerirse) en horario Hábil y No Hábil.
2.4.2.	**Mantenimiento Preventivo:** El proveedor deberá realizar Dos (2) visitas de soporte preventivo especializado en sitio durante el plazo del contrato, el cual será prestado por personal certificado en la marca y/o productos que componen la infraestructura de seguridad y de redes de la Entidad, dentro de las cuales y cuando haya lugar a soporte especializado remoto (si así se amerita y se solicita por la Entidad). El proveedor deberá tener en cuenta que se le podrá requerir: a. Reinstalación de algún componente de la infraestructura de seguridad y de redes de la Entidad, cuando por alguna razón no pueda ser realizados por el equipo técnico de la entidad. b. Atención de eventos de seguridad informática en donde se involucren los componentes de la solución. c. Los demás que sean solicitados por la entidad y que estén asociados con la solución de seguridad y de redes de la Entidad. d. Tareas de limpieza externa e interna de las plataformas de la solución Si el servicio de mantenimiento preventivo requiere cambio de plataformas que afecten la prestación del servicio, el tiempo de respuesta no debe superar las 48 horas después del diagnóstico.
2.4.3.	**Mantenimiento Correctivo:** Se realizará esta labor en el sitio y/o remoto, para los problemas de la soluciones ofertadas. El mantenimiento correctivo consiste en reparar aquello que se encuentre averiado, se realiza luego que ocurra una falla o avería en las plataformas que por su naturaleza no pueden planificarse en el tiempo o que bien se hayan identificado a través del mantenimiento preventivo. En la realización de estos mantenimientos, el proveedor deberá: a. Realizarlos cuantas veces la Entidad lo requiera en modalidad de (7x24x365), con un tiempo de respuesta no mayor a cuatro (4) horas, y deberá prestarse en las instalaciones en donde se encuentren instalados las plataformas que conforman la solución de seguridad informática perimetral. b. En caso de que el Firewall ofertado presente un daño que no pueda ser solucionado y que ocasione inactividad por más de cuatro (4) horas, el proveedor deberá realizar el proceso de RMA de la plataforma afectada, y deberá emitir un concepto técnico a más tardar el día hábil siguiente al reemplazo de la plataforma que justifique la salida de operación de esta.

2.5 TRANSFERENCIA DE CONOCIMIENTO

El Contratista deberá realizar la transferencia de conocimiento con una duración mínima de ocho (8) horas para mínimo tres (3) ingenieros designados por la Entidad, por cada uno de los componentes ofertados.

La capacitación deberá incluir todos los aspectos relacionados con la operación, administración, configuración, monitoreo, mantenimiento y solución de incidentes de la plataforma, así como los procedimientos necesarios para actuar en caso de contingencia o falla de la solución.

Como evidencia de su ejecución, el Contratista deberá expedir y entregar a la Entidad los certificados o constancias de participación, aprobación o asistencia, según corresponda, para cada uno de los asistentes designados, indicando como mínimo el nombre del participante, la intensidad horaria, las temáticas impartidas y la fecha de realización de la transferencia de conocimiento.

2.6 CONDICIONES DE GARANTÍA Y LICENCIAMIENTO

La garantía de los dispositivos y el licenciamiento será de un (1) año a partir de su activación el cual será expedido por el fabricante.

2.7 CUMPLIMIENTO TÉCNICO

El proponente cumplirá con las condiciones establecidas en las ESPECIFICACIONES TÉCNICAS, Especificaciones Técnicas Mínimas – Ficha técnica del proceso.

NOTA: Para que el proponente se entienda que cumple las especificaciones técnicas debe diligenciar la totalidad de los ítems.

3. INFORMACIÓN PRESUPUESTAL

La Superintendencia de Transporte fija como presupuesto oficial del presente proceso de selección, hasta la suma de **SETECIENTOS MILLONES SETECIENTOS NUEVE MIL DOSCIENTOS OCHENTA Y TRES PESOS M/CTE ($700.709.283)** incluido IVA y demás impuestos, tasas y contribuciones, costos directos e indirectos a que haya lugar, distribuido, así:

Componente	Descripción	Presupuesto por componente
1	SOLUCIÓN DE SEGURIDAD PERIMETRAL	$317.045.440
2	SOLUCIÓN DE ANTIVIRUS	$135.991.282
3	SOLUCIÓN DE COPIAS DE RESPALDO	$247.672.561

Nota: La oferta será rechazada cuando su valor total supere el presupuesto oficial establecido para el proceso. Superar el presupuesto estimado para uno o varios componentes no constituirá causal de rechazo, siempre que el valor total de la oferta no exceda dicho presupuesto.

Nota 2: La adjudicación del proceso, de los tres componentes, se realizará a un mismo proponente.

4. PLAZO

El plazo de ejecución del contrato es hasta el 31 de diciembre de 2026, previa expedición del registro presupuestal y aprobación de las garantías.

5. LUGAR DE EJECUCIÓN

La entrega de los bienes objeto del contrato se realizará en la sede de la entidad, ubicada en la ciudad de Bogotá (BURO Diagonal 25 G # 95 A - 85), sin perjuicio de que la Entidad pueda realizar cambios de domicilio en la ciudad de Bogotá D.C

6. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

OBLIGACIONES COMUNES A TODOS LOS COMPONENTES

1. Firmar el Acta de Inicio como requisito para la ejecución del contrato.
2. Cumplir con todos los ofrecimientos, condiciones y términos de la propuesta que hace parte integral del contrato, al igual que con todas las especificaciones técnicas mínimas exigidas en el ANEXO ESPECIFICACIONES TÉCNICAS MÍNIMAS, en los pliegos de condiciones, estudios previos y demás documentos que hagan parte del contrato.
3. Ajustar la oferta económica, con la totalidad de ítems presentados, conforme al valor final adjudicado, el cual resulte de la subasta inversa realizada.
4. Cumplir con el cronograma presentado al supervisor del contrato para la entrega, instalación y puesta en funcionamiento del licenciamiento adquirido.
5. Realizar la transferencia de conocimiento en la operación de los productos adquiridos e instalados a los funcionarios y/o contratistas que el supervisor establezca, de la cual se dejará un registro de asistencia, según lo dispuesto por la supervisión contractual, en los plazos dispuestos para ello y conforme a las especificaciones técnicas señaladas para el proceso de selección.
6. Cumplir, durante la ejecución del contrato, con toda la información y obligaciones relacionadas con las condiciones de posventa. Dichas condiciones deberán comprender, como mínimo, la prestación de los servicios de mantenimiento, la asistencia ante fallos cubiertos por garantía, incluyendo los tiempos de respuesta comprometidos.
7. Mantener durante la ejecución del contrato las condiciones presentadas en la propuesta, en forma permanente y con altos niveles de eficiencia técnica y profesional, para atender sus obligaciones, respetando y cumpliendo las condiciones establecidas en el pliego de condiciones y en la oferta.
8. Acatar las directrices que durante el desarrollo del contrato le imparta la Superintendencia de Transporte, a través del supervisor del contrato.
9. Presentar la factura electrónica para el trámite de pago de conformidad con lo establecido en la normatividad vigente, dentro del término indicado.
10. Asumir por cuenta propia todos los costos y gastos que se generen en el cumplimiento del contrato.
11. Dar respuesta en el término que indique el supervisor sobre los requerimientos de información o documentación que efectúen órganos de control, autoridades judiciales o cualquier tercero.
12. Informar de manera inmediata al supervisor sobre las eventualidades que se presenten durante la entrega, instalación y demás servicios conexos del objeto contractual.

13. Responder por las demoras que se generen en la entrega, instalación y puesta en marcha.
14. Ampliar la cobertura de cumplimiento, hasta que esté formalmente liquidado el contrato, de conformidad con lo regulado en el Decreto 1082 de 2015.
15. Las demás que se deriven del objeto contractual y las que sean exigidas por el supervisor y que se encuentren relacionadas con el cumplimiento del objeto contractual

OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

COMPONENTE No. 1 – SOLUCION DE SEGURIDAD PERIMETRAL

1. Renovar por un (1) año el licenciamiento y soporte del fabricante de las soluciones FortiWeb (serial FWBVMSTM25000368), FortiAnalyzer (serial FAZ3HGTA25000031) y FortiAuthenticator (serial FAC-VMTM25001799), de conformidad con las especificaciones técnicas solicitadas por la Entidad.
2. Entregar el documento físico o digital expedido por el fabricante donde conste la renovación asociada a cada número de serie y tiempo de garantía.
3. Escalar al fabricante los casos de soporte que lo requieran y hacer seguimiento hasta su solución, durante la vigencia de la renovación.
4. Suministrar un (1) firewall de nueva generación (NGFW) nuevo, que cumpla como mínimo las especificaciones técnicas descritas en el documento de ficha técnica.
5. Presentar al supervisor del contrato, el día de la firma del acta de inicio, un cronograma de actividades en formato Excel o PDF para la implementación y configuración y puesta en funcionamiento del Firewall de nueva generación.
6. Entregar la hoja de datos oficial del fabricante del equipo ofertado, que acredite el cumplimiento de las capacidades técnicas exigidas.
7. Realizar la entrega, instalación y puesta en funcionamiento del equipo en la sede principal de la entidad, conforme al cronograma aprobado por el supervisor del contrato.

COMPONENTE No. 2 – SOLUCION DE ANTIVIRUS

1. Suministrar el licenciamiento de productos y servicios del antivirus por un lapso de un (1) año contado a partir de la fecha de vencimiento de las licencias ya adquiridas por la entidad, para su suscripción, de conformidad con las especificaciones técnicas solicitadas por la Entidad.
2. Actualizar a la última versión estable el software antivirus, tanto para estaciones de trabajo como servidores y consolas de administración (biblioteca de definiciones).
3. Brindar asistencia remota del licenciamiento por parte del fabricante por un periodo de un (1) año en un esquema de 5x8x12, incluyendo mejoras del producto y correcciones durante el tiempo de vigencia del licenciamiento.
4. Cumplir las obligaciones relacionadas con el personal acreditado por el fabricante de las soluciones tecnológicas objeto del contrato y asignado para su ejecución, garantizando que cuente con la idoneidad, experiencia, formación y certificaciones técnicas.
5. Suministrar con el Acta de entrega los documentos que constituyen el dossier de entrega descritos en la FICHA TÉCNICA.
6. Entregar el documento físico o digital donde conste el derecho de uso de las licencias.

Adicionalmente, el proveedor debe incluir la siguiente información: ficha técnica, operación y mantenimiento y disposición final de los sistemas, con sujeción al procedimiento dispuesto por la Entidad.

7. Garantizar, como mínimo, la calidad e idoneidad del servicio por el término de vigencia del licenciamiento.

COMPONENTE No. 3 – SOLUCION DE COPIAS DE SEGURIDAD "BACKUP".

1. Renovar el licenciamiento, adquirir el almacenamiento en nube para la Solución de Copias de Seguridad – Backups y el soporte por un (1) año a partir del perfeccionamiento del contrato para los equipos físicos que componen la solución de backups, incluido el reemplazo de partes físicas, de conformidad con las especificaciones técnicas solicitadas por la Entidad.
2. Actualizar el firmware de los dispositivos a la última versión al momento de la entrega.
3. Brindar asistencia del licenciamiento por parte del fabricante y/o oferentes para el cambio de repuestos por un periodo de un (1) año en un esquema de 7 x 24 con portal de soporte y recursos técnicos asociados dentro del tiempo de ejecución del contrato. Para el caso puntual del fabricante IBM, se acepta la solicitud de que el servicio de soporte se preste a través de un tercero autorizado, siempre y cuando se cumpla con los mismos niveles de atención del servicio para la actualización del producto o hasta que la entidad realice el cambio del hardware por obsolescencia tecnológica o cambio de tecnología. El servicio de soporte de terceros debe garantizar la disponibilidad de los repuestos que requieran los dispositivos físicos.
4. Prestación de soporte técnico y reemplazo de partes físicas para el equipo Appliance de discos duros -MARCA: HUAWEI REFERENCIA: 2288H V5 por un periodo de un (1) año en un esquema de 7 x 24 con portal de soporte y recursos técnicos asociados dentro del tiempo de ejecución del contrato.
5. Entregar las certificaciones y catálogos requeridos por la entidad.
    a. Certificado de soporte técnico y reemplazo de partes físicas para el equipo Appliance de discos duros - MARCA: HUAWEI por un año.
    b. Certificado de soporte técnico y reemplazo de partes físicas para Unidad de cintas - 3 drives - MARCA: IBM por un año.
    c. Certificado de adquisición de espacio de nube privada con capacidad de 30 TB por un año
6. Entregar una carta formal en la que se detallen los Acuerdos de Nivel de Servicio (ANS), así como el cronograma de mantenimiento preventivo los primeros 5 dias hábiles a partir de la firma del acta de inicio, los cuales serán de obligatorio cumplimiento contractual.
7. Realizar tres (3) visitas durante el periodo de ejecución del contrato, garantizando el perfecto funcionamiento de la solución.
8. Mantener vigente la certificación de distribuidor y/o canal autorizado para veeam en el nivel ofrecido con la presentación de la oferta, o en uno superior.
9. Disponer del personal técnico idóneo necesario para realizar las actividades de actualización, configuración, optimización, integración, validación, soporte y transferencia de conocimiento de la solución Veeam Backup & Replication, para la ejecución de estas actividades.

7. DOCUMENTOS TÉCNICOS ADICIONALES

COMPONENTE No. 1: SOLUCION DE SEGURIDAD PERIMETRAL

El oferente deberá estar en alguno de los dos más altos niveles de membresía de los componentes ofertados, para garantizar que cuenta con la capacidad de ingeniería para este proyecto para lo cual deberá entregar una carta del fabricante certificando esta capacidad, deberá tener una vigencia no mayor a 30 días y deberá estar dirigida a la entidad.

COMPONENTE No. 2: SOLUCION DE ANTIVIRUS.

El oferente deberá estar en alguno de los dos más altos niveles de membrecía de los componentes ofertados, para garantizar que cuenta con la capacidad de ingeniería para este proyecto para lo cual deberá entregar una carta del fabricante certificando esta capacidad, deberá tener una vigencia no mayor a 30 días y deberá estar dirigida a la entidad.

COMPONENTE No. 3: SOLUCION COPIAS DE SEGURIDAD "BACKUP".

- ✓ Certificación como partner o distribuidor autorizado del fabricante – emitido por el fabricante no mayor a 30 días.
- ✓ Certificado del fabricante Veeam Backup de la renovación del licenciamiento actual por un año.

CERTIFICACIÓN PARA LA GARANTÍA TÉCNICA - EMITIDO POR EL FABRICANTE.

El proponente junto con su oferta deberá presentar certificación o acreditación dirigida a la Supertransporte, cuya fecha de expedición no podrá ser superior a treinta (30) días calendario anteriores a la fecha de cierre del proceso, expedida por parte el fabricante de cada una de las soluciones ofertadas, donde conste la garantía, soporte y adquisición de los ítems propuestos en la ficha técnica.

8. DEPENDENCIA SOLICITANTE

FIRMA DEL JEFE DE LA DEPENDENCIA SOLICITANTE	
NOMBRE COMPLETO DEL JEFE DE LA DEPENDENCIA SOLICITANTE	RAFAEL ENRIQUE NIEBLES FUENMAYOR
CARGO Y DEPENDENCIA	JEFE DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES (E)
NOMBRE COMPLETO ENLACE RESPONSABLE DE LA ADQUISICIÓN, DEL ÁREA TÉCNICA – ENLACE CONTRACTUAL	RUBEN ESTEBAN BUITRAGO (OTIC) PROFESIONAL ESPECIALIZADO

Proyectó: Erick Dovales
Aprobó: Rafael Enrique Niebles Fuenmayor