FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y/O SERVICIOS

FECHA	Día	Mes	Año
	06	05	2026

Línea PAA	1768

1. DEPENDENCIA SOLICITANTE

Oficina de Transformación Digital y Tecnologías de la Información

2. DESCRIPCIÓN DE LA NECESIDAD

El INSTITUTO DISTRITAL DE RECREACIÓN Y DEPORTE – IDRD es una entidad descentralizada del orden distrital, creada por el Acuerdo 4 de 1978 como un establecimiento público con personería jurídica, autonomía administrativa y patrimonio independiente adscrita a la Secretaria de Cultura, Recreación y Deporte del Distrito Capital y perteneciente al Sistema Nacional del Deporte, cuya misión es la de: "*Generar y fomentar espacios para la recreación, el deporte, la actividad física y la sostenibilidad de los parques y escenarios, mejorando la calidad de vida, el sentido de pertenencia y la felicidad de los habitantes de Bogotá D.C."*

El artículo 2 del Acuerdo 4 de 1978 precisa entre otras funciones del IDRD: "*1. Formular políticas para el desarrollo masivo del deporte y la recreación en el Distrito Especial, con el fin de contribuir al mejoramiento físico y mental de sus habitantes especialmente de la juventud. 2. Coordinar con otras entidades oficiales o privadas, dedicadas a estas materias, el planeamiento y ejecución de sus programas. (…) 4. Promover las actividades de recreación en los parques de propiedad distrital" y "8. En general, celebrar toda clase de negocios jurídicos, de administración, disposición, gravamen o compromiso de sus bienes o rentas, dentro de la órbita de sus funciones".(…)"*

Para el cumplimiento de las referidas funciones, la Resolución 006 de 2017 "*Por la cual se modifica la estructura organizacional y las funciones de las dependencias del Instituto Distrital de Recreación y Deporte y se dictan otras disposiciones*", modificada por las Resoluciones 007 de 2022, 002 de 2023 y 014 de 2025, prevé como parte de la estructura organizacional del IDRD, la incorporación de la Oficina de Transformación Digital y Tecnologías de la Información, estableciendo además las funciones para cada subdirección, a fin de lograr los objetivos institucionales esperados.

Dicha oficina tiene, entre otras, las siguientes funciones: (i) dirigir los procesos tecnológicos del IDRD conforme a los estándares, lineamientos y buenas prácticas impartidas por las entidades competentes; (ii) liderar el desarrollo, implementación, mantenimiento, interoperabilidad, integración y actualización de los sistemas de información y servicios digitales del Instituto, de acuerdo con la normatividad vigente; (iii) garantizar la disponibilidad de los servicios mediante la administración y soporte de la infraestructura tecnológica, incluyendo la plataforma de seguridad de TI, redes y comunicaciones de la entidad; (iv) dirigir, aprobar y liderar el diseño de políticas, lineamientos, planes y herramientas en materia de tecnologías de la información, así como realizar su respectivo seguimiento; (v) identificar las necesidades tecnológicas de la entidad y brindar acompañamiento y soporte técnico en los procesos de adquisición de bienes y servicios tecnológicos; (vi) dirigir y coordinar la integración de los sistemas de información del IDRD, garantizando su articulación con la arquitectura empresarial institucional; (vii) dirigir la política de provisión, implementación, mantenimiento y monitoreo de los sistemas y servicios de información y de los procesos de automatización requeridos por la entidad; y (viii) impartir lineamientos para

el cumplimiento de estándares de seguridad y ciberseguridad, privacidad, calidad, oportunidad de la información e interoperabilidad de los sistemas y aplicativos del IDRD.

En este marco, la Oficina de Transformación Digital y Tecnologías de la Información es responsable de la gestión y dirección de los procesos tecnológicos, así como de la administración y soporte de la infraestructura y los sistemas institucionales que garantizan la continuidad de los procesos administrativos, financieros y misionales del Instituto. Para ello, ejecuta acciones de actualización, mantenimiento, migración e integración de los sistemas de información y la infraestructura tecnológica.

Aunado a lo expuesto y de conformidad con lo previsto en el artículo 5 de la Resolución 014 de 2025 la Subdirección Administrativa y Financiera, tiene entre otras funciones, la de: "*Formular, ejecutar y controlar los planes, programas y proyectos de inversión a cargo de la Subdirección (núm. 2), Planificar, organizar, coordinar y ejecutar los programas de desarrollo institucional y proponer estrategias orientadas al mejoramiento continuo en la prestación de los servicios institucionales (núm. 3) y Administrar el desarrollo de las actividades que desde la dependencia sean requeridas para la implementación, mantenimiento y mejora continua del Sistema Integrado de Gestión (núm. 20)",* por tal motivo se contempla la necesidad de contar con los recursos tecnológicos necesarios para apoyar las gestiones administrativas de la entidad, aunando esfuerzos por su implementación, mejoramiento y sostenimiento, en términos de calidad y satisfacción social en la prestación de los servicios a la ciudadanía, realizando para el efecto un trabajo coordinado con las diferentes dependencias, que permita articular sus necesidades y aportes para incrementar la eficiencia.

En tal sentido y con el propósito de lograr el referido objetivo, la Subdirección Administrativa y Financiera tiene a su cargo el proyecto de funcionamiento que, en coherencia con el Plan Anual de Adquisiciones, permite la operación y sostenibilidad tecnológica institucional, incluyendo el suministro, servicios, administración, soporte de los servicios TIC y seguridad digital como elementos transversales para el desarrollo de los procesos misionales y administrativos de la Entidad.

En linea con lo anterior, y teniendo en cuenta que, en informática, un cortafuegos (del término original en inglés firewall) es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. 1. Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos y se utilizan con frecuencia para evitar que otros usuarios de Internet no autorizados tengan acceso a las redes privadas conectadas a Internet. Estos suelen actuar como un organismo de inspección que verifica las conexiones que se establecen entre una red y un equipo local. En síntesis, un cortafuego regula la comunicación entre ambos para proteger las redes internas contra programas maliciosos u otros peligros de Internet. 2. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

En esa medida, la Oficina de Transformación Digital y Tecnologías de la Información, debe proporcionar la infraestructura necesaria para el manejo de la seguridad a los servicios basados en tecnología que aseguren el correcto funcionamiento de estas infraestructuras tecnológicas. En cumplimiento de lo antedicho, el IDRD, ha implementado dentro del esquema de seguridad informática, soluciones de seguridad perimetral, con soluciones del fabricante PALO ALTO

NETWORKS, cuyo cubrimiento del licenciamiento y soporte vigente es hasta el 5 de agosto de 2026.

Es así como el Instituto cuenta conlos firewalls Palo Alto 460 y 410, los cuales se encuentran operando normalmente; el resultado del proceso de selección es contar con 1.) licenciamiento de la suscripción de seguridad de red (Prevención avanzada de amenazas, Filtrado avanzado de URL, Wildfire avanzado, Seguridad DNS avanzada y SD-WAN avanzada), 2.) Soporte premium, el cual ofrece soporte técnico a incidentes presentados en los firewalls, actualizaciones y parches y cubrimiento en cambio de partes físicas, incluso el cambio total ante cualquier falla presentada, realizando el cambio respectivo, solamente de los firewalls que se encuentran relacionados por el Institutoy 3.) licenciamiento de la herramienta de gestión y control, Panorama.

Es así como en la actualidad, el Instituto cuenta con los siguientes firewalls:

No.	Placa IDRD	Elemento	Firewall	Ubicación
1	51579	FIREWALL-SEDE PRINCIPAL	PA-460	CENTRO DE CABLEADO PRINCIPAL IDRD
2	51580	FIREWALL-SEDES EXTERNAS	PA-410	CENTRO DE CABLEADO PRD
3	51581	FIREWALL-SEDES EXTERNAS	PA-410	CENTRO DE CABLEADO UCAD
4	51582	FIREWALL-SEDES EXTERNAS	PA-410	CENTRO DE CABLEADO PRINCIPAL IDRD
5	51583	FIREWALL-SEDES EXTERNAS	PA-410	CENTRO DE CABLEADO PUENTE ARANDA

El firewall Palo Alto es el equipo central de seguridad de red, que controla la navegación en Internet, redirecciona todas las publicaciones y servicios del Instituto en Internet como por ejemplo el portal Contratistas, el Sistema de Gestión Documental ORFEO, El sistema de Calidad Isolucion, entre otros, permite la integración y seguridad con otras redes, debido a que controla el tráfico entre redes; así como el control del contenido y conexiones seguras por Internet.

En efecto, el Instituto cuenta actualmente con equipos de seguridad perimetral de la marca Palo Alto Networks, cuya operación depende de licencias, suscripciones, actualizaciones y soporte directamente asociados al fabricante, identificados mediante números de parte o referencias específicos. En este contexto, no es técnica ni funcionalmente viable sustituir dichos elementos por soluciones de otro fabricante sin incurrir en procesos de migración complejos, riesgos operativos, posibles afectaciones a la seguridad de la información y costos adicionales no previstos.

Así las cosas, la referencia a la marca y a los números de parte o referencias no obedece a una preferencia discrecional, sino a la necesidad de garantizar compatibilidad, continuidad del servicio, seguridad y correcto funcionamiento de una plataforma ya instalada, lo cual ha sido admitido por la normativa y la doctrina como una excepción válida al principio de neutralidad, siempre que esté debidamente justificada, como ocurre en este caso.

En consecuencia, la mención de la marca responde a un criterio técnico indispensable y verificable, orientado a proteger la operación de la Entidad y asegurar la eficiencia en el uso de los recursos públicos.

En consecuencia, la plataforma de seguridad Palo Alto, es de vital importancia para minimizar riesgos, por lo tanto las suscripciones del licenciamiento y soporte de los firewalls, aunado a los

resultados y estrategias planteadas para el fortalecimiento de la Seguridad informática y de la información determinada por la Oficina de Transformación Digital y Tecnologías de la Información, se concluye la necesidad en la renovación del soporte y licenciamiento de los firewalls que posee el Instituto, por el término de un (1) año, teniendo en cuenta las siguientes características:

1. Garantía de Seguridad Avanzada y Protección Continua

Los firewalls **Palo Alto PA-410** y **PA-460** son dispositivos de nueva generación (NGFW) diseñados para brindar seguridad integral, incluyendo funcionalidades como:

- Prevención de amenazas (Threat Prevention)
- Inspección profunda de paquetes (DPI)
- Prevención de intrusiones (IPS/IDS)
- Control de aplicaciones (App-ID)
- Filtrado de URL (URL Filtering)
- Antivirus y Anti-Spyware

Sin la renovación de los servicios de licenciamiento (como **Threat Prevention, WildFire, URL Filtering, DNS Security,** entre otros), estos dispositivos se limitan a funciones básicas, dejando expuesta la red a amenazas avanzadas y ataques desconocidos.

2. Acceso a Inteligencia en Tiempo Real (WildFire y DNS Security)

Servicios como **WildFire** permiten detectar malware de día cero mediante análisis en la nube, mientras que **DNS Security** protege contra dominios maliciosos, phishing y tunneling. La renovación asegura la protección proactiva frente a amenazas emergentes.

3. Soporte Técnico y Actualizaciones Críticas

Con el licenciamiento activo se mantiene:

- **Soporte técnico directo de Palo Alto Networks**, vital para la resolución de incidentes y configuraciones complejas.
- **Actualizaciones regulares** de firmas, reglas y software del sistema operativo **PAN-OS**, necesarias para mantener la compatibilidad, eficiencia y seguridad.

4. Cumplimiento Regulatorio y Buenas Prácticas de Seguridad

Organismos reguladores y marcos como **ISO 27001, PCI-DSS, NIST y GDPR** exigen mantener sistemas de protección actualizados contra amenazas. No renovar el licenciamiento podría representar un incumplimiento que derive en sanciones o vulnerabilidades graves.

5. Maximización de la Inversión en Infraestructura

Tanto el PA-410 como el PA-460 son dispositivos de alto rendimiento diseñados para proteger redes pequeñas y medianas con capacidades de NGFW. No renovar sus licencias representa una **subutilización de la inversión**, ya que gran parte de sus funcionalidades avanzadas quedarían inutilizadas.

6. Prevención de Riesgos Operativos y Financieros

El costo de renovación es predecible y presupuestable. En contraste, un ataque cibernético por falta de protección actualizada puede resultar en:

- Pérdida o robo de datos sensibles
- Interrupciones del servicio
- Costos legales y reputacionales

7. Soporte *Premium*: Descripción general del servicio

Este nivel de soporte brinda Garantía de Seguridad cuando se produzcan incidentes de seguridad y atención de soporte teniendo en cuenta el acceso a los siguientes servicios:

- Lanzamientos de funciones y actualizaciones de software.
- Actualizaciones de los servicios de suscripción (filtrado de URL, seguridad DNS, prevención de amenazas y el servicio WildFire).
- Garantía de seguridad. Análisis de cualquier actividad sospechosa
- Acceso directo con ingenieros expertos en productos y servicios de Palo Alto.
- Disponibilidad de soporte premium 24/7
- Servicio de RMA (*Return Merchandise Authorization*) en 4 horas para reemplazo de piezas y hardware.

8. Servicios de licenciamiento y soporte de la herramienta Panorama

Panorama es herramienta administrativa que hace parte del portafolio de servicios de seguridad de Palo Alto Networks, consolida la administración centralizada de los firewalls que posee actualmente el Instituto, obteniendo los siguientes beneficios:

- Control unificado de la seguridad.
- Reducción de riesgos y costos minimizando los tiempos de gestión por parte del equipo técnico que administra la plataforma.
- Mayor visibilidad para la toma de decisiones.
- Escalabilidad para el crecimiento del negocio.

De acuerdo con lo expuesto, se debe seguir contando con:

- Una herramienta de seguridad informática efectiva y dinámica, de direccionamiento y publicación de servicios, plataforma de interconexión de redes.

- Soporte técnico especializado para la solución de inconvenientes que se presenten con la plataforma o el equipo, amenazas, ataques o nuevas configuraciones que se requieran, mejoras o actualizaciones.

Por lo tanto, la renovación del licenciamiento y soporte de los firewalls PALO ALTO PA-410 y PA-460 y de la herramienta Panorama, es una necesidad crítica para garantizar la protección,

cumplimiento y estabilidad operativa de la red institucional de la Entidad, para evitar cualquier tipo de exposición innecesaria.

Es conveniente resaltar que los elementos descritos en la ficha técnica se les debe renovar el servicio de licenciamiento y soporte con una cobertura de un (01) año contado a partir de la fecha de activación, a fin de garantizar la continuidad del servicio de tal forma que no se vea afectada en su operación diaria en los servicios de red.

Adicionalmente en este ciclo anual de licenciamiento y soporte, de acuerdo con el estándar de la industria en la renovación de licenciamiento, entre otras ventajas da estabilidad a la operación del sistema, permite el cubrimiento de nuevas versiones y actualizaciones, con lo cual se garantiza la protección de datos y la seguridad de la información, sin ocasionar interrupciones o cambios abruptos.

3. OBJETO A CONTRATAR

Prestar los servicios de licenciamiento y soporte a la plataforma de seguridad de los firewall Palo Alto que posee el Instituto Distrital de Recreación y Deporte -IDRD-

4. CÓDIGO ESTÁNDAR DE PRODUCTOS Y SERVICIOS DE NACIONES UNIDAS (UNSPSC)

El servicio del presente Proceso de Contratación está codificado en el Clasificador de Bienes y Servicios de Naciones Unidas (UNSPSC) como se indica en la siguiente tabla:

Item	Clasificación UNSPSC					
	Código UNSPSC	**Segmento**	**Familia**	**Clase**	**Producto**	**Nombre**
1	**43222500**	43	22	25	00	Equipo de seguridad de red
2	**43231500**	43	23	15	00	Software funcional específico de la empresa
3	**43233200**	43	23	32	00	Software de seguridad y protección
4	**81111800**	81	11	18	00	Servicios de sistemas y administración de componentes de sistemas
5	**81112200**	81	11	22	00	Mantenimiento y soporte de software
6	**81112500**	81	11	25	00	Servicios de alquiler o arrendamiento de licencias de software de computador

5. NORMATIVIDAD APLICABLE

- **Constitución Política de Colombia**, artículos 2 y 209, que establecen los principios de la función administrativa y el deber de las entidades públicas de actuar con eficacia, economía, transparencia y responsabilidad.
- **Constitución Política de Colombia,** Artículo *61. El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la Ley*".
- **Ley 80 de 1993**, Estatuto General de Contratación de la Administración Pública, que regula los principios, modalidades y reglas generales de la contratación estatal.

- **Ley 1150 de 2007**, que introduce medidas para la eficiencia y transparencia en la contratación pública y desarrolla mecanismos de selección objetiva.
- **Decreto 1082 de 2015**, por medio del cual se reglamenta el Sistema de Compra Pública y se establece la obligación de elaborar estudios previos y análisis del sector como requisito para la estructuración de los procesos contractuales.
- **Ley 1474 de 2011**, Estatuto Anticorrupción, aplicable a las actuaciones contractuales de las entidades públicas.
- **Ley 2195 de 2022**, por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción, aplicable a los procesos de contratación estatal.
- **Ley 33 de 1987 (26 de octubre)** – "*Por medio de la cual se aprueba el 'Convenio de Berna para la protección de las obras literarias y artísticas', del 9 de septiembre de 1886, completado en París el 4 de mayo de 1896, revisado en Berlín el 13 de noviembre de 1908, completado en Berna el 20 de marzo de 1914 y revisado en Roma el 2 de junio de 1928, en Bruselas el 26 de junio de 1948, en Estocolmo el 14 de julio de 1967 y en París el 24 de julio de 1971.*"
- **Ley 565 del 2000** – "*Por medio de la cual se aprueba el "Tratado de la OMPI - Organización Mundial de la Propiedad Intelectual- sobre Derechos de Autor (WCT)", adoptado en Ginebra, el 20 de 1996*".
- **Decreto 1360 de 1989** - "*Por el cual se reglamenta la inscripción del soporte lógico (software en el Registro Nacional del Derecho de Autor)*"
- **La ley 44 de febrero 5 de 1993**, "*Por la cual se modifica y adiciona la ley 23 de 1982 y se modifica la ley 29 de 1944.*"
- **Ley 23 de 1982** - "*Sobre derechos de autor*"
- **Ley 603 de 2000** – "*Por la cual se modifica el artículo 47 de la Ley 222 de 1995*"
- **Concepto 17056** del 25 de agosto de 2017 – DIAN - Impuesto Sobre las Ventas.

6. DESCRIPCIÓN DEL BIEN Y/O SERVICIO, ESPECIFICACIONES TÉCNICAS Y DE CALIDAD

6.1 Elementos a efectuarles renovación

A continuación, se resume el inventario tecnológico sobre el cual el contratista deberá realizar la renovación del servicio de licenciamiento y soporte de los firewalls:

No.	Dispositivo / Núm. parte	Servicios	Serial	Ubicación	Cant.	Tiempo
1	PAN-PA-460-BND-PRECISIONAI-R	PA-460, Precision AI Network Security Subscription Renewal Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security, Advanced SD-WAN and Device Security), 1 years (12 months) term	23001005380	Sede Administrativa	1	1 año
2	PAN-SVC-BKLN-460-R	PA-460, Partner enabled premium support				
3	PAN-PA-410-BND-PRECISIONAI-R	PA-410, Precision AI Network Security Subscription Renewal Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, Advanced DNS Security, Advanced SD-WAN and Device Security), 1 years (12 months) term	23101004775 23101004885 23101004888 23101004923	Sede archivo central, Sede UCAD, Sede PRD y Administrativa	4	
4	PAN-SVC-BKLN-410-R	PA-410, Partner enabled premium support				
5	PAN-SVC-BKLN-PRA-25-R	Partner enabled premium support renewal (Panorama)	000702798488	Sede Administrativa	1	

6.2 Certificación requerida

El interesado deberá contar:

- Certificación vigente expedida no mayor a treinta (30) días calendario por el fabricante Palo Alto, donde conste que figura como mínimo en categoría Innovador o superior como socio o parther, lo cual lo hace idóneo para renovar el licenciamiento sobre los elementos de propiedad del Instituto, y además permite establecer que se encuentra en la capacidad de efectuar las implementaciones y reconfiguraciones de seguridad en la solución que posee la Entidad.
- El contratista deberá garantizar que el personal que preste los servicios de soporte cuenten con certificados de Palo Alto Networks, en PCNSE (Certified Network Security Engineer) y PCNSC (Certified Network Securiry Consultant).

7. OBLIGACIONES ESPECÍFICAS

1. Cumplir con todas las condiciones y especificaciones previstas en la ficha técnica y demás documentos que hacen parte integral del contrato, para lo cual, empleará todos sus recursos técnicos, económicos, físicos y logísticos, necesarios para garantizar el normal desarrollo del objeto contractual.
2. Activar la licencia de los firewalls Palo Alto dentro de los cuatro (04) días siguientes a la firma del acta de inicio, por el término de un año, contado a partir de la fecha de activación y de acuerdo con las cantidades y servicios requeridos en la ficha técnica, para tal efecto deberá entregar documentos donde se mencione la relación de las licencias correspondientes, indicando como mínimo: productos y servicios contratados, fecha de cobertura, cantidades, canales de atención, niveles de servicio, entre lo más relevante.
3. Garantizar la renovación del licenciamiento y del soporte con fabricante para los equipos de seguridad perimetral (firewalls) y para la plataforma de gestión centralizada Palo Alto Networks Panorama, asegurando la continuidad operativa de la solución actualmente instalada en la Entidad.
4. Cumplir con las funcionalidades del licenciamiento y soporte establecido por el fabricante en los equipos relacionados en la ficha técnica.

5. Realizar durante la vigencia de la cobertura del licenciamiento y soporte, el cambio de partes en caso de falla, sustituyendo el hardware que haya fallado o el elemento completo, al día hábil siguiente a la fecha del incidente reportado (8x5xNBD), como se encuentra establecido en las características descritas en la ficha técnica de acuerdo al Programa de servicios de atención al cliente adquirido.
6. Disponer de un medio de comunicación (correo electrónico, línea telefónica, chat o aplicación de mesa de ayuda entre otros) que permita al Instituto generar solicitudes de soporte y servicio (Incidentes o Requerimientos) relacionadas con el servicio contratado. Este medio de comunicación deberá estar disponible 7 días a la semana, las 24 horas del día como se describe en las características del soporte premium.
7. Garantizar la prestación del servicio Premium Support de Palo Alto Networks, el cual incluye soporte técnico especializado 24/7, atención de incidentes conforme a los niveles de severidad y tiempos de respuesta definidos por el fabricante, acceso a actualizaciones, parches de seguridad y portal de soporte, así como el acompañamiento técnico necesario para la resolución de fallas y la continuidad operativa de la plataforma de seguridad del Instituto.
8. Cumplir con las demás actividades que se requieran para el cumplimiento del objeto del contrato.

8. LUGAR DE EJECUCIÓN

Los servicios objeto de la presente contratación deberán ser prestados en la ciudad de Bogotá en las siguientes sedes o en el lugar en la cual se llegaren a trasladar las mismas.

- Sede Administrativa del IDRD ubicada en la Calle 63 No. 59A – 06.
- UCAD: Carrera. 60 No. 63c-21
- PRD: Avenida La Esmeralda # 63 – 63
- Archivo Central: Puente Aranda. Calle. 17 No 52-10

9. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de **DOCE (12) MESES** contados a partir de la suscripción del acta de inicio entre el supervisor y el contratista, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato.

PARÁGRAFO: La vigencia de la cobertura del licenciamiento y soporte requeridos por la entidad será por el término de un (01) año contado a partir de la fecha del vencimiento del licenciamiento actual.

10. FORMA DE PAGO

El valor del contrato será pagado por el INSTITUTO al contratista en un (1) solo pago correspondiente al 100% del valor del contrato, una vez se haya entregado y recibido a satisfacción donde conste la autorización de uso, vigencia y cantidad de licencias entregadas al Instituto de los Firewalls Palo Alto y certificado donde conste el cubrimiento de soporte premium de los firewall de la entidad por el término de un (01) año, con la entrega de los siguientes documentos, junto con la respectiva autorización del Supervisor del contrato:

a. Cuenta de Cobro y/o Factura y soportes.

b. Acta de recibo debidamente suscrita por el supervisor del contrato.
c. Acta de ingreso de los bienes al almacén (cuando aplique).
d. Copia de la planilla de pago de los aportes al régimen de seguridad social, correspondiente al periodo cobrado, en proporción al valor mensual del contrato, cuando se trate de personas naturales.
e. Certificación suscrita por el representante legal o revisor fiscal, que acredite el cumplimiento del pago de aportes al sistema de seguridad social integral de los últimos seis (6) meses, de conformidad con el artículo 50 de la Ley 789 de 2002 o aquella que lo modifique, adicione o sustituya cuando se trate de personas jurídicas.

Parágrafo 1. El contratista deberá acreditar el pago de los aportes parafiscales y su afiliación obligatoria y pago actualizado al sistema de seguridad social, salud y pensiones, conforme al artículo 182 de la ley 100 de 1993, Decreto Nacional 2353 de 2015, la Ley 789 de 2002, Ley 797 y 828 de 2003, Decreto 510 de 2003, Ley 1122 de 2007, Ley 1150 de 2007, Ley 1562 de 2012, Decreto 723 de 2013 y demás que las adicionen, reglamenten, complementen o modifiquen, so pena de hacerse acreedor a las sanciones establecidas en la mismas.

Parágrafo 2. El (los) pago (s) debe incluir los costos, gastos e impuestos a que haya lugar, así como la totalidad de los gastos directos e indirectos en que deba incurrir el contratista en relación con la suscripción, legalización y ejecución del contrato.

Parágrafo 3. En caso que el Contratista, esté obligado a facturar electrónicamente, debe presentar la factura electrónica o documento equivalente, según lo establecido en el artículo 616-1 del Estatuto Tributario, validada previamente por la DIAN, como requisito necesario para el pago, conforme con las disposiciones señaladas en el Decreto 358 de 2020, en concordancia con la Resolución 165 de 2023 modificada por la Resolución 119 de 2024 y demás normas que los modifiquen, complementen o sustituyan.

Parágrafo 4. El (los) pago (s) respectivo se hará con sujeción a la programación anual de caja PAC de conformidad con la Ley 80 de 1993, la Ley orgánica de presupuesto y sus decretos. Las sumas que la entidad contratante se obliga a pagar están sujetas a las apropiaciones presupuestales y a la situación de fondos del (PAC).

Parágrafo 5. De conformidad con lo dispuesto en la Ley 2024 de 2020, el Artículo 16 del Decreto Distrital 189 de 2020 y la Directiva 003 del 24 de febrero de 2021 de la Secretaría Jurídica Distrital, el plazo de pago por parte de la entidad debe ser máximo de treinta (30) días calendario luego de recibidos los bienes o servicios establecidos, siempre y cuando se cuente con el recibo a satisfacción del supervisor y se haya cumplido con los demás requisitos a cargo de contratista. En caso de que el IDRD requiera del contratista alguna aclaración, corrección o subsanación en la factura o documentos soporte, dicha solicitud interrumpirá el cómputo del plazo para pago, el cual se continuará calculando a partir del día siguiente en que el contratista realice los ajustes o subsanación requerida. En consecuencia, el tiempo que utilice el contratista para analizar y decidir sobre las observaciones formuladas por el IDRD, serán responsabilidad del CONTRATISTA y no tendrá por ello derecho a la causación o pago de interés moratorio alguno. o compensación de ninguna naturaleza.

Parágrafo 6. El pago se realizará a través de la cuenta (ahorros o corriente) que disponga el contratista, acorde con la certificación expedida por la entidad financiera.

Parágrafo 7. Para dar cumplimiento al derecho a turno, contemplado en el artículo 19 de la Ley 1150 de 2007, se deberá presentar toda la documentación necesaria para los pagos, a través de su radicación en la Sede Principal del IDRD ubicada en la Calle 63 No. 59a – 06 de la Ciudad de Bogotá D.C, o en el lugar donde llegaré a trasladarse la misma, previa comunicación al contratista.



JUAN CARLOS RODRÍGUEZ WALTERO
Subdirector Administrativo y Financiero

Revisó: Angela Riveros Sierra – Jefe Oficina de Transformación Digital y Tecnologías de la Información
Proyectó: Diego Alejandro Vargas – Técnico operativo Grado 07 - Oficina de Transformación Digital y Tecnologías de la Información