PRIMERA. - OBJETO: Adquirir para la solución de seguridad perimetral firewall el soporte, mantenimiento y garantía de fabrica con la actualización del software y de hardware de los equipos del Instituto Nacional de Salud.

SEGUNDA - VALOR: Para todos los efectos legales, presupuestales y fiscales pertinentes, el valor del presente contrato es por la suma **TRESCIENTOS NOVENTA Y TRES MILLONES QUINIENTOS CINCUENTA MIL PESOS M/CTE ($293.550.000)** incluido IVA, costos directos e indirectos, tasas, contribuciones y todos los impuestos en que incurra el contratista para la ejecución del contrato.

Ref. Artículo	Código UNSPSC	Descripción	Cantidad	Unidad	Precio unitario	Incluya el precio como lo indique la Entidad Estatal
1	43222500	PALO ALTO NUEVO	2,00	UN	88.084.125,00	176.168.250,00
2	43233200	SOLUCION SEGURIDAD EN LA NUBE	1,00	UN	88.084.125,00	88.084.125,00
3	81111800	SOPORTE	1,00	UN	29.297.625,00	29.297.625,00

TERCERA. - PLAZO Y LUGAR DE EJECUCIÓN: A) PLAZO DE EJECUCIÓN: Será a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato y hasta el 12 de diciembre de 2023. **B) LUGAR DE EJECUCIÓN**: El contrato se ejecutará en las instalaciones del contratista Avenida Calle 26 No. 51 – 20 en la ciudad de Bogotá D.C.

CUARTA. - OBLIGACIONES DEL CONTRATISTA:

A) Obligaciones Generales

1. Cumplir con el objeto, obligaciones y productos contractuales, de conformidad con lo establecido en los estudios, documentos previos y la oferta presentada dentro del proceso.
2. Constituir la garantía a favor del INSTITUTO en los términos establecidos en este documento y mantenerla vigente durante el término de ejecución del contrato y hasta la liquidación (cuando aplique), por los valores y con los amparos previstos en el mismo y presentarla dentro de los tres (3) días hábiles siguientes a la firma de contrato.
3. Estar al día con las obligaciones frente al Sistema de Seguridad Social Integral (salud, riesgos laborales, pensiones) y aportes parafiscales (Cajas de Compensación Familiar, ICBF y SENA) de conformidad con lo establecido en el artículo 50 de la Ley 789 de 2002, adicionado por el artículo 1 de la Ley 828 de 2003.
4. Presentar factura electrónica, conforme con las disposiciones señaladas en el Decreto 358 del 5 de marzo de 2020 y lo dispuesto en la Resolución No. 000042 del 5 de mayo de 2020, la misma debe contener cada uno de los ítems, con la cantidad, unidad de medida, descripción específica y valor que permitan la identificación de los bienes vendidos o servicios prestados de acuerdo con lo estipulado en el contrato.
5. Cargar la certificación de pago y/o factura con los soportes correspondientes en el SECOP II según periodicidad exigida en el contrato.
6. Cumplir con lo establecido en el POE-A01.2014-001 “Gestión de Seguridad y Salud en el trabajo”, especialmente lo dispuesto en el Anexo 1 sobre Normas y Requerimientos de Seguridad y Salud en el Trabajo para Contratistas, de acuerdo al objeto del contrato.
7. Cumplir con las disposiciones relacionadas con Gestión Ambiental, de conformidad con la normatividad vigente, comprometiéndose al uso racional de los recursos que utilice para el desarrollo del objeto contractual.
8. Cumplir con las políticas y lineamientos del Sistema de Gestión de la Seguridad de la Información del INSTITUTO.

9. Reportar de manera inmediata cualquier novedad o anomalía sobre la ejecución del contrato al Supervisor del mismo.
10. Respetar los derechos humanos en todas las actuaciones que realicen con ocasión de la ejecución del contrato
11. Responder ante terceros por los daños que se ocasionen y que provengan de causas que le sean imputables.
12. No acceder a peticiones o amenazas de quienes actúen por fuera de la ley con el fin de obligarlo a hacer u omitir algún acto o hecho. Cuando se presenten tales peticiones o amenazas, deberá informar inmediatamente de su ocurrencia al INSTITUTO y a las demás autoridades competentes para que ellas adopten las medidas y correctivos que fuesen necesarios
13. Atender los lineamientos que durante el desarrollo del contrato emita EL INSTITUTO.
14. Cumplir con las demás actividades que se deriven del objeto del contrato.

B) Obligaciones Específicas

1. Realizar los procesos técnicos necesarios para la puesta en funcionamiento de los equipos de seguridad perimetral en HA, evitando indisponibilidad en los servicios tecnológicos.
2. Entregar los equipos con todo el licenciamiento activo para su correcto funcionamiento y conforme a lo solicitado en las especificaciones técnicas.
3. Certificar previamente el personal que emplee para realizar la actualización de las licencias en los equipos.
4. Realizar el servicio de instalación y configuración en una ventana de mantenimiento previamente coordinada e informada por la Oficina de TIC del INS, en caso de que esta sea requerida, así como todas las actividades necesarias para la puesta en marcha de los equipos y servicios de seguridad.
5. Entregar en formato magnético e impreso dos (2) copias de la relación del licenciamiento de los dispositivos y servicios habilitados.
6. Entregar los bienes contratados conforme a las especificaciones técnicas exigidas por el Instituto.
7. Realizar el servicio y las actividades de soporte incluyendo atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil (7X24X365).
8. Ofrecer soporte y garantía por un (1) año para toda la solución adquirida, contados a partir de la puesta en funcionamiento en un horario 7X24x365.
9. Disponer de personal altamente capacitado para el desarrollo de las actividades.
10. Realizar transferencia de conocimiento de mínimo doce (12) horas para un grupo de máximo cinco (5) personas de la Oficina de TIC, en los procesos de administración de la solución onpremise y de nube adquirida
11. Informar de manera oportuna cada vez que el fabricante de la solución de seguridad libere actualizaciones de firmware durante el tiempo de ejecución del contrato, y brindar apoyo en caso de que sea requerido por la Oficina de TIC en los procesos de instalación.
12. Cumplir con las condiciones técnicas, jurídicas, económicas, financieras y comerciales presentadas en la propuesta.
13. Garantizar el oportuno cumplimiento y calidad del producto contratado y responder por este, de conformidad con lo dispuesto en el artículo 5 numeral 4 de la Ley 80 de 1993, independientemente de las garantías ofrecidas.
14. Las demás que se deriven de la naturaleza del contrato.

C. PRODUCTOS

1. Renovación y actualización de dos (2) equipos de seguridad perimetral firewall en la última versión publicada por el fabricante.
2. Documento que acredite el soporte y mantenimiento de los equipos de seguridad perimetral firewall por mínimo un (1) año
3. Documento que acredite el licenciamiento Threat Prevention (Prevención de amenazas), Url Filtering (software) Y Premium Support para el hardware adquirido por mínimo un (1) año.
4. Documento que acredite la suscripción de seguridad perimetral firewall para la nube con el fin de proteger servicios o aplicaciones que se pongan en operación sobre esta plataforma conforme a lo solicitado en las especificaciones técnicas por mínimo un (1) año.

D) ESPECIFICACIONES TÉCNICAS

Actualmente el Instituto Nacional de Salud cuenta con los siguientes dispositivos de seguridad perimetral – firewall en esquema de HA:

Equipo	Modelo	Serial
Palo Alto Principal	PA- 850	011901037912
Palo Alto Secundario	PA- 850	011901037998

Se requiere la renovación de hardware y software de los siguientes elementos que componen la solución seguridad perimetral – firewall:

DESCRIPCION	Cantidad
Solución Onpremise	
Firewall con licencias a 1 año:	**2**
Threat Prevention (software)	**2**
Url Filtering (software)	**2**
Premium Support	**2**
Solución nube	
Firewall con licencias:	**1**
Threat Prevention (software)	**1**
Url Filtering (software)	**1**
Wildfire (software)	**1**
Global Protect (software)	**1**
Instalación y Soporte	
Soporte 7x24x365 (1 año)	**1**
Instalación	1

A continuación, se detallan las especificaciones técnicas de las soluciones:

ITEM	ESPECIFICACIONES SOLUCIÓN DE SEGURIDAD PERIMETRAL
	Upgrade de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red.
1	**DESCRIPCIÓN**

1.1	Por plataforma de seguridad se entiende hardware y software integrados de tipo appliance y que deban ser del mismo fabricante.
1.2	El upgrade debe ser ofrecido en alta disponibilidad, se entiende por alta disponibilidad una solución redundante de por lo menos 2 (dos) appliances que cada uno cumpla con las características mínimas mencionadas en estas especificaciones.
1.3	El soporte y licencias ofrecido por el fabricante de la solución tienen que tener vigencia de 1(un) año en la modalidad 7x24.
2	**CAPACIDAD**
2.1	Throughput de 6.8 Gbps medido con tráfico real (transacciones http 64KB o transacciones usando una mixtura de aplicaciones). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.
2.2	No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde.
2.3	La plataforma de hardware debe soportar hasta 945,000 sesiones.
2.4	La plataforma de hardware debe soportar 100.000 nuevas sesiones por segundo.
2.5	IPsec VPN throughput 4.6 Gbps
2.6	IPS throughput 3.2 Gbps
2.7	Mínimo 8 interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de red de la Entidad.
2.8	Mínimo 6 interfaces de red 1G en formato SFP para el tráfico de datos de la red de la Entidad;
2.9	Mínimo 4 (cuatro) interfaces de red 10G en formato SFP+ para el tráfico de datos de la red de la Entidad;
2.10	Protección de amenazas throughput 3.2 Gbps
2.11	Mínimo 1 (una) interfaz de tipo consola RJ-45 o similar;
2.12	Disco de estado sólido interno de 120 GB o superior.
2.13	Soporte a, como mínimo, 10 ruteadores virtuales
2.14	Soporte a, como mínimo, 50 zonas de seguridad;
2.15	Raqueable en 1 unidad de rack como mínimo
2.16	Estar licenciada para 2,000 (dos mil) túneles de VPN IPSec del estilo sitio-a-sitio;
3	**GENERALES**
3.1	El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, LACP.
3.2	La solución debe haber sido nombrada 11 veces como líder en el cuadrante de Gartner de Network Firewalls.
3.3	Debe soportar enrutamiento estático y dinámico (RIP, BGP y OSPFv2/v3). También debe soportar Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3.
3.4	Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones;
3.5	Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo;

3.6	Los dispositivos de seguridad deben tener la capacidad de operar de forma simultánea mediante el uso de sus interfaces físicas en los siguientes modos dentro del mismo firewall, sin necesidad de tener que hacer uso de contextos o dominios virtuales: • Modo Sniffer, para inspección vía puerto espejo del tráfico de datos de la red; • Modo Capa – 2 (L2), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación; • Modo Capa – 3 (L3), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación operando como default gateway de las redes protegidas; • Modo Transparente, para poder inspeccionar datos en línea y tener visibilidad del control de tráfico a nivel de aplicación sobre 2 puertos en modo bridge/transparente.
3.7	Debe soportar SLAAC.
3.8	La solución debe ser líder en el Forrester Wave: Enterprise Firewalls, Q4 2022
3.9	La solución debe soportar aprendizaje automático para brindar protección empresarial en línea, proactiva y en tiempo real.
3.10	La solución debe soportar ML-powered que permita: • Según las pruebas, prevenir de forma proactiva hasta el 95 % de las nuevas amenazas al instante. • Detener scripts y archivos maliciosos sin sacrificar la experiencia del usuario. • Amplíar la visibilidad y la protección a los dispositivos IoT sin hardware adicional. • Reducir el error humano y automatiza las actualizaciones de políticas de seguridad para prevenir los ataques más avanzados.
3.11	El fabricante debe estar certificado por USGv6 para trabajar IPv6 tanto en Firewall como en IPS
3.12	Debe contar con un módulo en la consola web que permita identificar las reglas de firewall que no cuenten con un control basado en aplicaciones, con la finalidad de facilitar la adopción del control basado en aplicaciones.
3.13	La solución debe utilizar la aplicación, no el puerto, como base para todas sus decisiones de política de habilitación segura: permitir, denegar, programar, inspeccionar y aplicar modelado de tráfico.
3.14	La solucion debe soportar inspecionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independentes del puerto y protocolo. El chequeo de firmas tambien debe determinar si una aplicacion está utilizando su puerto default o no, incluyendo, mas no limitando a RDP en el puerto 80 en vez del 389.
3.15	Para direcciones y servicios, la solución debe soportar como mínimo lo siguiente: • Objetos de dirección: 20.000 • Objetos de dirección FQDN: 2048. • Etiquetas por dirección IP: 64 • Direcciones IP máximas DAG: 150.000.
3.16	Para el decifrado SSL, la solución debe soportar como mínimo lo siguiente: • Max SSL inbound certificates: 125. • Max concurrent decryption sessions: 51,200. • SSL certificate cache (forward proxy) • SSL Port Mirror.
3.17	La solución debe poseer por lo menos las siguientes funcionalidades: • Agregación de links 802. • Policy based routing o policy based forwarding; • Ruteo multicast (PIM-SM); • DHCP Relay; • DHCP Server; • Jumbo Frames;

3.18	La solución debe soportar OSPF *graceful restart*;
3.19	Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QOS, SSL y SSH Decryption y protocolos de enrutamiento dinâmico deben operar en caracter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe derecho de recibir actualizaciones o que no haya contrato de garantia de software con el fabricante.
3.20	Para el Network Address Translation, la solución debe soportar: • NAT modes (IPv4): static IP, dynamic IP, dynamic IP and port (port address translation) • NAT64. • NPTv6.
3.21	La solución debe soportar como mínimo: FCC Class A, CE Class A, VCCI Class A
3.22	Las Vlans deben soportar como mínimo: 802.1Q VLAN tags por dispositivo/por interface: 4,094/4,094 .
3.23	Para el enrutamiento la solución debe soportar como mínimo el tamaño de la tabla de reenvío de IPv6 de 12.000
3.24	La capacidad total de reglas NAT debe ser como mínimo 3.000
4	**FUNCIONALIDADES DEL FIREWALL**
4.1	Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.
4.2	Control, inspección y descifrado de SSL/TLS por política para tráfico de entrada (Inbound) y salida (Outbound).
4.3	Debe procesar e inspeccionar tráfico HTTP/2
4.4	Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.
4.5	Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules)
4.6	Debe contar con mecanismos que faciliten la optimización de reglas de seguridad: • Mostrar la primera y última vez que se utilizó una regla de seguridad • Mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.
5	**CONTROL DE APLICACIONES**
5.1	Reconocer por lo menos 2500 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail;
5.2	Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389;
5.3	Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado, incluyendo, más no limitado a Encrypted Bittorrent y aplicaciones VoIP que utilizan cifrado propietario;

5.4	Para tráfico cifrado (SSL/TLS y SSH), debe permitir la desencripción de paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante;
5.5	Debe realizar decodificación de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde con la especificación del protocolo. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, por ejemplo, compartir archivos dentro de una sesión Webex.
5.6	Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como: • Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol). • Nivel de riesgo de las aplicaciones. • Categoría y sub-categoría de aplicaciones. • Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda.
6	**PREVENCIÓN AMENAZAS CONOCIDAS**
6.1	Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus (Anti-malware de red), Anti-Spyware (o Antibot) integrados en el propio appliance.
6.2	Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
6.3	Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/Pasivo;
6.4	Cuando se utilicen las funciones de IPS, Antivirus y Anti-spyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Anti-Vírus y Antispyware habilitadas simultáneamente.
6.5	Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo;
6.6	Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.
6.7	Debe contar con firmas específicas para la mitigación de ataques DoS, buffer overflow, C2 (comando and control)
6.8	Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
6.9	Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, HTTP/2, FTP, SMB, SMTP e POP3;
6.10	Identificar y bloquear comunicaciones con botnets;
6.11	Debe soportar referencia cruzada como CVE;
	Cuando se utilicen las funciones de protección de amenazas como IPS, control de aplicación, maldware sandbox, bloqueo de archivos, proteccion DNS y protección de malware (antivirus, antispyware), el equipamiento debe entregar el mismo performance (no degradar) .
7	**FILTRADO DE CONTENIDO**
7.1	La solución debe soportar especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)

7.2	Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, e-Directory y base de datos local.
7.3	Debe permitir visualizar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio
7.4	Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs
7.5	Debe poseer al menos 60 categorías de URLs y permitir la creación de categorías personalizadas.
7.6	Debe permitir la customización de la página de bloqueo
7.7	Debe permitir bloquear o informar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site.
7.8	Debe evitar la fuga de credenciales corporativas desde o hacia sitios web, es decir debe identificar el envío de credenciales a sitios web no autorizados, previniendo ataques de phishing.
7.9	Debe poder prevenir acceso a páginas de malware y phishing.
8	**IDENTIFICACIÓN DE USUARIOS**
8.1	Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de directorio, autenticación vía LDAP, Active Directory, E- Novell directory, Exchange y base de datos local.
8.2	Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente instalado en un equipo del dominio.
8.3	Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x, soluciones NAC, soluciones proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API, así como la lectura mediante WMI a equipos Windows para la identificación de direcciones IP y usuarios
8.4	Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.
8.5	Debe soportar la identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tiene estos servicios.
9	**QoS**
9.1	Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, o Netflix por ejemplo), se requiere que la solución tenga la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones, tanto audio como vídeo streaming y todo el inventario de aplicaciones soportadas por la solución de seguridad.
9.2	El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad.
9.3	Soportar marcación de paquetes DSCP, inclusive por aplicaciones;
9.4	Disponer de estadísticas Real Time para clases de QoS, monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuario.
10	**VPN**
10.1	Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL

10.2	La VPN IPSec debe soportar como mínimo: • 3DES; AES 128, 192 y 256 bit. • Autenticación MD5, SHA-1, SHA-256, SHA-384, SHA-512 • Algoritmo Internet Key Exchange (IKEv1 & IKEv2)
10.3	Permitir la aplicación de políticas de seguridad y visibilidades para las aplicaciones que circulan dentro de los túneles VPN;
10.4	Debe tener la opción de ocultar el agente de VPN instalado en el cliente remoto, tornándose invisible para el usuario;
10.5	Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN client-to-site;
10.6	Soportar autenticación vía AD/LDAP, Secure id, doble factor de autenticación, certificado del lado del cliente y base de usuarios local;
10.7	El agente de VPN client-to-site debe validar la configuración del cliente antes de otorgar el acceso a la red. Se deberán soportar como mínimo los siguientes criterios de evaluación antes de otorgar el acceso a la red: actualización y marca de antivirus, parche del sistema operativo, dominio del equipo cliente, firewall host, solución y marca de herramienta de cifrado de disco. Se podrá usar un solo criterio o una combinación de los criterios de evaluación antes de otorgar el acceso a la red al cliente. Por ejemplo, deberá validar que el cliente tenga la última versión de parche de sistema operativo y/o tenga el antivirus actualizado y sea una marca especifica.
10.8	El agente de VPN client-to-site debe ser compatible al menos con: Windows XP, Vista, Windows 7, Windows 8, Windows 10, MacOS X, Chrome OS.
10.9	El agente de VPN client-to-site debe ser compatible con sistemas operativos Linux, Windows 10 UWP y dispositivos móviles Apple iOS y Android.

ITEM	ESPECIFICACIONES SOLUCIÓN DE PROTECCIÓN DE CARGAS DE TRABAJO EN AZURE
	Renovación de solución de protección de redes con características de Next Generation Firewall (NGFW) para la protección de las cargas de trabajo en Azure con control preciso y visibilidad de las aplicaciones.
1	**DESCRIPCIÓN**
1.1	La solución de seguridad es de arquitectura tipo software de paso único para minimizar la latencia, extendiendo la habilitación segura de aplicaciones en entornos virtualizados.
1.2	Debe soportar el uso de objetos de dirección dinámica e integración con los sistemas de orquestación utilizando una API de administración XML.
1.3	En caso de migración de servicios a otros tipos de escenarios, la plataforma deberá poder operar a través de la misma imagen en ambientes de nube pública como AWS, GCP y Oracle Cloud, en ambientes virtuales como VMware ESXi, Hyper-V y KVM, y en ambientes de nube privada como VMware NSX, Cisco ACI, Openstack y Nutanix.
1.4	Los planos de control y de datos deben estar separados de modo que los usuarios puedan asignar CPUs dedicadas a cada uno de ellos como medio para garantizar el acceso permanente a la administración independiente de la carga de tráfico.
1.5	Soportar la integración con las herramientas de automatización y plantillas del ARM de Azure, para el despliegue de la plataforma en este ambiente.
1.6	Debe soportar despliegues a través de múltiples nubes públicas o privadas usando herramientas de automatización de terceros como Terraform y Ansible.

1.7	Integración con Application Insights de Azure el monitoreo de salud de la plataforma para el seguimiento de las siguientes métricas: • % de utilización de sesiones • Total de sesiones activas • % de utilización de CPU del Dataplane • % de utilización del buffer de paquetes del Dataplane • % de túneles activos de VPN Client-to-Site
1.8	Integración con el Azure Security Center para enviarle los log´s de amenazas de la plataforma y poder monitorear desde una vista consolidada todos los eventos de seguridad del ambiente de Azure desde una única consola.
1.9	El soporte y licencias ofrecido por el fabricante de la solución tienen que tener vigencia de 1 (un) año en la modalidad 7x24
1.10	El fabricante debe estar en el cuadrante de líderes de Gartner para “Enterprise Network Firewall” o “Firewalls de Redes Empresariales” en los últimos 5 reportes.
1.11	La solución debe ser líder en el Forrester Wave: Enterprise Firewalls, Q4 2022
1.12	El fabricante debe estar certificado por USGv6 para trabajar IPv6 tanto en Firewall como en IPS
1.13	La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7 del modelo OSI.
2	**CAPACIDAD**
2.1	Throughput de 1Gbps con la funcionalidad de control de aplicaciones habilitada para todas las firmas que el fabricante posea, medido con transacciones HTTP de 64KB.
2.2	Throughput de 750Mbps Mbps medido con tráfico real (transacciones http 64KB o transacciones usando un mix de aplicaciones), con las siguientes funcionalidades habilitadas simultáneamente: Firewall con clasificación y control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Anti-malware de red, Anti-spyware (o AntiBot), control de amenazas avanzadas de día cero (Sandboxing) y logging activo. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.
2.3	Throughput de 500Mbps de tráfico VPN IPSec.
2.4	No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde.
2.5	La plataforma de hardware debe soportar hasta 250,000 conexiones simultaneas sin desencriptar.
2.6	La plataforma debe soportar 9,000 conexiones nuevas por segundo medido con transacciones HTTP de un (1) byte.
2.7	Soporte a, como mínimo, 3 (tres) ruteadores virtuales;
2.8	Soporte a, como mínimo, 40 (cuarenta) zonas de seguridad;
2.9	Estar licenciada para soportar 500 (quinientos) clientes de VPN SSL simultáneos del estilo cliente-servidor;
2.10	Estar licenciada para 1,000 (mil) túneles de VPN IPSec simultáneos del estilo sitio-a-sitio;
3	**GENERALES**
3.1	Proveer separación de los datos a través de las políticas de segmentación de aplicaciones para controlar el tráfico entre VNets y a través de las subnets.
3.2	Proveer protección de las cargas de trabajo de producción en el perímetro de internet del ambiente de Azure de la entidad para proteger las aplicaciones públicas de amenazas conocidas y desconocidas.
3.3	Proveer acceso remoto seguro a los usuarios y dispositivos que acceden al ambiente de Azure de la entidad.

3.4	Deberá poder crear listas dinámicas a partir del registro de algún evento en el log de seguridad, obteniendo leer de forma dinámica el origen y/o destino IP para asociarlo a una etiqueta dinámica, por ejemplo, a partir del registro de un evento tipo malware asociará a la dirección IP víctima de forma automática a una etiqueta dinámica de direcciones IPs, donde se asociarán a una política restrictiva de seguridad para impedir conexiones subsecuentes a dicho evento.
4	**ALTA DISPONIBILIDAD**
4.1	Soporte a configuración de alta disponibilidad Activo/Pasivo usando conjuntos de disponibilidad (Availability sets) dentro de un grupo de recursos (resource groups) de Azure.
4.2	Por escalabilidad, debe soportar alta disponibilidad nativa de nube a través de balanceadores de carga que puedan distribuir el tráfico a través de múltiples firewall virtuales dentro de un conjunto de disponibilidad (Availability set).
4.3	Soportar rápido crecimiento de los despliegues de Azure que consisten en muchas suscripciones o grupos de recursos a través de un enfoque de servicios compartidos usando una VNet de tránsito con auto-escalamiento para despliegues o remoción de máquinas virtuales según como los patrones de tráfico incrementen o se reduzcan.
5	**FUNCIONALIDADES DEL FIREWALL**
5.1	Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.
5.2	Control, inspección y descifrado de SSL/TLS por política para tráfico de entrada (Inbound) y salida (Outbound).
5.3	Debe procesar e inspeccionar tráfico HTTP/2
5.4	Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.
5.5	Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
5.6	Debe contar con mecanismos que faciliten la optimización de reglas de seguridad: • Mostrar la primera y última vez que se utilizó una regla de seguridad • Mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido de la plataforma.
6	**CONTROL DE APLICACIONES**
6.1	Reconocer por lo menos 2500 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail;
6.2	Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389;
6.3	Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado, incluyendo, más no limitado a Encrypted Bittorrent y aplicaciones VoIP que utilizan cifrado propietario;

6.4	Para tráfico cifrado (SSL/TLS y SSH), debe permitir la desencripción de paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante;
6.5	Debe realizar decodificación de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde con la especificación del protocolo. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, por ejemplo, compartir archivos dentro de una sesión Webex.
6.6	Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interfaz gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones de la empresa;
6.7	Debe alertar al usuario cuando una aplicación fuera bloqueada
6.8	Debe contar con un módulo en la consola web que permita identificar las reglas de firewall que no cuenten con un control basado en aplicaciones, con la finalidad de facilitar la adopción del control basado en aplicaciones.
7	**IDENTIFICACIÓN DE USUARIOS**
7.1	Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de directorio, autenticación vía LDAP, Active Directory, E- Novell directory, Exchange y base de datos local.
7.2	Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente instalado en un equipo del dominio.
7.3	Debe permitir el control, sin instalación de cliente de software, que solicite conexión a través de la VPN a un recurso de Azure, para que antes de iniciar la conexión, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.
7.4	Soporte a la creación de políticas de autenticación cuando el destino sea altamente restringido sin la necesidad de instalar algún cliente en el endpoint, es decir de forma transparente, solicitará automáticamente al usuario final autenticación tipo Multifactor (MFA), evitando el acceso a servidores únicamente por usuario y contraseña. Este módulo deberá ser compatible al menos con PingID, Duo y Okta.
8	**CONSOLA DE ADMINISTRACIÓN Y MONITOREO**
8.1	Debe soportar monitorear los eventos de la plataforma vía SNMP
8.2	Debe soportar la integración con soluciones de SIEM del mercado
8.3	Debe soportar la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración;
8.4	Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
9	**PREVENCIÓN DE AMENAZAS CONOCIDAS**
9.1	Para seguridad del ambiente contra ataques, la plataforma de seguridad debe poseer módulo de IPS (Intrusion Prevention System), Antivirus (Anti-malware de red), Anti-Spyware (o Antibot) y DNS Sinkhole integrados en la propia plataforma.
9.2	Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
9.3	Cuando se utilicen las funciones de IPS, Antivirus y Anti-spyware, la plataforma debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Anti-Vírus y Antispyware habilitadas simultáneamente.

9.4	Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo;
9.5	Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.
9.6	Debe contar con firmas específicas para la mitigación de ataques DoS, buffer overflow, C2 (comando and control)
9.7	Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
9.8	Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, HTTP/2, FTP, SMB, SMTP e POP3;
9.9	Identificar y bloquear comunicaciones con botnets;
9.10	Debe soportar referencia cruzada como CVE;
10	**ANÁLISIS DE MALWARE MODERNO**
10.1	Identificación de malware desconocido, incluyendo el análisis de más de 100 comportamientos maliciosos, así como la generación y distribución de protección automática en la siguiente actualización disponible.
10.2	La plataforma de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis en nube, donde el archivo será ejecutado y simulado en un ambiente controlado. La nube deberá ser propia del mismo fabricante y no tercerizada con otras empresas.
10.3	Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP, Windows 7, Windows 10, Mac OS X y Android;
10.4	Debe soportar el monitoreo de archivos transferidos por internet (HTTP, HTTP/2, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB.
10.5	El sistema de análisis en nube debe proveer informaciones sobre las acciones del malware en la máquina infectada, informaciones sobre cuales aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el malware, generar firmas de Antivirus y Anti-spyware automáticamente, definir URLs no confiables utilizadas por el nuevo malware y proveer información sobre el usuario infectado (su dirección IP y su login de red);
10.6	Debe permitir informar al fabricante cuando haya una sospecha de falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia interfaz de administración.
10.7	Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP y RAR) archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), email link, flash, archivos de MacOSX (mach-o, dmg, pkg) y Android APKs en el ambiente controlado.
10.8	Permitir el envío de archivos para análisis en el ambiente controlado vía web y de forma automática vía API.
10.9	La solución de sandboxing debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor, inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
10.10	La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.
11	**FILTRO DE CONTENIDO**
11.1	Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
11.2	Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, e-Directory y base de datos local.

11.3	Debe permitir visualizar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio
11.4	Debe soportar un cache local de URLs en la plataforma, evitando el delay de comunicación/validación de las URLs
11.5	Debe poseer al menos 60 categorías de URLs y permitir la creación de categorías personalizadas.
11.6	Debe permitir la customización de la página de bloqueo
11.7	Debe permitir bloquear o informar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al sitio.
11.8	Debe evitar la fuga de credenciales corporativas desde o hacia sitios web, es decir debe identificar el envío de credenciales a sitios web no autorizados, previniendo ataques de phishing.
11.9	Debe poder prevenir acceso a páginas de malware y phishing.
12	**VPN**
12.1	Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL
12.2	Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN client-to-site;
12.3	Soportar autenticación vía AD/LDAP, Secure id, doble factor de autenticación, certificado del lado del cliente y base de usuarios local;
12.4	El agente de VPN client-to-site debe validar la configuración del cliente antes de otorgar el acceso a la red. Se deberán soportar como mínimo los siguientes criterios de evaluación antes de otorgar el acceso a la red: actualización y marca de antivirus, parche del sistema operativo, dominio del equipo cliente, firewall host, solución y marca de herramienta de cifrado de disco. Se podrá usar un solo criterio o una combinación de los criterios de evaluación antes de otorgar el acceso a la red al cliente. Por ejemplo, deberá validar que el cliente tenga la última versión de parche de sistema operativo y/o tenga el antivirus actualizado y sea una marca especifica.
12.5	El agente de VPN client-to-site debe ser compatible al menos con: Windows XP, Vista, Windows 7, Windows 8, Windows 10, MacOS X, Chrome OS.
12.6	El agente de VPN client-to-site debe ser compatible con sistemas operativos Linux, Windows 10 UWP y dispositivos móviles Apple iOS y Android.

GARANTÍA Y SOPORTE:

Soporte y Garantía por 1 año para toda la solución adquirida, contados a partir de la puesta en funcionamiento.

QUINTA. - OBLIGACIONES A CARGO DEL INSTITUTO: En virtud del presente contrato, **EL INSTITUTO** tendrá los siguientes derechos y deberes:

1. Ejercer la supervisión general sobre el objeto del contrato.
2. Acudir ante las autoridades para obtener la protección de los derechos derivados de la presente contratación y sanción para quién los vulnere.
3. Exigir al CONTRATISTA la ejecución idónea y oportuna del objeto contratado.

4. Impartir las instrucciones que sean del caso, relacionadas con las actividades a realizar por EL CONTRATISTA.
5. Asignar las actividades a realizar por parte del contratista.
6. Poner a disposición del contratista la información necesaria para el desarrollo de las actividades.
7. Realizar la entrega de las pruebas y muestras necesarias para prestación del servicio por parte del contratista, cuando aplique.
8. Adelantar las gestiones necesarias para el reconocimiento y cobro de las sanciones pecuniarias, para lo cual la supervisión dará aviso oportuno a EL INSTITUTO sobre la ocurrencia de hechos constitutivos de mora o incumplimiento.
9. Adelantar las acciones conducentes a obtener la indemnización de los daños que sufran en desarrollo o con ocasión de la presente contratación.
10. Repetir contra los servidores públicos, el contratista o terceros por las indemnizaciones que deba pagar como consecuencia del contrato.
11. Adelantar revisiones periódicas, a través de la supervisión, para verificar que la ejecución del contrato cumpla con las condiciones ofrecidas, naturaleza del objeto contratado y los requisitos mínimos previstos en las normas sobre la materia y promover las acciones de responsabilidad contra EL CONTRATISTA y sus garantes si hay lugar a ello.
12. Cancelar oportunamente al CONTRATISTA el valor del contrato de conformidad con lo estipulado en la forma de pago.
13. Verificar, a través de la supervisión del contrato, el cumplimiento de lo establecido en el POE-A01.2014-001 "Gestión de Seguridad y Salud en el trabajo", especialmente lo dispuesto en el Anexo 1 sobre Normas y Requerimientos de Seguridad y Salud en el Trabajo para Contratistas, de acuerdo al tipo de actividad que desarrolla.
14. Verificar, a través de la supervisión del contrato, el cumplimiento de las normas de Gestión Ambiental, de conformidad con la normatividad vigente y de acuerdo al tipo de actividad desarrollada.

SEXTA. - FORMA DE PAGO: El valor del contrato que resulte del presente proceso de contratación se cancelará en un sólo pago una vez se realice la entrega a satisfacción de los elementos que acrediten el soporte, mantenimiento y garantía de fabrica con la actualización del software y de hardware de la solución de seguridad perimetral firewall, conforme a lo establecido en las especificaciones técnicas, previo visto bueno por parte del supervisor del contrato, así como también aportar la certificación sobre el cumplimiento en el pago de los aportes de sus empleados al Sistema General de Seguridad Social Integral (salud, riesgos laborales, pensiones) y aportes parafiscales (Cajas de Compensación Familiar, ICBF y SENA) y la factura respectiva.

PARAGRAFO PRIMERO: Para la cancelación **EL CONTRATISTA** debe cumplir a satisfacción con la prestación del servicio facturado y acorde con el objeto del contrato, previo visto bueno por parte del supervisor del contrato, así como también aportar la certificación sobre el cumplimiento en el pago de los aportes de sus empleados al Sistema General de Seguridad Social Integral (salud, riesgos laborales, pensiones) y aportes parafiscales (Cajas de Compensación Familiar, ICBF y SENA).

PARAGRAFO SEGUNDO: Para el pago **EL CONTRATISTA** deberá dar cumplimiento a las medidas para gestionar la facturación electrónica, establecidas en el Decreto 358 de 2020, Resoluciones 042 y 094 de 2020 expedidas por La DIAN, Directiva Presidencial 09 de 2020 y Circular Externa 016 del SIIF y demás normas que lo regulen, aclaren o modifiquen

PARAGRAFO TERCERO: El pago se efectuará mediante abono por Terminal vía ACH y estará sujeto a la situación de recursos por parte de la DTN de acuerdo al Programa Anual Mensualizado de Caja – PAC- aprobado para esta vigencia según programación mensual de giros.

El valor de la factura presentada no podrá exceder el valor del contrato.

SEPTIMA. - IMPUTACIÓN PRESUPUESTAL El valor del contrato se financiará con recursos de la vigencia fiscal 2023, para lo cual se cuenta con Certificado de Disponibilidad Presupuestal No. 76723 del 4 de agosto de 2023, expedido por el Grupo de Gestión Financiera, así:

PROYECTO (NOMBRE DEL RUBRO)	CÓDIGO DEL RUBRO Y RECURSO	VALOR POR CARGAR
ADQUISICIÓN DE BIENES Y SERVICIOS- SERVICIO DE IMPLEMENTACIÓN SISTEMAS DE GESTIÓN-FORTALECIMIENTO INSTITUCIONAL EN TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES NACIONAL.	C-1999-0300-5-0-1999061-02-10	$293.550.000

OCTAVA-. SUPERVISIÓN: La supervisión sobre la ejecución del cumplimiento del objeto y obligaciones del presente contrato será ejercida por la Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones o quien esta delegue, quienes deberán dar cumplimiento a lo indicado en los artículos 83 y 84 de la ley 1474 de 2011 y en la Resolución No. 0064 de 2017, mediante la cual se reglamentó el ejercicio de la interventoría y la supervisión y los demás actos administrativos que la reglamenten modifiquen y/o adicionen. Así mismo deberá remitir al Grupo de Gestión Contractual copia del/los informe(s) productos y soportes de ejecución del contrato. Cuando el supervisor sea un Director, Coordinador o Jefe de Área/Dirección/Grupo la responsabilidad quedara en quien lo remplace en el cargo.

NOVENA. - GARANTÍA ÚNICA: EL CONTRATISTA se compromete a constituir a favor del **INSTITUTO** una garantía única otorgada por una compañía de seguros legalmente establecida en Colombia y conforme a las disposiciones pertinentes, que ampare los siguientes riesgos: **A) CUMPLIMIENTO:** En cuantía equivalente al veinte por ciento (20%) del valor total del contrato, vigente por el término de ejecución del contrato y doce (12) meses más. **B) GARANTÍA DE CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES.:** En cuantía equivalente al veinte por ciento (20%) del valor total del contrato, vigente por el término de ejecución del contrato y doce (12) meses más.

PARÁGRAFO TERCERO: REPOSICIÓN DE LA GARANTÍA ÚNICA: EL CONTRATISTA se compromete a reponer el monto de la garantía única cada vez que en razón de sanciones impuestas o de otros hechos, se disminuyesen o agotasen.

DÉCIMA.- MULTAS: - En virtud de lo establecido en el artículo 40 de la Ley 80 de 1993, el artículo 17 de la Ley 1150 de 2007 en concordancia con lo dispuesto en el artículo 86 de la Ley 1474 de 2011, las partes acuerdan que en caso de mora o retardo en el cumplimiento de cualquiera de las obligaciones señaladas en el presente contrato a cargo del **CONTRATISTA**, y como apremio para que las atienda oportunamente, el **INSTITUTO** podrá imponerle mediante Resolución motivada, multas equivalentes al uno por ciento (1%) del valor total del contrato por cada día de atraso o retardo en el cumplimiento de sus obligaciones previo requerimiento al **CONTRATISTA**, sin que el valor total de ellas pueda llegar a exceder el veinte por ciento (20%) del valor total del contrato. EL **CONTRATISTA** autoriza desde ya, para que en caso de que el **INSTITUTO** le imponga multas, el valor de las mismas se descuenten del saldo a su favor o se ordene hacerlo efectivo con cargo a la garantía única de cumplimiento constituida, lo anterior, salvo que **EL CONTRATISTA** demuestre que su tardanza o mora obedeció a hechos constitutivos de caso fortuito o fuerza mayor, debidamente comprobados.

PARÁGRAFO: Para los efectos del cobro, se aplicarán las disposiciones establecidas en la Ley 1150 de 2007, en la Ley 1474 de 2011 y demás disposiciones que regulen la materia. El pago o la deducción de dichas sanciones

no exoneran a **EL CONTRATISTA** de su obligación de ejecutar el contrato, ni las demás responsabilidades y obligaciones del mismo.

DÉCIMA PRIMERA. - PENAL PECUNIARIA: En caso de incumplimiento total, defectuoso o parcial del objeto o las obligaciones emanadas del presente contrato, **EL CONTRATISTA** pagará al **INSTITUTO** el veinte por ciento (20%) del valor total del mismo como estimación anticipada de perjuicios, sin que lo anterior sea óbice para que se declare la caducidad del contrato, se impongan las multas a que haya lugar y se obtenga la indemnización de la totalidad de los perjuicios causados. **El INSTITUTO** podrá hacer efectivo el valor de la cláusula penal descontándola de las sumas que adeude al **CONTRATISTA** en desarrollo del contrato, o haciendo efectiva la garantía única de cumplimiento. En todo caso, el **INSTITUTO** podrá acudir ante las autoridades judiciales para reclamar por el mayor perjuicio ocasionado por el incumplimiento.

PARÁGRAFO: Para los efectos de la imposición y cobro, se aplicarán las disposiciones establecidas en el artículo 17 de la Ley 1150 de 2007 y el artículo 86 de la Ley 1474 de 2011.

DÉCIMA SEGUNDA. - INTERPRETACIÓN, MODIFICACIÓN Y TERMINACIÓN UNILATERALES, SOMETIMIENTO A LA LEY NACIONAL y CADUCIDAD DEL CONTRATO: De conformidad con lo dispuesto por los Artículos 14 al 18 de la Ley 80 de 1993, en concordancia con la Ley 1150 de 2007, las cláusulas excepcionales de interpretación, modificación y terminación unilaterales, sometimiento a la ley nacional y caducidad del contrato por parte de la Entidad, se entienden incorporadas en el presente contrato.

DÉCIMA TERCERA.- INDEMNIDAD: Con ocasión de la celebración y ejecución del presente contrato **EL CONTRATISTA** se compromete y acuerda en forma irrevocable a mantener indemne a **EL INSTITUTO** por cualquier daño o perjuicio originado en reclamaciones de tipo privada, administrativa o judicial proveniente de terceros y que se deriven de sus actuaciones o de las de sus subcontratistas o dependientes. Así mismo, **EL CONTRATISTA** mantendrá indemne al **INSTITUTO**, ante cualquier reclamación de carácter laboral o relacionado, así como contractual que se origine por el incumplimiento de las obligaciones laborales y/o contractuales que **EL CONTRATISTA** asume frente al personal, subordinados o terceros que se vinculen a la ejecución de las obligaciones derivadas del presente contrato.

DÉCIMA CUARTA. - RESERVA Y CONFIDENCIALIDAD: Toda la información que pueda conocer, manejar o desarrollar **EL CONTRATISTA**, durante la vigencia del presente contrato, será confidencial e intransferible, salvo que sea calificada como pública por parte de **EL INSTITUTO**. La información confidencial sólo podrá ser utilizada con el propósito de cumplir con el servicio ofertado, quedándole prohibido quien la recibe, compartirla con terceros.

DÉCIMA QUINTA. - RESPONSABILIDAD: EL CONTRATISTA responderá civil y penalmente tanto por el incumplimiento de las obligaciones derivadas del contrato, como por los hechos u omisiones que le fueren imputables y que causen daño o perjuicio a **EL INSTITUTO**, todo de conformidad con lo dispuesto por los artículos 52, 53 y 56 de la Ley 80 de 1993, modificado por el artículo 82 de la Ley 1474 de 2011.

DÉCIMA SEXTA. - CESIÓN: EL CONTRATISTA no podrá ceder a persona natural o jurídica alguna, los derechos y obligaciones emanados del presente contrato sin que medie previa autorización expresa por parte del **INSTITUTO**.

DÉCIMA SÉPTIMA. - SUSPENSIÓN: Las partes contratantes podrán suspender el contrato, mediante la suscripción de un acta en donde conste tal evento cuando medien circunstancias de fuerza mayor y caso fortuito, previa solicitud debidamente sustentada por una de las partes.

DÉCIMA OCTAVA. - SOLUCIÓN DE CONTROVERSIAS: Las partes contratantes en caso de controversias contractuales buscarán solucionar en forma ágil, rápida y directa las diferencias y discrepancias surgidas de la actividad contractual a través de los mecanismos de solución previstos por la Ley 80 de 1993 y la Ley 1150 de 2007, de conformidad con la naturaleza y cuantía del asunto.

DÉCIMA NOVENA. - AUSENCIA DE RELACIÓN LABORAL: El presente contrato será ejecutado por **EL CONTRATISTA** con la autonomía e independencia que sus obligaciones le señalen y el desarrollo del mismo no genera vínculo laboral alguno con **EL INSTITUTO** y por ende no tiene derecho al reconocimiento de prestaciones sociales.

VIGÉSIMA. - RESPONSABILIDAD AMBIENTAL: EL CONTRATISTA se compromete a dar cumplimiento a las normas legales de protección ambiental vigentes en Colombia, así como a la normatividad interna del **INSTITUTO**, relacionadas con el deber de proteger el medio ambiente y los recursos naturales y realizar la disposición final de residuos peligrosos, con responsabilidad social en procura del desarrollo sostenible del medio ambiente.

VIGÉSIMA PRIMERA.-. INHABILIDADES E INCOMPATIBILIDADES: EL/LA CONTRTISTA, con la aceptación del presente documento, afirma bajo juramento no encontrarse incurso ni él ni su representada en alguna de las causales de inhabilidad e incompatibilidad para contratar, y en especial las señaladas en los artículos 8º y 9º de la Ley 80 de 1993, la Ley 1150 de 2007, Ley 1474 de 2011, Ley 1778 de 2016 y demás disposiciones vigentes sobre la materia, ni ser responsable fiscalmente en virtud de lo señalado en la Ley 610 de 2000.

VIGÉSIMA SEGUNDA. - DOMICILIO CONTRACTUAL: Para todos los efectos legales, el domicilio contractual será la ciudad de Bogotá, D.C.

VIGÉSIMA TERCERA. - DOCUMENTOS CONTRACTUALES: Para todos los efectos, son documentos de este contrato y por lo tanto hacen parte integral del mismo, todos los documentos aquí citados y los demás que se generen con ocasión de la ejecución contractual, los cuales definen igualmente las actividades, alcance y obligaciones contractuales.

VIGÉSIMA CUARTA. - NOTIFICACIONES: Toda comunicación efectuada por el **INSTITUTO** que deba ser notificada a **EL CONTRATISTA** será realizada a través de medios electrónicos o digitales, especialmente a través de correo electrónico suministrado por **EL CONTRATISTA**.

VIGÉSIMA QUINTA. - PERFECCIONAMIENTO Y EJECUCIÓN: El presente documento se entiende perfeccionado con la firma de las partes a través de la plataforma del SECOP II. Para su ejecución requiere de la existencia de las disponibilidades y registros presupuestales correspondientes y la aprobación de la garantía única por parte del **INSTITUTO**.

Proyectó: Jasmín Julieth Ciro Cabrera– Contratista Grupo de Gestión Contractual
Revisó: Luz Angela Garzon Rojas – Contratista Grupo de Gestión Contractual
Dora Nelsy Beltrán Rincon – Coordinadora Grupo de Gestión Contractual