ANEXO 1: FICHA TÉCNICA

1. OBJETO

CONTRATAR LA RENOVACIÓN DEL SOPORTE, MANTENIMIENTO, GARANTÍA Y LICENCIAMIENTO DE LOS DISPOSITIVOS DE SEGURIDAD PERIMETRAL FORTINET, ASÍ COMO, LA ADQUISICIÓN DE COMPONENTES ADICIONALES PARA ROBUSTECER LOS CONTROLES DE SEGURIDAD DE LA ENTIDAD.

2. ALCANCE Y CONSIDERACIONES GENERALES DEL SERVICIO

El Instituto Geográfico Agustín Codazzi – IGAC, requiere mantener la seguridad, rendimiento y disponibilidad de la infraestructura tecnológica on premise (Sede Principal y Territoriales), así como la infraestructura tecnológica Cloud en Azure, por medio de plataformas tecnológicas actualizadas que permitan realizar de manera efectiva la detección de ciberataques, la gestión de políticas de tráfico y optimización de protocolos, mitigando las amenazas de red que se generan constantemente y para este efecto, se requiere **CONTRATAR LA RENOVACIÓN DEL SOPORTE, MANTENIMIENTO, GARANTÍA Y LICENCIAMIENTO DE LOS DISPOSITIVOS DE SEGURIDAD PERIMETRAL FORTINET, ASÍ COMO, LA ADQUSICION DE COMPONENTES ADICIONALES PARA ROBUSTECER LOS CONTROLES DE SEGURIDAD DE LA ENTIDAD**, servicios que deberán renovarse o adquirirse, según el caso, con una vigencia cotérmino al 30 de noviembre de 2028. Lo anterior, dado que, con el fin de facilitar la administración de su plataforma, la entidad pretende unificar la fecha de renovación de sus garantías y licencias que han venido siendo adquiridas en fechas diferentes a lo largo del tiempo, para optimizar sus procesos de renovación .

El proveedor debe contemplar la Instalación, configuración total de la plataforma (Integraciones de seguridad entre Firewalls, SD-WAN, ZTNA, VPN SSL, VPN Site to Site, Perfiles de Seguridad, Integración con SIEM, FORTIANALYZER , FORTIMANAGER y demás actividades de integración requeridas), puesta en producción, documentación, soporte y mantenimiento, de la infraestructura descrita en los siguientes sub numerales.

Hace parte del alcance del presente proceso los siguientes bienes y servicios:

1) **La Renovación del licenciamiento, soporte y garantía de fabricante para las siguientes soluciones tecnológicas**

   i. Solución Firewall Perimetral

ii. Solución Master /Slave (FortiManager)
iii. Firewall que soportan la solución SD-WAN (Firewalls compatibles con SD-WAN)
iv. Solución Firewall en nube VM16 CLOUD AZURE

2) Adquisición, upgrade tecnológico y/o suscripción con implementación y puesta en funcionamiento de los siguientes soluciones y servicios

i. Renovación del licenciamiento, soporte y garantía de fabricante con upgrade tecnológico a máquina virtual para la solución de análisis de logs (Fortinalyzer) de la sede principal
ii. Adquisición de siete (7) Firewall para la solución SD-WAN con su licenciamiento, soporte y garantía de fábrica.
iii. Renovación del licenciamiento, soporte y garantía del fabricante con upgrade de características para el FortiSIEM
iv. Suscripción al Servicio de Acceso Seguro –ZTNA RPP/ATP (1500)

3) Assesment y Optimización

4) Servicios de soporte y mantenimiento del proveedor

2.1 CONDICIONES GENERALES

Al momento de realizar el suministro, instalación y puesta en funcionamiento de los bienes y servicios objeto del presente proceso, se deberán tener en cuenta los aspectos generales que se relacionan a continuación:

1. El software y firmware que hacen parte de las soluciones de seguridad perimetral existentes y a adquirir, deberán actualizarse a la versión más reciente y estable en cada mantenimiento preventivo o cuando se detecte la necesidad de realizarlo debido a fallas o vulnerabilidades detectadas en la versión actual. Manifestar de manera clara, explícita y oportuna, los requerimientos que deba contemplar la Entidad, para proceder con la entrega y recibo a satisfacción de los servicios objeto del contrato que se suscriba.
2. Realizar un assessment de seguridad sobre las soluciones renovadas, para con dichos resultados implementar los ajustes de arquitectura, reconfiguración y parametrización a que haya lugar en los dispositivos, componentes y servicios de la plataforma de la entidad incluyendo los nuevos equipos adquiridos y con upgrade tecnológico.
3. Realizar la puesta en operación de las soluciones renovadas y adquiridas con todas las integraciones de seguridad entre Firewall, SD-WAN, ZTNA, Fortimanager, Fortianalyzer, SIEM, VPN SSL, VPN Site to Site, así como,

optimizaciones y/o configuración de perfiles de Seguridad que se requieran en el marco de mejores prácticas del fabricante y las necesidades de la entidad. El proveedor deberá contemplar todos los conectores, transceivers, componentes, licenciamiento y software necesario para realizar dicha puesta en operación e integraciones, sin que esto implique costos adicionales para el IGAC.

4. Adoptar todas las medidas de seguridad que se requieran para la entrega y traslado, en especial de las personas que realizarán las actividades en el marco del Sistema de Seguridad y Salud en el Trabajo. Presentar la afiliación a seguridad social (Riesgos laborales, Salud y Pensión) y recibos de pago, del personal que realizará las tareas contractuales, dando cumplimiento al artículo 2.2.4.6.28 contratación del Decreto Único Reglamentario del Sector Trabajo 1072 de 2015 del Ministerio de Trabajo.
5. Acuerdo de confidencialidad y seguridad informática: El proveedor deberá firmar y entregar al momento de la suscripción del Acta de Inicio, un Acuerdo de Confidencialidad, el cual debe estar suscrito por el Representante Legal del proveedor dirigido al Instituto Geográfico Agustín Codazzi – IGAC, donde garantizará la confidencialidad de la información Institucional a la cual tengan acceso directamente o por intermedio de terceros. Así mismo, el personal del proveedor deberá firmar un (1) Compromiso de Confidencialidad para mantener la confidencialidad y exposición de la información y componentes tecnológicos con que cuenta la entidad.
6. El proveedor deberá disponer de todas las herramientas, instrumentos y equipos, necesarios para realizar las actividades objeto del proceso, así como la dotación de personal, de salud ocupacional y las que se requieran en el cumplimiento del contrato.
7. El proveedor deberá tener en cuenta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, entre otros), requerida para que el personal asignado al proyecto pueda cumplir sus funciones, los cuales deberán ser asumidos por el contratista, sin ningún costo adicional para la entidad.
8. Para todos los equipos físicos, virtuales y suscripciones parte de este proceso, incluidos los de renovación, upgrade tecnológico, adquisiciones y a los que se incorporan nuevas características, el proveedor deberá hacer entrega de los documentos del fabricante donde indique los derechos de uso, el periodo de renovación del licenciamiento (o la suscripción incluido) y el soporte con el fabricante FortiCare Premium a nombre de IGAC.

2.2 REQUISITOS PARA FIRMA DEL ACTA DE INICIO

El acta de inicio del contrato se firmará una vez se cumpla los requisitos de perfeccionamiento y ejecución del contrato, dentro de los, dos (2) días hábiles máximo después del inicio del contrato, el proveedor deberá entregar al

supervisor del contrato, los siguientes documentos y planes.

2.2.1 PLANES Y DOCUMENTOS INICIALES DEL CONTRATO

a. Hojas de vida del personal mínimo requerido para la ejecución del contrato y evidencias que permitan verificar el cumplimiento de los perfiles académicos y de experiencia, así mismo, allegar el "compromiso de confidencialidad" de cada uno de los perfiles requeridos por el IGAC, debidamente suscrito entre el trabajador asignado al proyecto y el proveedor seleccionado.
b. Plan de trabajo para la entrega de los bienes y servicios, su instalación, configuración y puesta en funcionamiento, así mismo, para las actividades de Assessment, mantenimiento y las sesiones de transferencia de conocimiento.
    - El plan de trabajo deberá contener como mínimo, el cronograma que contemple las actividades que se indican en el ALCANCE del presente documento, identificando para cada una de ellas los siguientes aspectos: Fecha de inicio y terminación de cada actividad
    - Dependencia de tareas (actividades predecesoras y sucesoras)
    - Ruta Crítica
    - Hitos

    Nota 1: El proveedor deberá entregar a la entidad los equipos de upgrade tecnológico y adquiridos en un plazo máximo en treinta (30) días calendario, contados a partir del inicio del contrato, lo anterior, sin exceder el 10 de diciembre de 2025.
    Nota 2: para el caso del Assessment, como se indica en el numeral **3.3** – **Assessment**, el proveedor tendrá hasta 10 días hábiles contados a partir de la firma del acta de inicio para hacer entrega del resultado del Assesment (levantamiento de información y evaluación), la propuesta de optimización y ajuste para aprobación del Supervisor del Contrato.
c. Compromiso y Acuerdos de Confidencialidad
d. Plan de continuidad y contingencia
e. Plan de Manejo Ambiental
f. Plan de Trasferencia de Conocimiento
g. El documento que informe el esquema y gestión del escalamiento definido para la atención de solicitudes (requerimientos e incidentes) de acuerdo con los niveles de criticidad definidos por la entidad (incidentes que generan o no indisponibilidad), donde mínimo se debe informar sobre:
    - Descripción de los procesos de escalamiento técnico y gerencial.
    - Matriz de comunicación para la atención de incidentes y problemas (Medios de contacto, nombre, teléfono, correo electrónico y cargo de

cada persona descrita en la matriz).

Nota 3: Los documentos serán objeto de revisión por la entidad y deberán ser ajustados, si hay lugar a ello, a los dos (2) días hábiles siguientes a la realización de la reunión de Inicio – Kickoff del proyecto.

Nota 4: En ningún caso, los plazos establecidos por el proveedor en el plan de trabajo podrán superar el plazo de ejecución del contrato, el cual está establecido hasta el 31 de diciembre de 2025.

2.3 REUNIÓN DE INICIO – KICKOFF

A los tres (3) días hábiles siguientes a la notificación del Acta de inicio, se realizará la reunión de inicio del proyecto (Kickoff), mediante la cual el Instituto, por medio del supervisor del contrato o su delegado, indicará los lineamientos a tener en cuenta por parte del contratista dentro de la ejecución del contrato y que estarán enmarcados dentro de las obligaciones y especificaciones establecidas en la ficha técnica y estudio previo. Asimismo, dará entrega de las observaciones, solicitud de ajuste o cambio o complementación o aprobación de los planes y documentación solicitada en el numeral **2.2.1.PLANES Y DOCUMENTOS PARA INICIO DEL CONTRATO.**

Por otro lado, para esta fecha, para los equipos físicos y virtuales del numeral 3.1 RENOVACIÓN DE LICENCIAMIENTO, SOPORTE Y GARANTIA DEL FABRICANTE, el proveedor deberá hacer entrega al supervisor del contrato, del documento emitido por el fabricante con la Certificación de Activación de la Garantía del fabricante, las certificaciones de renovación de las licencias y el soporte del fabricante a nombre del IGAC de acuerdo con lo requerido en la presente ficha técnica, los estudios previos y demás documentos del proceso de contratación.

Nota: Para los equipos del numeral 3.2. ADQUISICIÓN, UPGRADE TECNOLÓGICO Y/O SUSCRIPCIÓN CON IMPLEMENTACIÓN Y PUESTA EN FUNCIONAMIENTO los certificados emitidos por el fabricante de activación de las licencias, soporte y garantía del fabricante de las nuevas soluciones adquiridas o con upgrade tecnológico o de funcionalidades deberán entregarse luego de realizada la instalación de los equipos en las ubicaciones correspondientes y para el caso de las nuevas características del FortiSIEM estas podrán activarse y entregarse máximo 10 días calendario luego de realizado el KickOff.

3. ESPECIFICACIONES TECNICAS MINIMAS DE LOS BIENES Y SERVICIOS

A continuación, se detallan las especificaciones de los bienes a adquirir y de los servicios de renovación del licenciamiento, soporte y garantía del fabricante, así como de los servicios conexos, y de mantenimiento preventivo y correctivo de las soluciones objeto del presente proceso.

3.1 RENOVACIÓN DE LICENCIAMIENTO, SOPORTE Y GARANTIA DEL FABRICANTE

3.1.1 Renovación del licenciamiento, soporte y garantía del fabricante para la solución de firewall perimetral de la sede principal

a. El proveedor deberá contemplar la renovación del licenciamiento con todas las características y funcionalidades con las que se cuenta actualmente, así como con las suscripciones de seguridad y soporte de fábrica para los dispositivos Firewall de nueva Generación con los que cuenta la entidad, la cual corresponde a la plataforma FORTIGATE 1800F con los siguientes seriales:

ITEM	DESCRIPCIÓN	NUMERO_SERIAL	MARCA	CANTIDAD
1	FotiGate	FG180FTK22902354	FORTINET	1
2	FotiGate	FG180FTK22902708	FORTINET	1

Tabla 1: Seriales Solución Firewall perimetral Sede principal

b. El proveedor deberá prestar los servicios de soporte y mantenimientos preventivos y correctivos a que haya lugar durante el plazo del servicio, de acuerdo con lo indicado en el **numeral 3.4** del presente documento.
c. El proveedor debe renovar el licenciamiento, soporte y la garantía de fabricante cotérmino hasta el 30 de noviembre de 2028 y la entrega de los certificados de renovación de licenciamiento, soporte y garantía.

3.1.2 Renovación del licenciamiento, soporte y garantía del fabricante para la solución master/slave (Fortimanager), de la sede principal

a. El proveedor deberá contemplar la renovación del licenciamiento, el soporte y la garantía de fabricante, bajo las mismas características con que cuenta actualmente la solución, la cual está constituida por los seriales de los dispositivos descritos a continuación:

SOLUCION MASTER/SLAVE (FORTIMANAGER) DE LA SEDE PRINCIPAL

ITEM	DESCRIPCIÓN	NUMERO_SERIAL	MARCA	MODELO	CANTIDAD
1	Manager Master	FMG2HGTA23000057	FORTINET	FMG-200G	1
2	Manager Slave	FMG2HGTA23000028	FORTINET	FMG-200G	1

Tabla 2: Seriales Solución Mater/Slave Sede principal

b. El proveedor deberá prestar los servicios de soporte y mantenimientos preventivos y correctivos a que haya lugar durante el plazo del servicio, de acuerdo con lo indicado en el **numeral 3.4** del presente documento.
c. El proveedor debe renovar el licenciamiento, soporte y la garantía de fabricante, cotérmino hasta el 30 de noviembre de 2028 y la entrega de los certificados de renovación de licenciamiento, soporte y garantía.

3.1.3 Renovación del licenciamiento, soporte y garantía de fabricante para los firewall que soportan la solución SD-WAN

a. El proveedor debe realizar la renovación del licenciamiento, el soporte y la garantía, de fabricante cotérmino hasta el 30 de noviembre de 2028 y la entrega de los certificados de renovación de licenciamiento, soporte y garantía, bajo las mismas características con que cuenta actualmente la solución descrita en la arquitectura y constituida por los seriales de los dispositivos referidos a continuación:

SOLUCIÓN SD-WAN					
ITEM	DESCRIPCIÓN	NUMERO_SERIAL	MARCA	MODELO	CANTIDAD
1	SD-WAN	FWF61FTK20000181	FORTINET	FWF-61F	1
2	SD-WAN	FWF61FTK20000502	FORTINET	FWF-61F	1
3	SD-WAN	FWF61FTK20000629	FORTINET	FWF-61F	1
4	SD-WAN	FWF61FTK20000566	FORTINET	FWF-61F	1
5	SD-WAN	FWF61FTK20000780	FORTINET	FWF-61F	1

SOLUCIÓN SD-WAN					
ITEM	DESCRIPCIÓN	NUMERO_SERIAL	MARCA	MODELO	CANTIDAD
6	SD-WAN	FWF61FTK20000442	FORTINET	FWF-61F	1
7	SD-WAN	FWF61FTK20000509	FORTINET	FWF-61F	1
8	SD-WAN	FWF61FTK20000411	FORTINET	FWF-61F	1
9	SD-WAN	FWF61FTK20000950	FORTINET	FWF-61F	1
10	SD-WAN	FWF61FTK20000400	FORTINET	FWF-61F	1
11	SD-WAN	FWF61FTK20000304	FORTINET	FWF-61F	1
12	SD-WAN	FWF61FTK20000904	FORTINET	FWF-61F	1
13	SD-WAN	FGT90GTK24003020	FORTINET	FG-90G	1
14	SD-WAN	FGT90GTK24003626	FORTINET	FG-90G	1

Tabla 3: Seriales de la Solución SD-WAN del IGAC

b. El proveedor deberá prestar los servicios de soporte y mantenimientos preventivos y correctivos a que haya lugar durante el plazo del servicio, de acuerdo con lo indicado en el **numeral 3.4** del presente documento.
c. El proveedor debe renovar el licenciamiento, soporte y la garantía de fabricante, cotérmino hasta el 30 de noviembre de 2028 y la entrega de los certificados de renovación de licenciamiento, soporte y garantía.

3.1.4 Renovación de licencia, soporte y garantía del fabricante para Firewall VM16 Cloud Azure

a. El IGAC requiere mantener las características, funcionalidades, seguridad, rendimiento y disponibilidad de la infraestructura tecnológica Cloud en Azure, integrando a la misma, controles de tráfico por medio de una solución de Firewall Perimetral de tipo VM que pueda integrarse a las soluciones de seguridad existente en la entidad e implementarse en Azure.
b. El proveedor deberá incluir el licenciamiento, soporte y garantía de fábrica

cotérmino hasta el 30 de noviembre de 2028 y la entrega de los certificados de renovación de licenciamiento, soporte y garantía.

c. El firewall VM debe cumplir con las siguientes características:

SOLUCIÓN FIREWALL VM16 CLOUD AZURE					
ITEM	**DESCRIPCIÓN**	**NUMERO_SERIAL**	**MARCA**	**MODELO**	**CANTIDAD**
1	Firewall Perimetral VM16 Cloud Azure	FGVM16TM24000442	FORTINET	FGT VM16	1

Tabla 4: Serial de la solución Firewall VM16 Cloud Azure

d. El proveedor deberá prestar los servicios de soporte y mantenimientos preventivos y correctivos a que haya lugar durante el plazo del servicio, de acuerdo con lo indicado en el **numeral 3.4** del presente documento.

3.2 ADQUISICIÓN, UPGRADE TECNOLÓGICO Y/O SUSCRIPCIÓN CON IMPLEMENTACIÓN Y PUESTA EN FUNCIONAMIENTO

3.2.1 Renovación del licenciamiento, soporte y garantía de fabricante con upgrade tecnológico a máquina virtual para la solución de análisis de logs (Fortinalyzer) de la sede principal

a. El proveedor deberá contemplar la renovación con upgrade tecnológico del licenciamiento, suscripciones de seguridad y soporte de fábrica para el dispositivo analizador de logs con el que cuenta la entidad, la cual corresponde a la plataforma Fortianalyzer 400E con el siguiente serial:

ANALIZADOR LOG´s DE LA SEDE PRINCIPAL					
ITEM	**DESCRIPCIÓN**	**NUMERO_SERIAL**	**MARCA**	**MODELO**	**CANTIDAD**
3	Analizador de Logs	FL-4HET321900029	FORTINET	FL-400E	1

Tabla 5: Seriales Solución Analizador Logs Sede principal

b. El proveedor deberá suministrar el Upgrade tecnológico a licenciamiento de Máquina Virtual requeridos para que la solución soporte las siguientes características de desempeño:

- Máquina Virtual compatible de acuerdo con el literal c

- Capacidad de Logs por Día: Mínimo 500 GB/Day Central Logging & Analytics
- FortiCare Premium support
- IOC
- Security Automation Service
- FortiGuard Outbreak Detection Service.

c. La máquina virtual **deberá** ser desplegada sobre la infraestructura de hiperconvergencia y virtualización Nutanix, propiedad de la entidad y ubicada en sus instalaciones (on-premise), la cual opera bajo las siguientes versiones mínimas de software:
   - Acropolis Hypervisor (AHV): el8.nutanix.20230302.102001
   - Acropolis Operating System (AOS): 6.10
   - Foundation: 5.7
   - Licensing: LM.2023.4
   - Nutanix Cluster Check (NCC): 5.1.0

d. El proveedor **será responsable** de garantizar la compatibilidad de la solución con dicha infraestructura y deberá realizar las validaciones técnicas necesarias para asegurar su correcto funcionamiento.

e. El proveedor **debe** realizar la instalación, aprovisionamiento y configuración completa de la máquina virtual, incluyendo todas las tareas necesarias para asegurar el correcto funcionamiento del servicio FortiAnalyzer. Lo anterior incluye, pero no se limita a: la adecuación del sistema operativo, la configuración de red, la integración con la infraestructura existente, la aplicación de parámetros de seguridad, y la validación operativa del servicio. El proveedor deberá garantizar que el servicio quede plenamente operativo, de acuerdo con los requerimientos técnicos y funcionales establecidos por la entidad.

d. La máquina virtual desplegada sobre la plataforma de hiperconvergencia y virtualización de la entidad **debe** ser compatible con la solución de respaldo existente (Veeam Backup), permitiendo la realización de copias de seguridad conforme a los mecanismos implementados por la entidad.

e. El proveedor deberá prestar los servicios de soporte y mantenimientos preventivos y correctivos a que haya lugar durante el plazo del servicio, de acuerdo con lo indicado en el **numeral 3.4** del presente documento.

f. El proveedor debe renovar el licenciamiento, soporte y la garantía de fabricante cotérmino hasta el 30 de noviembre de 2028 y la entrega de los certificados de renovación de licenciamiento, soporte y garantía y del recibo a satisfacción del equipo debidamente instalado, configurado y puesto en funcionamiento dentro de la solución de la entidad.

3.2.2 Adquisición de siete (7) firewall con licenciamiento, soporte y garantía del fabricante para la solución SD_WAN

a. El IGAC requiere complementar la solución SD-WAN, mediante la adquisición de siete (7) firewall que incluyen el licenciamiento, soporte y garantía de fábrica cotérmino hasta el 30 de noviembre de 2028 y la entrega de los certificados de renovación de licenciamiento, soporte y garantía y recibo a satisfacción de los equipos debidamente instalados, configurados y puestos en funcionamiento dentro de la solución SD-WAN de la entidad, y que cumplan con las siguientes características:

CARACTERISTICAS DE FIREWALL PARA ADQUISICIÓN				
ITEM	**DESCRIPCIÓN**	**CARACTERISTICAS**	**MARCA**	**MODELO**
1	SD-WAN	Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	FORTINET	FG-90G

Tabla 6: Características Equipos SD-WAN

b. El proveedor debe contemplar la Instalación, configuración total de la plataforma (Integraciones de seguridad con Firewall, FortiAnalyzer, Fortimanager, VPN SSL, VPN Site to Site, Configuración Perfiles de Seguridad, Integración con SIEM y demás actividades solicitadas por la entidad) y puesta en producción.
c. El proveedor deberá proyectar y entregar toda la documentación generada en las actividades requeridas en este numeral.
d. El proveedor deberá prestar los servicios de soporte y mantenimientos preventivos y correctivos a que haya lugar durante el plazo del servicio, de acuerdo con lo indicado en el numeral 3.4 del presente documento.

3.2.3 Renovación del licenciamiento, soporte y garantía del fabricante con upgrade de características para el FortiSIEM

a. El proveedor debe realizar la renovación del licenciamiento, el soporte y la garantía de fabricante con upgrade incluyendo los IOC (Indicadores de Compromiso) y el incremento de los EPS (Eventos Por Segundo) de 3500

a 7000, cotérmino hasta el 30 de noviembre de 2028 y la entrega de los certificados de renovación de licenciamiento, soporte y garantía y del recibo a satisfacción de los certificados de renovación a nombre del IGAC, bajo las mismas características con que cuenta actualmente la solución, la cual está asociada al serial del dispositivo descrito a continuación:

SOLUCIÓN SIEM					
ITEM	**DESCRIPCIÓN**	**NUMERO_SERIAL**	**MARCA**	**MODELO**	**CANTIDAD**
1	FORTISIEM	FSM2KFT321000058	FORTINET	FSM-2000F	1

Tabla 9: Serial de la Solución SIEM

b. El proveedor deberá asegurar la inclusión de capacidades de detección de Indicadores de compromiso (IOC)
c. El proveedor deberá asegurar en el licenciamiento el incremento de los eventos por segundo EPS de 3500 a 7000
d. El proveedor debe realizar un Assessment de seguridad sobre la solución renovada, actualización, optimización en sus configuraciones (Integraciones con soluciones de seguridad, integración con servidores y aplicaciones con que cuenta la entidad, generación de mínimo cinco (5) casos de uso por tipo de solución integrada (Seguridad, aplicaciones y servidores) y demás actividades requeridas por la entidad) y puesta en producción.
e. El proveedor deberá proyectar y entregar toda la documentación generada en las actividades requeridas en este numeral.
f. El proveedor deberá prestar los servicios de soporte y mantenimientos preventivos y correctivos a que haya lugar durante el plazo del servicio, de acuerdo con lo indicado en el **numeral 3.4** del presente documento.

3.2.4 Suscripción al servicio de acceso seguro – ZTNA epp/atp incluye licenciamiento y soporte del fabricante

a. El control de acceso remoto a los servicios on-premise y cloud con que cuenta la entidad son de vital importancia por cuanto aportan al propósito de mantener la seguridad, rendimiento, disponibilidad y confidencialidad de la infraestructura tecnológica, por lo cual se requiere implementar una solución de Servicios de Acceso Seguro basada en Zero Trust Network Access (ZTNA), que permita validar continuamente la identidad del usuario y el estado del dispositivo antes de permitir el acceso a los recursos.

b. El servicio FortiClient EPP/ATP se requiere para una cantidad de 1500 usuarios, que además incluya licenciamiento y soporte de fábrica de la solución cotérmino hasta el 30 de noviembre de 2028 y la entrega de los certificados de renovación de licenciamiento, soporte y garantía. Y recibo a satisfacción del certificado de la suscripción y soporte a nombre del IGAC y que dicho servicio se encuentre debidamente instalado, configurado y puesto en funcionamiento), cumpliendo con las siguientes características:

ADQUISICIÓN SOLUCIÓN COMO SERVICIO ZTNA RPP/ATP			
ITEM	**DESCRIPCIÓN**	**CARACTERISTICAS**	**CANTIDAD**
1	Control de Acceso Remoto	Subscripción para 1500 Usuarios, con servicios incluidos de (IPS, Web, DNS, SSL, Anti-Malware, ZTNA y soporte Premium.	1
El servicio debe contemplar las siguientes funcionalidades mínimas a. Permitir acceso seguro por aplicación, basado en identidad de usuario, perfil del dispositivo, y cumpliendo de políticas de seguridad, habilitando el cambio de un modelo de confianza implícita a confianza explicita mediante ZTNA. b. Analizar el comportamiento del endpoint y del usuario para detectar comportamientos sospechosos o irregulares y generar alertas por comportamiento malicioso. c. Realizar análisis activo de detección de virus, troyanos y código malicioso. d. Brindar protección en tiempo real contra malware, spyware, ramsomware y amenazas avanzadas. e. Soportar escaneo bajo demanda y programado de archivos, procesos y sistema operativo. f. Habilitar aislamiento automático del endpoint ante detección de amenazas. g. Debe poseer la capacidad de antivirus/antimalware en línea h. Incluir integración con FortiSandbox Cloud para el análisis dinámico de archivos sospechosos. i. La solución debe proveer control de navegación web, incluyendo categorización de sitios, patrones específicos de URL y filtrado de contenido. j. Debe brindar protección de DNS a través del uso de categorías, así de patrones personalizados, también debe reconocer y bloquear conexiones a sitios de Bonet y C&C			

k. Debe proporcionar capacidades de Intrusión Prevention (IPS) para la detección y mitigación de ataques de red. l. Debe permitir la autenticación de usuarios de locales, así como remotos de Active Directory/LDAP, RADIUS. m. Debe brindar capacidades de escaneo de vulnerabilidades del sistema operativo y aplicaciones instaladas en el endpoint. n. Debe soportar conectividad ZTNA a través de auto túneles, como de navegador web

Tabla 10: Especificaciones de Solución como Servicio ZTNA RPP/ATP

c. El proveedor de este servicio deberá contemplar su Instalación, configuración total de la solución entre ellas despliegue y configuración del EMS perfiles y reglas de ZTNA **RPP/ATP** (Integraciones de seguridad con Firewalls, Fortimanager, Fortianalyzer, VPN SSL, VPN Site to Site, Configuración Perfiles de Seguridad, Integración con SIEM , así como automatizaciones requeridas por la entidad).
d. La entidad actualmente cuenta con el servicio de SASE, el cual debe ser completamente desinstalado por el proveedor. Esta desinstalación deberá incluir todos los componentes de las soluciones Fortinet que diere lugar. Asi mismo, el proveedor deberá garantizar que la implementación de la solución de ZTNA no se vea afectada ni tenga interferencia con algún componente de SASE.
   El servicio debe ser implementado en on-premise máquina virtual VM, y será administrado y gestionado por el IGAC. De acuerdo con el literal C.
e. El proveedor deberá proyectar y entregar toda la documentación generada en las actividades requeridas en este numeral.
f. El proveedor deberá prestar los servicios de soporte y mantenimientos preventivos y correctivos a que haya lugar durante el plazo del servicio, de acuerdo con lo indicado en el **numeral 3.4** del presente documento.
g. El proveedor deberá realizar todas las actividades tendientes a implementar, integrar y poner en operación el ZTNA con todas su funcionalidades, para lo cual deberá contemplar todos los conectores, componentes, licenciamiento y software necesario para realizar dicha puesta en operación e integraciones, sin que esto implique costos adicionales para el IGAC.

3.3 Assessment y optimización de la solución

El proveedor dentro de los diez (10) días hábiles siguientes a la firma del acta de inicio, deberá realizar el levantamiento de información para dimensionar y

programar las actividades de ASSESSMENT sobre las soluciones de seguridad perimetral objeto de renovación de este proceso, ver numerales 3.1.1, 3.1.2, 3.1.3, 3.1.4 del presente documento.

El proveedor debe realizar un Assessment de seguridad incluyendo los equipos que hacen parte de la renovación y su integración con los equipos con upgrade tecnológico, los nuevos adquiridos, las nuevas funcionalidades y las necesidades del IGAC, para con la información recolectada proponer si es necesario la reconfiguración total de la solución (Integraciones de seguridad entre Firewall, Fotianalyzer, FortiManager, SIEM, SD-WAN, ZTNA RPP/ATP, VPN SSL, VPN Site to Site, Configuración de Perfiles de Seguridad y demás actividades requeridas), y puesta en producción.

De esta manera, el proveedor deberá analizar, planear y proponer los cambios de las configuraciones de acuerdo con los resultados obtenidos en el Assessment realizado, para lo cual deberá presentar el resultado del Assesment con una propuesta para aprobación del Supervisor del contrato con los ajustes de arquitectura, acciones, configuraciones y demás recomendados para optimizar y fortalecer la solución (hardware, software y configuraciones), las cuales deben estar respaldadas en las recomendaciones del fabricante y mejores prácticas del mercado. Para este efecto, además deberá presentar el Plan y Cronograma de Instalación también para aprobación del supervisor del contrato.

Una vez aprobados los cambios en la configuración por el supervisor del contrato, el proveedor deberá realizar la implementación, configuración, optimización y puesta en funcionamiento de los equipos que hacen parte de las soluciones de seguridad a optimizar o reconfigurar, considerando para el diseño del Plan y Cronograma de instalación, los siguientes aspectos:

a. Realizar los backups previos a las intervenciones sobre la plataforma, verificando el procedimiento de copia de respaldo para la plataforma que integran solución de seguridad a optimizar o reconfigurar.
b. Configurar, afinar y revisar los reportes / logs de la plataforma que integran solución de seguridad a optimizar o reconfigurar.
c. Realizar la puesta en producción de las soluciones, proyección y entrega de la documentación e informes de optimización de configuraciones.
d. Realizar las pruebas de funcionamiento necesarias para garantizar una óptima puesta en marcha.

El proveedor deberá entregar toda la documentación, así como los diagramas topológicos y planos editables bajo formatos de VISIO o Architect o Powerpoint, o cualquier formato estándar de diagramación de arquitectura editable, así como

diagramas de ingeniería de detalle donde se indique como mínimo: Configuración de puertos en la solución de seguridad objeto de este proceso, renovación y adquisición, así como, integración entre plataformas de seguridad que sea requerida por la entidad.

Seis (6) días hábiles luego de finalizada la actividad de configuración y optimización, el proveedor deberá entregar al supervisor del contrato, el INFORME DE ASSESSMENT Y OPTIMIZACIÓN (en formatos editables de office), que consolide las actividades y resultados de la implementación de las recomendaciones del Assessment realizadas, incluyendo como mínimo:

a. Los parámetros de hardware y de software, reglas, así como las configuraciones cuyos valores fueron ajustados o reconfigurados para la optimización de la solución.
b. La arquitectura de la solución implementada.
c. Recomendaciones sobre las plataformas de seguridad objeto del presente proceso.

3.4 SERVICIO DE MANTENIMIENTOS PREVENTIVOS Y CORRECTIVOS

3.4.1 MANTENIMIENTO PREVENTIVO

El proveedor deberá adelantar actividades de mantenimiento preventivo con el fin de minimizar problemas y mantener actualizadas las soluciones de seguridad de propiedad del IGAC objeto de este proceso, las rutinas de mantenimiento deberán realizarse durante la vigencia del servicio contado a partir del recibo a satisfacción de los equipos debidamente instalados, configurados y puestos en funcionamiento.

El proveedor deberá realizar como mínimo dos (2) mantenimientos preventivos durante la vigencia del servicio, así:

a. El primero, un mes contado a partir de la suscripción del acta de inicio, aplicado a los equipos a los que se les renovó el licenciamiento y soporte.
b. El segundo mantenimiento preventivo, según lo acordado con el supervisor del contrato.

Nota: Sin perjuicio de lo anterior, el proveedor deberá aplicar las actualizaciones de versionamiento cada vez que se genere una versión nueva y estable por parte de fabricante, siempre y cuando sea compatible con la plataforma existente en el IGAC, durante la vigencia del servicio.

Durante las visitas de mantenimiento preventivo, el proveedor deberá llevar a cabo todas las labores pertenecientes a este tipo de mantenimiento tales como:

a. Realizar la limpieza general de las partes.
b. Realizar la limpieza física y lógica de los equipos
c. Realizar la revisión de indicadores visuales.
d. Verificar el rendimiento de cada equipo y alarmas.
e. Realizar un análisis de logs de eventos de los equipos
f. Diagnosticar la solución, informando si se hace necesario el cambio de partes deterioradas
g. Aplicar actualizaciones de versionamiento (actualización del software y firmware del hardware a la última versión estable aprobada por el fabricante).
h. Realizar la Instalación de upgrade y parches.
i. Afinar las políticas de protección de las soluciones de seguridad objeto de este proceso, con el fin de validar su correcto funcionamiento.
j. Entregar en un plazo máximo de cinco (5) días hábiles contados a partir de la de la ejecución de la actividad de mantenimiento, los resultados de este en un Informe Técnico, indicando las actividades desarrolladas, las recomendaciones sobre políticas aplicadas y a aplicar a los equipos, considerado una arquitectura de red segura y de acuerdo con las recomendaciones del fabricante y buenas prácticas de la industria.

Para la realización del mantenimiento preventivo, el proveedor debe contar con un equipo de respaldo de características similares, en caso de que sea necesario utilizarlo como contingencia por posibles fallas en alguno de los equipos de la entidad, de tal manera que, durante y después de realizadas las rutinas de mantenimiento, el proveedor deberá mantener en correcta condición de funcionamiento, seguridad y presentación todos los equipos y servicios objeto del presente proceso.

Nota 1: Los servicios de mantenimiento preventivo no generan costo adicional alguno para el IGAC.

3.4.2 MANTENIMIENTO CORRECTIVO

Durante el plazo de vigencia del servicio el proveedor deberá prestar el servicio de mantenimiento correctivo, las veces que sea necesario, en un esquema de atención de 7x24x4 (Siete días a la semana, veinticuatro horas al día, y un tiempo de respuesta máximo de 4 horas).

El proveedor deberá atender la solicitud del supervisor del contrato de diagnosticar la falla presentada y determinar si se requieren repuestos.

En caso de determinarse que un problema no puede ser resuelto dentro de las ocho (8) horas hábiles siguientes, el proveedor deberá reemplazar el elemento averiado con un equipo de su propiedad de características idénticas o superiores y compatible con las soluciones de seguridad objeto de este proceso e instalarlo temporalmente en el sitio por un término máximo de cuarenta y cinco (45) días calendario, mientras se surte el trámite de RMA ante el fabricante, lapso dentro del cual el proveedor deberá dar la solución definitiva. La acción correctiva para dejar la solución de seguridad en perfecto estado de funcionamiento no será en ningún caso superior a los tiempos aquí descritos.

En caso de que el problema o falla a nivel de hardware pueda solucionarse con reemplazo de partes, el proveedor deberá reemplazar la parte por una nueva de iguales o superiores características, sin costo alguno para el IGAC, esto, durante el plazo de ejecución del servicio.

El proveedor debe suministrar las partes nuevas de iguales o superiores características a los originales, nuevos, no remanufacturados, con el fin de garantizar el correcto funcionamiento de las soluciones de seguridad objeto de este proceso, lo cual, no deberán significar costo adicional alguno para el IGAC.

Nota: Tanto los servicios de mantenimiento correctivo, como los repuestos/partes, traslado de equipos requeridos no generan costo adicional alguno para el IGAC.

4. SOPORTE DEL PROVEEDOR

El Servicio de Soporte del Proveedor, debe incluir atención de incidentes y consultas a través de mínimo, los siguientes medios:

- Llamadas telefónicas,
- Correo electrónico,
- Sesiones remotas y,
- Atención en sitio en horario Hábil y No Hábil en horario continuo.

4.1 ATENCIÓN DE INCIDENTES

Los requerimientos de soporte por parte del IGAC al proveedor, se deben atender en sitio y/o remoto durante el período de la garantía, en la modalidad 7x24x4, es decir, los siete días a la semana, veinticuatro horas al día, con un máximo tiempo de respuesta de cuatro (4) horas y tiempo de solución de ocho (8) horas hábiles, a partir de la solicitud del servicio, tras haberse solicitado por el supervisor del contrato o quien este designe, en el tiempo de vigencia del mismo, para los bienes, relacionados con componentes de software y/o firmware, configuración, etc.

El proveedor deberá garantizar que los tickets o solicitudes de soporte, sean registrados, clasificados y asignados según su criticidad, en la herramienta de mesa de ayuda del proveedor, así mismo, que tenga un seguimiento adecuado y cumplan con los esquemas de escalamiento definidos

Nota 1: Este soporte deberá ser suministrado por personal especializado del proveedor y certificado por el fabricante como mínimo en la administración de los dispositivos Fortinet en los dispositivos renovados y adquiridos (FortiGate, SD-WAN (FortiWifi), FortiManager, FortiAnalyzer, FortiSIEM), así como en la solución como Servicio de **ZTNA RPP/ATP**.

Nota 2: El proveedor deberá contactar al fabricante en los casos que sea requerido para que brinde atención del incidente, dentro del rango de tiempo máximo de dos (2) horas calendario para el diagnóstico y dentro de las doce (12) horas calendario para brindar la solución al incidente, por el término de duración del servicio contratado.

Nota 3: En el caso que el proveedor requiera más tiempo para dar la solución al incidente y se necesite dar solución o apoyo con asistencia del fabricante, se deberá sustentar al supervisor del contrato este hecho, y proponer medida(s) de contingencia dentro de los tiempos establecidos por la entidad para brindar solución al requerimiento.

Nota 4: El IGAC deberá tener la capacidad de registrar casos directamente en la plataforma de FortiCare Services y deberá tener la capacidad de hacer seguimiento a los casos puestos por la entidad o por el proveedor.

4.2 ATENCIÓN DE REQUERIMIENTOS

El proveedor, deberá atender y resolver cualquier requerimiento (configuraciones, consultas técnicas, etc), sobre la solución (dispositivos renovados y adquiridos), tanto en el software (configuraciones) como en el hardware, en un esquema de atención 5x8, en los medios definidos.

Nota 1: Este soporte deberá ser suministrado por personal especializado del proveedor y certificado por el fabricante como mínimo en la administración de los dispositivos Fortinet en los dispositivos renovados y adquiridos (FortiGate, SD-WAN (FortiWifi), FortiManager, FortiAnalyzer, FortiSIEM, ZTNA RPP/ATP.),
Nota 2: El proveedor deberá contactar al fabricante en los casos que sea requerido para que brinde atención del requerimiento, dentro del rango de tiempo máximo de dos (8) horas calendario para el diagnóstico y cuarenta (40) horas calendario para brindar la solución al requerimiento, por el término de duración del servicio contratado.

Nota 3: En el caso que el proveedor requiera más tiempo para dar la solución al incidente y se necesite dar solución o apoyo con asistencia del fabricante, se deberá sustentar al supervisor del contrato este hecho, y proponer medida(s) de contingencia dentro de los tiempos establecidos por la entidad para brindar solución al requerimiento.

5. GARANTÍA

El licenciamiento renovado deberá contemplar garantía de partes o totalidad del dispositivo por parte del Fabricante, por cada uno de los dispositivos que conforman la solución de seguridad, ver tablas:

- Tabla 1: Seriales Solución Firewall perimetral Sede principal
- Tabla 2: Seriales Solución Mater/Slave de la **Sede principal**
- Tabla 3: Seriales de la Solución SD-WAN del IGAC
- Tabla 4: Serial de la solución Firewall VM16 Cloud Azure

El licenciamiento deberá contemplar garantía de partes o totalidad del dispositivo por parte del Fabricante, por cada uno de los dispositivos que conforman las soluciones adquiridas o con upgrade tecnológico, ver tablas:

- Tabla 5: Seriales Solución Analizador Logs Sede principal
- Tabla 6: Características Equipos SD-WAN
- Tabla 7: Características Equipos SD-WAN
- Tabla 8: Serial de la Solución SIEM
- Tabla 9: Especificaciones de Solución como Servicio ZTNA RPP/ATP

6. TRANSFERENCIA DE CONOCIMIENTO

El proveedor deberá realizar transferencia de conocimiento en sitio y virtual, a mínimo cuatro (4) participantes definidos por el IGAC, con una intensidad mínima de diez (10) horas sobre el manejo de la plataforma, la cual debe contemplar como minino los siguientes aspectos:

a. Instalación de la solución
b. Configuración de módulos de seguridad
c. Integración de plataformas
d. Funcionamiento de SD-WAN
e. Integraciones y Análisis de logs
f. Comandos e identificación y resolución de fallas comunes
g. Configuración de casos de uso en herramienta FortiSIEM.
h. Configuración perfiles y reglas de ZTNA **RPP/ATP**

La transferencia de conocimiento deberá ser dictada por personal idóneo y certificado y deberá incluir material adecuado para llevar dicha transferencia, el cual será verificado y aprobado por el supervisor del contrato.

El proveedor deberá programar con la Entidad, las fechas y horas en que se adelantará la actividad.

Las actividades de transferencia de conocimiento deberán quedar registradas mediante acta que se deberá anexar y se deberá entregar manuales físicos y digitales de usuario y mantenimiento.

7. RESPONSABILIDAD AMBIENTAL

El proveedor deberá cumplir con las normas y leyes colombianas sobre el medio ambiente (a nivel nacional, regional y local), vigentes durante este contrato. El proveedor deberá en todo momento minimizar el impacto ambiental de cualquier actividad realizada por él en el desarrollo de este contrato, de conformidad con las normas aplicables. El proveedor conoce y acepta que las autoridades competentes nacionales, regionales o locales que tengan jurisdicción sobre el área donde realizará las actividades podrán disponer la suspensión de las actividades objeto de este contrato hasta que el proveedor cumpla con dichas normas y leyes ambientales o subsane los efectos causados por el incumplimiento de dichas normas y leyes, motivo por el cual, asumirá las consecuencias que se deriven frente al contrato cuando la suspensión de las actividades le sea imputable.

Se debe tener presente el cumplimiento de la normatividad ambiental aplicable al tema de baterías de plomo-ácido: Ley 430 de 1998, el Decreto 1220 de 2005 y el Decreto 4741 de 2005.

Así mismo, el proveedor entregará los certificados de disposición final o de aprovechamiento de los RESPEL, en caso de llegar a generarse durante el servicio, también deberá presentar el Plan de Manejo Ambiental, para ello el proveedor deberá considerar que, al momento de realizar el mantenimiento preventivo y correctivo a los equipos y sistemas objeto del presente proceso, se deberá verificar que todo residuo que se genere durante esa actividad se disponga de una manera ambientalmente adecuada, y en caso de generarse residuos de los aparatos eléctricos y electrónicos - RAEE objeto del contrato, estos deben ser gestionados con una empresa que cuente con licencia ambiental para este tipo de residuos.

En consecuencia, el proveedor seleccionado deberá presentar el Plan de Manejo Ambiental donde establezca el plan para el manejo y el proceso detallado de recolección de residuos que se generan durante la prestación del servicio. La vigencia del plan de manejo ambiental no podrá ser inferior a la duración del contrato y deberá como mínimo ejecutarse cada vez que se adelanten las actividades de mantenimiento.

8. PLAN DE CONTINGENCIA Y CONTINUIDAD DE LA PLATAFORMA Y SERVICIOS DE SEGURIDAD PERIMETRAL

El proveedor seleccionado deberá presentar el Plan de Continuidad y Contingencia que permita evidenciar las posibles anomalías que ponen en riesgo la correcta prestación del servicio y que impidan el normal funcionamiento y atención de incidentes de seguridad.

El Plan de Continuidad, se debe centrar en establecer los posibles riesgos que sugiere la prestación de los servicios de actualización, mantenimiento, instalación, configuración y puesta en funcionamiento de equipos y soluciones objeto de presente proceso, así mismo, en gestionar los incidentes, aplicando las medidas correctas para reanudar las operaciones ante posibles fallas, lo anterior, con el objetivo de mantener el rendimiento y la disponibilidad del servicio de misión crítica de la plataforma de seguridad perimetral del IGAC, servicios que pueden fallar antes, durante y después de realizadas las actividades, para este efecto, el plan en mención deberá considerar las mejores prácticas de la industria, las recomendaciones del fabricante y estar alineado con los procesos y procedimientos del IGAC.

9. DOCUMENTOS

9.1 HOJA DE VIDA DE LOS EQUIPOS

Una vez el proveedor concluya las actividades de renovación y/o de mantenimiento de las soluciones de seguridad adquiridas, deberá hacer entrega al supervisor del contrato de las Hojas de Vida de los equipos que integran las soluciones de seguridad.

Las Hojas de vida deben ser actualizadas y presentadas al supervisor del contrato, cada vez que se efectué un mantenimiento preventivo o correctivo junto con el informe de mantenimiento correspondiente.

La hoja de vida del equipo debe presentar como mínimo la siguiente información:

a. Fecha de instalación del equipo.
b. Ubicación.
c. Nombre de equipo y placa.
d. Tipo de equipo.
e. Reemplazo de insumos y partes.
f. Estado de funcionamiento.
g. Fecha próximo mantenimiento.

9.2 OTROS DOCUMENTOS

El proveedor deberá presentar, a la finalización del plazo de ejecución del contrato, los siguientes documentos:

a. Informes de Implementación y/o optimización de las soluciones de seguridad.
b. Manuales de Operación, Mantenimiento y de Configuración.

10. PERSONAL MINIMO REQUERIDO

Se debe garantizar todo el personal profesional y técnico necesario para dar cumplimiento a lo establecido en este documento, en los tiempos y calidad requeridos. Todo el personal dispuesto por el proveedor estará bajo cuenta y riesgo de quien suministra los bienes y presta los servicios solicitados, entendiéndose que no se genera relación laboral alguna por parte de la Entidad con éste ni el personal a su cargo, en consecuencia, tampoco existirá pago de prestaciones sociales ni de ningún tipo de costos distintos al valor acordado, por parte de la Entidad.

Se debe contar con el personal mencionado a continuación, el cual debe cumplir con los requisitos de perfil académico y de experiencia, así como la disponibilidad establecida, no obstante, como ya se mencionó, en caso de que el proveedor,

requiera personal adicional al aquí mencionado, deberá disponer del mismo para cumplir el objeto contractual con la calidad y oportunidad, en cumplimiento de las obligaciones pactadas.

PERSONAL MÍNIMO REQUERIDO PARA LA EJECUCIÓN DEL CONTRATO					
Cantidad	**Cargo a desempeñar**	**Formación Académica**	**Experiencia General mínima solicitada**	**EXPERIENCIA ESPECIFICA**	**Porcentaje de dedicación mínima**
				Como / En:	
1	**Gerente de Servicio**	Ingeniero Electrónico, de Sistemas o de Telecomunicaciones/o afines según lo establecido en su Núcleo Básico de Conocimiento de acuerdo con el SNIES	Experiencia general igual o mayor a seis (6) años, contados a partir de la Expedición de la tarjeta profesional.	Experiencia especifica igual o mayor a cuatro (4) años, como director o Coordinador en contratos de instalación o Implementación o mantenimiento de Sistemas de Seguridad perimetral	30% durante la ejecución del contrato
1	**Ingeniero Implementador (para Assesment)**	Ingeniero Electrónico, de Sistemas o de Telecomunicaciones/o afines según lo establecido en su Núcleo Básico de Conocimiento de acuerdo con el SNIES Certificado por fabricante Fortinet como:	Experiencia general igual o mayor a cuatro (4) años, contados a partir de la Expedición de la tarjeta profesional.	Experiencia específica igual o mayor a tres (3) años, como ingeniero responsable de realizar Assessmnet en sistemas de Seguridad perimetral	100% durante el plazo de realización del Assessment

		• NSE5 o Certified Associate (FCA-Cybersecurity) • **Certified Associate (FCA Cybersecurity)**, con la certificación **Certified Professional (FCP)** con énfasis en almenos una de las siguientes (FCP - FortiAnalyzer Administrator o FCP - FortiClient EMS Administrator o FCP - FortiManager Administrator)			
1	**Ingeniero Implementador**	Ingeniero Electrónico, de Sistemas o de Telecomunicaciones Certificado por fabricante Fortinet como: • NSE 6 o Certified Professional (FCP) o, • NSE 7 o Certified Solution Specialist (FCSS)	Experiencia general igual o mayor a cuatro (4) años, contados a partir de la Expedición de la tarjeta profesional.	Experiencia específica igual o mayor a tres (3) años, como ingeniero responsable de realizar Actividades de Migración, Implementación y puesta en producción de las plataformas Ofertadas	100% durante el plazo de puesta en producción de las soluciones de seguridad perimetral objeto del presente proceso

Nota 1: El personal anteriormente descrito será de carácter obligatorio durante la ejecución del contrato por lo cual, los oferentes lo deberán tener en cuenta y considerarlo en su totalidad al momento de elaborar su oferta económica.

Nota 2: Si el oferente requiere personal adicional al anteriormente mencionado para llevar a cabo las actividades relacionadas con el objeto contractual, este deberá proveerlo sin costo adicional para la entidad.

Nota 3: En caso de ser necesario el cambio del equipo mínimo de trabajo, el proveedor deberá informar previamente al supervisor del contrato y dispondrá de hasta cinco (5) días hábiles para aportar los soportes y las certificaciones del nuevo personal. Durante la ejecución del contrato, solamente se podrá cambiar el equipo mínimo de trabajo, siempre y cuando se cuente con previa autorización y verificación por parte del supervisor del contrato del cumplimiento del perfil requerido.

Nota 4: Todo el personal designado por el proveedor debe cumplir con los lineamientos establecidos por el IGAC en el Manual de Seguridad de la Información, procedimiento, formatos y demás controles que se tengan establecidos.

11. ANALISIS Y MATRIZ DE RIESGOS

Ver Anexo No. 2 – Matriz de Riesgos

12. CLASIFICACIÓN CÓDIGO UNSPSC

Clasificación UNSPSC	Segmento	Familia	Clase	Producto
43233200 Software de seguridad y protección	43 – Difusión de Tecnologías de Información y Telecomunicaciones	4323 - Software	432332 - Software de seguridad y protección	43233200 Software de seguridad y protección
43222500 Equipo de seguridad de red	43 – Difusión de Tecnologías de Información y Telecomunicaciones	4322 – Equipos o Plataformas y accesorios de redes multimedia o de voz y datos	432225 – Equipo de seguridad de red	43222500 Equipo de seguridad de red

81111801	81 – Servicios Basados en ingeniería, investigación y Tecnología	8111 – Servicios informáticos	811118 - Servicios de sistemas y administración de componentes de sistemas	81111801 Seguridad de los computadores, redes o internet
81112200	81 – Servicios Basados en ingeniería, investigación y Tecnología	8111 – Servicios informáticos	811122 - Mantenimiento y soporte de software	81112200 Mantenimiento y soporte de software

ROBERTO CARLOS PANTOJA BENITEZ
SUBDIRECTOR DE INFRAESTRUCTURA TECNOLÓGICA (E)

Proyección	**Revisión**
Firma: JUAN GABRIEL TELLEZ	Firma:
Juan Gabriel Téllez Gallegos	Karen Viviana Gutiérrez García
Cargo: Contratista Subdirección de Infraestructura Tecnología	Cargo: Contratista
Dependencia: Subdirección de Infraestructura Tecnológica - DTIC	Dependencia: Subdirección de Infraestructura Tecnológica - DTIC

Revisión	**Revisión**
Firma:	Firma: Viviana A. Navarrete R.
Carlos Arturo Abril Triviño	Viviana Astrid Navarrete Ramírez
Cargo: Contratista DTIC	Cargo: Contratista DTIC
Dependencia: Subdirección de Infraestructura Tecnológica	Dependencia: Dirección de Tecnologías de la Información y Comunicaciones