FIDUCIARIA CENTRAL S.A.

INVITACIÓN PÚBLICA

FECHA DE APERTURA:

10/12/2026

FECHA DE CIERRE:

22/12/2025

HORA DE CIERRE:

04:30 P.M.

ENTREGA DE LAS PROPUESTAS: Carlos.SanchezR@fiducentral.com - valeria.marconi@fiducentral.com

OBJETO: SERVICIO DE OUTSOURCING PARA LA IMPLEMENTACIÓN DE UNA SOLUCIÓN INTEGRAL DE SEGURIDAD Y GESTIÓN DE RED, CONFORMADA POR SWITCHES ADMINISTRABLES, SERVICIO DE ANÁLISIS Y MONITOREO, APPLIANCES DE SEGURIDAD PARA LA FIDUCIARIA CENTRAL

BOGOTA D. C., DICIEMBRE DE 2025

CAPÍTULO I

CONDICIONES GENERALES

1.1. NATURALEZA JURÍDICA FIDUCIARIA CENTRAL S.A.

FIDUCIARIA CENTRAL S.A. es una sociedad de economía mixta constituida bajo la forma de sociedad anónima, con aportes estatales y de capital privado, de carácter indirecto y del orden territorial, sometida al régimen de las empresas industriales y comerciales del Estado de acuerdo con el parágrafo del artículo 97 de la Ley 489 de 1998; el giro ordinario de sus negocios se rige por el derecho privado, particularmente por las disposiciones legales y reglamentarias aplicables a las actividades económicas y comerciales propias de las sociedades de servicios financieros y en especial de las sociedades fiduciarias, sometida al control y vigilancia de la Superintendencia Financiera de Colombia.

1.2. RÉGIMEN JURÍDICO APLICABLE

El presente proceso de contratación así como el contrato a suscribirse se encuentran sujetos a la legislación y jurisdicción colombiana y se rigen por el régimen especial de contratación, según como se preceptúa en los artículos 13 y 15 de la ley 1150 de 2007; igualmente este proceso está sometido a los principios de la función estatal, preceptuados por el artículo 209 de la Constitución Política, al Régimen de Inhabilidades e Incompatibilidades previstas en el artículo 8 de la Ley 80 de 1993, artículo 18 de la Ley 1150 de 2007, artículos 1° y 4° de la Ley 1474 de 2011, al Manual de Contratación de la Fiduciaria y demás normas concordantes.

1.3. NECESIDAD DEL SERVICIO

Con el fin de dar cumplimiento a las recomendaciones emitidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), así como a los lineamientos establecidos en la norma ISO 27001:2022, la guía de implementación ISO 27002:2022, el marco de referencia COBIT 2019 para el gobierno de datos, y la normatividad vigente expedida por la Superintendencia Financiera de Colombia, la Fiduciaria requiere fortalecer su infraestructura tecnológica para garantizar la correcta operación del negocio, la ejecución del plan de recuperación ante desastres (DRP) y el cumplimiento de los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad.

En este sentido, la Fiduciaria requiere la contratación de una solución integral de seguridad y gestión de red, que contemple los siguientes componentes configurados en Alta Disponibilidad: Firewall de próxima generación (NGFW), que brinde protección avanzada, inspección profunda de paquetes, segmentación de red y control de aplicaciones. Switches administrables, que permitan una gestión centralizada, segura y eficiente de la red de datos, con capacidad de monitoreo, segmentación y optimización del tráfico. Servicio de análisis y monitoreo (Analyzer), orientado a la recolección, correlación y visualización de eventos de red, para fortalecer la detección temprana de incidentes y la toma de decisiones en materia de ciberseguridad.

1.4. SITUACIÓN ACTUAL

En la actualidad **FIDUCIARIA CENTRAL S.A.** cuenta un contrato de outsourcing encargado de la seguridad perimetral de la sede Bogotá garantizando los servicios profesionales de instalación, configuración, migración de políticas y puesta en funcionamiento de dos firewall Fortinet 120g en configuración HA para garantizar la seguridad perimetral, monitoreo y disponibilidad de la infraestructura tecnológica que soporta los accesos a: servidores, aplicaciones, control de navegación, IPS, IDS, servicios de conectividad con la BVC y Deceval, portales bancarios, segmentación de las redes LAN y WAN y demás servicios que estén configurados en Fiducentral, adicionalmente prestar los servicios de soporte técnico, mantenimiento preventivo y gestión de incidentes de seguridad perimetral, los cuales son identificados mediante el monitoreo 7x24 que ejecuta el proveedor. La principales características del servicio son:

- ✓ **Sistema de prevención contra intrusiones de última generación**.
- ✓ **Protección contra amenazas avanzadas.**
- ✓ **Security Heartbeat.**
- ✓ **Tecnologías VPN avanzadas.**
- ✓ **Políticas web potentes para grupos y usuarios.**
- ✓ **Protección avanzada contra amenazas web.**
- ✓ **Proxy transparente de alto rendimiento.**
- ✓ **Calidad de servicio y control de aplicaciones de nivel 8.**

1.5. OBJETIVO

FIDUCIARIA CENTRAL S.A. adelanta la presente invitación con el fin de contratar, bajo la modalidad outsourcing con opción de compra, los servicios profesionales para el suministro, implementación y administración de una solución integral de seguridad y gestión de red, conformada por dos (2) equipos Next Generation Firewall Fortinet nuevos y de última generación, así como la infraestructura de comunicaciones dos (2) Switches de Core configurados en alta disponibilidad y de seis (6) switches de acceso, junto con los servicios de instalación, configuración, puesta en funcionamiento, administración, gestión y soporte de toda la plataforma de seguridad perimetral y un servicio de análisis y monitoreo (Analyzer). Este proyecto tiene como propósito fortalecer la infraestructura tecnológica en cumplimiento de las recomendaciones del MinTIC, las normas ISO 27001:2022 y 27002:2022, el marco COBIT 2019 y la normatividad de la Superintendencia Financiera de Colombia, asegurando la integridad, disponibilidad y confidencialidad de la información, así como la continuidad y correcta operación del negocio.

1.6. OBJETIVOS ESPECIFICOS

El proveedor debe estar en la capacidad de proveer los siguientes servicios tecnológicos:

1. **SOLUCION DE FIREWALL DE NUEVA GENERACIÓN EN ALTA DISPONIBILIDAD**
2. **ACCESO SEGURO PARA REDES LAN**
3. **SERVICIOS PROFESIONALES Y DE SOPORTE**

1. SOLUCION DE FIREWALL DE NUEVA GENERACIÓN EN ALTA DISPONIBILIDAD

El firewall NGFW deberá incluir de manera nativa y estar habilitadas para su uso inmediato todas las funcionalidades descritas en el presente documento, operando en una configuración de Alta Disponibilidad (HA) que garantice plena compatibilidad entre los equipos, continuidad operativa de los servicios y una gestión centralizada, eficiente y segura de la infraestructura perimetral.

Descripción General

Suministrar dos (2) appliance como solución de seguridad perimetral con sistema operativo propietario del fabricante, correspondiente a un Firewall de Nueva Generación (NGFW). El equipo deberá incluir de manera nativa y estar habilitadas para su uso inmediato todas las funcionalidades descritas en el presente documento.

La solución de seguridad perimetral deberá soportar y entregarse funcionando en configuración de Alta Disponibilidad (HA), esta integración deberá garantizar plena compatibilidad, asegurar la continuidad operativa de los servicios y permitir una gestión centralizada, eficiente y segura de la infraestructura perimetral, suministrando equipos de propósito específico, no se aceptan implementaciones en sistemas de propósito general como PC o servidor, usando sistemas operativos genéricos como Windows, Linux, Solaris, Apple MacOS o GNU.

- ✓ Ninguno de los modelos entregados podrá estar listado en el site del fabricante como End of Life (EoL), End of Sale y End of Support (EoS).
- ✓ Equipos nuevos de fábrica; no se aceptarán equipos remanufacturados o reparados.
- ✓ Debe ser la última versión disponible del fabricante.
- ✓ Debe soportar e incluir todas las funcionalidades del equipo.

Características de la solución

- ✓ Debe contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de tráfico.
- ✓ Debe soportar e incluir las funcionalidades de: Firewall, IPS, Control de Aplicaciones, Filtrado Web, Antivirus perimetral, SDWAN.
- ✓ La solución deberá contar con Fuente de poder redundante incluida en la oferta no por separado.

- ✓ Debe estar configurada y en la capacidad de soportar alta disponibilidad.
- ✓ Deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad podrá dar seguimiento a los casos abiertos por el oferente.
- ✓ Deberá proporcionar una cuenta de acceso al portal oficial de educación del fabricante, donde la Entidad podrá acceder, de manera gratuita y a demanda, a cursos en línea sobre las diversas tecnologías del fabricante.
- ✓ El fabricante debe estar catalogado como líder en el último reporte de Hybrid Mesh Firewall en Gartner
- ✓ El fabricante debe estar catalogado como líder en el último reporte de SD-WAN en Gartner.

Rendimiento

El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:

- ✓ Rendimiento de Firewall de al menos 39 Gbps o superior
- ✓ Rendimiento de IPS de al menos 9 Gbps o superior
- ✓ Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) de al menos 7 Gbps o superior
- ✓ Rendimiento Protección de amenazas de al menos 6 Gbps o superior
- ✓ Rendimiento IPSec VPN de al menos 35 Gbps o superior
- ✓ Soporte de 11 Millones sesiones concurrentes o superior
- ✓ Rendimiento de Inspección SSL de al menos 7 Gbps o superior
- ✓ Soporte de 500 usuarios VPN SSL o superior
- ✓ Rendimiento de VPN SSL de al menos 2.8 Gbps o superior

Conectividad

Los equipos que hacen parte de la solución de seguridad perimetral deberán contar con las siguientes interfaces de conexión

- ✓ 1 puerto de consola (Administración)
- ✓ 2x RJ45 HA/Management Ports
- ✓ 8x GE RJ45 Ports
- ✓ 8 x 5/2.5/GE RJ45 Ports
- ✓ 8 x 10 GE SFP+/SFP
- ✓ 4 x GE SFP Slots

Address Traslation

Los equipos que hacen parte de la solución de seguridad perimetral deberán soportar e incluir los siguientes tipos de traducción de direcciones:

- ✓ NAT y PAT
- ✓ NAT estático
- ✓ NAT: destino, origen
- ✓ NAT, NAT64 persistente

Funciones básicas de Firewall

El NGFW debe incluir la capacidad de operar en los siguientes modos:

- ✓ Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- ✓ La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo con el grupo de pertenencia de los usuarios.
- ✓ Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada
- ✓ Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS, Azure, Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP, TAG etc) de las instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall
- ✓ Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface) como por GUI (Graphical User Interface).
- ✓ La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP
- ✓ El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces
- ✓ El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.
- ✓ Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis.
- ✓ El equipo firewall debe permitir limitar el número de dispositivos asociados a un mismo invitado.
- ✓ Debe soportar e incluir la identificación de dispositivos y sistemas operativos, con clasificación automática, y permitir la visualización de esta información.
- ✓ Soporte de reglas basadas en servicios cloud populares de Internet, en donde se tiene una base de datos que se actualiza dinámicamente. Esta base de datos puede usarse también en enrutamiento y balanceo de enlaces o SD-WAN.
- ✓ Permitir almacenar localmente versiones de configuración despues de acceder al equipo, y permitir hacer rollback a una configuración anterior en caso de ser necesario. Debe ser posible comparar dos versiones de configuración para per las diferencias entre las mismas, en la GUI del Firewall. El histórico de versiones de configuración debe ser visible tanto por GUI como por CLI.
- ✓ La solución de firewall deberá permitir la visibilidad de la red a través de una interfaz simple, flexible y de acceso vía web. Deberá estar en capacidad de almacenar un historial detallado de atributos de todos los puntos finales que se conectan a la red, usuarios (incluidos tipos como invitados, empleados, contratistas, etc.) en la red hasta los detalles de la aplicación de punto final.

Conectividad y Enrutamiento

- ✓ Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.
- ✓ Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
- ✓ Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP
- ✓ La solución podrá habilitar políticas de ruteo en IPv6
- ✓ La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6.
- ✓ El dispositivo debe realizar balanceo de carga de enlaces mediante el uso de los siguientes algoritmos:
  - Ancho de banda
  - Sesiones
  - Spillover
  - IP fuente – destino
  - IP fuente
- ✓ La Solución deberá soportar e incluir el balanceo de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en: Aplicaciones Cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes)

VPN IPSEC

El NGFW debe deberá soportar las siguientes características:

- ✓ Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
- ✓ Soporte para IKEv2 y IKE Configuration Method.
- ✓ Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES
- ✓ Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits
- ✓ Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN client-to-site.
- ✓ Se deben soportar VPNs basadas en rutas y VPNs basadas en políticas.

VPN SSL

- ✓ Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.
- ✓ Soporte a SSL 2.0 y 3.0, TLS 1.0,1.1 y 1.2
- ✓ Soporte para modo de operación basado en web o modo túnel.
- ✓ Debe soportar Split Tunel, de tal forma que el tráfico hacia internet no se enrute por la VPN
- ✓ Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- ✓ Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.
- ✓ Capacidad de realizar SSL VPNs por usuarios sin incurrir en costos adicionales.
- ✓ Soporte a certificados PKI X.509 para construcción de VPNs SSL.

- ✓ Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
- ✓ Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL
- ✓ Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo con el grupo de pertenencia de dichos usuarios.

Autenticación

El NGFW deberá manejar los siguientes tipos de autenticación:

- ✓ Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS, LDAP o TACACS+.
- ✓ Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On".
- ✓ Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID.
- ✓ Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo.
- ✓ Capacidad de realizar 2FA mediante tokens que se integren a la plataforma.
- ✓ Debe estar en capacidad de proporcionar autenticación fuerte por medio de software token para al menos los siguientes entornos: A. Portales Web de la Entidad. B. VPNs IPSec y SSL Actuales de la Entidad. C. Logon de estaciones Windows.
- ✓ Debe estar en capacidad de administrar switches y Access point para servir como plataforma de una red Secure SD-LAN.
- ✓ La solución debe estar en capacidad de integrarse con el Directorio Activo de la entidad
- ✓ 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.
- ✓ Debe soportar la identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server.

Manejo de tráfico y calidad de servicio.

- ✓ Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix, por ejemplo), se requiere que la solución incluya la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones.
- ✓ El NGFW debe soportar e incluir traffic shaper basado en fuente (dirección IP, usuarios locales y grupos), destino (dirección IP, FQDN, URL o categoría), servicio (General, acceso web, acceso a archivos, servicios de correo y red, autenticación, acceso remoto, tunneling, VoIP, mensajería y otras aplicaciones, web proxy), aplicación, categoría de aplicaciones, categoría de URLs.

- ✓ Capacidad de poder asignar parámetros de traffic shapping a través de reglas de manera independiente
- ✓ Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión
- ✓ Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación y categoría URL de las mismas para la regla en general.
- ✓ Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo

Antimalware

- ✓ Debe soportar e incluir granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, 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.
- ✓ Capacidad de realizar filtrado por interceptación de tráfico DNS Sinkhole para el bloqueo de tráfico hacia dominios maliciosos.
- ✓ El IPS debe tener la posibilidad de tomar las siguientes acciones: permitir, monitorear, bloquear, resetear la sesión, guardar copia de los paquetes que coincidan con las firmas, hacer cuarentena con base en dirección IP del atacante y tiempo basado en días, horas o minutos
- ✓ Debe estar en capacidad de detener más de 11000 amenazas, incluyendo evasiones.
- ✓ El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.
- ✓ El antivirus deberá escanear tráfico de compartición de archivos: CIFS, SMB y SAMBA.
- ✓ La solución debe incluir mecanismos para detectar y detener conexiones a redes Botnet y servidores C&C.
- ✓ Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP, MAPI
- ✓ El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deberán ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma.
- ✓ Debe soportar la inspección de archivos comprimidos como los son: GZIP, RAR, LZH, IHA, CAB, ARJ; ZIP entre otros con el fin de proteger contra estas técnicas de evasión.
- ✓ El Antivirus deberá integrarse de forma nativa con una solución sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis.

Filtrado WEB

- ✓ Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 78 categorías y por lo menos 47 millones de sitios web en la base de datos.
- ✓ Debe poder categorizar contenido Web requerido mediante Ipv6.
- ✓ Será posible exceptuar la inspección de HTTPS por categoría.
- ✓ Debe contar con la capacidad de bloquear contenido de youtube usando el Channel ID
- ✓ El firewall deberá contar con bloquea de dominios asociados con phishing, malware, botnets y otras categorías de alto riesgo (criptominería, dominios recién vistos, etc.)
- ✓ Debe permitir notificar al usuario, mostrándole solo una página de alerta.
- ✓ El filtrado debe ser sobre tráfico http y https.

Protección contra intrusos (IPS)

- ✓ El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en SPAN o MIRROR.
- ✓ Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico Ipv6. A través de sensores.
- ✓ Capacidad de detección de más de 7000 ataques.
- ✓ El sistema de detección y prevención de intrusos deberá estar integrado a la plataforma de seguridad ***"appliance"***. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.
- ✓ Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.

Control de Aplicaciones

- ✓ La solución debe soportar e incluir la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
- ✓ 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, Browser Based, Network Protocol).
  - Nivel de riesgo de las aplicaciones.
  - Categoría y sub-categoría de aplicaciones.
- ✓ La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
- ✓ La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante.

- ✓ Reconocer por lo menos 4000 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, email.
- ✓ Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión
- ✓ Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.

Inspección de Contenido SSL/SSH

- ✓ La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura
- ✓ Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad.
- ✓ La inspección deberá realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection.

Alta Disponibilidad

- ✓ El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6.
- ✓ Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico.
- ✓ Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces.
- ✓ La configuración en alta disponibilidad debe sincronizar: Sesiones; Certificados de descifrado, Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red.
- ✓ El equipo debe soportar mínimo 2 equipos en esquema de HA.
- ✓ Debe incluir doble fuente.
- ✓ Debe tener máximo 2 unidad de Rack por equipo.

Visibilidad

- ✓ La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional.
- ✓ El sistema deberá contar con una gestión centralizada que permita la configuración, el registro, la supervisión e informes de eventos.
- ✓ Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma.

Características de Administración

- ✓ Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS)
- ✓ Interfaz basada en línea de comando (CLI) para administración de la solución.
- ✓ Debe permitir exportar las reglas de seguridad en al menos dos de los siguientes formatos: CSV, JSON y PDF
- ✓ Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos
- ✓ La solución de firewall deberá permitir la creación de políticas y ver informes por usuario (Directorio Activo), red (por IP), dispositivo de red, subred interna.
- ✓ Debe tener la capacidad de gestionar todas las políticas de seguridad, además de poder gestionar Switches y APs dentro de una única consola de gestión.
- ✓ Debe estar en capacidad de administrar switches y Access point para generar una red SD-LAN administrada y gestionada desde el mismo Firewall.

Virtualización

- ✓ El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains"
- ✓ Debe soportar e incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer.
- ✓ Cada instancia virtual debe poder tener un administrador independiente
- ✓ Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red
- ✓ Se debe poder ver el consumo de CPU y memoria de cada instancia virtual.

Licenciamiento y actualizaciones

- ✓ El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.
- ✓ La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos doce (12) o veinticuatro (24) meses, según sea la necesidad de FIDUCIARIA CENTRAL S.AS.
- ✓ La plataforma es requerida por un periodo de doce (12) o veinticuatro (24) meses, según sea la necesidad de FIDUCIARIA CENTRAL S.AS. en un esquema de soporte 7x24 ante el fabricante.

2. ACCESO SEGURO PARA REDES LAN

La solución de Firewall de nueva generación en alta disponibilidad debe incluir 2 Switches capa 2/3 de 48 puertos POE, no se aceptarán soluciones OEM. El Hardware y Software deberán ser fabricados

y/o ensamblados por la misma marca y el fabricante debe estar en el cuadrante de lideres de Gartner para soluciones empresariales LAN/WLAN del último año publicado.

Descripción General

El proveedor de servicios debe implementar switches de última generación que garanticen seguridad, facilidad de gestión e integración con la infraestructura de seguridad perimetral, permitiendo una administración centralizada de red y seguridad en un solo punto de control.

Debe Integrarse de manera nativa con la infraestructura de seguridad perimetral Firewall, de forma que actúen como una extensión lógica del firewall corporativo, permitiendo que éste gestione directamente las funcionalidades de los switches, incluyendo su configuración, monitoreo y la aplicación de políticas de seguridad en el Switch.

Para garantizar la protección de inversión, alineación con las tendencias tecnológicas de la industria, soporte y vigencia tecnológica y estar preparados para los requerimientos futuros, los equipos de comunicación ofertados deben corresponder a una marca o fabricante que figure como líder en el cuadrante de Cuadrante Mágico Gartner para soluciones de LAN inalámbrica y cableada empresarial en su último reporte realizado.

No se aceptarán soluciones OEM. El Hardware y Software deberán ser fabricados y/o ensamblados por la misma marca.

Equipos nuevos de fábrica. No se aceptarán equipos remanufacturados o reparados.

La solución deberá ser licenciada con soporte y garantía ante el fabricante por dos (2) años con Equipos nuevos de fábrica, no se aceptarán equipos remanufacturados o reparados.

Capacidades específicas de los Switches de Distribución y/o CORE

Número de puertos: 48 puertos distribuidos así:

- ✓ 32x 1GE/2.5GE RJ45
- ✓ 16x 1GE/2.5GE/5GE RJ45
- ✓ 8X1GE/10/GE/25GE SFP/SFP+/SFP28 ports
- ✓ 1x Dedicated Management 10/100/1000 Ports
- ✓ 1x RJ-45 Serial Console Port
- ✓ Debe ser máximo de 1 Unidad de rack EIA estándar de 19 in.
- ✓ Capacidad de Conmutación >= 720 Gbps
- ✓ Capacidad de transmisión de Paquetes Throughput >=1071 Mpps
- ✓ Latencia <= 1 Microseg
- ✓ Packet buffer minimo de 8MB
- ✓ Memory 4GB
- ✓ Garantía limitada de por vida (5 años después de fin de venta)
- ✓ Administración mediante consola para CLI (Command Line Interface)

- ✓ No se admiten equipos de línea small business: equipos cuya administración sea únicamente a través de http / https
- ✓ Debe contar con fuente de poder redundante
- ✓ MAC address Storage >= 64.000
- ✓ Instancias de spanning tree minimo 64
- ✓ Enrutamiento: 300K rutas IPv4 | 75K rutas IPv6
- ✓ La solución Switches de Core y/o Distribución ofertada debe ser de la misma marca de la solución de Seguridad de firewall perimetral y se deben poder administrar a través del dispositivo de seguridad perimetral.
- ✓ El switch debe permitir descargar políticas de seguridad desde el firewall perimetral.
- ✓ Se debe poder administrar los Switches a través del Firewall dejando así una única consola de administración.
- ✓ Debe permitir la autenticación y autorización Local RADIUS y TACACS+.
- ✓ Debe soportar SSH.
- ✓ Debe soportar DHCP snooping, Dynamic ARP.
- ✓ MTBF 10 Años
- ✓ 8 Transceiver module 10 GE SFP+ LC connector

Generalidades Switches de acceso

El servicio debe incluir 6 Switches capa 2/3 de 48 puertos POE

- ✓ No se aceptarán soluciones OEM. El Hardware y Software deberán ser fabricados y/o ensamblados por la misma marca.
- ✓ El fabricante debe estar en el cuadrante de lideres de Gartner para soluciones empresariales LAN/WLAN del último año publicado.
- ✓ Implementar switches de última generación que garanticen seguridad, facilidad de gestión e integración con la infraestructura de seguridad perimetral, permitiendo una administración centralizada de red y seguridad en un solo punto de control.
- ✓ Integrarse de manera nativa con la infraestructura de seguridad perimetral Firewall, de forma que actúen como una extensión lógica del firewall corporativo, permitiendo que éste gestione directamente las funcionalidades de los switches, incluyendo su configuración, monitoreo y la aplicación de políticas de seguridad en el acceso.
- ✓ La solución deberá ser licenciada con soporte y garantía ante el fabricante por un (2) años
- ✓ Equipos nuevos de fábrica.
- ✓ No se aceptarán equipos remanufacturados o reparados

Capacidades específicas de los Switches de Acceso

Los Switches de acceso deben contar con 48 puertos distribuidos así:

- ✓ 48x GE RJ45 POE
- ✓ 4x 10GE SFP+ ports
- ✓ 1X Dedicated Management 10/100 Port

- ✓ 1X RJ-45 Serial Console Port
- ✓ Debe ser máximo de 1 Unidad de rack
- ✓ Capacidad de Conmutación >= 176 Gbps
- ✓ Capacidad de transmisión de Paquetes Throughput >=262 Mpps
- ✓ latencia <= 1 Microseg
- ✓ Debe contar con fuente de poder redundante
- ✓ Packet buffer mínimo de 4MB
- ✓ Memory 1GB
- ✓ Garantía limitada de por vida
- ✓ Administración mediante consola para CLI (Command Line Interface)
- ✓ No se admiten equipos de línea small business: equipos cuya administración sea únicamente a través de http / https
- ✓ MAC address storage>= 32K
- ✓ Instancias de spanning tree mínimo: 32

Soportar Enrutamiento

- ✓ 16K rutas IPv4
- ✓ 8K rutas IPv6
- ✓ La solución Switches de Core y/o distribución ofertada debe ser de la misma marca de la solución de Seguridad de firewall perimetral y se deben poder administrar a través del dispositivo de seguridad perimetral.
- ✓ El switch debe permitir descargar políticas de seguridad desde el firewall perimetral.
- ✓ Se debe poder administrar los Switches a través del Firewall dejando así una única consola de administración.
- ✓ Debe permitir la autenticación y autorización Local RADIUS y TACACS+
- ✓ Debe soportar SSH
- ✓ Debe soportar DHCP snooping, Dynamic ARP
- ✓ 10 Transceiver module 10 GE SFP+ LC connector

PLATAFORMA DE GESTIÓN DE LOGS Y REPORTES

Se requiere que la solución de seguridad perimetral cuente con una solución de analítica, registro y correlación de eventos de seguridad en formato Virtual Machine (VM), con capacidad de recolección de hasta 10 GB de logs diarios, incluyendo soporte especializado 24x7 y un asistente de inteligencia artificial para el análisis e investigación de incidentes.

La solución deberá integrarse con la plataforma de seguridad perimetral de manera nativa, permitiendo el almacenamiento, correlación, visualización y generación de reportes de eventos de seguridad, conforme a las mejores prácticas de monitoreo cumpliendo con las siguientes condiciones:

- ✓ Registrar y analizar todos los logs generados por los dispositivos de seguridad (firewall).
- ✓ Generar reportes personalizables y programables.
- ✓ Operar bajo licenciamiento escalable (capacidad de 10 GB/día con posibilidad de ampliación).

- ✓ Licenciamiento por suscripción a doce (12) o veinticuatro (24) meses, según sea la necesidad de FIDUCIARIA CENTRAL S.AS., con opción de crecimiento modular.
- ✓ Capacidad diaria de logs: 10 GB/día mínimo.
- ✓ Compatibilidad de hipervisores: VMware, Hyper-V, KVM, Citrix Xen, Nutanix AHV, Oracle Virtualización o equivalentes.
- ✓ Consola centralizada con dashboards personalizables.
- ✓ Visor de tráfico en tiempo real e histórico.
- ✓ Búsqueda avanzada sobre logs (por IP, usuario, aplicación, evento).
- ✓ Reportes predefinidos y personalizados.
- ✓ Paneles ejecutivos e informes técnicos automatizados.
- ✓ Asistente virtual de IA con capacidad para consultas en lenguaje natural.
- ✓ Eventos del sistema y auditoría.
- ✓ Reportes de tráfico, ancho de banda y uso web.
- ✓ Informes de VPN y accesos remotos.
- ✓ Integración con repositorios de IOC y Outbreak Detection Service.
- ✓ Los recursos de cómputo serán suministrados por Fiduciaria Central S. A.

3. SERVICIOS PROFESIONALES Y DE SOPORTE

Generalidades

El proveedor debe asignar un ingeniero remoto exclusivo para la administración de la solución de seguridad Perimetral en la modalidad 5x8

El proveedor deberá implementar solución de seguridad perimetral en los sitio indicado por la entidad.

El ingeniero deberá presentar informes semanales sobre los hallazgos en las plataformas y su acción ante ellas.

Instalación, Implementación, configuración y puesta en marcha de las soluciones de seguridad y conectividad ofertadas.

El proveedor deberá realizar la instalación y configuración de los equipos con personal certificado por el fabricante con el cual se esté presentando.

Todas las plataformas deben ser de propósito específico y nuevas, no se aceptan soluciones genéricas ni remanufacturadas.

El proveedor deberá presentar certificación de distribuidor autorizado del fabricante donde se evidencie que tiene el nivel de membresía más alto o ser categoría **EXPERT**. Lo anterior con el fin de garantizar la experiencia en la implementación de las soluciones que requiere la entidad. Esta certificación debe ser dirigida a la Entidad, especificando el número del proceso y objeto del mismo, con una vigencia no mayor a 30 días.

El proveedor deberá presentar dentro de la certificación de distribuidor autorizado del fabricante que cuenta y posee la categoría de **Engage Tech Support Partner**, lo que garantiza que cuenta y dispone con los recursos técnicos de fabricante para la implementación de las soluciones.

El proveedor deberá presentar al menos cinco especialidades técnicas del mismo fabricante con el cual se está presentando, dentro de la cuales son obligatorias **Secure Networking Firewall, Security Operations, SD-WAN y Secure Networking LAN**.

En caso de uniones temporales y/o consorcios cada uno de los integrantes deberá aportar las certificaciones mencionadas en los requerimientos anteriores, con los mismos criterios y alcances mínimos establecidos para cada integrante del consorcio, no se realizará sumatoria y/o validación de tiempos de vigencia de las certificaciones para cumplir lo establecido.

El proveedor debe entregar junto con la propuesta una certificación emitida directamente de los fabricantes de las soluciones ofertadas donde se evidencie que los equipos suministrados no se encuentran en fin de venta y contaran con extensión de soporte por mínimo 5 años, estas cartas deben ser dirigidas a la Entidad, especificando el número del proceso y objeto del mismo. Con una vigencia no mayor a 30 días.

El proveedor debe entregar los documentos técnicos y/o datasheet del fabricante de las soluciones ofertadas, donde se evidencie el cumplimiento de cada uno de los ítems solicitados en los requerimientos técnicos de las soluciones.

El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil por el tiempo contratado.

Implementación y puesta en marcha solución de seguridad perimetral

La implementación deberá contemplar como mínimo:

- ✓ Planeación de cada una de las actividades, validadas en conjunto con la entidad.
- ✓ Configuración y alistamiento del software y firmware del hardware a la última versión estable aprobada por el fabricante para todas las plataformas.
- ✓ Afinamiento y estabilización de las plataformas.
- ✓ Pruebas de Servicio de las plataformas.
- ✓ Entrega de las plataformas a satisfacción de la entidad.
- ✓ Las actividades de afinamiento de las plataformas deberán ser realizadas por personal certificado por el fabricante.
- ✓ La entidad requiere que se realicen pruebas / muestras de las plataformas donde se evidencie la correcta configuración y afinamiento de la plataforma.
- ✓ Organizar 400 puntos de red aproximadamente del rack con su respectivo marquillado.

Soporte solución de seguridad perimetral

El proveedor deberá garantizar un servicio de soporte de Niveles I, II y III para administración y gestión de incidentes, soporte a fallas y garantía para las plataformas ofertadas, en un esquema de 7 días x 24 horas, por la vigencia del contrato, con soporte remoto o en sitio en caso de requerirse.

El soporte deberá contemplar como mínimo:

- ✓ Atención de incidentes sobre las plataformas ofertadas.
- ✓ Consultas a través de llamadas telefónicas, correo electrónico.
- ✓ Sesiones remotas y atención en sitio (En caso de requerirse) en horario Hábil y No Hábil.
- ✓ Todo con respecto a la solución de seguridad perimetral, las plataformas ofertadas y objeto del contrato.

El proveedor deberá realizar y documentar entre otras, las siguientes actividades previa coordinación con el supervisor del contrato en desarrollo:

- ✓ Revisar la consistencia de los Backups realizados a la solución implementada. Hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma, en forma escrita.
- ✓ Configurar, afinar y revisar los reportes / logs de las plataformas.
- ✓ Mantener actualizados los niveles de Firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante.
- ✓ El horario de atención para el mantenimiento correctivo y preventivo deberá ser de 7x24 en sitio, sin costo adicional para la entidad.

Mantenimiento de la solución de seguridad perimetral

El proveedor de servicios debe disponer de un servicio de mantenimiento preventivo para mantener operativa la solución de seguridad perimetral y la infraestructura suministrada, los componentes, partes o elementos que fallen o afecten la solución deben ser reemplazados sin costo adicional al valor total del contrato.

Se deben incluir en la oferta dos (02) actividades sin costo de mantenimiento preventivo y afinamiento por año, con el fin de minimizar problemas y mantener los sistemas actualizados, estas actividades deberán ser con previa aprobación del responsable TI de la entidad.

El proveedor debe contemplar una transferencia de conocimientos para 3 funcionarios de la entidad por 8 horas, la cual debe incluir como mínimo temas de administración, configuración y afinamiento de las plataformas.

Al finalizar cada visita correctiva y/o preventiva el contratista deberá:

- ✓ Generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones.

- ✓ Consignar en la misma acta o informe de servicio si hubo cambio de software y/o en la configuración.
- ✓ Contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que el personal asignado al proyecto pueda cumplir sus funciones.

Modalidad de atención

El proveedor de servicios debe ofrecer un SOC que garantice como mínimo:

- ✓ Operación, monitoreo y actualización de dispositivos del servicio de seguridad perimetral (Firewall y Switches).
- ✓ Detección, respuesta coordinada, investigación de ciberataques, ciberamenazas y resolución de incidentes de seguridad asociados al firewall perimetral y switches.
- ✓ Cuando un evento de seguridad ocurre o está en suceso, el servicio de monitoreo SOC deberá identificarlo y estar en la capacidad de relacionar de forma directa o indirecta con otros eventos de seguridad asociados, determinando el patrón de ataque.
- ✓ El servicio debe permitir la integración del envío de alarmas automáticas vía correo electrónico.
- ✓ De forma permanente el servicio de monitoreo SOC realizará una valoración de las amenazas existentes en la región y el mundo, determinando cuál de estos exponen a un riesgo a la entidad, resumiendo los resultados en Boletines o Informes extraordinarios de SOC. Los servicios de gestión de SOC realizarán seguimiento 7x24 a los ataques originados desde Internet al igual que los originados en la entidad.
- ✓ El proponente deberá tener un SOC Propietario.
- ✓ El SOC debe permitir a la entidad realizar auditorías sobre los procesos, tecnologías, logs y personas que operan en el SOC, en caso de ser requerido.

El SOC debe generar los siguientes informes integrados e históricos con una periodicidad mensual:

- ✓ Informes de servicio, intentos de intrusión, ATP, inalámbrico, latido de seguridad, VPN y más (Según la alternativa de servicio contratada)
- ✓ Informes de cumplimiento: HIPAA, PCI DSS, GLBA, SOX y FISMA
- ✓ Informes del motor de búsqueda: Google, Yahoo, Bing, Wikipedia, Rediff, eBay
- ✓ Informes de tendencia
- ✓ Informes personalizados y especiales con opciones de búsqueda granulares de acuerdo con las necesidades del servicio y las áreas de cumplimiento como Control Interno y Riesgos
- ✓ Estos informes se acordarán en conjunto con las áreas solicitantes.
- ✓ El contratista deberá entregar un informe preliminar de un incidente sucedido. Este debe ser remitido a la entidad posterior a la declaración del evento o incidente y después de la investigación de la actividad sospechosa o incidentes de seguridad se entregará el informe final detallado del mismo.

Visita técnica por parte de la Entidad

- La entidad podrá realizar una visita presencial a las instalaciones del SOC, donde el oferente deberá cumplir con las garantías de las normativas en ISO 27001. Esta visita deberá ser coordinada con el Supervisor del Contrato y Gerencia de Riesgos.

Licenciamiento soluciones de seguridad perimetral

El oferente deberá garantizar el licenciamiento, soporte y garantía de las soluciones adquiridas por la vigencia del contrato, de acuerdo a la oferta aceptada, en un esquema 7x24 ante el fabricante.

El oferente debe entregar a la Entidad un usuario de acceso al portal de los fabricantes de la solución, para la creación de casos, soporte de fábrica, actualización firmware de los dispositivos.

EQUIPO MINIMO DE TRABAJO REQUERIDO

Equipo	Título / Certificaciones / Cursos	Experiencia Profesional Especifica
Gerente de Proyecto Un (01) Ingeniero	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones, industrial o carreras afines. Tarjeta Profesional con expedición mínimo de diez (10) años. Posgrado en Gerencia de Proyectos y/o Certificación PMP. Certificación Vigente ITIL 4 Managing Professional. Certificación Vigente ITIL 4 Strategist Direct, Plan and Improve	Experiencia mínima 5 proyectos gerenciando y/o coordinando proyectos de TI y/o Seguridad Informática.
Líder Técnico Un (01) Ingeniero	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. Especialización o maestría en Seguridad de la Información o informática.	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo de tres (3) años como líder o coordinador o gerente de servicio de TI. Certificaciones de Experiencia especifica de mínimo años (4) años en

	Certificación vigente en SCRUM Fundations Professional (SFPC)	implementación o administración en plataformas de seguridad La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
	Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018	
	Certificación vigente en AUDITOR LIDER en la norma ISO/IEC 27001:2022	
	Certificación vigente en LIDER GESTOR CIBERSEGURIDAD en la norma ISO/IEC 27032:2023	
	Certificación vigente en Especialista en Security Operations y Specialist Network Security	
Implementador Un (01) Ingeniero	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo de cuatro (4) año en implementación, soporte y monitoreo de soluciones de seguridad La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
	Especialización o maestría en Seguridad de la Información o informática.	
	Certificación vigente en AUDITOR LIDER en la norma ISO/IEC 27001:2022	
	Certificación vigente en Profesional de Seguridad de Redes.	
Un (01) Ingeniero de soporte II	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo de cuatro (4) año en implementación, soporte y monitoreo de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
	Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018	

	Certificación vigente en Auditor Interno ISO/IEC 27001:2022	
	Certificación vigente en Profesional de Seguridad de Redes.	
	Certificación vigente en Especialista de Soluciones en Seguridad en Redes.	
Un (01) Ingeniero de soporte I	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.	Experiencia general de cuatros (4) años en proyectos de TI, de los cuales mínimo de tres (3) años en implementación, soporte y monitoreo de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
	Certificación vigente en Profesional de Seguridad de Redes.	
	Certificación vigente en Especialista de Soluciones en Seguridad de Cero Confianza en la Red.	

Nota: El personal de nivel técnico requerido debe ser propio del oferente, no se aceptan figuras de tercerización de servicios o prestación de servicios, para ello se deberán enviar las hoja de vida y/o contrato de vinculación laboral en conjunto con la propuesta.

Actualización Tecnológica

El proveedor del servicio de outsourcing de seguridad perimetral, se compromete a realizar el reemplazo o actualización de los equipos instalados (firewall, switches u otros componentes) en caso de que, durante la vigencia del contrato, surja una nueva tecnología o versión que permita mejorar el rendimiento, la seguridad, la cobertura o la eficiencia del servicio sin generar un costo adicional.

Esta actualización deberá realizarse sin afectar la continuidad del servicio y sin generar costos adicionales para Fiduciaria Central, salvo acuerdo expreso mediante adenda contractual.

El proveedor deberá notificar oportunamente la disponibilidad de nuevas tecnologías o versiones relevantes, presentar una propuesta técnica de actualización que se revisará y aprobará por las parte y el proveedor asumirá la responsabilidad de la instalación, configuración, pruebas de funcionamiento y documentación de los nuevos equipos, así como del retiro adecuado de los anteriores.

Transferencia de Propiedad de Bienes

El proyecto comprende la adquisición e implementación de una solución integral de seguridad y gestión de red, conformada por switches administrables, un servicio de análisis y monitoreo (Analyzer) y dos (2) appliances de seguridad perimetral con sistema operativo propietario del fabricante, operando bajo un esquema de alta disponibilidad (HA).

Al finalizar el presente contrato de outsourcing con opción de compra, y siempre que el **CONTRATANTE** haya cumplido con todas las obligaciones contractuales, incluyendo el pago total de las cuotas pactadas, la propiedad de los bienes objeto del servicio de solución integral de seguridad perimetral y gestión de red será transferida al **CONTRATANTE** sin costo adicional, salvo que se indique lo contrario en el presente contrato.

La transferencia se formalizará mediante la firma de un acta de entrega y cesión de propiedad, en la cual se detallarán los bienes entregados, su estado, y cualquier observación pertinente. A partir de dicha firma, el **CONTRATANTE** asumirá la plena responsabilidad sobre los bienes, incluyendo su mantenimiento, uso y disposición.

Esta cláusula no aplicará en caso de terminación anticipada del contrato por incumplimiento del **CONTRATANTE**, salvo acuerdo expreso entre las partes.

1.7. FUNCIONES Y TAREAS PARA DESARROLLAR

El proveedor debe garantizar que el personal designado para la ejecución del servicio cumpla como mínimo con las siguientes funciones para la gestión y soporte de la solución seguridad perimetral contratada:

- ✓ En el proceso de implementación ejecutar la respectiva revisión general de la configuración actual y generar las respectivas recomendaciones tomando como referencia las mejores prácticas emitidas por el fabricante de la solución administrada propuesta.
- ✓ Realizar la instalación y configuración de los equipos solicitados garantizando la operación funcional correcta.
- ✓ Realizar todas las configuraciones necesarias en la solución de seguridad perimetral que garantice su funcionamiento y el cumplimiento de las políticas de seguridad de la información.
- ✓ El servicio contratado debe garantizar el correcto funcionamiento y operación de los equipos.
- ✓ El proveedor del servicio contratado será el administrador de la plataforma contratada y se encargará de su correcto funcionamiento.
- ✓ Instalar, configurar, gestionar y soportar todas las actualizaciones liberadas por el fabricante a la solución propuesta.
- ✓ Realizar semanalmente revisión proactiva de posibles alertas y errores en los logs de eventos que sean generados por la plataforma de seguridad.
- ✓ Atender de manera oportuna dando cumplimiento al capítulo de ANS, todos los requerimientos presentados por parte de la Fiduciaria Central.

- ✓ Una vez realizados los soportes técnicos (remotos o en sitio) o mantenimientos (preventivos y/o correctivos) el oferente debe hacer entrega de un informe técnico donde se indique las actividades y se detallen los procedimientos realizados.
- ✓ Al finalizar cada periodo, el proveedor de servicios deberá entregar el respectivo informe de gestión mensual, el cual será obligatorio para el pago de la facturación de servicios, el presente informe se entregará a la Dirección de Tecnología e Innovación en un tiempo máximo de cinco días hábiles del siguiente periodo para revisión y aceptación de este.
- ✓ Definir los indicadores, variables y umbrales a monitorear en las herramientas de monitoreo dispuestas para la prestación del servicio.
- ✓ Ejecutar diagnósticos y pruebas de vulnerabilidades mensuales (health check) para verificar y garantizar el óptimo funcionamiento de la plataforma contratada.
- ✓ Hacer entrega de los respectivos informes de gestión, correspondiente a los diagnósticos y pruebas de vulnerabilidad realizado mensualmente.
- ✓ Planear, ejecutar y reportar el estado de las pruebas que corresponden al plan de recuperación de desastres.
- ✓ El proveedor de servicios se deberá ajustar y cumplir con la política de seguridad de la información establecida en la Fiduciaria Central, para garantizar el desarrollo del objeto contractual.
- ✓ El proveedor deberá apoyar a las áreas de sistemas y seguridad de la información de la fiduciaria central, para la mitigación de vulnerabilidades de seguridad detectadas, así como ejecutar procesos de acompañamiento a proveedores y terceros que lo requieran, para garantizar la disponibilidad operacional.
- ✓ Garantizar la correcta configuración de los servicios de seguridad perimetral en la sede de Bogotá y todas aquellas que se requieran durante la vigencia del contrato.
- ✓ Gestionar la configuración de reglas y servicios tecnológicos actuales y todos los que se requieran implementar durante la vigencia del contrato.
- ✓ Mejorar los parámetros en la configuración de las políticas de seguridad, como resultado del monitoreo en tiempo real y el análisis de los eventos de salud y seguridad de la información.
- ✓ Efectuar los procesos de revisión y análisis del log, acompañado de la respectiva transferencia de conocimiento a nivel general del servicio de seguridad perimetral y las capacitaciones requeridas por los funcionarios del área de Tecnología e Innovación de la Fiduciaria Central.
- ✓ La solución de seguridad perimetral se debe entregar correctamente configurados y licenciados dentro de la vigencia del presente contrato, en la sede principal ubicada en la Avenida El Dorado No. 69 A 51 en la ciudad de Bogotá.
- ✓ El contratista debe garantizar el correcto funcionamiento de los equipos y el esquema de alta disponibilidad los 365 días del año.
- ✓ Respaldo completo de las configuraciones de la solución de seguridad perimetral, esto debe ser entregado a la Dirección de Tecnología e Innovación.
- ✓ Contraseñas de acceso del administrador de las consolas de administración y cualquier otra clave o acceso necesario para la administración del servicio.
- ✓ Cualquier documento técnico que explique la estructura y configuración implementada, que permita a otro proveedor o al personal de Fiduciaria Central gestionar correctamente la infraestructura.
- ✓ El proveedor debe coordinar con la Dirección de Tecnología e Innovación de la Fiduciaria Central, las ventanas de mantenimiento que se requieran a nivel físico y lógico para garantizar el correcto funcionamiento del hardware y software instalados.

- ✓ Cumplir con los ANS definidos en el presente documentos y detallados en la propuesta comercial que sustenta el presente contrato de prestación de servicios.
- ✓ Generar el respectivo informe sobre eventos de seguridad detectados, aclarando si se llegó a materializar un riesgo y el impacto generado.
- ✓ Asistir con carácter obligatorio a las reuniones y ventanas de mantenimiento previamente acordadas.
- ✓ En caso de que el contratista detecte como producto de su análisis alguna falla, degradación de servicio o problema, que debe ajustar las configuraciones realizadas sobre los equipos y consolas de administración, estas se deben notificar previamente a la Dirección de Tecnología e Innovación de la Fiduciaria, con el objetivo de validar el alcance y el plan de implementación bajo el procedimiento de control de cambios definido por la Fiduciaria.
- ✓ El proveedor no podrá realizar cambios sobre la configuración de la solución de seguridad perimetral y consolas de administración de manera independiente sin la autorización respectiva por parte del supervisor del contrato a cargo de la Fiduciaria, de hacerlo se expondrá a sanciones y multas teniendo en cuenta el impacto generado sobre los servicios afectados.
- ✓ Programar mínimo dos (2) ventanas de mantenimiento físico al año.
- ✓ Cumplir con las especificaciones técnicas, económicas, jurídicas y con los máximos estándares de la industria, conforme a las condiciones contempladas en la oferta comercial y en el contrato.
- ✓ El proveedor deberá notificar oportunamente la disponibilidad de nuevas tecnologías o versiones relevantes, presentar una propuesta técnica de actualización sin generar costos adicionales a Fiducentral y asumir la responsabilidad de la instalación, configuración, pruebas de funcionamiento y documentación de los nuevos equipos, así como del retiro adecuado de los anteriores.

1.8. DISPONIBILIDAD DE SERVICIOS

El proveedor seleccionado deberá garantizar una disponibilidad 7x24 para trabajar o atender incidentes críticos o labores de mantenimiento programadas en horario no hábil (nocturno y fines de semana) en primera instancia en modalidad remota o en sitio cuando así se requiera por la Dirección de Tecnología e Innovación de **FIDUCIARIA CENTRAL S.A.**

Dentro de lo posible, las labores fuera del horario normal serán programadas por la Fiduciaria con al menos un día de antelación, el apoyo en sitio fuera de horario será solicitado y escalado al proveedor para casos de alta severidad (casos críticos y urgentes) y/o mantenimientos cuando no exista la posibilidad de trabajar o dar una solución remotamente.

1.9. COMPETENCIAS REQUERIDAS EQUIPO DE TRABAJO Y PERFILES

El personal designado por el proveedor para la gestión y soporte del servicio de outsourcing con modalidad de compra para implementación de una solución integral de seguridad y gestión de red debe cumplir obligatoriamente con los siguientes perfiles:

Equipo	Título / Certificaciones / Cursos	Experiencia Profesional Especifica
Gerente de Proyecto Un (01) Ingeniero	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones, industrial o carreras afines. Tarjeta Profesional con expedición mínimo de diez (10) años.	Experiencia mínima 5 proyectos gerenciando y/o coordinando proyectos de TI y/o Seguridad Informática.
	Posgrado en Gerencia de Proyectos y/o Certificación PMP. Certificación Vigente ITIL 4 Managing Professional. Certificación Vigente ITIL 4 Strategist Direct, Plan and Improve	
Líder Técnico Un (01) Ingeniero	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo de tres (3) años como líder o coordinador o gerente de servicio de TI. Certificaciones de Experiencia especifica de mínimo años (4) años en implementación o administración en plataformas de seguridad La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
	Especialización o maestría en Seguridad de la Información o informática.	
	Certificación vigente en SCRUM Fundations Professional (SFPC)	
	Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018	
	Certificación vigente en AUDITOR LIDER en la norma ISO/IEC 27001:2022	
	Certificación vigente en LIDER GESTOR CIBERSEGURIDAD en la norma ISO/IEC 27032:2023	

	Certificación vigente en Especialista en Security Operations y Specialist Network Security	
Implementador Un (01) Ingeniero	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo de cuatro (4) año en implementación, soporte y monitoreo de soluciones de seguridad La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
	Especialización o maestría en Seguridad de la Información o informática.	
	Certificación vigente en AUDITOR LIDER en la norma ISO/IEC 27001:2022	
	Certificación vigente en Profesional de Seguridad de Redes.	
Un (01) Ingeniero de soporte II	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines.	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo de cuatro (4) año en implementación, soporte y monitoreo de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
	Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018 Certificación vigente en Auditor Interno ISO/IEC 27001:2022	
	Certificación vigente en Profesional de Seguridad de Redes.	
	Certificación vigente en Especialista de Soluciones en Seguridad en Redes.	
Un (01) Ingeniero de soporte I	Título Ingeniero Eléctrico, electrónico, sistemas,	Experiencia general de cuatros (4) años en proyectos de TI, de los cuales mínimo de tres (3) años en implementación,

	telecomunicaciones o carreras afines.	soporte y monitoreo de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
	Certificación vigente en Profesional de Seguridad de Redes.	
	Certificación vigente en Especialista de Soluciones en Seguridad de Cero Confianza en la Red.	

1.10. CERTIFICACIONES EMPRESARIALES

Los proponentes que deseen participar en el proceso de selección deben cumplir con los siguientes requisitos obligatorios:

- ✓ Certificación de distribuidor autorizado del fabricante donde se evidencie que tiene el nivel de membresía más alto o ser categoría **EXPERT.** Lo anterior con el fin de garantizar la experiencia en la implementación de las soluciones que requiere la entidad. Esta certificación debe ser dirigida a la Entidad, especificando el número del proceso y objeto de este. Con una vigencia no mayor a 30 días.
- ✓ El proveedor deberá presentar dentro de la certificación de distribuidor autorizado del fabricante que cuenta y posee la categoría de **Engage Tech Support Partner**, lo que garantiza que cuenta y dispone con los recursos técnicos de fabricante para la implementación de las soluciones.
- ✓ El proveedor deberá presentar al menos cinco especialidades técnicas del mismo fabricante con el cual se está presentando, dentro de la cuales son obligatorias **Secure Networking Firewall, Security Operations, SD-WAN y Zero Trust Network Access**.

En caso de uniones temporales y/o consorcios cada uno de los integrantes deberá aportar las certificaciones mencionadas en los requerimientos anteriores, con los mismos criterios y alcances mínimos establecidos para cada integrante del consorcio, no se realizará sumatoria y/o validación de tiempos de vigencia de las certificaciones para cumplir lo establecido.

El proveedor debe entregar junto con la propuesta una certificación emitida directamente de los fabricantes de las soluciones ofertadas donde se evidencie que los equipos suministrados no se encuentran en fin de venta y contaran con extensión de soporte por mínimo 5 años, estas cartas deben ser dirigidas a la Entidad, especificando el número del proceso y objeto del mismo, con una vigencia no mayor a 30 días.

1.11. SOPORTE Y MANTENIMIENTO

El proponente debe relacionar la dirección de su sede administrativa y operativa ubicada en la ciudad de Bogotá, con el objetivo de poder realizar una visita de verificación al centro de soporte y servicio destinado para el desarrollo del objeto contractual.

Soporte Técnico

Garantizar el servicio de soporte técnico de Niveles I, II y III, la administración, gestión y atención de incidentes. Estos incidentes serán clasificados y resueltos por especialista de soporte.

Garantizar que los equipos se encuentren actualizados con el último firmware de versión estable.

Mantenimiento

Realizar el mantenimiento correctivo y preventivo de toda la infraestructura contratada al menos dos (2) veces al año, en caso de presentarse alguna falla el proponente deberá reemplazar los equipos por unos de igual o mejor características a las contratadas.

1.11.1 Garantía Técnica

Todos los ingenieros involucrados en el proceso de implementación, administración y/o gestión, deben contar con las respectivas certificaciones relacionadas en las competencias requeridas para el desarrollo del objeto contractual.

1.11.2 Estructura de Soporte

1.11.2.1 Canales de atención

Los proponentes deben contar obligatoriamente con los diferentes canales de atención como son, servicio telefónico, sistema de mesa de ayuda, sistema de correo electrónico para el registro y seguimiento de requerimientos y/o atención de incidentes reportados.

1.11.2.2 Matriz de Escalamiento

El proponente debe presentar la respectiva matriz de escalamiento de todos los involucrados en el proyecto, donde se detalle la siguiente información:

- ✓ Detalle niveles de atención.
- ✓ Nombre del gerente de proyecto asignado.
- ✓ Nombre del responsable técnico asignado.

- ✓ Números Telefónicos.
- ✓ Números Celulares.
- ✓ Cuentas de correo electrónico.

1.11.2.3 Llamadas de Servicio Técnico

El proponente debe estar en capacidad de atender todas las llamadas telefónicas que se generen 7x24, para la atención de requerimientos presentados por Fiduciaria Central.

1.11.2.4 ANS – Tiempos de Respuesta

En la siguiente tabla se detalla los niveles de criticidad para la atención de requerimientos y los % de penalización en caso de que no se cumpla con la atención esperada:

PRIORIDAD		DESCRIPCION
1	CRITICA	La operación está parada o severamente impactada de manera que no se puede continuar trabajando. La operación es de misión crítica para la entidad y/o está en situación de emergencia.
2	ALTA	Experimenta perdida del servicio, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera restringida.
3	MEDIA	Experimenta una pérdida de servicio menor, el impacto es un inconveniente.
4	BAJA	No impacta la operación del programa, no se experimenta perdida del servicio y no se impide la operación de los sistemas.

PRIORIDAD		TIEMPO DE ATENCIÓN
1	CRITICA	1 Hora
2	ALTA	2 Horas
3	MEDIA	4 Horas

4	**BAJA**	ND
5	**Planeado**	ND

Nivel de cumplimiento de ANS % de penalidad	
Desde - Hasta	%
90 - 99%	1
80 - 89%	2
70 - 79%	3
60 - 69%	4
50 - 59%	5
40 - 49%	6
30 - 39%	7
20 - 29%	8
10 - 19%	9
1 - 9 %	10

1.11.2.5 Seguimiento del servicio

El proponente debe asistir a las reuniones programadas por la Dirección de Tecnología e Innovación de Fiduciaria Central S.A. en caso de requerirse, para revisar el estado del servicio.

1.11.2.6 Capacitación

El oferente deberá contemplar dentro de su propuesta la transferencia de conocimiento dirigida a tres (3) funcionarios de la **FIDUCIARIA CENTRAL S.A.,** con una duración mínima de ocho (8) horas, orientada al fortalecimiento de las competencias técnicas en la administración, configuración y afinamiento de las plataformas implementadas.

Asimismo, el proponente deberá estar en la capacidad de programar y ejecutar las capacitaciones correspondientes, dirigidas al equipo de ingenieros del área de Tecnología e Innovación de la Fiduciaria Central S.A., garantizando la transferencia efectiva de conocimientos que permita la gestión autónoma, segura y eficiente de las soluciones instaladas.

1.12. CRONOGRAMA DEL PROCESO

ACTIVIDAD	FECHA Y HORA	LUGAR
Publicación de la propuesta	10/12/2025	Página web https://www.fiducentral.com
Recibo solicitudes de aclaración	12/12/2025	Correo electrónico Carlos.SanchezR@fiducentral.com y valeria.marconi@fiducentral.com
Respuesta a solicitudes de aclaración	16/12/2025	Correo electrónico del proponente
Entrega de propuestas	17/12/2025	Correo electrónico Carlos.SanchezR@fiducentral.com y valeria.marconi@fiducentral.com
Evaluación de propuestas	19/12/2025	Avenida El Dorado # 69 A – 51 Torre B Piso 3 Bogotá
Resultados de evaluaciones, y selección (aceptación de la oferta) o desistimiento del proceso	22/12/2025	Correo electrónico de los proponentes
Recibo de documentos necesarios para firma de contrato	26/12/2025	Correo electrónico Carlos.SanchezR@fiducentral.com y valeria.marconi@fiducentral.com
Suscripción del contrato	02/01/2026	Avenida El Dorado # 69 A – 51 Torre B Piso 3 Bogotá

1.12.1. PLAZO DE LA INVITACIÓN PÚBLICA

1.12.1.1. FECHA DE REVISIÓN - TÉRMINOS DE REFERENCIA

La revisión de las ofertas recibidas se realizará el 19/12/2025

1.12.1.2. LUGAR, FECHA Y HORA DE CIERRE DE LA INVITACIÓN:

La invitación se cierra formalmente el 17/12/2025, hasta las 4:30 pm. Solo se aceptarán propuestas a través del correo electrónico Carlos.SanchezR@fiducentral.com y valeria.marconi@fiducentral.com

- **a.** La propuesta debe ser presentada en idioma castellano.
- **b.** No debe haber tachaduras ni enmendaduras. Cualquier corrección realizada en la propuesta debe ser explicada y validada con la firma del Representante Legal del oferente en la misma propuesta. No se admitirán ofertas parciales o alternativas.
- **c.** En cada una de las propuestas recibidas por correo electrónico se hará constar el nombre del proponente y su dirección comercial, y se presentará de la siguiente forma:

FIDUCIARIA CENTRAL S.A.

INVITACIÓN PÚBLICA PARA CONTRATRATAR SERVICIO DE OUTSOURCING DE SEGURIDAD PERIMETRAL E INFRAESTRUCTURA DE COMUNICACIONES.

VIGENCIA PROPUESTA: TRES (3) MESES.

NOMBRE DEL PROPONENTE:

DIRECCIÓN:

TELÉFONO:

CORREO ELECTRÓNICO:

La dirección, teléfono y correo electrónico que aparezcan en cada propuesta, serán los que el oferente utilice para todos los efectos relacionados con las comunicaciones y notificaciones a las que se refiere esta Invitación. Es responsabilidad exclusiva de cada oferente informar con la debida anticipación y por escrito el cambio en cualquiera de dichos datos.

d. Es recomendable que la oferta presentada este completamente acorde con sus anexos.
e. La oferta presentada deberá contemplar dos alternativas: Una por un periodo de doce (12) meses y otra por veinticuatro (24) meses de servicio. La entidad seleccionará la opción que resulte más favorable, de acuerdo con sus necesidades y criterios de evaluación.
f. La propuesta debe presentar el valor y cantidad para cada uno de los servicios ofertados.
g. Si se detecta una diferencia entre los valores expresados en números y en letras, se considerará el valor expresado en letras.
h. No se aceptarán ofertas físicas, vía fax o cualquier otro medio que no sea el correo electrónico designado Carlos.SanchezR@fiducentral.com y valeria.marconi@fiducentral.com. Las ofertas serán recibidas hasta la fecha y hora establecidas en el CRONOGRAMA DEL PROCESO y/o posibles adendas que puedan surgir. Las propuestas recibidas con posterioridad a esta fecha y hora no serán tenidas en cuenta por ser extemporáneas y en consecuencia serán rechazadas.
i. Una vez presentada la oferta, no se admitirán documentos adicionales, excepto aquellos que sean solicitados expresamente que no mejoren la oferta comercial o aquellos referidos en la Solicitud de Subsanación.
j. En la fecha y hora indicada, se declarará cerrada la Invitación y se levantará el Acta respectiva. A continuación, se contarán las propuestas y se procederá a relacionarlas una a una indicando el nombre del proponente, el número de folios y los datos de la garantía de seriedad de la propuesta.

1.13. DOCUMENTOS CONFIDENCIALES

Si se presenta alguna información o documentación que el proponente considere que es confidencial o privada, es necesario que en la carta de presentación de la propuesta se indique el carácter

confidencial de la misma y se entregue en sobre separado indicando la confidencialidad. En caso de no indicarse que alguno de los documentos aportados en la propuesta goza de confidencialidad, Fiduciaria Central S.A. entiende que se encuentra autorizado para expedir copia del mencionado documento. Aquellos documentos marcados como confidenciales y que NO sean entregados en sobre separado indicando su confidencialidad, no serán tenidos en cuenta como confidenciales.

1.14. INTERPRETACIONES, MODIFICACIONES Y ACLARACIONES A LOS TÉRMINOS DE REFERENCIA

Si un proponente encuentra incongruencias, errores u omisiones o necesita alguna aclaración al contenido de los presentes términos de referencia, podrá, dentro del plazo establecido para ello en el cronograma contenido en el numeral 1.12., presentar su solicitud escrita al correo electrónico Carlos.SanchezR@fiducentral.com y valeria.marconi@fiducentral.com

Si **FIDUCIARIA CENTRAL S.A.** estima conveniente efectuar, de oficio o con base en las consultas que se formulen, modificaciones o adiciones a los presentes términos, lo hará mediante documento de Subsanaciones, en cualquier momento hasta antes de la selección.

Cuando se trate de aclaraciones, modificaciones, suspensión o terminación de la presente Invitación, éstas se remitirán al correo electrónico suministrado por el proponente.

1.15. DEBER DE DEBIDA DILIGENCIA E INFORMACIÓN

El Proponente será el responsable de conocer todas y cada una de las implicaciones del ofrecimiento que realice en el presente proceso, y realizar todas las valoraciones y estimaciones que sean necesarias para presentar su propuesta.

Con la sola presentación de la propuesta, se considera que el Proponente ha realizado el examen completo de todos los aspectos que inciden y determinan la presentación de la misma.

La exactitud y confiabilidad de la información que tenga a bien consultar el Proponente se encuentra bajo su propia responsabilidad, así como la interpretación que haga de la misma.

Como consecuencia de lo anterior, el Proponente, al elaborar su propuesta, deberá tener en cuenta el cálculo de los costos y gastos, los cuales se deberán basar estrictamente en sus propios estudios y estimaciones.

1.16. CONDICIONES Y CALIDADES EXIGIDAS EN CUANTO A LOS PROPONENTES

De acuerdo con lo establecido en los artículos 8 y 9 de la Ley 80 de 1993, el artículo 18 de la ley 1150 de 2007 y los artículos 1° y 4° de la ley 1474 de 2011, los participantes no deberán estar incursos en ninguna de las inhabilidades, incompatibilidades y prohibiciones que la ley establece.

El Proponente (tanto la persona jurídica como su representante legal y sus accionistas o socios) deberá manifestar que no se encuentra incluido dentro de las listas restrictivas que hagan referencia al Lavado de Activos y la Financiación del Terrorismo. El Proponente deberá manifestar que los recursos que componen su patrimonio no provienen de lavado de activos, financiación del terrorismo, narcotráfico, captación ilegal de dineros y en general de cualquier actividad ilícita; de igual manera deberá manifestar que los recursos recibidos en desarrollo del contrato que se pretende suscribir, no serán destinados a ninguna de las actividades antes descritas.

No podrán presentar propuestas las sociedades que tengan por si o a través de sus socios, participación en otra sociedad que simultáneamente presente propuesta separada.

1.17. REQUISITOS DE LA PÓLIZA DE GARANTÍA DE SERIEDAD DE LA OFERTA

Los proponentes deberán presentar con su oferta garantía de seriedad de la misma a favor de **FIDUCIARIA CENTRAL S.A.,** identificada con NIT. 800.171.372- 1, por una cuantía equivalente al diez por ciento (10%) de su propuesta económica y una vigencia no inferior a tres (3) meses contados a partir de la fecha de cierre del proceso de selección, pero el adjudicatario estará obligado a extender dicha vigencia, si fuere necesario, hasta la aprobación de la garantía que ampara los riesgos propios de la etapa contractual, tal y como lo establece el numeral 6.6. del Manual de Contratación de la entidad.

En Formato: Formato ante entidades públicas con régimen privado de contratación

Tomador: Firma proponente.

Asegurado: Fiduciaria Central S.A. NIT: 800.171.372-1

Beneficiario: Fiduciaria Central S.A. NIT: 800.171.372-1

Vigencia: Por el término tres (3) meses contados a partir de la fecha y hora prevista para el cierre de la Invitación Pública, incluyendo las prórrogas o ampliaciones del proceso.

Cuantía: Por un valor asegurado equivalente al diez por ciento (10%) del valor total de la propuesta económica.

Objeto: Garantizar la seriedad de la oferta y legalización del contrato, producto de la Invitación Pública, en la que se busca contratar bajo la modalidad outsourcing con opción de compra, los servicios profesionales para el suministro, implementación y administración de una solución integral de seguridad y gestión de red, conformada por de dos (2) equipos Next Generation Firewall Fortinet nuevos y de última generación, así como la infraestructura de comunicaciones dos (2) Switches de Core configurados en alta disponibilidad y de seis (6) switches de acceso, junto con los servicios de instalación, configuración, puesta en funcionamiento, administración, gestión y soporte de toda la plataforma de seguridad perimetral y un servicio de análisis y monitoreo (Analyzer). Este proyecto tiene como propósito fortalecer la infraestructura tecnológica en cumplimiento de las recomendaciones del MinTIC, las normas ISO 27001:2022 y 27002:2022, el marco COBIT 2019 y la normatividad de la Superintendencia Financiera de Colombia, asegurando la integridad, disponibilidad y confidencialidad de la información, así como la continuidad y correcta operación del negocio.

Firma: El tomador deberá firmar la Póliza de Seriedad de Oferta.

Recibo de pago de la póliza: Se deberá adjuntar el documento donde conste el pago de la póliza por parte del tomador a la compañía de seguros.

Igualmente se debe anexar el recibo original de pago correspondiente a la prima por concepto de seguro de la respectiva póliza. Dicha garantía debe ser expedida por una compañía de seguros legalmente establecida en Colombia.

FIDUCIARIA CENTRAL S.A. hará efectiva la garantía de seriedad de la propuesta en los siguientes casos:

- ✓ Cuando se solicite el retiro de la oferta después de la fecha de cierre de la presente invitación.
- ✓ Cuando el proponente favorecido con la selección no proceda a firmar el contrato.

1.18. COSTO DE PREPARACIÓN DE LA PROPUESTA

Serán a cargo del Proponente todos los costos asociados a la preparación y presentación de su propuesta, y **FIDUCIARIA CENTRAL S.A.** en ningún caso será responsable de los mismos.

1.19. PROPUESTA ECONÓMICA

El proponente debe presentar su propuesta económica en pesos colombianos e indicar si incluye o no IVA; y demás impuestos que correspondan.

Para efectos de presentar la propuesta económica, el proponente deberá especificar los respectivos costos de la ejecución del contrato en la ciudad de Bogotá, teniendo en cuenta que, durante la vigencia del contrato, **FIDUCIARIA CENTRAL S.A.** no reconocerá ningún reajuste adicional de tarifas o precios, distintos a los establecidos en la propuesta que presente el Proponente.

Cualquier impuesto de timbre que se genere o se llegare a generar en virtud de la celebración, ejecución o liquidación del contrato que se celebre, será asumido por el Proponente.

1.20. PLAZO DE EVALUACIÓN

El plazo para la evaluación será el señalado en el cronograma del presente documento. Durante este plazo, **FIDUCIARIA CENTRAL S.A.** podrá solicitar aclaraciones sobre las propuestas recibidas, mediante comunicación dirigida al proponente al correo electrónico informado en su oferta. La respuesta a esta solicitud de aclaraciones en ningún momento podrá utilizarse para mejorar la propuesta presentada.

Este plazo puede ser prorrogado mediante comunicación dirigida a cada uno de los proponentes, de acuerdo con las necesidades de **FIDUCIARIA CENTRAL S.A.**

1.21. INFORMES DE EVALUACIÓN

Los resultados de la verificación y evaluación se enviarán a los correos electrónicos de los proponentes una vez sea realizada la misma.

Al día siguiente hábil de la publicación del resultado de la evaluación, los proponentes podrán presentar las observaciones que consideren pertinentes al correo electrónico Carlos.SanchezR@fiducentral.com y valeria.marconi@fiducentral.com.

Solo serán atendidas aquellas observaciones que hayan sido radicadas con el cumplimiento de los anteriores requisitos y durante el periodo establecido para tal fin. En ningún caso, se podrán mejorar las propuestas ni aportar nuevos documentos que impliquen la variación de la calificación de la oferta.

1.22. SELECCIÓN

Se seleccionará al proveedor que tenga el mayor puntaje en cumplimiento de los términos de referencia expuestos en el presente documento.

La presentación de la oferta y su evaluación en la presente invitación no implica la aceptación de esta, por lo tanto, la Fiduciaria podrá dar por terminado el proceso de invitación a contratar sin seleccionar contratista, si considera que las ofertas no se ajustan a sus necesidades.

1.23. SUSCRIPCIÓN DEL CONTRATO

Si el proponente seleccionado no suscribe el contrato correspondiente por causa no imputable a Fiduciaria Central S.A., esta última hará efectiva la garantía de seriedad de la propuesta, sin menoscabo de las acciones legales conducentes al reconocimiento de perjuicios causados y no cubiertos por el valor de la citada garantía.

Si el proponente seleccionado no remite los documentos necesarios para la suscripción del contrato, tres (3) días hábiles siguientes a la selección, Fiduciaria Central S.A. podrá seleccionar la segunda propuesta más favorable, conforme a la calificación obtenida.

1.24. EVENTOS DE IMPOSIBILIDAD PARA LA SELECCIÓN DEL CONTRATISTA

Habrá imposibilidad de seleccionar al contratista en los siguientes casos:

I. Cuando no se presenten propuestas.
II. Cuando ninguna de las propuestas que se presente cumpla con los requisitos exigidos en los presentes Términos de Referencia.
III. Cuando por razones de utilidad o conveniencia para la Entidad, no sea procedente continuar con el proceso de contratación, en razón a circunstancias técnicas, operativas, económicas, de mercado, fuerza mayor, orden de autoridad, o acto irresistible de terceros, debidamente justificados.

1.25. RESERVA DURANTE EL PROCESO DE EVALUACIÓN

Todo intento de un proponente para influir en el proceso de selección, dará lugar al rechazo de la propuesta.

CAPÍTULO II

OBJETO Y CONDICIONES DE LA INVITACIÓN PÚBLICA

2.1. OBJETO

La Fiduciaria Central S.A. adelanta la presente invitación con el fin de contratar, bajo la modalidad outsourcing con opción de compra, los servicios profesionales para el suministro, implementación y administración de una solución integral de seguridad y gestión de red, conformada por de dos (2) equipos Next Generation Firewall Fortinet nuevos y de última generación, así como la infraestructura de comunicaciones dos (2) Switches de Core configurados en alta disponibilidad y de seis (6) switches de acceso, junto con los servicios de instalación, configuración, puesta en funcionamiento,

administración, gestión y soporte de toda la plataforma de seguridad perimetral y un servicio de análisis y monitoreo (Analyzer). Este proyecto tiene como propósito fortalecer la infraestructura tecnológica en cumplimiento de las recomendaciones del MinTIC, las normas ISO 27001:2022 y 27002:2022, el marco COBIT 2019 y la normatividad de la Superintendencia Financiera de Colombia, asegurando la integridad, disponibilidad y confidencialidad de la información, así como la continuidad y correcta operación del negocio.

2.2. CONDICIONES DE LA PRESENTE INVITACIÓN

El estudio y evaluación de las propuestas presentadas oportunamente que realizará Fiduciaria Central S.A. se dividirá así:

a) Estudio y verificación de requisitos habilitantes. Estos requisitos comprenden el aporte de documentos de carácter jurídico, financiero y técnico. Quien cumpla con la totalidad de documentos exigidos pasará a la siguiente etapa de evaluación; al proponente que no los cumpla y/o no subsane adecuadamente en el periodo otorgado por Fiduciaria Central S.A. se le rechazará la propuesta. (El cumplimiento de este requisito no dará lugar a puntuación, únicamente permitirá continuar en el proceso).

b) Evaluación de las propuestas. Solo quien haya cumplido con los requisitos habilitantes, será sujeto de evaluación y puntuación de acuerdo con los criterios señalados en el punto 2.2. del presente documento.

2.2.1. REQUISITOS HABILITANTES

Cualquiera de los requisitos o condiciones solicitadas en los presentes requerimientos mínimos habilitantes podrán ser subsanables, a solicitud de Fiduciaria Central S.A., hasta antes de la selección siempre y cuando, a criterio de la Fiduciaria, no implique modificación de las condiciones del servicio ofertado.

Los proponentes presentarán la siguiente documentación y formatos anexos, diligenciados:

2.2.1.1 DOCUMENTOS JURÍDICOS

a) Carta de Presentación de la Propuesta (**Anexo 1**)

Carta de presentación de la propuesta de acuerdo con el modelo suministrado en el Anexo 1, el cual deberá estar firmado por el Representante Legal o por quien tenga facultades para contratar en cuantía igual o superior a la del valor de la propuesta del presente proceso de contratación.

En la carta de presentación, el proponente debe manifestar que conoce y acepta todas las especificaciones y condiciones señaladas en estos términos de referencia, y bajo la gravedad de juramento, declarar que ni él ni la sociedad que representa se encuentran incursos en las

inhabilidades o incompatibilidades establecidas en la Constitución Política, la Ley 80 de 1993 y 1150 de 2007 y demás normas vigentes.

De igual forma deberá manifestar que ni él como Representante Legal, ni la sociedad que representa ni los socios o accionistas, se encuentran incluidos dentro de las listas restrictivas que hagan referencia al Lavado de Activos y la Financiación del Terrorismo, así como que los recursos que componen su patrimonio no provienen de lavado de activos, financiación del terrorismo, narcotráfico, captación ilegal de dineros y en general de cualquier actividad ilícita; también deberá manifestar que los recursos recibidos en desarrollo del contrato que se pretende suscribir no serán destinados a ninguna de las actividades antes descritas. Si es persona jurídica, esta manifestación debe hacerse respecto al Representante Legal, a la sociedad que representa y a sus socios o accionistas.

La presentación de la carta y la manifestación expresa de su conformidad con los términos de referencia y documentos presentados por el proponente, no significa por si sólo que la propuesta cumpla con los requisitos exigidos en estos requerimientos mínimos.

b) Certificado de existencia y representación legal expedido por la Cámara de Comercio respectiva

El Proponente deberá acreditar su existencia y representación legal mediante el certificado expedido por la Cámara de Comercio de su domicilio, en el cual se acredite que está debidamente constituida y su término de duración no será inferior a la duración del contrato y un (1) año más; con fecha de expedición no mayor a un (1) mes con relación a la fecha de presentación de la propuesta.

c) Autorización para contratar

Si del documento anterior se desprende que las facultades del Representante Legal están restringidas, el Proponente deberá adjuntar el certificado, extracto o copia del acta expedida por la Asamblea, Junta Directiva o Junta de Socios, según sea el caso, en donde conste la autorización dada al Representante Legal para comprometer a la sociedad en la presente Invitación.

d) Certificación de antecedentes

Los proponentes deberán presentar el certificado de antecedentes fiscales del proponente. Además de las certificaciones de antecedentes fiscales (Contraloría General de la Nación), disciplinarios (Procuraduría General de la República) y judiciales (Policía Nacional) del Representante Legal y de sus suplentes.

e) Fotocopia Documentos de Identidad

Los proponentes deberán presentar la fotocopia de la cédula de ciudadanía del Representante Legal y de sus suplentes.

f) Registro Único Tributario

Se deberá aportar copia del Registro Único Tributario (RUT) del proponente.

g) Certificación Pago Seguridad Social y Aportes Parafiscales

El Proponente deberá aportar certificación expedida por el por el Representante Legal o el Revisor Fiscal, en donde se certifique que el proponente se encuentra al día en el pago de lo estipulado en el artículo 50 de la Ley 789 de 2002.

Para acreditar lo anterior, el Proponente deberá adjuntar con su propuesta la certificación expedida por el Representante Legal o el Revisor Fiscal, según corresponda, en la cual conste el cumplimiento de sus obligaciones con los sistemas de salud, riesgos profesionales, de pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje de sus empleados en Colombia. En el evento en que el Proponente no tenga empleados en su nómina, deberá certificarse este hecho mediante una declaración juramentada del Representante Legal, con lo cual se entenderá satisfecho el requisito aquí previsto.

h) Autorización de Tratamiento de Datos Personales (Anexo 2)

Se deberá remitir el formato debidamente diligenciado, según la ley 1581 de 2012.

i) Diligenciar y remitir Formato vinculación proveedores actualización persona jurídica (Anexo 3)

El Proponente deberá diligenciar, firmar y radicar con su propuesta el Formato vinculación proveedores actualización persona jurídica o natural según sea el caso.

j) Documentos adicionales para consulta en listas restrictivas

El proponente deberá aportar los siguientes documentos los cuales se adjuntarán a los numerales anteriores para generar las consultas en listas restrictivas:

- Certificación bancaria no mayor a 3 meses
- Certificado de afiliación y/o cobertura vigente de ARL
- Resultado de última Autoevaluación del SG-SST presentada ante la ARL

2.2.1.2 DOCUMENTOS FINANCIEROS

El Proponente debe presentar con la propuesta los siguientes documentos:

a) Estados Financieros y notas a los Estados Financieros con corte al 31 de diciembre de 2024, en los términos establecidos por la ley vigente.

b) El certificado de los Estados Financieros con corte a 31 de diciembre de 2024 firmados por el Representante Legal y Contador Público.
c) Estados Financieros y notas a los Estados Financieros con corte al 30 de junio de 2025, en los términos establecidos por la ley vigente.
d) Fotocopia legible de las tarjetas profesionales del Contador Público y del Revisor Fiscal (de ser procedente).
e) Fotocopia legible de la cédula del Contador Público que elabora los estados financieros y del Revisor Fiscal (de ser procedente).
f) Fotocopia del certificado de antecedentes disciplinarios, expedido por la Junta Central de Contadores, del Revisor Fiscal (de ser procedente) y del Contador Público, vigentes a la fecha de recepción de la propuesta.

La información financiera tendrá que ser presentada en pesos (moneda legal colombiana) y deberá venir firmada por el Representante Legal y el Contador Público y/o el Revisor Fiscal.

Los Estados Financieros presentados deben cumplir con la técnica contable, en especial con las directrices impartidas por las normas de contabilidad y de información financiera aceptadas en Colombia (NCIF), establecidas en la Ley 1314 de 2009, reglamentadas por el decreto único reglamentario 2420 de 2015 modificado por el decreto 2496 de 2015 y demás normas que lo adicionen, modifiquen o sustituyan.

De conformidad con los artículos 37 y 38 de la ley 222 de 1995 y la circular 037 del 20 de diciembre de 2001 expedida por la Junta Central de Contadores, los estados financieros se encuentran debidamente certificados cuando vienen firmados por el Representante Legal y el Contador Público que preparó la información financiera y acompañados del respectivo certificado; y dictaminados cuando son suscritos por el Revisor Fiscal, anteponiendo la expresión "Ver opinión adjunta u otra similar", la cual es de carácter obligatorio, y se acompañen de la opinión profesional del Revisor Fiscal o del Contador Público independiente a falta de este, de conformidad con las normas de auditoría, generalmente aceptadas.

Se solicita a los proponentes para cierre de vigencia presentar los estados financieros auditados, un paquete completo de estados financieros acompañado por sus revelaciones y dictamen de revisor fiscal, firmados por un Contador Público, Representante Legal y Revisor Fiscal.

Para estados financieros intermedios un paquete completo de estados financieros acompañado por sus revelaciones, firmados por un Contador Público y Representante Legal.

2.2.1.2.1. EVALUACIÓN FINANCIERA

Para este caso se medirá la capacidad financiera del año 2024 y a junio de 2025 de la siguiente manera:

1. Índice de liquidez (Deberá ser mayor o igual a 1.5)

$$Razón\ Corriente = \frac{Activo\ Corriente}{Pasivo\ Corriente}$$

2. Índice de endeudamiento (Deberá ser menor o igual a 0.7)

$$índice\ de\ Endeudamiento = \frac{Pasivo\ Total}{Activo\ Total}$$

2.2.1.3. DOCUMENTOS TÉCNICOS

El Proponente debe presentar el Anexo 1. CARTA DE PRESENTACIÓN DE LA PROPUESTA. Este anexo es fundamental para demostrar el compromiso y la conformidad con los requerimientos establecidos en la propuesta.

En caso de que en la validación de las condiciones técnicas se identifique que no se cumplen los requisitos habilitantes de participación, la oferta será inhabilitada y se solicitará la subsanación al oferente. En caso de no subsanar en los tiempos definidos, la oferta será rechazada.

2.2.1.4. PLAN DE CONTINGENCIA

El proponente deberá certificar un Plan de Contingencia vigente.

2.2.1.5. CONTINUIDAD DE LA OPERACIÓN DEL NEGOCIO

El proponente deberá certificar un Plan de Continuidad de Operación del Negocio vigente.

2.2.1.6. CERTIFICACIÓN ISO 27001:2022

El proponente deberá presentar certificación ISO 27001:2022 vigente.

2.2.2. EVALUACIÓN DE LAS PROPUESTAS

Una vez cumplidos y aprobados los requisitos habilitantes de la oferta y proporcionados todos los documentos necesarios, se procederá a evaluar las ofertas conforme a los siguientes criterios:

Criterio	Mayor puntaje
• Propuesta económica	**550**
• Certificación ISO/IEC 20000-1:2018	**150**
• Un curso para 1 persona de 40 horas de seguridad de redes con su respectivo váucher para certificación.	**150**

• Certificado de Membresía FIRST	**150**

2.2.3. Oferta Económica

Se otorgará el mayor puntaje **(550 puntos)** a la propuesta económica más baja. El puntaje de las demás propuestas será calculado mediante la siguiente fórmula matemática:

Puntaje Oferta económica = 550 x (costo mínimo / costo del oferente)

2.2.4. Certificación ISO/IEC 20000-1:2018

Se otorgará el mayor puntaje de (150 puntos) si se aporta la certificación de seguridad **ISO/IEC 20000-1:2018** vigente a nombre del proveedor de servicio.

2.2.4.4. Un curso para 1 persona de 40 horas de seguridad de redes

Se otorgará el mayor puntaje (150 puntos) a la propuesta que ofrezca un curso para 1 persona de 40 horas de seguridad de redes con su respectivo váucher para certificación.

2.2.4.5. Certificado de Membresía FIRST

Se otorgará el mayor puntaje (150 puntos) si se aporta la **certificación de Membresía FIRST** vigente a nombre del proveedor de servicio.

2.2.5. Desempate

FIDUCIARIA CENTRAL S.A. celebrará el contrato con el Proponente que obtenga el mayor puntaje.

En caso de proponentes que empaten en el total de puntos, Fiduciaria Central S.A. invitará a los proponentes empatados a una reunión en las instalaciones de la Entidad, y en su presencia realizará un sorteo mediante la inclusión de balotas, siendo el ganador aquel Proponente que saque la balota de mayor puntaje; el mínimo de balotas que se incluirá será cinco (5); el resultado de dicho sorteo definirá quien será el seleccionado.

CAPÍTULO III

CONDICIONES GENERALES DEL CONTRATO

3.1. OBJETO

FIDUCIARIA CENTRAL S.A. adelanta la presente invitación con el fin de contratar, bajo la modalidad outsourcing con opción de compra, los servicios profesionales para el suministro, implementación y administración de una solución integral de seguridad y gestión de red, conformada por de dos (2) equipos Next Generation Firewall Fortinet nuevos y de última generación, así como la infraestructura de comunicaciones dos (2) Switches de Core configurados en alta disponibilidad y de seis (6) switches de acceso, junto con los servicios de instalación, configuración, puesta en funcionamiento, administración, gestión y soporte de toda la plataforma de seguridad perimetral y un servicio de análisis y monitoreo (Analyzer). Este proyecto tiene como propósito fortalecer la infraestructura tecnológica en cumplimiento de las recomendaciones del MinTIC, las normas ISO 27001:2022 y 27002:2022, el marco COBIT 2019 y la normatividad de la Superintendencia Financiera de Colombia, asegurando la integridad, disponibilidad y confidencialidad de la información, así como la continuidad y correcta operación del negocio.

3.2. PLAZO

El contrato tendrá una vigencia de doce (12) o veinticuatro (24) meses, según sea la necesidad de **FIDUCIARIA CENTRAL S.AS.,** los cuales serán contados a partir de la legalización de este e instalación de la solución, es decir, una vez estén instalados y operativos los equipos tecnológicos, iniciará la vigencia de este.

3.3. VALOR

Corresponderá a la remuneración total del servicio en la oferta que resulte seleccionada.

3.4. FORMA DE PAGO

El pago se efectuará mes vencido previa presentación de los soportes y entrega del informe de supervisión, el cual deberá ser avalado por la Dirección de Tecnología e Innovación de **FIDUCIARIA CENTRAL S.A.,** junto con los documentos estipulados en el contrato de servicios. Con uno o dos meses de antelación a la finalización del contrato, **FIDUCIARIA CENTRAL S.A.** tendrá la opción de decidir si continúa o no con el servicio ofrecido.

3.5. REQUISITOS PARA EL PAGO

a) Presentación de la factura con el cumplimiento de los requisitos de Ley.
b) Presentación de certificación a la fecha, expedida por el Revisor Fiscal o el Representante Legal, de conformidad con lo establecido en el artículo 50 de la ley 789 de 2002, en la cual se acredite el cumplimiento del pago de las obligaciones derivadas de los aportes de sus empleados, a los sistemas de Salud, Riesgos Profesionales, Pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Sena, según aplique.

3.6. OBLIGACIONES DEL CONTRATISTA

3.6.1. OBLIGACIONES GENERALES

a) Ejecutar idónea y oportunamente el objeto del contrato.
b) Cumplir con las obligaciones establecidas en la Ley para la prestación de los servicios de objeto del presente contrato.
c) Mantener estricta reserva y confidencialidad sobre la información que conozca por causa o con ocasión del contrato, así como, respetar la titularidad de los derechos de autor, en relación con los documentos, obras, creaciones que se desarrollen en ejecución del contrato.
d) Garantizar la oportuna, eficaz y eficiente prestación del objeto contratado, dando estricto cumplimiento al mismo y por ningún motivo suspender o abandonar el objeto contratado.
e) Obrar con lealtad y buena fe en las diferentes etapas contractuales.
f) Entregar la certificación suscrita por el Representante Legal o Revisor Fiscal, que acredite el cumplimiento del pago de aportes al sistema de seguridad social integral, parafiscales, ICBF, SENA y cajas de compensación familiar de los últimos seis (6) meses, de conformidad con el artículo 50 de la Ley 789 de 2002 o aquella que lo modifique, adicione o complemente.

3.6.2. OBLIGACIONES DE LA SOCIEDAD FIDUCIARIA

a) Designar supervisor para la vigilancia y control de la ejecución del objeto contratado.
b) Entregar la información y datos necesarios para la ejecución del contrato.
c) Pagar la remuneración pactada en los términos que se consignen en el contrato.
d) Verificar que el contratista realice el pago de aportes al sistema de seguridad social integral, parafiscales, ICBF, SENA y cajas de compensación familiar (cuando a ello haya lugar), en las condiciones establecidas por la normatividad vigente.

3.7. SUPERVISIÓN

FIDUCIARIA CENTRAL S.A. efectuará la supervisión y control de la ejecución del contrato que se derive del presente proceso de selección a través de un funcionario designado por Fiduciaria Central S.A., el supervisor del contrato está facultado para hacer solicitudes e impartir instrucciones al contratista, quien debe dar respuesta de manera oportuna; así mismos la Fiduciaria podrá efectuar visitas no programadas a las instalaciones del proveedor, para evaluar la calidad del servicio prestado y el licenciamiento de todos los componentes que estén involucrados en la prestación del servicio a nivel de hardware y software.

Todas las comunicaciones y solicitudes destinadas al contratista serán expedidas y radicadas por escrito.

3.8. GARANTÍA A FAVOR DE FIDUCIARIA CENTRAL S.A.

Dentro de los cinco (5) días hábiles siguientes a la a la fecha de suscripción del contrato, el Contratista deberá constituir una póliza de garantía única de cumplimiento a favor de entidades estatales con régimen privado de contratación cuyo beneficiario sea **Fiduciaria Central S.A.,** identificada con NIT. 800.171.372-1, expedida por una compañía de seguros legalmente constituida en Colombia, que incluya el siguiente amparo:

a. Cumplimiento del Contrato: por un monto equivalente al veinte por ciento (20%) del valor total del presente Contrato y con una vigencia igual al término de duración de este y seis (6) meses más.

b. Calidad del Servicio: por un monto equivalente al veinte por ciento (20%) del valor total del presente contrato y con una vigencia igual al término de duración de este y cuatro (4) meses más.

c. Pago de Salarios y Prestaciones Sociales: por el diez por ciento (10%) del valor total del contrato y con una vigencia igual al término de duración de este y tres (3) años más.

d. Responsabilidad Civil Extracontractual: Doscientos (200) SMMLV y con una vigencia desde la firma del contrato hasta la fecha de terminación.

ANEXO 1
CARTA DE PRESENTACIÓN DE LA PROPUESTA
RAZÓN SOCIAL PROPONENTE

Señores
FIDUCIARIA CENTRAL S.A.
Bogotá D. C.

Referencia: FIDUCIARIA CENTRAL S.A. - PROCESO DE INVITACIÓN PRIVADA PARA CONTRATAR SERVICIOS PROFESIONALES DE SEGURIDAD PERIMETRAL

El suscrito _____ identificado con la cédula de ciudadanía _____ expedida en _____, actuando en nombre de _____ y/o en calidad de representante legal de _____, domiciliada en _____ y suficientemente autorizado según consta en _____, me permito manifestar mi interés de participar en el proceso de la referencia. Declaro aceptar y haber entendido en toda su extensión sus alcances y significado los términos de referencia. Así mismo, en el evento de resultar favorecido con la adjudicación me comprometo a notificarme, perfeccionar el contrato y legalizarlo dentro de los cinco (5) días siguientes a su notificación y ejecutar el objeto contractual de acuerdo con lo establecido en los documentos que hacen parte del proceso de selección, así como los de la propuesta y del contrato.

El suscrito declara:

1. Que conozco los Términos de Referencia, anexos, aclaraciones e informaciones sobre preguntas y respuestas, así como los demás documentos relacionados con este proceso y acepto cumplir todos los requisitos en ellos exigidos conforme la documentación que estoy aportando y las declaraciones que en cada caso particular realizo. De igual forma manifiesto que acepto las consecuencias que se deriven por el incumplimiento de los requisitos antes expuestos.

2. Que ninguna persona o entidad distinta a las aquí nombradas tiene intereses en esta propuesta, ni en el contrato que como consecuencia de ella llegare a celebrarse y que, por consiguiente, solo compromete a los firmantes.

3. Que conozco y acepto en todo las leyes generales y especiales aplicables a este proceso contractual y al objeto del mismo.

4. Que con la firma de la presente carta manifiesto, bajo la gravedad del juramento, que ni la persona jurídica que represento ni el suscrito nos encontramos incursos dentro de ninguna de las causales de inhabilidad e incompatibilidad o prohibiciones establecidas en la Ley 80 de 1993, en el artículo 4 del Decreto 679 de 1994 y las demás disposiciones constitucionales y legales vigentes sobre la materia, ni hay conflictos de intereses de por medio, ni en ninguno de los eventos de prohibición especiales para contratar.

5. Que con la firma de la presente carta manifiesto, bajo la gravedad del juramento, que ni la persona jurídica que represento ni sus socios o accionistas ni el suscrito nos encontramos

incluidos dentro de las listas restrictivas que hagan referencia al Lavado de Activos y la Financiación del Terrorismo, así como que los recursos que componen nuestro patrimonio no provienen de lavado de activos, financiación del terrorismo, narcotráfico, captación ilegal de dineros y en general de cualquier actividad ilícita; también manifiesto que los recursos recibidos en desarrollo del contrato que se pretende suscribir no serán destinados a ninguna de las actividades antes descritas.

6. Que leí cuidadosamente los términos de referencia y todos y cada uno de sus Anexos y elaboré mi propuesta ajustada a los mismos. Por tanto, conocí y tuve las oportunidades establecidas para solicitar aclaraciones, formular objeciones, efectuar preguntas y obtener respuestas a mis inquietudes.

7. Que con la firma de este anexo autorizo el tratamiento de datos personales según la ley 1581 de 2012 y sus decretos reglamentarios, De manera que se gestione la información de manera adecuada para las acciones correspondientes al presente proceso.

8. Autorizo el tratamiento de mis datos personales según la ley 1581 de 2012 y sus decretos reglamentarios, para que Fiduciaria Central S.A. los gestione de manera adecuada para las acciones correspondientes al presente proceso.

9. Igualmente declaro bajo la gravedad del juramento que toda la información aportada y contenida en mi propuesta es veraz y susceptible de comprobación.

10. Que durante la vigencia del contrato se mantendrá la calidad del servicio prestado.

11. Que durante la vigencia del contrato se mantendrá el personal mínimo obligatorio ofrecido y me comprometo a facilitar los insumos necesarios para la prestación del servicio.

12. El valor de mi propuesta económica es (letras y números).

Para todos los efectos informo a ustedes que toda la correspondencia relacionada con esta contratación la recibiremos en:

Dirección: _____
Ciudad: _____
Fax: _____ Teléfono: _____
Correo electrónico 1: _____
Correo electrónico 2: _____

Cordialmente,

Firma Representante Legal: _____
Nombre: _____
Identificación: _____

ANEXO 2
AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

Autorizo de manera libre, expresa, inequívoca e informada, a FIDUCIARIA CENTRAL S.A., o a quien represente sus derechos en los términos del literal a) artículo 6 de la ley 1581 de 2012, para que:

i) Realice la recolección, almacenamiento, uso, supresión y en general, el tratamiento de mis datos personales con fines: realización de contactos, estudios estadísticos, cursos y contenidos de Fiduciaria Central S.A., así como los de las compañías vinculadas, y para facilitarle el acceso general a la información de estos; informar sobre nuevos productos o servicios que estén relacionados con el o los contratado(s) o adquirido(s); informar sobre cambios de los productos o servicios; evaluar la calidad del servicio y realizar estudios internos sobre hábitos de consumo.

ii) Comparta información con los terceros que colaboran con la entidad que para el cumplimiento de sus funciones deben acceder en alguna medida a la información tales como: proveedores del servicio de mensajería, entidades de administración y gestión de cobranza y profesionales que colaboran con la entidad en la recuperación de la cartera. Solo en aquellos casos en que yo sea deudor de Fiduciaria Central S.A., de los fondos de inversión colectiva o de los negocios fiduciarios por ella administrados, autorizo que dichos fines se extiendan a: (a) gestión y administración de recuperación de la cartera, productiva e improductiva, (b) Recopilación de información de deudores y acreedores respectivos. Declaro que se me ha informado de manera clara y comprensible que tengo derecho a conocer, actualizar y rectificar los datos personales proporcionados, a solicitar prueba de esta autorización, a solicitar información sobre el uso que se le han dado a mis datos personales, a presentar quejas ante la superintendencia de Industria y Comercio por el uso indebido de mis datos personales, a revocar esta autorización o solicitar la supresión de los datos personales suministrados y acceder de forma gratuita a los mismos.

iii) Realice reportes y consultas de mis obligaciones vigentes o en mora de las centrales de riesgos crediticios legalmente establecidas, a cualquier operador de información, cualquier entidad del sector financiero, real, la matriz y las vinculadas de la Fiduciaria, de la información acerca del nacimiento, modificación extinción de mis obligaciones directas, contingentes o indirectas, información acerca del incumplimiento de tales obligaciones, cualquier novedad en relación con mis obligaciones contraídas para con la Fiduciaria, entidades del sector financiero o del sector real, y en general de mi endeudamiento y comportamiento crediticio con la Fiduciaria y/o terceros, con el fin, entre otros, de que sea incluido mi nombre y documento de identificación en los registros de deudores morosos o con referencias negativas, mi endeudamiento, mis operaciones y/o obligaciones vigentes y las que adquiera o en el futuro llegare a celebrar con la Fiduciaria. La autorización faculta a la Fiduciaria no solo para procesar y reportar, mi información a los operadores de información sino también para que la Fiduciaria pueda solicitar y consultar información sobre mí, las relaciones comerciales con terceros, con el sector real o Financiero, el cumplimiento de sus obligaciones, contratos, hábitos de pago, etc, y para que la información reportada pueda ser circulada por el operador de información. Esta autorización comprende la información presente, pasada y futura referente al manejo, estado y cumplimiento de mis obligaciones, contratos y servicios con los sectores real, Financiero y cualquier otro tercero; y la permanencia de los reportes anteriormente mencionados en el término fijado en la ley, los fallos de la corte constitucional y/o los reglamentos de cada uno de los operadores de información; que en caso de que quede algún saldo insoluto de alguna obligación o contingencia, saldo de

intereses, comisiones, gastos, avalúos, seguros o cualquier suma adecuada la Fiduciaria, este se lleve una cuenta por cobrar a mi cargo y dicha obligación sea reportada a cualquier operador de información, así como su incumplimiento, tiempo de mora, etc.

Declaro que conozco y acepto el Manual Políticas y Procedimientos de Datos Personales de Fiduciaria Central S.A. y que la información por mí proporcionada es veraz, completa, exacta, actualizada y verificable. Mediante la firma del presente documento, manifiesto que reconozco y acepto que cualquier consulta o reclamación relacionada con el tratamiento de mis datos personales podrá ser elevada verbalmente o por escrito ante Fiduciaria Central S.A., quien es responsable del tratamiento, cuya página web es http://www.fiducentral.com/ su teléfono y correo electrónico de atención son 4124707 y habeasdata@ducentral.com, respectivamente, y su dirección es Avenida El Dorado No. 69a-51 Torre B Piso 3 Bogotá, D.C."

Firma,

Firma Representante Legal: _____
Nombre: _____
Identificación: _____

La presente política hará parte del formato de vinculación

Ciudad:		**Fecha:**	

Espacio exclusivo para Fiduciaria Central S.A.	
Productos o servicios a prestar	
Funcionario solicitante	

Análisis de Seguridad de la Información y Ciberseguridad. ¿La solicitud implica la adopción de nuevas tecnologías (nuevas aplicaciones, infraestructura tecnológica, nuevo software o cambios de proveedores que soportan la infraestructura crítica)? En caso de que la respuesta a la anterior pregunta sea **SI**, el funcionario solicitante, deberá efectuar el análisis correspondiente de Seguridad de la información y ciberseguridad con el responsable destinado en la entidad *(PV01-FMT-011 Valoración se Seguridad de la Información y Ciberseguridad a Terceros Críticos)*	SI_____NO_____

PERSONA JURIDICA	
Razón Social	
Identificación	☐NIT_____Otro☐¿cuál?_____
Nombre del Representante Legal Principal	
Identificación	☐ C.C. ☐C.E. Otro ☐¿cuál?
Nombre del Representante Legal Suplente	
Identificación	☐ C.C. ☐C.E. Otro ☐¿cuál?
Ciudad	
Teléfono	
Celular	
Dirección	

COMPOSICION ACCIONARIA

Por favor relacione sus accionistas hasta el nivel de persona natural (Beneficiario final)

Primer Nivel	%	Segundo Nivel	%	Tercer Nivel	%

REFERENCIAS COMERCIALES	
Referencia Comercial 1 Empresa Actividad Nombres y apellidos de contacto Teléfono	
Referencia Comercial 2 Empresa Actividad Nombres y apellidos de contacto Teléfono	

FIRMA REPRESENTANTE LEGAL

Observaciones Verificación SARLAFT – FATCA (Uso exclusivo Fiducentral)

NOMBRE QUIEN VERIFICA

SARLAFT- FATCA:_____**FECHA:**_____

SEG. DE LA INF. Y CIBERSEG.:_____**FECHA:** _____

POR FAVOR ADJUNTAR LOS SIGUIENTES DOCUMENTOS:

1. Registro Único Tributario
2. Cámara de Comercio no mayor a 30 días
3. Planilla o certificado Pago de Seguridad Social y Parafiscales del último mes
4. Certificado de afiliación y/o cobertura vigente de ARL.
5. Certificación bancaria no mayor a 3 meses
6. Declaración de Renta
7. Antecedentes judiciales (Policía Nacional) de los Representantes Legales registrados en Cámara de Comercio.
8. Resultado de la Autoevaluación del SG-SST presentada ante la ARL en la vigencia anterior.

IMPORTANTE:

Le recordamos remitir factura a nombre de Fiduciaria Central S.A Nit. 800.171.372-1, adjuntando certificación de los Seguridad Social y Parafiscales antes del día 25 de cada mes.

Le recordamos leer y acatar las Políticas definidas para el SG-SST por parte de la Fiduciaria, contenidas en la Cartilla de Contratistas que puede consultar en el siguiente link https://www.fiducentral.com/images/files/2023/Cartilla_Contratistas_2023.pdf

Le recordamos leer y acatar los lineamientos normativos con proveedores por parte de la Fiduciaria tendientes al manejo de la información y tratamiento de datos, contenidas en el documento que puede consultar en el siguiente link https://www.fiducentral.com/images/files/2024/LINEAMIENTOS%20NORMATIVO%20CON%20PROVEEDORES%20V0.pdf

El presente formato contempla como aprobación para el mismo la firma electrónica simple, firma electrónica certificada o la firma digital.