RESPUESTA A OBSERVACIONES PRESENTADAS AL PROYECTO DE PLIEGO DE CONDICIONES

SELECCIÓN ABREVIADA DE MENOR CUANTIA SAMC-005-2026 *"ADQUISICION DE BIENES Y SERVICIOS TECNOLOGICOS PARA FORTALECER LA SEGURIDAD DE LA INFORMACION DEL FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA"*

El Fondo de Previsión Social del Congreso de la República, en ejercicio de sus facultades legales y en aras de garantizar los principios de transparencia, selección objetiva y libre concurrencia, se permite dar respuesta a las observaciones presentadas por los interesados en desarrollo del Proceso de Contratación SAMC-005-2026, en los siguientes términos:

Chía, 30 de Agosto de 2026.

TecnoPhone

Señores:
FONDO DE PREVISIÓN SOCIAL DEL CONGRESO DE LA REPÚBLICA
Oficina Asesora de Planeación y Sistemas / Área de Contratación
Bogotá D.C.

Referencia: Observaciones al Proyecto de Pliego de Condiciones - Proceso de Selección Abreviada de Menor Cuantía No. **SAMC-005-2026.**

Respetados señores,

En calidad de interesados en participar en el proceso de la referencia, y obrando dentro de la oportunidad procesal correspondiente, nos permitimos presentar las siguientes observaciones al Proyecto de Pliego de Condiciones para su análisis y respectiva aclaración:

1. OBSERVACIÓN RESPECTO A LOS DESCUENTOS POR ESTAMPILLAS E IMPUESTOS

Revisado el documento, solicitamos amablemente a la Entidad aclarar cuáles son los descuentos exactos por concepto de estampillas y sus respectivos porcentajes que aplicarán sobre los pagos derivados de la ejecución de este contrato. Esta aclaración es fundamental para estructurar de manera precisa nuestra oferta económica, garantizando así la correcta viabilidad financiera del proyecto.

Respuesta:
En atención a la observación presentada, el Fondo de Previsión Social del Congreso de la República se permite informar, que los descuentos por concepto de estampillas únicamente se aplican para los contratos de obra pública cuya tarifa es el 0,5% del valor bruto del contrato, correspondiente a la Estampilla 50 años de labor de la Universidad Pedagógica Nacional.

2. OBSERVACIÓN POR INCONGRUENCIAS RESPECTO A EXIGENCIAS DEL SECTOR SEGUROS

Hemos evidenciado que en el Proyecto de Pliego de Condiciones quedaron consignados textos que corresponden a un proceso de contratación de seguros, los cuales no guardan ninguna relación con el objeto tecnológico (adquisición de Firewalls y Access Points) del presente proceso. Solicitamos corregir y suprimir las siguientes menciones:

Página 19 (Acreditación de la existencia): Se exige que el objeto social "deberá contemplar la celebración de contratos de seguros".
Página 34 (Evaluación de Propuestas): Se indica que la evaluación "se hará con el acompañamiento del Intermediario de seguros".
Página 38 (Causales de rechazo, numeral 7): Se indica como causal de rechazo presentar más de una propuesta "para cada uno de los ramos que conforman el programa de seguros".

Solicitamos a la Entidad suprimir estas referencias de manera integral en el Pliego de Condiciones Definitivo, adecuando la redacción estrictamente al objeto de bienes y servicios tecnológicos de la presente selección.

Respuesta:

En atención a la observación presentada, la entidad se permite informar que, una vez revisada la información señalada por la empresa observante, le asiste razón, por lo tanto, la entidad procederá a realizar la respectiva corrección en el pliego definitivo de condiciones.

Bogotá, D.C., 04 de septiembre de 2026

Cordialmente,

DANIEL FERNANDO GARZÓN ARDILA.
Profesional Especializado
Subdirección Administrativa y Financiera
Evaluador Jurídico
.

FONDO DE PREVISION SOCIAL DEL CONGRESO DE LA REPUBLICA

Cra. 10 N° 24-55 piso 2° y 3°. Tel. (57) 601 3415566 Ext 2011- 2012. Cel. 3174637146 – 3153456245- 3134125975
www.fonprecon.gov.co. BOGOTA.D.C – COLOMBIA

RESPUESTA A OBSERVACIONES

PLIEGO DE CONDICIONES SELECCIÓN ABREVIADA DE MENOR CUANTÍA SAMC-005-2026

En cumplimiento de lo establecido en el **PLIEGO DE CONDICIONES SELECCIÓN ABREVIADA DE MENOR CUANTÍA SAMC-005-2026** se procede a dar respuesta a las observaciones recibidas:

De conformidad con la necesidad expuesta por el Fondo de Previsión Social del Congreso de la República indicada en el Proyecto **PLIEGO DE CONDICIONES SELECCIÓN ABREVIADA DE MENOR CUANTÍA SAMC-005-2026**, y frente a los Requisitos Técnicos Habilitantes.

1. El oferente COLSISTEC S.A.S presenta las siguientes observaciones:

OBSERVACIÓN

I. Observación – Indicador de Endeudamiento numeral 2.2.1 Indicadores Financieros
De manera respetuosa, solicitamos a la Entidad ajustar el requisito habilitante correspondiente al indicador de endeudamiento, pasando de ≤60% a ≤70%.
El indicador se encuentra definido como:
Endeudamiento Total = (Pasivo Total / Activo Total) x 100%
Al respecto, es pertinente señalar que, conforme a lo dispuesto en la Ley 80 de 1993, en su artículo 24, los procesos de contratación deben garantizar la selección objetiva, la libre concurrencia y la igualdad de oportunidades para los proponentes. En igual sentido, la Ley 1150 de 2007 establece que los requisitos habilitantes deben ser adecuados y proporcionales al objeto a contratar, evitando condiciones restrictivas que limiten injustificadamente la participación.
Adicionalmente, el Decreto 1082 de 2015 dispone que las entidades estatales deben estructurar los procesos contractuales de manera que se promueva la pluralidad de oferentes, definiendo requisitos financieros acordes con las condiciones del mercado y el riesgo del contrato.
En este contexto, el umbral establecido de ≤60% resulta restrictivo frente a la realidad financiera de múltiples empresas del sector que, aun contando con solidez económica, capacidad de ejecución y experiencia acreditada, presentan niveles de endeudamiento ligeramente superiores sin que ello implique un riesgo en el cumplimiento de sus obligaciones contractuales.
Por lo anterior, el ajuste del indicador a ≤70% mantiene un criterio prudente de evaluación del riesgo financiero, sin desnaturalizar el requisito habilitante, y permite ampliar la participación de oferentes idóneos, garantizando los principios de transparencia, economía, selección objetiva y pluralidad de oferentes.
En consecuencia, solicitamos a la Entidad acoger la presente observación y ajustar el indicador en los términos propuestos.

RESPUESTA:

El Fondo de Previsión Social del Congreso de la República, con estricto cumplimiento de los principios que rigen la contratación estatal, estableció los requisitos de capacidad financiera, entre ellos el indicador de nivel de endeudamiento, con base en los estudios previos y estudio de mercado realizados para el presente proceso. Dichos estudios permiten concluir que los indicadores establecidos, resultan razonables, favorables y adecuados para garantizar la participación de empresas del sector tecnológico, asegurando la solvencia y la capacidad operativa necesarias para el cumplimiento del objeto contractual.

Una vez revisada la observación la Entidad No acepta, esta observación.

OBSERVACIÓN

II. Observación técnica numeral 1.1 ESPECIFICACIONES TÉCNICAS

1. Nomenclatura de funcionalidades asociada a un fabricante específico. Los ítems de "Controles de seguridad UTM" (WebBlocker, spamBlocker, Gateway AntiVirus, APT Blocker, DNSWatch, IntelligentAV, ThreatSync XDR, EDR Core) y las categorías "Branch Office VPN" / "Mobile VPN" corresponden a nomenclatura comercial registrada de un único fabricante. Verificamos que un equipo equivalente de mercado (SonicWall NSa 3800/2800) ofrece la misma funcionalidad bajo nomenclatura genérica de la industria (filtrado web por reputación, antispam, antivirus de gateway, sandboxing/APT, protección DNS, antivirus con IA, XDR/EDR gestionado), pero no puede acreditar cumplimiento bajo los nombres comerciales exigidos por tratarse de marcas de un competidor. Solicitamos su reemplazo por descripciones funcionales genéricas.

RESPUESTA

Los requisitos buscan garantizar capacidades de protección, prevención, detección y respuesta frente a amenazas, incluyendo seguridad perimetral, control de tráfico, filtrado web y DNS, protección contra malware y amenazas avanzadas, VPN, acceso remoto seguro, correlación de eventos e integración con directorios y mecanismos de autenticación.
La solución debe garantizar las funcionalidades esperadas, teniendo presente que lo solicitado es una solución unificada de amenazas UTM donde los nombres de la nomenclatura pueden diferir entre fabricantes, pero no así el alcance funcional de esta como se describe a continuación:

Nomenclatura	Alcance funcional
SD-WAN	WAN Definida por Software (SD-WAN) como solución de enrutamiento basada en software, que distribuye automáticamente el tráfico de red a través de múltiples conexiones WAN, según las políticas que se definan.
Access Portal	Portal de acceso remoto seguro a aplicaciones web comunes que utilizan tecnologías HTML, HTML5 y JavaScript, para conectividad a través de un explorador web para conectarse a estos tipos de recursos: Aplicaciones web externas de terceros, Sesiones RDP y SSH a recursos locales, Aplicaciones internas (proxy inverso).
Intrusion Prevention Service (IPS)	Detección automática de intrusiones en tiempo real con acciones preventivas de bloqueo
Application Control	Gestión de aplicaciones para restringir o permitir.
WebBlocker	Filtrado de contenido web, bloqueo explícito de categorías y sitios no autorizados, con posibilidad de seleccionar la aplicación por nombre para bloquear/permitir el tráfico para esa aplicación o para la categoría de aplicación
spamBlocker	Combinación de reglas, coincidencia de patrones y reputación del remitente para identificar y bloquear mensajes spam
Gateway AntiVirus	Servicio para prevenir el ingreso de virus a la red a través de un mensaje de correo electrónico, web o tráfico FTP.
Reputation Enabled Defense	Permitir / denegar el acceso a los sitios basados en su reputación.
Network Discovery	Detección y visibilidad de red para: Dirección IP, Nombre de dispositivo y nombre de host, Dirección MAC, Sistema operativo y servicios, Puertos de red abiertos, Dispositivos de Mobile Security
APT Blocker	Detección y bloqueo de amenazas persistentes avanzadas y ataques de día cero.
DNSWatch	Monitorizar las solicitudes de DNS tanto dentro como fuera de la red para evitar conexiones a dominios maliciosos conocidos y bloqueo de contenido según las categorías

Nomenclatura	Alcance funcional
IntelligentAV	Identificar y bloquear malware conocido y desconocido mediante mecanismos de aprendizaje automático o apoyo de inteligencia artificial
ThreatSync XDR, EDR Core	Detección y respuesta extendida (XDR) con capacidad de correlación de eventos de red y endpoint; protección de endpoint (EDR) integrada con el firewall
"Branch Office VPN" / "Mobile VPN"	Red Privada Virtual de Sucursal (BOVPN) para posibilitar las conexiones seguras y cifradas entre redes en lugares geográficamente separados, con VPN mobil que permite a un equipo remoto una conexión segura hacia la red protegida a través de una red desprotegida, tal como la Internet, mediante seguridad de Capa de Transporte (TLS) para asegurar la conexión.
Retención y gestión de logs	Retención de datos de la plataforma de seguridad perimetral para su análisis y correlación posterior o en tiempo real, con capacidad de retención de al menos 3 meses.

OBSERVACIÓN

2. Compatibilidad de migración dirigida a marca. El requisito de compatibilidad textual con *"Watchguard Firebox M370"* dirige el requerimiento a un fabricante puntual. Un equipo equivalente (NSa 3800/2800) puede garantizar la migración funcional de políticas, NAT, objetos y VPN mediante servicio profesional, pero no bajo la literalidad "compatible con Firebox M370". Solicitamos ajustar a un requisito funcional de migración, sin nombrar el fabricante destino.

RESPUESTA

La referencia de WatchGuard Firebox M370 corresponde a la plataforma actualmente implementada y tiene como propósito permitir al oferente conocer la infraestructura existente y planificar adecuadamente la migración en todos sus servicios, configuraciones y funcionalidades.
La migración deberá contemplar acciones manuales, export/import o el mecanismo disponible según corresponda para llevar las funcionalidades a la nueva solución representado en reglas y objetos de seguridad, VLAN y segmentación, NAT, filtrado web, VPN, configuraciones de propósito especifico como las conexiones con el CSIRT del sector salud, usuarios, autenticación e integraciones con las plataformas tecnológicas existentes.

Entre los elementos críticos a considerar en el proceso de migración se incluyen los siguientes, entre otros que surjan del análisis y que sean requeridos para la funcionalidad:
Reglas de tráfico, VLANs, conectividad IPSEC con el CSIRT del sector salud, reglas de NAT, reglas de filtrado web, reglas de navegación, integración con el directorio activo on premise para reglas de proxy https http, reglas de geolocalización, configuraciones de ocho interfaces (3 ISP, 3 de tráfico switch core, 1 vlan csirt, 1 vlan AP), configuraciones de conmutación por error de dos ISP, configuraciones VPN SSL con usuarios y credenciales, integración con la gestión de logs, lista negra de urls, puertos y direcciones ip bloqueadas manualmente, lista blanca de direcciones ip y url permitidas manualmente, registros de alias para identificación de activos.
El oferente deberá formular y presentar un cronograma y plan de trabajo con actividades de levantamiento de información, análisis y planeación, migración e integración, configuración y pruebas, puesta en marcha, afinamientos y estabilización; todo ello garantizando continuidad operativa con el mínimo impacto, acordando con la entidad las ventanas de mantenimiento respectivas.

OBSERVACIÓN

3. Métrica de "conexiones concurrentes" desproporcionada frente al resto del ítem. Contrastamos los requisitos contra un equipo real de mercado equivalente en tier (NSa 3800 para CD Principal, NSa 2800 para CD Alterno): en ambos casos, dicho equipo supera entre 1.4x y 6.9x los requisitos de throughput de firewall, IPS, antivirus y VPN exigidos en el mismo ítem, pero no alcanza la cifra de conexiones concurrentes solicitada (4.500.000 y 3.500.000 respectivamente vs. las cifras máximas certificadas por el fabricante consultado, entre 2 y 3 millones según metodología de conteo). Esta desproporción es un indicio técnico de que el valor se tomó de una ficha de un fabricante específico, sin un ejercicio de dimensionamiento proporcional.
Solicitamos precisar la metodología de medición exigida (conexiones por inspección de estado, por inspección profunda, o por sesión TLS — cada una arroja cifras distintas para un mismo equipo) y **ajustar el valor a una cifra proporcional al resto del ítem, así:**

- **CD Principal:** reducir de 4.500.000 a un mínimo de **3.000.000 de conexiones concurrentes**, cifra que sí es alcanzable por equipos de este mismo tier de desempeño (coherente con los 12 Gbps de firewall throughput, 8 Gbps de IPS y 8 Gbps de VPN que sí se piden y se cumplen en el mismo ítem).
- **CD Alterno:** reducir de 3.500.000 a un mínimo de **2.000.000 de conexiones concurrentes**, cifra coherente con los 5.8 Gbps de firewall throughput y demás métricas ya exigidas para este sitio.

RESPUESTA

- Las capacidades requeridas para el Centro de Datos Principal y el Centro de Datos Alterno han sido definidas con base en el dimensionamiento técnico de la operación actual y proyectada de la entidad.

El Centro de Datos Principal demanda mayor capacidad por soportar la operación permanente, mientras que el Alterno está orientado a contingencia y continuidad.

- En cuanto a la métrica de conexiones concurrentes, se precisa que la metodología de medición corresponde a conexiones concurrentes por inspección de estado, incluyendo las sesiones gestionadas por los servicios de seguridad habilitados (Firewall, IPS, Antivirus, VPN), asegurando uniformidad en la comparación de equipos y coherencia con las demás métricas de desempeño exigidas.
- Reducir la cifra de manera aislada, tomando como referencia únicamente otras métricas, no refleja adecuadamente las necesidades reales de la entidad ni la evolución prevista de sus servicios tecnológicos. Por lo anterior, se mantienen como capacidades mínimas requeridas:
- Centro de Datos Principal: 4.500.000 conexiones concurrentes
- Centro de Datos Alterno: 3.500.000 conexiones concurrentes

4. Firewall throughput UDP1518 del CD Principal desproporcionado frente al resto de la ficha. El requisito de 18 Gbps resultó, al contrastarlo contra un equipo equivalente en tier (NSa 3800), entre 1.5x y 5x superior a las demás métricas de seguridad exigidas en el mismo ítem — que sí se cumplen y superan con margen (IPS 8 Gbps vs. 3.3 requeridos, antivirus 8 Gbps vs. 3.1, VPN 8 Gbps vs. 5.2). Un desbalance de esta magnitud entre el firewall throughput "puro" y el resto de métricas de inspección del mismo equipo no es típico de un dimensionamiento real de tráfico, sino propio de una ficha de fabricante específico donde esa cifra particular resulta más alta que el resto de su propio portafolio.
Solicitamos confirmar si 18 Gbps es indispensable para la operación real de la entidad o, en su defecto, **ajustar el valor a un mínimo de 12 Gbps de firewall throughput (UDP1518)**, cifra que sí resulta coherente y proporcional con el resto de las métricas ya exigidas y validadas en el mismo ítem (IPS, antivirus y VPN), y que es alcanzable por equipos de este mismo tier de desempeño.
Alternativamente, si la Entidad considera indispensable mantener la cifra original de 18 Gbps, solicitamos admitir una **tolerancia de ±20%** (equivalente a un mínimo de 14.4 Gbps), o bien exigir que el valor se sustente con datasheet oficial del fabricante bajo metodología de medición estandarizada (RFC 2544, tamaño de paquete UDP 1518 bytes), para evitar que la cifra excluya soluciones técnicamente equivalentes en el resto del ítem por una sola métrica aislada.

RESPUESTA

La capacidad mínima de 18 Gbps de Firewall Throughput UDP 1518 para el Centro de Datos Principal corresponde al dimensionamiento técnico requerido para soportar la operación actual, donde se incluye integración con el CSIRT del sector salud, el crecimiento proyectado y la incorporación de nuevos servicios tecnológicos.

Las métricas de Firewall Throughput, IPS, Antivirus, VPN y conexiones concurrentes corresponden a capacidades diferentes y, por tanto, no deben analizarse de manera aislada ni asumirse como proporcionales entre sí.

En consecuencia, se mantiene el requisito mínimo de 18 Gbps y no resulta procedente reducirlo a 12 Gbps ni establecer una tolerancia del ±20%.

OBSERVACIÓN

5. Requisito de fuente redundante no proporcional al tier exigido en el CD Alterno. Al validar contra un equipo de mercado dimensionado exactamente para el throughput exigido en este ítem (NSa 2800), encontramos que dicho equipo no ofrece fuente redundante en su configuración estándar — función que sí está disponible en el tier inmediatamente superior. Esto sugiere una inconsistencia entre el nivel de desempeño solicitado (propio de un equipo de entrada/medio) y el nivel de redundancia eléctrica exigido (propio de un equipo de gama superior). Solicitamos revisar la proporcionalidad de este requisito frente al resto del ítem, o aceptar redundancia mediante arquitectura externa (PDU redundante, ATS) como alternativa equivalente.

RESPUESTA

El requerimiento técnico establecido para la solución de seguridad del Centro de Datos Alterno no contempla como condición la utilización de fuentes de alimentación redundantes.
El requisito establecido en las especificaciones técnicas corresponde únicamente a: Energía: Fuente de 110 V.
Por lo anterior, no se exige que la solución ofertada cuente con dos (2) fuentes de alimentación (fuentes redundantes), PDU redundante, ATS o mecanismos equivalentes de redundancia eléctrica.
El oferente deberá garantizar que la solución propuesta cumpla con el requerimiento de alimentación eléctrica de 110 V con una única fuente.

OBSERVACIÓN

6. Licenciamiento de MFA atado a un modelo comercial específico. El pliego exige *"Licencia MFA para 80 usuarios"* (y en el CD Alterno, "80 usuarios x 3 años"), redacción propia del modelo de licenciamiento por usuario/año de un producto MFA propietario de un fabricante puntual. Verificamos que otros fabricantes de firewall de tier equivalente ofrecen autenticación TOTP nativa (compatible con aplicaciones estándar de autenticación) sin licenciamiento adicional por usuario, y MFA avanzado (push, token físico, SMS) mediante integración RADIUS/SAML con proveedores de identidad externos, facturado por dicho proveedor y no por el fabricante del firewall. Esta arquitectura no encaja en un ítem redactado

como licencia de MFA propia del firewall. Solicitamos: (a) redactar el requisito como "solución de segundo factor de autenticación para 80 usuarios, nativa o integrada vía RADIUS/SAML con proveedor de identidad", sin atarlo a un modelo de licenciamiento comercial específico, y (b) aclarar si la exigencia de 80 usuarios aplica de forma consolidada para la entidad o de forma independiente por sede, dado que el pliego la repite en ambos ítems.

RESPUESTA

La cantidad requerida de licencias MFA es como mínimo de ochenta (80) disponibles para la entidad y que se pueden utilizar en cualquiera de las dos sedes de centro de datos. La solución deberá integrar MFA con la seguridad perimetral y permitir su gestión centralizada desde una única plataforma unificada de servicios. Como mínimo, deberá contemplar:

- Autenticación mediante Push.
- OTP mediante códigos de un solo uso.
- Enrolamiento mediante código QR.
- Soporte para token físico o equivalente.
- Administración de usuarios, dispositivos, políticas y eventos.
- Monitoreo y generación de reportes.

La solución deberá garantizar estas funcionalidades durante el periodo de servicio, sin requerir servicios externos adicionales con una única integración y gestión centralizada de las capacidades MFA, así como la integración con sistemas CLOUD y On premise de servicios de la entidad.

OBSERVACIÓN

7. Gestión unificada de Access Points atada a la marca del firewall. Solicitamos que este requisito se redacte como gestión centralizada (nube o on-premise) integrada con la solución ofertada, sin exigir que el fabricante del AP coincida con el del firewall.

RESPUESTA

La solución deberá contar con una única plataforma de gestión centralizada, ya sea en la nube o local, con capacidades de configuración, monitoreo, aplicación de políticas, generación de alertas y gestión de eventos. Esta plataforma deberá integrarse de manera automática con el equipo de seguridad perimetral y los servicios de MFA, garantizando la correlación de eventos, la identificación de amenazas y la aplicación de mecanismos de protección cuando técnicamente corresponda.

No se exige que el fabricante de los Access Points coincida con el del firewall, siempre que la gestión centralizada asegure la integración funcional entre los AP y los mecanismos de seguridad de la solución ofertada.

OBSERVACIÓN

8. Requisito "IPv4/IPv6 dual stack" a nivel de Access Point. El soporte dual-stack a nivel de firewall está ampliamente documentado en la industria y confirmado en el equipo de referencia consultado; sin embargo, el soporte dual-stack de gestión a nivel del propio Access Point no está documentado de forma uniforme entre fabricantes, dado que la mayoría de los AP empresariales operan en modo puente (bridge) de capa 2. Solicitamos aclarar si el requisito se refiere al tráfico transportado (estándar en cualquier AP) o a la IP de gestión propia del equipo (no uniforme en la industria).

RESPUESTA

El requisito de IPv4/IPv6 Dual Stack para los Access Points busca garantizar la operación de la infraestructura inalámbrica en entornos donde coexistan ambos protocolos y su integración con la infraestructura actual y futura de la entidad.
El requisito aplica tanto al tráfico transportado por los AP (estándar en cualquier dispositivo de capa 2) como a la IP de gestión propia del equipo, de manera que la administración, monitoreo y aplicación de políticas puedan realizarse de forma nativa en entornos dual stack.
Esta condición asegura que la infraestructura adquirida no limite la transición hacia IPv6 ni la interoperabilidad con los servicios de seguridad y gestión centralizada.
El requerimiento se alinea al proceso de adopción de IPv6 en las entidades públicas y a los lineamientos del MinTIC, garantizando que la solución ofertada sea compatible con la evolución tecnológica de la Entidad.

OBSERVACIÓN

9. Especificación "Max Data Rate 574 Mbps" para AP WiFi 6. Esta cifra corresponde a un único stream en banda 2.4 GHz. Verificamos que un AP WiFi 6 real de mercado entrega tasas agregadas muy superiores (1.15 Gbps en banda 2.4 GHz y 4.8 Gbps en banda 5 GHz). Solicitamos ajustar la cifra a un estándar WiFi 6 real.

RESPUESTA

El valor de 574 Mbps corresponde a la capacidad de transmisión de datos requerida para un Access Point WiFi 6 en banda 2.4 Ghz, de acuerdo con las especificaciones técnicas del proceso. Este valor se toma como referencia de cumplimiento y no como límite máximo de desempeño.Dicha cifra corresponde a un stream en

banda 2.4 GHz, y que serán igualmente admisibles soluciones que presenten tasas agregadas superiores en bandas de 2.4 GHz y 5 GHz, conforme a las capacidades reales de los equipos WiFi 6 disponibles en el mercado.
El oferente deberá demostrar mediante ficha técnica oficial del fabricante o documentación verificable que el modelo ofertado soporta capacidad de transmisión de datos en banda de 2.4 GHz a 574 Mbps y bajo la configuración técnica declarada por el fabricante.
En consecuencia, la condición exigida es garantizar que el Access Point ofertado cumpla con los 574 Mbps en banda de 2.4 GHz, sin que ello limite la aceptación de equipos que acrediten mayores capacidades, siempre que cumplan integralmente con las demás especificaciones técnicas requeridas.

OBSERVACIÓN

10. Criterio de fabricante subjetivo. Sugerimos reemplazar "marca reconocida en soluciones de seguridad de borde" por un criterio objetivo y verificable (posicionamiento en informes independientes de analistas de la industria en los últimos 2 años, y/o certificaciones ICSA Labs, Common Criteria NDPP o FIPS 140-2/3 vigentes).

RESPUESTA

El cumplimiento del criterio debe ser de una marca acreditada del mercado mediante certificaciones o constancias del fabricante, informes de analistas independientes, certificaciones de seguridad vigentes, acreditaciones técnicas o documentación oficial y verificable de terceros que permitan demostrar su trayectoria, reconocimiento y respaldo tecnológico.

La documentación deberá identificar claramente al fabricante y, cuando corresponda, la solución ofertada.

El reconocimiento o trayectoria del fabricante no sustituye el cumplimiento de los requisitos técnicos y funcionales establecidos en el Pliego de Condiciones y sus anexos.

En consecuencia, la única condición para acreditar el criterio es presentar evidencia documental objetiva, vigente y verificable que permita demostrar el reconocimiento o respaldo del fabricante, sin establecer una marca específica como condición de participación y manteniendo el cumplimiento integral de los requisitos técnicos mínimos.

2. El oferente DATASEC S.A.S. presenta las siguientes observaciones

OBSERVACIÓN 1:

Requerimiento:
"Controles de seguridad UTM: SD-WAN, Access Portal, Intrusion Prevention Service (IPS), Application Control, WebBlocker, spamBlocker, Gateway AntiVirus, Reputation Enabled Defense, Network Discovery, APT Blocker, DNSWatch, IntelligentAV, ThreatSync (XDR), EDR Core, Retención y gestión de logs."

Justificación:
Las denominaciones WebBlocker, spamBlocker, APT Blocker, DNSWatch, IntelligentAV, ThreatSync, Reputation Enabled Defense, Network Discovery, Access Portal y EDR Core corresponden a nombres comerciales registrados y de uso exclusivo de un único fabricante (WatchGuard). Ningún otro fabricante del mercado puede acreditar estas funcionalidades bajo dicha nomenclatura literal, aun cuando cuente con capacidades técnicas equivalentes o superiores. Esta redacción restringe la pluralidad de oferentes y direcciona el proceso hacia una única marca, contraviniendo los principios de selección objetiva, libre concurrencia y transparencia que rigen la contratación estatal (art. 24 y 30 de la Ley 80 de 1993, y art. 5 de la Ley 1150 de 2007), los cuales exigen que las especificaciones técnicas se definan en términos de funcionalidades y estándares, y no de marcas o nombres comerciales, salvo que se justifique la excepción correspondiente.

Solicitud:
Solicitamos respetuosamente a la entidad ajustar la redacción del requerimiento, describiendo los controles exigidos en términos de funcionalidad técnica y no de nombres comerciales, de manera que cualquier fabricante pueda acreditar el cumplimiento con su propia nomenclatura. Se sugiere la siguiente redacción alternativa:
"Controles de seguridad de nueva generación (NGFW/UTM), integrados en una misma plataforma y consola de gestión del mismo fabricante: SD-WAN; portal de acceso remoto seguro; sistema de prevención de intrusiones (IPS); control de aplicaciones; filtrado de contenido web por categorías y reputación; antispam; antivirus/antimalware de pasarela; análisis de amenazas avanzadas en sandbox

para protección contra APT y amenazas de día cero; seguridad y filtrado DNS; antimalware basado en inteligencia artificial o aprendizaje automático; detección y respuesta extendida (XDR) con correlación de eventos de red y endpoint; protección de endpoint (EDR) integrada con el firewall; inspección de tráfico cifrado TLS/SSL; acceso de red de confianza cero (ZTNA); retención y gestión centralizada de logs."
Lo anterior garantiza pluralidad de oferentes sin sacrificar el nivel técnico ni funcional requerido por la entidad.

RESPUESTA

Los requisitos buscan garantizar capacidades de protección, prevención, detección y respuesta frente a amenazas, incluyendo seguridad perimetral, control de tráfico, filtrado web y DNS, protección contra malware y amenazas avanzadas, VPN, acceso remoto seguro, correlación de eventos e integración con directorios y mecanismos de autenticación.
La solución debe garantizar las funcionalidades esperadas, teniendo presente que lo solicitado es una solución unificada de amenazas UTM donde los nombres de la nomenclatura pueden diferir entre fabricantes, pero no así el alcance funcional de esta como se describe a continuación:

Nomenclatura	Alcance funcional
SD-WAN	WAN Definida por Software (SD-WAN) como solución de enrutamiento basada en software, que distribuye automáticamente el tráfico de red a través de múltiples conexiones WAN, según las políticas que se definan.
Access Portal	Portal de acceso remoto seguro a aplicaciones web comunes que utilizan tecnologías HTML, HTML5 y JavaScript, para conectividad a través de un explorador web para conectarse a estos tipos de recursos: Aplicaciones web externas de terceros, Sesiones RDP y SSH a recursos locales, Aplicaciones internas (proxy inverso).
Intrusion Prevention Service (IPS)	Detección automática de intrusiones en tiempo real con acciones preventivas de bloqueo
Application Control	Gestión de aplicaciones para restringir o permitir.
WebBlocker	Filtrado de contenido web, bloqueo explícito de categorías y sitios no autorizados, con posibilidad de seleccionar la aplicación por nombre para bloquear/permitir el tráfico para esa aplicación o para la categoría de aplicación
spamBlocker	Combinación de reglas, coincidencia de patrones y reputación del remitente para identificar y bloquear mensajes spam
Gateway AntiVirus	Servicio para prevenir el ingreso de virus a la red a través de un mensaje de correo electrónico, web o tráfico FTP.
Reputation Enabled Defense	Permitir / denegar el acceso a los sitios basados en su reputación.

Nomenclatura	Alcance funcional
Network Discovery	Detección y visibilidad de red para: Dirección IP, Nombre de dispositivo y nombre de host, Dirección MAC, Sistema operativo y servicios, Puertos de red abiertos, Dispositivos de Mobile Security
APT Blocker	Detección y bloqueo de amenazas persistentes avanzadas y ataques de día cero.
DNSWatch	Monitorizar las solicitudes de DNS tanto dentro como fuera de la red para evitar conexiones a dominios maliciosos conocidos y bloqueo de contenido según las categorías
IntelligentAV	Identificar y bloquear malware conocido y desconocido mediante mecanismos de aprendizaje automático o apoyo de inteligencia artificial
ThreatSync XDR, EDR Core	Detección y respuesta extendida (XDR) con capacidad de correlación de eventos de red y endpoint; protección de endpoint (EDR) integrada con el firewall
"Branch Office VPN" / "Mobile VPN"	Red Privada Virtual de Sucursal (BOVPN) para posibilitar las conexiones seguras y cifradas entre redes en lugares geográficamente separados, con VPN mobil que permite a un equipo remoto una conexión segura hacia la red protegida a través de una red desprotegida, tal como la Internet, mediante seguridad de Capa de Transporte (TLS) para asegurar la conexión.
Retención y gestión de logs	Retención de datos de la plataforma de seguridad perimetral para su análisis y correlación posterior o en tiempo real, con capacidad de retención de al menos 3 meses.

OBSERVACIÓN 2:

Requerimiento:
Compatible para migración transparente de plantilla de reglas desde Watchguard Firebox M370." "Migraciones: Migración de reglas y configuraciones desde Firebox M370, afinamiento y estabilización."

Justificación:
La exigencia de "migración transparente de plantilla de reglas" desde un equipo WatchGuard Firebox M370 constituye un requisito que, en la práctica, solo puede acreditar el mismo fabricante del equipo saliente (WatchGuard) o un partner que utilice sus herramientas propietarias de exportación/importación

de configuración. No existe en el mercado una herramienta estándar e interoperable que permita a fabricantes distintos migrar de forma "transparente" y automática una plantilla completa de reglas entre plataformas de diferente marca, dado que cada fabricante utiliza formatos de configuración, sintaxis de políticas y estructuras de objetos propios y no interoperables entre sí.
Exigir transparencia en dicha migración, en lugar de exigir el resultado funcional equivalente, direcciona el proceso hacia un único oferente y desconoce que la migración de reglas entre plataformas de seguridad perimetral de distintos fabricantes es una práctica de mercado habitual, que se ejecuta mediante análisis, mapeo y reconfiguración manual o asistida de las políticas existentes, sin que ello dependa de la marca de la solución entrante.
Este tipo de condicionamiento contraviene los principios de selección objetiva y libre concurrencia de oferentes (art. 24 y 30 de la Ley 80 de 1993, y art. 5 de la Ley 1150 de 2007).

Solicitud:
Solicitamos respetuosamente a la entidad ajustar la redacción del requerimiento, eliminando la exigencia de "migración transparente de plantilla" y reemplazándola por una obligación de resultado, que garantice la continuidad operativa sin condicionar el mecanismo técnico a una marca específica. Se sugiere la siguiente redacción alternativa:
"El contratista deberá garantizar la migración completa de la totalidad de las reglas, objetos, políticas de NAT, VPN, VLAN, usuarios y demás configuraciones vigentes en la plataforma de seguridad perimetral actual de la Entidad (WatchGuard Firebox M370) hacia la nueva solución ofertada, incluyendo las labores de afinamiento (tuning) y estabilizaciones necesarias para asegurar la continuidad operativa y de seguridad durante y después del proceso de migración." **DATASEC S.A.S. Nit:901.223.827-1** Carrera 14 a # 101 - 11 Of. 201, Bogotá 323 2901254

Lo anterior asegura que la entidad reciba el mismo resultado funcional exigido, sin limitar la pluralidad de oferentes a quienes puedan ofrecer una herramienta de migración propietaria de un único fabricante.

RESPUESTA

La referencia de WatchGuard Firebox M370 corresponde a la plataforma actualmente implementada y tiene como propósito permitir al oferente conocer la infraestructura existente y planificar adecuadamente la migración en todos sus servicios, configuraciones y funcionalidades.
La migración deberá contemplar acciones manuales, export/import o el mecanismo disponible según corresponda para llevar las funcionalidades a la nueva solución representado en reglas y objetos de seguridad, VLAN y segmentación, NAT, filtrado web, VPN, configuraciones de propósito especifico como las conexiones con el CSIRT del sector salud, usuarios, autenticación e integraciones con las plataformas tecnológicas existentes.

Entre los elementos críticos a considerar en el proceso de migración se incluyen los siguientes, entre otros que surjan del análisis y que sean requeridos para la funcionalidad:
Reglas de tráfico, VLANs, conectividad IPSEC con el CSIRT del sector salud, reglas de NAT, reglas de filtrado web, reglas de navegación, integración con el directorio activo on premise para reglas de proxy https http, reglas de geolocalización, configuraciones de ocho interfaces (3 ISP, 3 de tráfico switch core, 1 vlan csirt, 1 vlan AP), configuraciones de conmutación por error de dos ISP, configuraciones VPN SSL con usuarios y credenciales, integración con la gestión de logs, lista negra de urls, puertos y direcciones ip bloqueadas manualmente, lista blanca de direcciones ip y url permitidas manualmente, registros de alias para identificación de activos.
El oferente deberá formular y presentar un cronograma y plan de trabajo con actividades de levantamiento de información, análisis y planeación, migración e integración, configuración y pruebas, puesta en marcha, afinamientos y estabilización; todo ello garantizando continuidad operativa con el mínimo impacto, acordando con la entidad las ventanas de mantenimiento respectivas.

OBSERVACIÓN 3:

Requerimiento:
Los valores reproducen exactamente la hoja técnica de dos modelos de un mismo fabricante y usan la nomenclatura de pruebas propia de ese fabricante. No se indica que sean mínimos ni se admiten valores superiores.

- Donde dice (CD principal): "UTM (full scan) 2.4 Gbps / VPN (IMIX) 1.8 Gbps / HTTPS Content Inspection (IPS enabled) 1.32 Gbps / Antivirus 3.1 Gbps / IPS (full scan) 3.3 Gbps / Firewall (UDP 1518) 18.0 Gbps / VPN (UDP 1518) 5.2 Gbps / Concurrent connections 4.500.000"

- Donde dice (CD alterno): "UTM (full scan) 1.18 Gbps / VPN 800 Mbps / HTTPS Content Inspection (IPS enabled) 696 Mbps / Antivirus 1.47 Gbps / IPS (full scan) 1.3 Gbps / Firewall (UDP 1518) 5.8 Gbps / VPN (UDP 1518) 2.4 Gbps / Concurrent connections 3.500.000"

Justificación:
Estos valores replican exactamente la hoja técnica de dos modelos de un mismo fabricante, incluida su nomenclatura propia de pruebas (p. ej. "UDP 1518"). Al no indicarse expresamente que son valores mínimos ni admitirse valores superiores, el requisito se interpreta como una ficha técnica cerrada que solo esos dos modelos pueden cumplir exactamente, restringiendo la pluralidad de oferentes.

Solicitud:
Solicitamos respetuosamente a la entidad aclarar que los valores corresponden a umbrales mínimos, admitiendo equipos con desempeño igual o superior, y ajustar la redacción así:

"Los equipos deberán contar con aceleración por hardware mediante procesadores de propósito específico para funciones de red y seguridad, con rendimiento acreditado por el fabricante en su hoja técnica, así:
- CD principal: throughput de firewall ≥ 18 Gbps; IPS ≥ 3.3 Gbps; protección contra amenazas (IPS+antivirus+control de aplicaciones simultáneos) ≥ 2.4 Gbps; inspección SSL/TLS ≥ 1.3 Gbps; IPsec VPN ≥ 5 Gbps; sesiones concurrentes ≥ 4.500.000.
- CD alterno: throughput de firewall ≥ 5.8 Gbps; IPS ≥ 1.3 Gbps; protección contra amenazas ≥ 1.18 Gbps; inspección SSL/TLS ≥ 700 Mbps; IPsec VPN ≥ 2.4 Gbps; sesiones concurrentes ≥ 3.500.000."
DATASEC S.A.S. Nit:901.223.827-1 Carrera 14 a # 101 - 11 Of. 201, Bogotá 323 2901254

RESPUESTA
Los valores descritos corresponden a capacidades mínimas, por lo cual, el oferente podrá proponer una solución con capacidades iguales o superiores.

OBSERVACIÓN 4:
Requerimiento:
8 interfaces Giga ethernet para conexiones RJ45 / 2 interfaces ten giga SFP+ PARA CONEXIONES DAC"
"Suplementos físicos: dos (2) Trasceiver para los puertos 10giga, para conexiones DAC"

Justificación:
Un cable DAC (Direct Attach Copper) trae integrados en sus extremos los conectores SFP+ necesarios, por lo que no requiere transceptores ópticos adicionales; estos solo son necesarios para conexiones de fibra óptica. Exigir simultáneamente "conexión DAC" y "transceiver para los puertos 10G" resulta contradictorio y puede inducir a los oferentes a cotizar elementos innecesarios o a interpretar el requisito de forma distinta, afectando la comparabilidad de las ofertas. Tampoco se precisa si las 2 interfaces de 10G deben ser puertos SFP+ nativos o si se admite su habilitación mediante módulo adicional, lo cual también puede generar ambigüedad en la cotización.

Solicitud:
Solicitamos respetuosamente a la entidad aclarar y ajustar la redacción del requerimiento, precisando el medio de conexión deseado y eliminando la inconsistencia:
"8 interfaces Gigabit Ethernet para conexiones RJ45; 2 interfaces 10 Gigabit SFP+ (nativas o mediante módulo adicional). En caso de requerirse conexión mediante cable DAC, deberán incluirse los cables DAC 10G correspondientes, los cuales no requieren transceptor óptico adicional dado que este viene integrado en el propio cable."

RESPUESTA

Los valores descritos a nivel de requerimiento de conexión e interfaces son los mínimos solicitados por la entidad, los dispositivos deben tener la capacidad para transceiver SFP + o en caso de que se requiera la posibilidad de DAC directamente de fabricante mínimo a 10 G. El oferente debe entregar los respectivos Transceiver a 10 G o los cables DAC según la solución ofertada, el mínimo requerimiento debe permitir conexiones a 10 G.

OBSERVACIÓN 5:

Requerimiento:
"Marca reconocida en soluciones de seguridad de borde."

Justificación:
El término "marca reconocida" no cuenta con una definición objetiva ni un criterio verificable de cumplimiento, lo que lo convierte en un requisito subjetivo sujeto a la interpretación discrecional del evaluador. Esto vulnera el principio de selección objetiva (art. 5 de la Ley 1150 de 2007), que exige que los factores de escogencia sean claros, medibles y verificables por igual para todos los oferentes, evitando ambigüedades que puedan derivar en calificaciones arbitrarias o en el rechazo injustificado de propuestas técnicamente idóneas.

Solicitud:
Solicitamos respetuosamente a la entidad reemplazar el criterio subjetivo por un parámetro objetivo y verificable, acorde con estándares reconocidos en la industria de ciberseguridad: **DATASEC S.A.S. Nit:901.223.827-1** Carrera 14 a # 101 - 11 Of. 201, Bogotá 323 2901254

"El fabricante de la solución de seguridad perimetral deberá figurar en la última edición publicada del Magic Quadrant de Gartner para Network Firewalls, o acreditar evaluaciones independientes vigentes en la categoría de firewall empresarial (CyberRatings, MITRE ATT&CK Evaluations o ICSA Labs)."

RESPUESTA

En aras de maximizar los principios de selección objetiva (Art. 5 de la Ley 1150 de 2007) y libre concurrencia, se precisar el alcance de dicha expresión.
El cumplimiento del criterio debe ser de una marca acreditada del mercado mediante certificaciones o constancias del fabricante, informes de analistas independientes, certificaciones de seguridad vigentes, acreditaciones técnicas o documentación oficial y verificable de terceros que permitan demostrar su trayectoria, reconocimiento y respaldo tecnológico.
La documentación deberá identificar claramente al fabricante y, cuando corresponda, la solución ofertada.

El reconocimiento o trayectoria del fabricante no sustituye el cumplimiento de los requisitos técnicos y funcionales establecidos en el Pliego de Condiciones y sus anexos.

En consecuencia, la única condición para acreditar el criterio es presentar evidencia documental objetiva, vigente y verificable que permita demostrar el reconocimiento o respaldo del fabricante, sin establecer una marca específica como condición de participación y manteniendo el cumplimiento integral de los requisitos técnicos mínimos.

OBSERVACIÓN 6:
Requerimiento:
"Seguridad: Gestión unificada en Firewall de borde" "Throughput: Max Data rate up to 574 Mbps" "Integraciones: Integrar la gestión centralizada desde el firewall de borde"

Justificación:
El valor de 574 Mbps corresponde a la tasa de datos de un modelo específico de access point en banda de 2.4 GHz y se presenta como techo ("up to") y no como umbral mínimo, lo que puede interpretarse como una ficha técnica cerrada que direcciona hacia un único fabricante o modelo. Adicionalmente, el requerimiento no especifica estándares de seguridad inalámbrica, versión de Wi-Fi ni capacidades de banda dual, lo cual deja abierto un margen de ambigüedad en la evaluación técnica.

Solicitud:
Solicitamos respetuosamente a la entidad ajustar la redacción, indicando expresamente que los valores corresponden a mínimos y admitiendo especificaciones superiores, así como precisar los estándares de seguridad esperados:
"Seguridad: WPA3; autenticación 802.1X; aislamiento de SSID para invitados; gestión unificada e integrada desde el firewall de borde; instalación de firmware y actualizaciones desde el fabricante."
"Throughput: tasa de datos mínima de 574 Mbps en 2.4 GHz y 1.2 Gbps en 5 GHz (se admiten valores superiores); Wi-Fi 6 (802.11ax) en ambas bandas; MU-MIMO."

RESPUESTA

Los valores de 574 Mbps en banda 2.4 GHz y 1.2 Gbps en banda 5 GHz corresponden a la capacidad mínima de transmisión de datos requerida para un Access Point Wi-Fi 6 (802.11ax) con soporte MU-MIMO. Dichos valores se establecen como mínimos de referencia y no constituyen un límite máximo de desempeño, por lo que serán admitidas soluciones que acrediten capacidades superiores en cualquiera de las bandas, siempre que cumplan integralmente con las demás condiciones técnicas exigidas.
En materia de seguridad, la solución deberá integrar de manera nativa:

- WPA3 como estándar de cifrado inalámbrico.

- Autenticación 802.1X para control de acceso.
- Aislamiento de SSID para invitados.
- Gestión unificada e integrada desde el firewall de borde, garantizando correlación de eventos y administración centralizada.
- Instalación de firmware y actualizaciones directamente desde el fabricante, asegurando trazabilidad y soporte oficial.

OBSERVACIÓN 7:
Requerimiento:
"Segundo factor de autenticación MFA: Licencia MFA para 80 usuarios, 3 años."

Solicitud:
Se solicita amablemente a la entidad confirmar y unificar en el pliego el número exacto de usuarios a licenciar para la solución MFA (80 o 90 usuarios), corrigiendo la inconsistencia identificada.
Se solicita amablemente de la misma manera a la entidad precisar si la solución de autenticación multifactor debe corresponder al mismo fabricante del firewall ofertado, con el fin de garantizar la integración nativa entre ambas soluciones, reduciendo la complejidad operativa y los riesgos de incompatibilidad entre soluciones de distintos fabricantes. **DATASEC S.A.S. Nit:901.223.827-1** Carrera 14 a # 101 - 11 Of. 201, Bogotá 323 2901254

Especificar el mecanismo de segundo factor requerido, indicando si es aceptable o exigible el token por aplicación móvil (notificación push y OTP), o si se admiten otros mecanismos equivalentes (SMS, hardware token, biometría, etc.).

RESPUESTA

La cantidad requerida de licencias MFA es como mínimo de ochenta (80) disponibles para la entidad y que se pueden utilizar en cualquiera de las dos sedes de centro de datos. La solución deberá integrar MFA con la seguridad perimetral y permitir su gestión centralizada desde una única plataforma unificada de servicios. Como mínimo, deberá contemplar:

- Autenticación mediante Push.
- OTP mediante códigos de un solo uso.
- Enrolamiento mediante código QR.
- Soporte para token físico o equivalente.
- Administración de usuarios, dispositivos, políticas y eventos.
- Monitoreo y generación de reportes.

La solución deberá garantizar estas funcionalidades durante el periodo de servicio, sin requerir servicios externos adicionales con una única integración y gestión centralizada de las capacidades MFA, así como la integración con sistemas CLOUD y On premise de servicios de la entidad.

OBSERVACIÓN 8:
Requerimiento:
"INGENIERO ESPECIALISTA EN REDES Y SEGURIDAD: (...) Deseable certificación en seguridad o redes (CCNA o CCNP, Certificación Networking de Watchguard, etc.)"

Solicitud:
Solicitamos respetuosamente a la entidad ajustar la redacción del requisito, de manera que la certificación exigida se relacione con la solución efectivamente ofertada y no con una marca en particular:
"INGENIERO ESPECIALISTA EN REDES Y SEGURIDAD: (...) Deseable certificación vigente del fabricante de la solución ofertada, en nivel profesional o superior, para la línea de firewall de nueva generación; o certificación en redes (CCNA/CCNP o equivalente)."
Al mencionar expresamente "Certificación Networking de WatchGuard" como ejemplo de certificación deseable, sin indicar su equivalente para otros fabricantes de soluciones de firewall, el requisito favorece indirectamente a los oferentes que representan dicha marca, en detrimento de quienes ofertan soluciones de otros fabricantes cuyo personal certificado no podría acreditar una condición equivalente bajo esa misma denominación.

RESPUESTA

La Entidad, en aras de garantizar la pluralidad de oferentes y la libre concurrencia en el presente proceso de selección, aclara que el propósito de incluir este requisito como deseable es asegurar que el personal técnico encargado de implementar los firewalls cuente con el conocimiento avanzado y específico de la tecnología que se desplegará en la infraestructura del Fondo de Previsión Social del Congreso de la República.
Sin embargo, para garantizar la equidad y permitir que los proponentes oferten la solución tecnológica se ajustará la redacción para que la certificación exigida corresponda al fabricante de la solución que cada oferente proponga, manteniendo el rigor técnico de que dicha certificación sea de nivel profesional/avanzado y específica para la tecnología de Firewall.

La Entidad acepta la observación parcialmente, aunado a lo anterior la entidad modificará el Numeral 7.1.5 PERSONAL MÍNIMO REQUERIDO: INGENIERO ESPECIALISTA EN REDES Y SEGURIDAD, la cual quedará de la siguiente manera:

INGENIERO ESPECIALISTA EN REDES Y SEGURIDAD: Profesional Ingeniería de Sistemas, Electrónica, Telecomunicaciones o carreras afines. Deseable: Certificación vigente de nivel profesional, avanzado o superior, emitida por el fabricante de la solución de Firewall ofertada, que acredite competencias en administración, implementación, diseño o seguridad de firewalls, experiencia Mínimo cuatro (4) años en proyectos relacionados con seguridad de la información y gestión de red en procesos de transición o disposición de equipos

OBSERVACIÓN 9

Requerimiento:
"INGENIERO DE INFRAESTRUCTURA: (...) Certificaciones o diplomados en gestión de infraestructura, ciberseguridad y redes, preferiblemente en las marcas y soluciones ofrecidas."

Solicitud:
Solicitamos respetuosamente a la entidad ajustar la redacción, de manera que el requisito sea objetivo y verificable:
"INGENIERO DE INFRAESTRUCTURA: (...) Certificación vigente del fabricante de la solución ofertada, en administración de la plataforma de seguridad perimetral." **DATASEC S.A.S. Nit:901.223.827-1** Carrera 14 a # 101 - 11 Of. 201, Bogotá 323 2901254

RESPUESTA

La Entidad acepta la observación parcialmente, aunado a lo anterior la entidad modificará el Numeral 7.1.5 PERSONAL MÍNIMO REQUERIDO: "INGENIERO DE INFRAESTRUCTURA, la cual quedará de la siguiente manera:

INGENIERO DE INFRAESTRUCTURA: Profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Telecomunicaciones o carreras afines. Certificación vigente emitida por el fabricante de la solución de seguridad perimetral ofertada, que acredite competencias en la administración, configuración e implementación de la plataforma de seguridad perimetral. Experiencia mínima de doce (12) meses en la implementación, configuración, migración o administración de soluciones de seguridad perimetral (Firewall / UTM)

OBSERVACIÓN 10
Requerimiento:
[No se especifica un requerimiento puntual sobre certificaciones organizacionales del proponente en materia de seguridad de la información dentro del pliego.]

Solicitud:
Se solicita a la Entidad incluir como requisito habilitante o como factor de calidad puntuable, la acreditación por parte del proponente de certificación vigente en ISO/IEC 27001, así como certificación o alineación con ISO/IEC 27032, mediante la presentación del certificado vigente expedido por un organismo de certificación acreditado.

El pliego no exige al proponente acreditar certificaciones internacionales vigentes en materia de gestión de seguridad de la información, lo cual resulta relevante tratándose de un proyecto de ciberseguridad que involucra el manejo de infraestructura crítica y activos de información sensibles de la Entidad. Contar con proponentes certificados en normas como ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información) e ISO/IEC 27032 (Ciberseguridad) permite garantizar que la compañía ejecutora cuenta con procesos, controles y buenas prácticas estandarizadas internacionalmente para la implementación, operación y soporte de soluciones de seguridad, reduciendo el riesgo de una ejecución contractual deficiente y brindando mayor trazabilidad y confianza sobre la idoneidad técnica y organizacional del oferente.

RESPUESTA

No se considera procedente ni necesario incluir las certificaciones ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información) ni ISO/IEC 27032 (Directrices para la Ciberseguridad) como requisitos habilitantes o factores de calidad puntuables, por las siguientes razones:

1. Vulneración al Principio de Libre Concurrencia y Pluralidad de Oferentes: Exigir certificaciones corporativas específicas y vigentes al momento de la presentación de la oferta limita el acceso al proceso a un número reducido de proponentes que cuentan con el músculo financiero para costear dichas auditorías de certificación. Esto vulnera el artículo 24 de la Ley 80 de 1993 y el principio de libre concurrencia, al excluir del mercado a oferentes técnicamente idóneos que cumplen con las fichas técnicas de los bienes o servicios requeridos, pero no ostentan el sello de la norma ISO en mención.
2. Falta de Proporcionalidad y Relación Directa con el Objeto (Art5, Ley 1150 de 2007): El Estatuto General de Contratación Pública señala que los requisitos habilitantes deben ser adecuados y proporcionales al objeto a contratar. Las normas ISO 27001 e ISO 27032 certifican procesos internos de gestión de la empresa, no la calidad específica del producto o servicio final que se va a entregar a la Entidad. Exigir que toda la organización del proponente esté certificada resulta desproporcionado frente a las necesidades identificadas en los estudios previos.

OBSERVACIÓN 11

Requerimiento:

"GERENTE DE PROYECTOS: Profesional con formación académica en áreas relacionadas con sistemas, informática, tecnologías de la información. Posgrado en Gerencia de Proyectos Tecnológicos, experiencia Mínimo cuatro (4) años gestión y coordinación de proyectos de tecnología."

Solicitud: Se solicita a la Entidad ampliar la formación académica exigida al Gerente de Proyectos para admitir título profesional en Ingeniería Eléctrica, Electrónica, Sistemas, Telecomunicaciones, Industrial o carreras afines; así como admitir como alternativa al posgrado en Gerencia de Proyectos, la certificación PMP vigente. Igualmente, se solicita incluir como requisito la certificación vigente en ITIL Foundation v3 o superior, dado su aporte a la correcta gestión de los servicios de TI derivados del proyecto. **DATASEC S.A.S. Nit:901.223.827-1** Carrera 14 a # 101 - 11 Of. 201, Bogotá 323 2901254

RESPUESTA

La Entidad acoge la solicitud de forma parcial, considerando que las disciplinas de Ingeniería de Sistemas, Informática, Tecnologías de la Información, Ingeniería Eléctrica, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, o carreras afines debidamente justificadas, poseen planes de estudio y competencias que se alinean directamente con la naturaleza de esta contratación. Sin embargo, la Ingeniería Industrial se enfoca en la optimización de procesos, logística, productividad y cadenas de suministro, su formación de base no incluye arquitectura de redes, protocolos de seguridad, topologías de firewall o infraestructura TI, que son objeto de esta contratación.

La Entidad reconoce que considerar equivalente esta certificación internacional a un posgrado en Gerencia de Proyectos no solo es técnicamente válida, sino que amplía el mercado de profesionales idóneos que pueden participar en el proceso.

Frente a las demás certificaciones PMP e ITIL Foundation v3 o superior. La Entidad considera que estas son importantes en el ámbito tecnológico; no obstante, para este objeto contractual no lo vemos necesario como requisito habilitante. Esta contratación radica en la adquisición e implementación de infraestructura de seguridad perimetral

La Entidad acepta la observación parcialmente, aunado a lo anterior la entidad modificará el Numeral 7.1.5 PERSONAL MÍNIMO REQUERIDO: GERENTE DE PROYECTOS, la cual quedará de la siguiente manera:

GERENTE DE PROYECTOS: Profesional con formación académica de pregrado en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Eléctrica, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería de Tecnologías de la Información, o carreras afines. Posgrado en Gerencia de Proyectos o en su defecto, certificación vigente como Project Management Professional (PMP). Experiencia: Mínimo cuatro (4) años en gestión y coordinación de proyectos de tecnología.

OBSERVACIÓN 12:
Requerimiento:
"Distribuidor certificado y partner oficial del fabricante."

Solicitud:
Se solicita a la Entidad precisar el documento idóneo mediante el cual se debe acreditar la condición de partner oficial y distribuidor certificado, exigiendo específicamente una carta o certificado expedido directamente por el fabricante de la solución ofertada, vigente a la fecha de presentación de la oferta, en la que conste de manera expresa la membresía, nivel de partnership y autorización del proponente para comercializar, implementar y/o soportar dicha solución.
Esto puede generar ambigüedad al momento de estructurar la oferta y dificulta a la Entidad verificar de manera objetiva el cumplimiento de este requisito durante la evaluación. Ante la falta de un mecanismo de acreditación claro, podrían presentarse interpretaciones distintas entre los proponentes (autodeclaraciones, certificados de programas de canal, capturas de portales de partners, etc.), afectando la comparabilidad de las ofertas y el principio de selección objetiva.

RESPUESTA

La certificación o carta exigida en el pliego es un documento oficial emitido directamente por el fabricante de la solución ofertada, el cual cuenta con formatos, membretes y procedimientos estandarizados a nivel mundial. Los fabricantes de soluciones de seguridad perimetral y tecnologías de la información emiten este tipo de certificaciones de manera formal. De acuerdo con lo anteriormente mencionado la Entidad acepta la observación parcialmente, aunado a lo anterior modificará el Numeral *2.5.1.1 OBLIGACIONES ESPECIFICAS:* la cual quedará de la siguiente manera:

El proponente deberá anexar, certificación o carta vigente expedida directa y exclusivamente por el fabricante, en la que se acredite expresamente su condición de distribuidor o partner autorizado para la comercialización de los productos ofertados. Dicha documentación deberá contar con una fecha de expedición no superior a treinta (30) días.

GERMAN ARMANDO CORREA AMADO
Jefe Oficina Asesora de Planeación y Sistemas.