POSITIVA COMPAÑIA DE SEGUROS	**MACROPROCESO**: GESTIÓN DE ABASTECIMIENTO **PROCESO**: GESTIÒN PRECONTRACTUAL **SUBPROCESO:** ANÁLISIS EXTERNO E INTERNO	Código:	APO_10_1_2_FR02
		Versión	06
		Clasificación	Publica Clasificada
		Fecha:	19/04/2021
	FORMATO **ESTUDIOS Y DOCUMENTOS PREVIOS**		

Aprobó: Sol Yadira Rojas Rivera Gerente Abastecimiento Estratégico	Revisó: **Martha Cecilia Florez Sanchez** Profesional Universitario **Líder SIG**	Elaboró: **Nicolás Martínez Benavides** Profesional Universitario

1. DATOS GENERALES DE LA CONTRATACIÓN		
DESCRIPCIÓN DEL CONTRATO A CELEBRAR		
Número CDP	C05762021 – C0606201 – C0607201	
Nombre de Proveedor y NIT(Si Aplica)	SONDA DE COLOMBIA S.A. 830.001.637-7	
Objeto	Prestación de servicios para el licenciamiento, soporte y bolsa de horas de soporte local con apoyo tecnológico y demás soportes para el correcto funcionamiento del firewall.	
Plazo y/o vigencia del contrato	12 meses a partir de la firma del acta de inicio.	
Lugar(es) de ejecución	El servicio se prestará en la Ciudad de Bogotá en las Instalaciones de Datacenter de ETB en la carrera 11C No. 116 – 65 Barrio Santa Bárbara y en las instalaciones de Positiva Casa Matriz en Bogotá en la Avenida Carrera 45 No. 94-72.	
Supervisor del contrato	Nombre: Jesús Alfredo Vargas Carvajal	
	Cargo: Profesional Especializado - Líder Infraestructura	
	Dependencia: Oficina de Tecnología de la Información	
Código de las Naciones Unidas (UNSPSC)	43222501: Equipo de seguridad de red cortafuegos. 81111801: Seguridad de los computadores, redes o internet 81112208: Mantenimiento de software de protección y seguridad	
¿El contrato requiere acta de inicio?	Si ☒	No ☐
¿El contrato requiere Interventoría?	Si ☐	No ☒
Interventoría del contrato *(En caso de no requerir interventoría, diligencie con N/A)*	Nombre: N/A	
	Razón Social: N/A	
	Correo Electrónico: N/A	
Alcance de la interventoría *(En caso de no requerir interventoría, diligencie con N/A)*	N/A	
Clase de contrato	Prestación Servicios	
¿El contrato se encuentra incluido dentro de un acuerdo comercial?	Si ☐	No ☒
2. CONDICIONES DEL CONTRATO A CELEBRAR		
Forma de Pago	Se realizará el pago de los servicios en un (1) único pago por parte de POSITIVA al CONTRATISTA, una vez se	

	realice por parte de éste la entrega a POSITIVA de la certificación de licenciamiento por el año adquirido, de acuerdo con las tarifas previstas en la propuesta de servicios del CONTRATISTA que forma parte de los estudios previos y del contrato y previo recibido a satisfacción por parte del supervisor del contrato de la factura y de los soportes respectivos, en forma mensual vencida, dentro de los 30 días siguientes a la fecha de la presentación de la factura, previa aceptación de la factura por Positiva Compañía de Seguros S.A. con base en la expedición y suscripción del certificado de recibo a satisfacción junto con los documentos soporte; si la factura no es presentada con los documentos solicitados, el plazo de treinta (30) días no comenzará a contarse hasta tanto no se aporten, dicha demora no generará a EL CONTRATISTA el derecho al pago de intereses o de compensación monetaria alguna. ***Gestión del pago:*** Para el pago de la factura deberán presentarse los siguientes documentos: a) Factura en original; b) certificación expedida por el Revisor Fiscal y/o Representante Legal de encontrarse al día en los pagos a la Seguridad Social y Parafiscales y c) entrega de certificado de licenciamiento. ***Facturación Electrónica:*** Si de conformidad con las normas legales vigentes el CONTRATISTA debe cumplir con el proceso de facturación electrónica o decide adoptar dicho mecanismo, aunque éste no le sea legalmente obligatorio, deberá atender el procedimiento adoptado para tal efecto por POSITIVA. En el evento en que no proceda el proceso de facturación electrónica de acuerdo con lo antes mencionado, el CONTRATISTA deberá aplicar el proceso de radicación en físico de las facturas adoptado por POSITIVA para tal efecto.	
¿El contrato requiere Liquidación?	Si ☒	No ☐

3. DEPENDENCIA		
VICEPRESIDENCIA / GERENCIA / OFICINA	**SUCURSAL COORDINADORAS**	**SUCURSAL TIPO**
Oficina de Tecnologías de la información	N/A	N/A

4. MODALIDAD DE SELECCIÓN			
¿Es objeto complejo?	Si ☐	No ☒	
¿Es Objeto análogo?	Si ☐	No ☒	
¿Se contratará un servicio especializado con alto contenido de trabajo intelectual?	Si ☐	No ☒	
Instrumentos de Agregación de Demanda: ¿Hará uso de Acuerdo Marco para la Contratación?	Si ☐	No ☒	NA ☐

Describa la Justificación, Si se aparta de los Instrumentos de Agregación Demanda "Acuerdo Marco" para la contratación.	se buscó el servicio de firewall de nueva generación en los acuerdos marco de TI que se encuentran disponibles en la tienda virtual del estado colombiano (TVEC) https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia/conectividad-iii la cual está vigente hasta noviembre 19 de 2022. Como resultado de la búsqueda No se encuentra el producto como tal.	
¿Se aplicará alguna de las causales para invitación directa?	Si ☒	No ☐
Tipo de invitación	Invitación Directa	
Describa la Justificación de la modalidad de contratación de acuerdo con el Manual para la Gestión de Abastecimiento	La contratación se realiza con base en el Manual para la Gestión de Abastecimiento Versión 4: Artículo 9. Numeral 9.4, ítems o) y k) Para garantizar la selección objetiva del contratista y la eficiencia de la gestión contractual, e independientemente de la cuantía, en los siguientes contratos, POSITIVA COMPAÑÍA DE SEGUROS S.A. podrá contratar directamente sin que se requiera obtener previamente varias ofertas: Ítem *o). "Para la adquisición de bienes y/o servicios que por razones tecnológicas y/o económicas, sean necesarios para no incurrir en cambios o aumentos de tecnologías de los sistemas con que se cuenta al momento de la adquisición."* Ítem *k). "Para la adquisición de bienes y/o servicios que aseguren o garanticen la continuidad del objeto contractual, previniendo colapsos e interrupciones de las actividades que conforman el objeto social, y que el mismo proveedor esté en capacidad de prestar."* En la actualidad se cuentan con diferentes fabricantes que ofrecen los NGFW como son Juniper, Sophos, Palo alto, Checkpoint, Fortinet, Hillstone, etc. Con el fin de optimizar los recursos actuales de las herramientas de seguridad, enfocando el control, protección y detección de las amenazas, se opta por adquirir los equipos FORTIGATE 601E, los cuales se integran de manera nativa con las soluciones que actualmente se encuentran operativas en Positiva: FORTIEDR (prevención y detección de amenazas en	

endpoint) y FORTISIEM (Gestion de eventos e incidentes).

Se realiza estudio de mercado donde se invitan 4 proveedores, con los siguientes resultados:

PROVEEDOR	VALOR, IVA incluido
WEXLER	$ 292,102,183
SONDA	$ 222,424,473
STS	$ 274,615,067
INTERLAN	No presentó

El proveedor SONDA actualmente nos brinda el servicio del SOC. Dentro de este contrato se tiene la administración de las herramientas de FortiSIEM y FortiEDR. Esto nos permitirá orquestar los 3 servicios por el mismo proveedor, reduciendo costos de administración, garantizando la disponibilidad, integridad y confidencialidad de las herramientas de seguridad informatica. Adicionalmente el proveedor ya conoce la infraestructura instalada en Positiva, por lo tanto consideramos viable hacer la contratación con este proveedor.

5. INSTANCIAS		
Requiere Comité Asesor de Contratación	Si ☐	No ☒
Requiere Informar a Junta Directiva	Si ☐	No ☒

6. DESCRIPCIÓN DE LA NECESIDAD A SATISFACER CON LA CONTRATACIÓN	
Objetivo estratégico corporativo, que se impactará a través de la contratación	6. Disponer de información confiable y oportuna
Describa la necesidad, que genera la solicitud de la contratación	Positiva Compañía de Seguros S.A., con el fin de garantizar la Integridad de la información de negocio, por más de 6 años ha contado con el servicio de seguridad perimetral firewall de la serie SRX de Juniper Networks. Estos equipos combinan características como son cortafuegos y servicios de gestión unificada de amenazas (UTM) con enrutamiento y conmutación en un dispositivo de red único, de alto rendimiento y rentable. Estos equipos el fabricante Juniper ha informado que su ciclo de vida tecnológica y de servicio finaliza en dos años. https://support.juniper.net/support/eol/product/srx_series/ Adicionalmente a lo anterior y debido a las constantes amenazas de ciberseguridad, su fluctuante cambio de

	vectores de ataque, el incremento de intentos de intrusión a las entidades estatales, Positiva debe renovar su seguridad perimetral remplazando los firewalls tradicionales UTM por los firewalls de nueva generación (NGFW). ¿Qué es un firewall de nueva generación (NGFW)? Un firewall de nueva generación (NGFW) es más potente que un firewall tradicional. Los NGFW tienen las mismas capacidades que los tradicionales, pero además incluyen una serie de funciones adicionales que sirven para abordar muchas más necesidades organizativas y para bloquear más amenazas potenciales. Se llaman "de nueva generación" para diferenciarlos de otros más antiguos que carecen de tales funcionalidades. La diferencia entre los firewalls de nueva y de vieja generación es como la que existe entre un smartphone y un móvil antiguo. Ambos tienen algunas características en común, como el envío de mensajes, las llamadas de voz, las listas de contactos, etc., pero el smartphone dispone además de tantas funcionalidades avanzadas que es prácticamente un producto distinto, y por ese motivo existe una denominación diferente para este. https://www.cloudflare.com/es-es/learning/cloud/what-is-a-next-generation-firewall/ En la actualidad se cuentan con diferentes fabricantes que ofrecen los NGFW como son Juniper, Sophos, Paloalto, Checkpoint, Fortinet, Hillstone, etc.
Describa los beneficios que obtendrá la Compañía, con la contratación	Al integrar las soluciones de Fortinet se obtienen las siguientes ventajas: • Visibilidad unificada a través de toda la superficie de ataque (endpoint y red) • Gestión unificada de remediación • Respuesta automatizada de fabrica entre EndPoint y perímetro • Acelera la respuesta y detección de incidentes • Proceso continuo de automatización • Acelera la adopción de SD-WAN y protección de nubes públicas. Adicionalmente se tiene que la marca Fortinet se encuentra dentro de los líderes del mercado según el cuadrante Gartner para noviembre de 2020.

7. FICHA TÉCNICA DEL BIEN, SERVICIO Y/O OBRA

Ficha técnica Bienes

Nombre del Producto	Appliance FortiGate 601E con garantía y soporte por 12 meses
Especificaciones Técnicas	Los appliances FortiGate 601E con licenciamiento Unified Threat Prevention (UTP), estos firewalls deben cumplir la totalidad de requerimientos indicados por POSITIVA para las funcionalidades descritas así: Características generales Servicios de red Firewall IPS Antivirus Filtro URL Botnet IP Reputation SSL Decryption Identificación y control QoS SLB SD-WAN VPN Virtualización IPv6 Alta disponibilidad ***Licenciamiento y soporte***

		Los firewalls vienen licenciados con el bundle UTP de Fortinet, que incluye los siguientes features: - ***Antispam perimetral:*** el servicio de Antispam de Fortiguard permite detectar y filtrar spam procesado por las organizaciones. La tecnología de dual-pass reduce de forma drástica el volumen de spam en el perímetro, aumentando el control de ataques e infecciones. En el 2015 el test VBSPAM del Virus Bulletin, posiciono el antispam de Fortinet como el segundo mejor en la industria, con un 99.98% de efectividad. - ***Content disarm and reconstruction:*** la tecnología CDR desarma el contenido de los archivos en tiempo real, creando un archivo plano saneado. Todo el contenido es tratado como sospechoso y es tratado. CDR procesa todos los archivos entrantes, los descompone, y remueve todos los elementos que no coinciden con las políticas del firewall. CDR fortalece la estrategia de ataques de día cero, removiendo de forma proactiva contenido malicioso de los archivos. - ***Application control & Intrusion Prevention System:*** el servicio de application control e IPS está disponible como parte del servicio de NGFW a través de las plataformas FortiGate y es parte del porque Fortinet está catalogado como el firewall con mayor efectividad en la identificación de aplicaciones y amenazas, con un 99.97% en las pruebas de seguridad realizadas por NSS labs. Incluye la detección de más de 4 mil tipos de aplicaciones, divididas en más de 20 categorías: - Botnet - Business - Cloud IT - Collaboration - Email - File sharing - Games - General interest - Instant messaging - Industrial - Mobile - Network service - P2P - Proxy - Remote Access - Social media - Special - Storage Backup - Update - Video/audio	

		- VoIP - Web others - Web client - Unknown - ***Virus Outbreak protection:*** el servicio de VOS cierra la brecha entre los updates del antivirus con el análisis de SandBox en Forticloud para detectar y detener amenazas de malware descubiertos entre los updates de las firmas antes que se desplieguen por la organización. El OS inicia una verificación en tiempo real con la base de datos global. - ***Web filtering:*** web filtering de FortiGuard es el único servicio web en la industria certificado por Virusl Bulletin como VBWeb. Bloquea el 97.7% de las descargas de malware y detiene el 83.5% del malware entregado a través de los diferentes métodos probados por el Virus Bulletin en las pruebas VBWeb del 2015. De acuerdo con el Virus Bulletin. - ***SandBox Malware Análisis:*** el servicio de análisis se hace en dos etapas a través del servicio FortiSandbox Cloud, los archivos sospechosos son objeto del primer filtro de análisis con el motor de AV de Fortinet, emulación de código y consultas a FortiGuard Global Intelligence. La segunda etapa del análisis es realizada en un ambiente contenido para descubrir el ciclo completo del ataque usando la actividad del sistema (emulación, interacción con SO y comportamiento de memoria) y detección de callback. - ***Mitigación de amenazas:*** la integración nativa del SandBox Cloud a través del framework Security Fabric de Fortinet ofrece protección automática con una configuración simple. Una vez el código malicioso es detectado, el FortiSandbox entregará un rating de riesgo y la inteligencia local se compartirá en tiempo real con toda la infraestructura de Fortinet (Firewalls, Antispam, etc.) y otros equipos de terceros registrados, con el fin de remediar e inmunizar contra amenazas avanzadas. A nivel de soporte, la solución de seguridad perimetral debe venir cubierta con un contrato de soporte por 12 meses directo con fabricante, el servicio de FortiGuard incluye reemplazo de partes con SLA 7x24 con disponibilidad de un equipo como remplazo en caso de que cualquiera de los equipos instalados presente falla y requiera cambio de este una vez el proveedor diagnostique esto, con entrega máxima de 4 horas en el datacenter principal de Positiva, actualización de software, acceso a la mesa de soporte de fabrica en SLA 7x24, y gestión de licencias por medio del portal de soporte de Fortinet.	

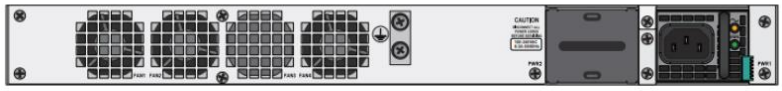
La solución de analítica y recolección de logs estará cubierta por medio del despliegue actual de FortiSIEM con el que cuenta POSITIVA para la gestión de incidentes, por medio de esa plataforma se cumplirán los siguientes puntos requeridos por POSITIVA:

- Logs y reportes
- Monitoreo

Hardware y Software

A nivel de hardware el siguiente grafico ilustra los appliances físicos solicitados:

FortiGate 600E/601E



Interfaces

1. 1x USB Port
2. 1x Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 8x GE RJ45 Ports
5. 8x GE SFP Slots
6. 2x 10 GE SFP+ Slots

Hardware Features

La solución incluye las siguientes características generales a nivel físico:

- Fuente redundante en cada appliance
- 8 puertos RJ-45 embebidos
- 8 puertos duales (RJ-45 o SFP),
- 8 transceivers RJ-45 por appliance
- 2 puertos de 10G para disponibilidad de SFP+

Requisitos de Calidad y Oportunidad

CARACTERISTICAS GENERALES		
ITEM	**DESCRIPCION**	**CUMPLE (SI/NO)**
1	La solución propuesta debe ser capaz de operar en modalidad capa 3 (enrutamiento), modalidad en línea (bridge) y capa 2 (port mirroring) de forma simultánea (sin necesidad de virtualizar el equipo)	SI
2	La solución propuesta debe ser un Firewall de Próxima Generación y no un sistema UTM.	SI
3	La solución propuesta debe tener al menos un puerto de consola dedicado, un puerto AUX y al menos un puerto USB.	SI
4	La solución propuesta debe tener al menos 6 puertos Gigabit Ethernet y 4 puertos combinados (Gigibit Ethernet o SFP), cualquiera de ellos puede ser utilizado como interfaz WAN o LAN	SI
5	La solución propuesta debe tener un puerto dedicado para alta disponibilidad (HA) en Gigabit Ethernet y un puerto de administración (MGT) en Gigabit Ethernet.	SI

		6	La solución propuesta debe permitir a futuro migrar de puertos Gigabit Ethernet a puertos de fibra óptica, plantear las posibles soluciones (módulos de expansión, uso de transceiver SFP, etc).	SI
		7	La solución propuesta debe ser poseer fuente redundante.	SI
		8	Se deben mencionar las certificaciones técnicas nacionales e internacionales con las que cuenta la solución propuesta.	SI
		9	Adicional al punto 8 la solución propuesta debe tener las certificaciones de Internet Computer Security Association (ICSA): Cortafuegos, IPSec, IPS, Antivirus, SSL VPN; NSS Labs y Common Criteria.	SI
		10	La solución propuesta debe operar mínimo en 6 Gpbs de Throughput con todas las funcionalidades solicitadas en operación.	SI
		11	La solución propuesta debe admitir sesiones concurrentes de hasta 2M.	SI
		12	La solución propuesta debe soportar 80,000 nuevas sesiones por segundos bajo tráfico TCP.	SI
		13	La solución propuesta debe admitir Throughput VPN IPSec de 3 Gbps y 4000 túneles VPN IPSec.	SI
		14	La solución propuesta debe admitir Throughput de AV de 1.2 Gbps.	SI
		15	La solución propuesta debe admitir Throughput de IPS de 1.8 Gbps.	SI
		16	La solución propuesta debe admitir un máximo de 2000 usuarios SSLVPN concurrentes, y con 8 usuarios SSLVPN de forma gratuita.	SI
		SERVICIOS DE RED		
		17	La solución propuesta debe ser compatible con los protocolos de enrutamiento dinámico OSPF, BGP, RIPv2 e IS-IS.	SI
		18	La solución propuesta debe ser compatible con enrutamiento estático y basado en políticas (PBR).	SI
		19	La solución propuesta debe ser compatible con enrutamiento basado en aplicaciones, para poder enrutar aplicaciones como P2P, video en línea, etc., con números de puerto dinámicos al enlace WAN seleccionado.	SI
		20	La solución propuesta debe ser compatible con los servicios de red DHCP, NTP, Servidor DNS y proxy DNS integrados.	SI
		21	La solución propuesta debe soportar modo de operación routing o NAT.	SI
		22	La solución propuesta debe poder ser configurada en modo TAP.	SI
		23	La solución propuesta debe ser compatible con el modo de operación transparente (bridge)	SI
		24	La solución propuesta debe ser compatible con el modo de operación mixto (NAT, routing y bridge)	SI
		25	La solución propuesta debe admitir los siguientes modos de interfaz: sniffer, puerto agregado, loopback, VLANS (802.1Q y Trunking)	SI
		26	La solución propuesta debe ser compatible con conmutación y enrutamiento (capa 2 y capa 3).	SI
		27	La solución propuesta debe ser compatible con la función de virtual switch, cada virtual switch tiene su propia tabla de direcciones MAC.	SI
		28	La solución propuesta debe ser compatible con la función de enrutamiento virtual, cada v-router tiene su propia tabla de enrutamiento.	SI
		29	La solución propuesta debe ser compatible con la duplicación de tráfico al puerto configurado en el dispositivo para el análisis del tráfico (port mirror), éste puede estar basado en la IP de origen, IP de destino, puerto de origen, puerto de destino, protocolo de red (TCP, UDP o ICMP), etc. El port mirror puede ser configurado para el tráfico de ingreso, el tráfico de egreso o ambos.	SI
		30	La solución propuesta debe soportar SNAT, DNAT, PAT. Debe admitir por política la configuración de NAT y la configuración central de la tabla de NAT.	SI
		31	La solución propuesta debe ser compatible con NAT dinámico y NAT estático, multi-a-uno, uno-a-multi, NAT uno a uno.	SI
		32	La solución propuesta debe ser compatible con NAT444 (CGNAT) y con la exportación de la tabla de asignación estática NAT444 como un archivo	SI

		33	La solución propuesta debe ser compatible con la detección de reenvío bidireccional (BFD), la interacción BFD con la ruta estática, OSPF o BGP.		SI
		34	La solución propuesta debe ser compatible con NAT46, NAT64, DNS64.		SI
		35	La solución propuesta debe ser compatible con Full Cone NAT, STUN.		SI
		36	La solución propuesta debe ser compatible con la función NetFlow, el dispositivo puede recopilar el tráfico de ingreso del usuario y enviarlo al servidor con la herramienta de análisis de datos NetFlow, para detectar, monitorear y cobrar el tráfico.		SI
		37	Soporte para ver información de estado de enlaces de múltiples interfaces al mismo tiempo para análisis comparativo.		SI
		38	Soporte para identificar el comportamiento de acceso compartido en la red.		SI
		39	Admite la función de habilitar la detección de un nombre de dominio específico, que se puede especificar como un modo de indagación o iniciar un modo de solicitud de DNS.		SI
		40	El modo de traducción de puerto dinámico SNAT es compatible con Round-robin, es decir, la sesión generada por cada IP de origen se sondeará para asignar la dirección IP.		SI
			FIREWALL		
		41	La solución propuesta debe admitir objetos de políticas predefinidos y personalizados. Debe soportar la agrupación de objetos.		SI
		42	La solución propuesta debe ser compatible con la política de seguridad basada en aplicación, el rol del usuario y la ubicación geográfica.		SI
		43	La solución propuesta debe admitir ALG para al menos los siguientes protocolos: MSRCP, PPTP, RAS, RSH, RTSP, SIP, SQLNetV2, SUNRPC, FTP, TFTP, HTTP, DCERPC, DNS-TCP, DNS-UDP, H. 245, H.323, Q.931, XDMCP		SI
		44	La solución propuesta debe ser compatible con NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN		SI
		45	La solución propuesta debe ser compatible con VoIP: SIP, H.323, SCCP, NAT transversal, RTP pin holing		SI
		46	La solución propuesta debe permitir la creación de una sola política para el control de aplicaciones, control basado en el usuario, prevención de amenazas, antivirus, filtrado de archivos, dentro de una sola política.		SI
		47	La solución propuesta debe soportar la verificación de redundancia de las políticas de seguridad.		SI
		48	La solución propuesta debe admitir el recuento de visitas de políticas en WebUI (hit counts).		SI
		49	La solución propuesta debe ser compatible con la búsqueda de políticas en WebUI.		SI
		50	La solución propuesta debe ser compatible con la política programada, una sola vez o recurrente.		SI
		51	La solución propuesta debe ser compatible para configurar el grupo de políticas a través de WebUI		SI
		52	La solución propuesta debe admitir el límite de sesión en función de la IP de origen, la IP de destino, la programación, el protocolo de la aplicación (mysql, ms-sql, sqlnet, descarga de P2P, video, juego, etc.) y limitar las nuevas conexiones, sesiones simultáneas.		SI
		53	La solución propuesta debe soportar defensa contra protocolos anormales.		SI
		54	La solución propuesta debe soportar defensa contra ataques ARP.		SI
		55	La solución propuesta debe ser compatible con la protección DDoS, contra inundaciones de consultas DNS, inundaciones SYN, inundaciones UDP, inundaciones ICMP, ping de la muerte, pitufo, WinNuke, TCP Split Handshake; la acción soportada incluye registro y reinicio.		SI

		56	La solución propuesta deberá soportar diferentes configuraciones para las diferentes zonas de seguridad.	SI
			IPS	
		57	La solución debe soportar al menos 2000 firmas. Debe admitir firmas personalizadas, actualizaciones automáticas de inserción o extracción de firmas y una enciclopedia de amenazas integrada.	SI
		58	La solución debe ser compatible con la protección contra ataques de inyección SQL, ataques CC y XSS.	SI
		59	La solución debe admitir detección de anomalías de protocolo, la detección basada en la velocidad.	SI
		60	La solución debe ser compatible con las siguientes acciones de IPS: predeterminado, monitoreo, bloqueo, restablecimiento (IP de los atacantes o IP de la víctima, interfaz de entrada) con tiempo de caducidad	SI
		61	Los perfiles de seguridad IPS deben poder establecerse según la gravedad, el sistema operativo, la aplicación o el protocolo.	SI
		62	La solución debe admitir la exención de IP de firmas IPS específicas.	SI
		63	La solución debe ser compatible con el modo de operación de IDS sniffer.	SI
		64	La solución debe ser compatible con la protección DoS basada en IPv4 e IPv6 con configuraciones de umbral contra ataques del tipo flood de TCP Syn, TCP/UDP/SCTP, barrido de ICMP, inundación de sesión de TCP/UDP/SCIP/ICMP (origen / destino)	SI
		65	La solución debe contar con perfiles predefinidos de IPS.	SI
		66	La solución propuesta debe ser compatible la funcionalidad de IP Reputation y el bloqueo de IPs de servidores botnet apoyados en una base datos de reputación de IPs global.	SI
		67	La solución propuesta debe ser compatible para filtrar las firmas IPS buscando ID de CVE	SI
			ANTIVITURUS	
		68	La solución debe admitir al menos 2 millones de firmas de antivirus, con actualizaciones de firma manual o automática.	SI
		69	La solución debe ser compatible con Antivirus basado en flujo de red: los protocolos incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP.	SI
		70	La solución debe admitir la detección de virus para archivos comprimidos como RAR, ZIP, GZIP, BZIP2, TAR; admite la detección de archivos comprimidos de múltiples capas para no menos de 5 capas de descompresión y personaliza la acción para cuando supera los comportamientos	SI
		71	La solución debe admitir acciones personalizadas para archivos comprimidos cifrados.	SI
		72	La solución debe admitir al menos 3 acciones: fill magic, reset a la conexión o solo registrar el log cuando se detecte un virus o un sitio web malicioso	SI
		73	La solución debe admitir la advertencia de virus y sitios web maliciosos, alertar al usuario de que el sitio web es un sitio web malicioso o que se detectó un virus.	SI
			FILTRO URL	
		74	La solución debe ser compatible con el filtrado web dinámico con una base de datos de categorización en tiempo real basada en la nube: más de 140 millones de URL con no menos de 64 categorías (no menos de 8 de las cuales están relacionadas con la seguridad)	SI
		75	La solución debe ser compatible con la inspección de filtrado web basada en flujo.	SI
		76	La solución debe admitir el filtrado web definido manualmente en función de la URL, el contenido web y el encabezado MIME	SI
		77	La solución debe ser compatible con las siguientes funciones de filtrado web adicionales:	SI
			- Filtro de Java Applet, ActiveX y / o cookie.	SI
			- Bloquear HTTP Post	SI

			- Registrar palabras clave de búsqueda		SI
			- Excepción de escaneo de conexiones cifradas en ciertas categorías para privacidad		SI
		78	La solución debe admitir la anulación del perfil de filtrado de URL, para que el administrador pueda asignar temporalmente diferentes perfiles a usuario/grupo/IP		SI
		79	La solución debe permitir personalizar la página de advertencia para el filtrado de URL.		SI
		80	La solución debe ser compatible para configurar el filtrado de URL según la zona de seguridad.		SI
			BOTNET		
		81	La solución debe descubrir de forma efectiva los bots de la intranet y evitar nuevos ataques de amenazas avanzadas mediante la comparación de la información obtenida con la base de datos de direcciones de C&C.		SI
		82	La solución debe ser compatible con las actualizaciones regulares de la dirección del servidor Botnet.		SI
		83	La solución debe admitir dos tipos de base de datos de direcciones C&C: la base de datos de direcciones IP y la base de datos del dominio.		SI
		84	La solución debe admitir la detección de los protocolos TCP, HTTP y DNS.		SI
		85	La solución debe permitir la creación de una lista blanca C&C (IPs y dominio)		SI
			IP REPUTATION		
		86	Soporte para filtrar el tráfico de IPs con baja reputación, incluidos Botnet, Spam, nodos comprometidos, fuerza bruta, etc.		SI
		87	Soporte para registrar, eliminar o bloquear paquetes si el tráfico malicioso llega a la lista de reputación de IP.		SI
		88	Soporte para actualizar la base de datos de reputación de IP instalando una licencia para este fin.		SI
		89	Soporte para filtrar la dirección IP de los bots y del sevidor botnet.		SI
			SSL DECRYPTION		
		90	La solución debe admitir la identificación de la aplicación para el tráfico cifrado SSL		SI
		91	La solución debe soportar IPS para tráfico cifrado SSL		SI
		92	La solución debe soportar AV para tráfico cifrado SSL		SI
		93	La solución debe admitir el filtrado de URL para el tráfico cifrado SSL		SI
		94	La solución debe ser compatible con el modo de descarga de proxy SSL.		SI
		95	El proxy SSL se configura según la política y no en la configuración global (después de vincular el perfil del proxy SSL a una regla de política, el sistema procesará el tráfico que coincide con la regla de acuerdo con la configuración del perfil)		SI
		96	El Proxy SSL podría ejecutarse en Require mode (el dispositivo realiza la función de proxy SSL en la comunicación cifrada por el certificado del sitio web especificado) o el modo exento (el dispositivo no realiza la función de proxy SSL en la comunicación cifrada por el certificado del sitio web especificado)		SI
		97	La solución debe soportar lista de recursos.		SI
			IDENTIFICACION Y CONTROL		
		98	La solución debe admitir la identificación de al menos 10 sistemas operativos en el end point: como Windows, IOS, Android, etc.		SI
		99	La solución debe admitir consultas basadas en IP y cantidad de puntos finales.		SI
		100	La solución debe admitir más de 3,000 aplicaciones, debe admitir el filtro de aplicaciones por nombre, categoría, subcategoría, tecnología y riesgo.		SI
		101	La solución debe admitir la visualización de la descripción, los factores de riesgo, las dependencias, los puertos típicos utilizados y las URL para obtener referencias adicionales, y la información para cada aplicación en WebUI.		SI

		102	La solución debe admitir el bloqueo, reinicio, el monitoreo y la configuración del tráfico para las aplicaciones.		SI
		103	La solución debe ser capaz de identificar y controlar las aplicaciones en la nube, debe proporcionar monitoreo y estadísticas multidimensionales para las aplicaciones en la nube, incluyendo la categoría de riesgo y las características.		SI
		104	La solución debe admitir el control de transferencia de archivos en función del nombre, tipo y tamaño del archivo.		SI
		105	La solución debe soportar el control de transferencia de archivos en los siguientes protocolos: HTTP, HTTPS, FTP, SMTP, POP3		SI
		106	La solución debe admitir la firma de archivos y la identificación de sufijos para más de 100 tipos de archivos		SI
		107	La solución debe admitir el filtrado de contenido para los protocolos HTTP-GET, HTTP-POST, FTP y SMTP.		SI
		108	La solución debe ser compatible con la identificación de IM y la auditoría de comportamiento de la red.		SI
		109	La solución debe soportar la base de datos de usuarios local.		SI
		110	La solución debe admitir la autenticación de usuarios con TACACS +, LDAP, Radius, Active Directory		SI
		111	La solución debe admitir la interacción con el sistema de autenticación de terceros a través de la API abierta.		SI
		112	La solución debe ser compatible con la autenticación de 2 factores, ya sea con soporte de terceros, servidor de token integrado y SMS		SI
		113	La solución debe admitir la sincronización de grupos de usuarios basada en AD y LDAP.		SI
		114	La solución debe ser compatible con 802.1X, SSO Proxy		SI
		115	La solución debe ser compatible con la página de autenticación web personalizada.		SI
		116	La solución debe ser compatible con la autenticación activa basada en la interfaz.		SI
		117	La solución debe ser compatible con el inicio de sesión único: Windows AD, función SSO de AD sin agente (AD Polling)		SI
		118	La solución debe admitir el protocolo SSO-monitor para la sincronización de usuarios autorizados.		SI
		119	La solución debe ser compatible con WebAuth basada en MAC.		SI
			QoS		
		120	La solución debe ser compatible con el control de ancho de banda máximo o garantizado, en una dirección IP o usuario.		SI
		121	La solución debe admitir la asignación de túneles en función del dominio de seguridad, la interfaz, la dirección, usarios o grupo de usuarios, servidores o grupo de servidores, aplicaciones o grupo de aplicaciones, los TOS, las VLAN.		SI
		122	La solución debe admitir el ancho de banda asignado por tiempo, prioridad o el mismo ancho de banda compartido.		SI
		123	La solución debe ser compatible con TOS y DiffServ.		SI
		124	La solución debe soportar políticas de QoS programada.		SI
		125	La solución debe admitir la asignación flexible y priorizada del ancho de banda restante no utilizado		SI
		126	La solución debe admitir dos niveles de configuración de tráfico que permitan la configuración del tráfico en diferentes dimensiones, como usuarios y aplicaciones. La solución debe admitir al menos cuatro túneles por nivel, lo que proporciona una jerarquía de control de tráfico.		SI
		127	La solución debe admitir la asignación de ancho de banda según la categoría de URL		SI
		128	La solución debe admitir direcciones IPv6 en la función QoS.		SI
		129	El monitor iQoS admite mostrar las tendencias del tráfico de carfa, el tráfico de descarga y el tráfico total de todos los pipes o sub-pipes (se entiende como pipe al objeto de control de tráfico en QoS).		SI

		SLB		
		130	La solución debe ser compatible con SLB (Balanceo de carga de servidores)	SI
		131	La solución debe ser compatible con los algoritmos de SLB: Weighted hasing, Weighted least connection y round-robin.	SI
		132	La solución debe ser compatible con la protección de la sesión, la persistencia de la sesión y el monitoreo del estado de la sesión.	SI
		133	La solución debe ser compatible con la comprobación del estado del servidor, la supervisión de la sesión y la protección de la sesión.	SI
		LLB		
		134	La solución debe ser compatible con LLB (Link load balancing) bidireccional	SI
		135	La solución debe ser compatible con LLB de salida, incluido el enrutamiento basado en políticas, ECMP y pesos, enrutamiento de ISP incorporado y detección dinámica de la calidad del enlace.	SI
		136	La solución debe ser compatible con LLB entrante, compatible con SmartDNS y la detección dinámica de la calidad del enlace.	SI
		137	La solución debe ser compatible con la conmutación automática de enlaces basada en el ancho de banda, la latencia, el jitter, la conectividad y la aplicación.	SI
		138	La solución debe admitir la protección de sobrecarga de enlaces, el tráfico cambiará a otros enlaces cuando el enlace actual esté sobrecargado; el sistema continuará supervisando el ancho de banda de los enlaces y bloqueará las nuevas sesiones al enlace que se sobrecarga de acuerdo con la configuración del umbral.	SI
		139	La solución debe admitir la inspección del estado del enlace con ARP, PING y DNS.	SI
		VPN		
		140	La solución debe ser compatible con las siguientes funciones de VPN IPSec:	SI
			- Modo IPSEC Fase 1: modo de protección agresivo y principal	SI
			- Compatible con IKEv1 e IKEv2 (RFC 4306)	SI
			- Método de autenticación: certificado y clave precompartida.	SI
			- Soporte de configuración del modo IKE (como servidor o cliente)	SI
			- DHCP sobre IPSEC	SI
			- Cifrado de Fase 1 / Fase 2: DES, 3DES, AES128, AES192, AES256	SI
			- Autenticación Fase 1 / Fase 2: MD5, SHA1, SHA256, SHA384, SHA512	SI
			- Soporte Fase 1 / Fase 2 Diffie-Hellman: 1,2,5	SI
			- XAuth como modo servidor y para usuarios de acceso telefónico.	SI
			- Replay detection.	SI
			- Autokey keep-alive para Phase 2 SA	SI
		141	La solución debe ser compatible con VPN IPSec basada en rutas y políticas.	SI
		142	La solución debe ser compatible con los siguientes modos de implementación VPN IPSEC: puerta de enlace a puerta de enlace, malla completa, hub y spoke, túnel redundante, terminación de VPN en modo transparente.	SI
		143	La solución debe ser compatible con SSLVPN para Linux, iOS, Android y Windows XP/Vista/ Windows 10, incluido sistemas operativos Windows de 64 bits.	SI
		144	La solución debe ser compatible con SSLVPN con un inicio de sesión único que evita inicios de sesión simultáneos con el mismo nombre de usuario	SI
		145	La solución debe soportar el portal SSL limitando a los usuarios	SI
		146	La solución debe ser compatible con SSL. El módulo de reenvío de puerto VPN cifra los datos del cliente y los envía al servidor de aplicaciones.	SI
		147	La solución debe admitir la comprobación de la integridad del host y la comprobación del sistema operativo antes de la conexión del túnel SSL.	SI
		148	La solución debe ser compatible con la verificación de MAC por portal.	SI

		149	La solución debe admitir la opción de limpieza de la memoria caché antes de finalizar la sesión SSL VPN	SI	
		150	La solución debe permitir múltiples inicios de sesión SSL VPN personalizados asociados con grupos de usuarios (rutas de URL, diseño)	SI	
		151	La solución debe admitir la autenticación SSL con una llave USB	SI	
		152	La solución debe ser compatible con el modo de servidor y cliente L2TP, L2TP sobre IPSEC y GRE sobre IPSEC	SI	
		153	La solución debe ser compatible con PnPVPN para el despliegue rápido de múltiples sucursales VPN de sitio a sitio.	SI	
		VSYS			
		154	La solución debe ser compatible con VSYS (sistemas virtuales).	SI	
		155	La solución debe admitir la asignación de recursos del sistema a cada VSYS. El recurso del sistema incluye recursos de CPU, número de sesiones, número de reglas de política, número de zonas de seguridad, número de reglas de NAT, número de túneles IPSec, límites de sesión, IPS, URL, categoría de palabras clave, registros de amenazas.	SI	
		156	La solución debe tener VSYS no root para admitir la función de firewall básico, VPN IPSec, VPN SSL, IPS, filtrado de URL, bloqueo de palabras clave, monitoreo de usuarios y monitoreo de aplicaciones.	SI	
		157	La solución debe soportar el monitoreo y la estadística de VSYS.	SI	
		IPV6			
		158	La solución debe ser compatible con la administración de dispositivos a través de IPv6, el registro de IPv6 y HA en IPV6.	SI	
		159	La solución debe ser compatible con túneles IPv6, DNS64 / NAT64, etc.	SI	
		160	La solución debe ser compatible con los protocolos de enrutamiento IPv6 de enrutamiento estático, enrutamiento de políticas, ISIS, RIPng, OSPFv3 y BGP4 +	SI	
		161	La solución debe ser compatible con IPSec VPN para IPv6.	SI	
		162	La solución debe ser compatible con IPv6 IPS, identificación de la aplicación, filtrado de URL, antivirus, control de acceso, defensa de ataque ND	SI	
		163	La solución debe ser compatible con el conjunto estadístico, registro y monitoreo para IPv6.	SI	
		164	La solución debe ser compatible para configurar y bloquear direcciones IPv6.	SI	
		Alta Disponibilidad (HA)			
		165	La solución debe ser compatible con los modos Activo/Activo y Activo/Pasivo	SI	
		166	La solución debe admitir interfaces redundantes heartbeats para HA	SI	
		167	La solución debe admitir la sincronización de sesiones standalone.	SI	
		168	La solución debe ser compatible con la conmutación por error de alta disponibilidad basada en la interfaz, HTTP, ICMP, ARP, DNS y seguimiento de objetos basados en TCP.	SI	
		169	La solución debe admitir las siguientes opciones de implementación de HA:	SI	
			- HA con agregación de enlaces	SI	
			- HA de malla completa	SI	
			- HA geográficamente disperso	SI	
		170	La solución debe ser compatible con HA en peer-mode, para evitar problemas de enrutamiento asimétrico en la implementación del modo Activo-Activo.	SI	
		LOGS Y REPORTES			
		171	La solución debe admitir el rollback del sistema operativo, debe admitir al menos dos copias de firmware en la memoria flash del sistema.	SI	

		172	La solución debe guardar diez versiones del archivo de configuración.	SI	
		173	La solución debe admitir la exportación de configuraciones actuales y de respaldo a destinos externos, incluidos el servidor FTP, el servidor TFTP y a una flash USB.	SI	
		174	La solución debe soportar SNMP	SI	
		175	La solución debe ser accesible mediante la interfaz de usuario web integrada (WebUI) y la interfaz de línea de comandos (CLI)	SI	
		176	La solución debe admitir el acceso de administración desde HTTP/HTTPS, SSH, telnet, consola	SI	
		177	La solución debe admitir al menos 3 roles de administrador, incluidos administrador, operador y auditor	SI	
		178	La solución debe poder proteger el sistema de ataques de fuerza bruta en el nombre de usuario y la contraseña	SI	
		179	La solución debe admitir la política de seguridad de contraseña para las cuentas de administrador.	SI	
		180	La solución debe ser compatible con la implementación rápida mediante la instalación automática de USB, la ejecución local y remota de scripts.	SI	
		181	La solución debe ser compatible con SYSLOG estándar y registro de formato binario; el almacenamiento distribuido de registro binario a múltiples servidores de registro, el algoritmo distribuido es compatible con Round robin, Src IP HASH	SI	
		182	La solución debe admitir el registro en la memoria local o en los servidores de syslog.	SI	
		183	La solución debe admitir el registro para el cambio de la política de seguridad.	SI	
		184	La solución debe ser compatible con el registro confiable utilizando la opción TCP (RFC 3195)	SI	
		185	La solución debe soportar el envío de log en formato binario o de texto.	SI	
		186	La solución debe admitir la transferencia de registros a través del protocolo UDP, TCP, Secure-TCP	SI	
		187	La solución debe admitir al menos tres informes predefinidos: seguridad, flujo e informes de red.	SI	
		188	La solución debe admitir informes definidos por el usuario. El informe se puede exportar en PDF a través de correo electrónico o FTP.	SI	
		189	La solución debe ser compatible con RESTAPI para la libreta de direcciones IP, AV, IPS, regla de políticas, NAT, interfaz, zona de seguridad, enrutamiento, administración de actualizaciones	SI	
			MONITOREO		
		190	Soporta las estadísticas de tráfico de aplicaciones por usuario	SI	
		191	La solución debe ser compatible con el monitoreo de estadísticas multidimensionales para aplicaciones basadas en riesgo, categoría, características y tecnología.	SI	
		192	La solución debe admitir estadísticas para la visita de URLs y categoría de URLs.	SI	
		193	Soporta estadísticas y análisis de tráfico en tiempo real	SI	
		194	Estadísticas de eventos de seguridad	SI	
		195	Soporte de monitoreo definido por el usuario	SI	
		196	Soporte para monitorear el estado del dispositivo, como CPU, memoria, temperatura, etc.	SI	
		197	Los reportes podrán ser exportados en formatos PDF, Word o HTML.	SI	
		198	La solución deberá contar con un monitoreo centralizado para múltiples dispositivos, incluyendo CPU, memoria, tráfico, sesiones, aplicaciones, usuarios, amenazas, etc. a través de una aplicación móvil, de los últimos 7 días.	SI	
		199	La aplicación de monitoreo deberá soportar acceso web y acceso a través de aplicaciones en dispositivos móviles	SI	

	200	La aplicación de monitoreo proporcionará informes personalizados y programados.	SI

Cantidad	<table><tr><th>Descripción del producto</th><th>No. de parte</th><th>Cantidad</th></tr><tr><td>Firewalls FortiGate 601E</td><td>FortiGate 601E</td><td>2</td></tr><tr><td>Fuente de poder adicional - FortiGate 601E</td><td>FG-300 – Power Supply</td><td>2</td></tr><tr><td>Licenciamiento Unified Threat Protection - vigencia 12 meses</td><td>Lic UTP</td><td>2</td></tr><tr><td>Soporte de fabricante - vigencia 12 meses</td><td>FortiCare</td><td>2</td></tr><tr><td>Implementación y despliegue clúster FortiGate 601E con soporte por bolsa de horas (208 horas) con vigencia de 12 meses</td><td>Implementación y soporte</td><td>1</td></tr></table>
Condiciones de Conservación	El chasis para el appliance debe ser de materiales duraderos y cumpliendo con estándares medioambientales.
Dimensiones	1 UR 44.45 X 432 X 380 mm
Vida Útil	El appliance a recibir debe contar como mínimo 5 años de vida útil a partir de recibido el bien.
Información adicional / Observaciones	N/A

Ficha técnica Servicios

Dependencias Usuarias	POSITIVA COMPAÑIA DE SEGUROS S.A., a nivel nacional
Requisitos de Calidad y Oportunidad	Los servicios de implementación generales (instalación y configuración) cubren las plataformas citadas anteriormente. La propuesta básica incluye la habilitación de los siguientes servicios: •Configuración de características de filtrado de contenido web •filtrado de aplicaciones •Antivirus perimetral •IPS para servidores expuestos a internet •Servicio de Sandboxing cloud La propuesta incluye los servicios de consultoría necesarios para el diseño e implementación de la solución, así: ***Levantamiento de información y diseño:*** plan de trabajo inicial con POSITIVA para definición de la arquitectura de la solución, direccionamiento IP, rutas, políticas, perfiles generales de web filtering, app control, conexiones VPN, parámetros de gestión; para el diseño de la solución se tendrán en cuenta las siguientes premisas:

		• la integración contra el AD para políticas basadas en usuarios se hará para un máximo de 3 grupos del AD (Avanzada, media, baja). • Toda labor de configuración sobre los controladores de dominio, así como los end users será responsabilidad del área de IT de POSITIVA. • La generación de certificados y despliegue de los mismos en los equipos de los usuarios será responsabilidad de POSITIVA. • La solución debe garantizar integración con las herramientas que tiene Positiva definidas para los servicios de sus sistemas de información, sin incurrir en tener que incluir equipos adicionales, licencias ni cualquier otra cosa. • Toda configuración o modificación que se requiera hacer sobra la infraestructura LAN/WAN de la red será responsabilidad del área de IT de POSITIVA. • La responsabilidad de las condiciones físicas para la instalación de los equipos será del área de IT de POSITIVA. • La coordinación para conexión VPN site to site con terceros e instalación del agente de VPN en los equipos de usuarios finales será responsabilidad del área de IT de POSITIVA. ***Implementación:*** instalación de equipos en el espacio provisto por POSITIVA, configuración según plan de trabajo inicial, configuración de servicios y pruebas de operación. Los servicios por implementar en los firewalls se describen a continuación: • Configuración de direccionamiento IP y enrutamiento (tablas de enrutamiento, enrutamiento basado en políticas, enrutamiento basado en ISDB) para el acoplamiento de los equipos con la arquitectura de TI de POSITIVA. • Creación de reglas de firewall basados en las reglas existentes sobre la solución Juniper. • Creación de perfiles de seguridad para los servicios de web filtering, filtrado de aplicaciones, inspección SSL, Intrusion prevention System IPS, Antivirus perimetral y aplicación de estos perfiles en las reglas de firewall. • Configuración de políticas de DoS para los recursos publicados hacia internet, protección contra escaneos e inundaciones de sesiones TCP, UDP, ICMP y SCTP. • Creación de VPN IPsec site to site, cliente to site y VPN SSL según el plan de implementación acordado con POSITIVA. • Integración con el servidor LDAP de POSITIVA para creación de perfiles de navegación basado en autenticación del directorio activo (Single sign On) • Integración con la solución de detección de amenazas avanzadas SandBox en la nube, para análisis de malware y ataques de día cero.	

		• Integración con la solución de administración centralizada FortiManager, para gestión y reporteria. • Configuración de herramientas administrativas y de alertamiento vía correo (puertos de acceso, perfiles administrativos, logs, reporteria, etc.). La implementación de los servicios de recolección de logs, analítica y reportes se realizará por medio del FortiAnalyzer, los servicios de implementación contemplados son los siguientes: • Módulo de reporteria para creación de reportes ajustados según los requerimientos de POSITIVA en la etapa de planeación (amenazas detectadas, ataques de día cero, consumo de canales, top de usuarios, top de conexiones y reportes) • Recolección de logs y analítica de la solución, los resultados de la analítica se pueden ver a través de reportes o en tiempo real. ***Puesta en marcha y normalización:*** la entrada en operación incluye el despliegue de los equipos en el entorno de producción, esto se hará a través de ventanas de mantenimiento concertadas con POSITIVA, estas ventanas incluyen el minutograma de implementación, protocolo de pruebas de servicios y protocolo de rollback en caso de necesitar reversar cambios; una vez finalizada las ventanas de implementación de los equipos se prestara un servicio de normalización por 2 días adicionales después de la migración. Dentro de esta etapa también se harán las pruebas de funcionamiento de los firewalls donde se evidencia el correcto funcionamiento de los servicios de seguridad requeridos, políticas de seguridad y gestión de los equipos. Las pruebas incluyen: • Pruebas administrativas • Verificación de inventario y licenciamiento • Pruebas de navegación (filtrado web) • Pruebas de aplicaciones (bloqueo y/o autorización de aplicaciones) • Pruebas de acceso (verificación de acceso a servicios publicados a internet, verificación de puertos bloqueados) • Pruebas de continuidad de servicio (pruebas de redundancia de canales de internet, pruebas de puertos etherchannel, fuentes eléctricas) Entrega proyecto: documentación de ingeniería, manuales y guías de fabricante. El cronograma general para la implementación y puesta en marcha de la solución es el siguiente:	

	<table><tr><th colspan="2">FASE DEL PROYECTO TIEMPO ESTIMADO</th></tr><tr><td>Levantamiento información</td><td>0,5 semanas</td></tr><tr><td>Diseño plan de trabajo</td><td>0,5 semanas</td></tr><tr><td>Instalación y configuración Firewalls</td><td>3,5 semanas</td></tr><tr><td>Documentación y entrega</td><td>0,5 semanas</td></tr><tr><td>TOTAL TIEMPO PROYECTADO EJECUCION</td><td>5 semanas</td></tr></table>
Cobertura	El Servicio será prestado en el Datacenter de ETB Barrio Santa Bárbara – Bogotá y/o Casa Matriz de Positiva; ubicados en la ciudad de Bogotá.
Activos de Información Externos	N/A
Activos de Información Internos	N/A
Información adicional / Observaciones	La oferta debe contemplar que el licenciamiento de 12 meses será activado durante la implementación para todo lo que tiene que ver con el despliegue de la solución, para la estrategia de migración se activarían las licencias 2 semanas antes de finalizar el cronograma de implementación, de esta forma se aprovecha la mayor cantidad de tiempo útil de las licencias (11 meses y 2 semanas) sin generar mayores costos al proyecto.

8. VALOR ESTIMADO DEL BIEN, SERVICIO Y/O OBRA

Estimación del presupuesto oficial: El valor estimado del contrato con IVA en NÚMERO	$222.424.473
Estimación del presupuesto oficial: El valor estimado del contrato con IVA en LETRAS	DOCIENTOS VEINTE Y DOS MILLONES CUATROCIENTOS VEINTE Y CUATRO MIL CUATROCIENTOS SETENTA Y TRES PESOS M/CTE.

9. RECURSOS FINANCIEROS DEL CONTRATO

Fuente de los recursos	Código de Orden

VIGENCIA ACTUAL	
Número Código de Orden	C05762021
Fecha de expedición	10 de septiembre de 2021
Rubro/Ramo	Depreciaciones
Valor	$105.933.836

VIGENCIA ACTUAL	
Número Código de Orden	C06062021
Fecha de expedición	10 de septiembre de 2021
Rubro/Ramo	Arrendamientos
Valor	$63.049.520

VIGENCIA ACTUAL	
Número Código de Orden	C06072021
Fecha de expedición	10 de septiembre de 2021

VIGENCIA FUTURA	
Año	N/A
Número Código de Orden	N/A

Rubro/Ramo	Mantenimiento, reparaciones y adecuaciones	Fecha de expedición	N/A
Valor	$53.441.117	Valor	N/A

10. OBLIGACIONES DE LAS PARTES

Obligaciones por parte del Proveedor

Generales	1. Cumplir con el objeto contractual. 2. Realizar las actividades de acuerdo con los parámetros indicados en la oferta aprobada por POSITIVA, garantizando el cumplimiento del cronograma. 3. Guardar absoluta confidencialidad del "Know How" de los procesos y directrices de POSITIVA Compañía de Seguros S.A., que conozca con ocasión de la ejecución del presente Contrato. 4. Obrar con lealtad y buena fe durante la ejecución del presente Contrato, evitando dilaciones. 5. No acceder a peticiones o amenazas de quienes actúan por fuera de la ley con el fin de hacer u omitir algún hecho. 6. Radicar la factura de cobro dentro de los plazos establecidos. 7. Cumplir con las disposiciones legales y reglamentarias referentes a Higiene y Seguridad Industrial. 8. Cumplir con sus obligaciones frente al Sistema de Seguridad Social Integral. 9. Responder por el manejo y confidencialidad total de la información proporcionada por POSITIVA Compañía de Seguros S.A. durante el desarrollo del Contrato, ciñéndose al esquema de la Compañía en cuanto al manejo de información, requerimientos de información, oportunidad de la entrega de informes, atención de situaciones de contingencia y los demás aspectos que se puedan derivar del Contrato. 10. EL CONTRATISTA en virtud del desarrollo del Contrato, cuando conozca y tenga acceso a los datos personales de terceros o a los que se realicen la consulta, debe garantizar el cumplimiento de lo establecido en la Ley 1581 de 2012 – HABEAS DATA y lo consagrado en el Manual Interno de Políticas y Procedimientos para la Protección de Datos Personales de POSITIVA Compañía de Seguros S.A. 11. Cuando del objeto del Contrato se desprenda la necesidad de hacer uso de la imagen de POSITIVA Compañía de Seguros S.A., EL CONTRATISTA se orientará por el Manual de Manejo de Marca. 12. Acatar las disposiciones del Manual para la Gestión de Riesgos del Negocio, el cual se entrega con la minuta del Contrato. 13. Las demás que por ley o Contrato le correspondan.
Especificas	1. Suministro de 2 appliance con soporte y garantía de fábrica 2. El throughput del FW una vez estén todas las funcionalidades, servicios, características (IPS, Antvirus, VPN y en general todo lo solicitado) no debe ser menor a 8 Gigas. 3. Servicio de implementación y puesta en marcha 4. Servicio de bolsa de horas de soporte local 5. (Actividades descritas en el numeral 7) **<u>Valores agregados</u>** 6. La oferta presentada incluye cuatro (4) cursos de NSE4 para los funcionarios de POSITIVA, este curso se imparte en modalidad virtual e incluye el voucher de certificación para los cuatro funcionarios. La vigencia de estos cursos, así como los voucher de certificación serán durante la misma vigencia del contrato.

Entregables del proveedor	1. ***Entrega de los equipos adquiridos:*** Estos se recibirán en el datacenter principal de Positiva, tal como se indicó en el lugar de ejecución del numeral 1 y deberán ser entregados en los siguientes 30 días calendario a la firma del contrato. 2. ***Plan de trabajo propuesto:*** Como resultado de la fase de INICIO del proyecto, se elaborará y entrega un plan de proyecto, que constituye la línea base para la ejecución de este. 3. ***Documento de ingeniería:*** resumen con el despliegue de la solución, arquitectura, licencias, vigencias, información de soporte con fabricante, resumen de políticas e inventario de equipos instalados. 4. ***Reunión de inicio de proyecto:*** El gerente de proyecto de SONDA coordinará y asistirá a la reunión de inicio de proyecto en conjunto con el Gerente General del proyecto provisto por POSITIVA y los demás recursos involucrados en el proyecto donde se validarán los alcances, entregables, asignación de recursos y cronograma definitivo del proyecto. 5. ***Reuniones de seguimiento del proyecto***: El gerente de proyecto de SONDA realizara una reunión periódica de seguimiento del proyecto con el gerente del proyecto de POSITIVA y las personas que estén involucradas en el mismo, que sean relevantes en estas reuniones. 6. ***Reunión de cierre de proyecto:*** El gerente de proyecto de SONDA coordinará y asistirá a la reunión de cierre de proyecto en conjunto con el Gerente General del proyecto provisto por POSITIVA y los demás recursos involucrados en el proyecto donde se validarán los alcances, entregables, asignación de recursos y acta de cierre del proyecto.		
Obligaciones por parte de Positiva			
Generales	1. Pagar en la forma establecida, la factura presentada por EL CONTRATISTA. 2. Suministrar en forma oportuna la información que requiera EL CONTRATISTA. 3. Resolver las peticiones que le sean presentadas por EL CONTRATISTA en los términos consagrados en la Ley. 4. Cumplir y hacer cumplir las condiciones pactadas en el contrato y en los documentos que de él forman parte. 5. Cuando del objeto contractual se desprenda la necesidad de hacer uso del manual de marca y de políticas de manejo de la información POSITIVA hará entrega a EL CONTRATISTA de dicha información, en medio magnético		
Especificas	Positiva gestionara los permisos y requerimientos necesarios para realizar cualquier instalación en el Datacenter para la prestación del servicio.		
Requiere ANS (Acuerdo de Nivel de Servicio)		Si ☒	No ☐
Requiere Garantías		Si ☒	No ☐
EL CONTRATISTA se obliga a tomar en favor de **POSITIVA**, la Póliza Única de Seguro de Cumplimiento a favor de **Entidades Estatales** con Régimen Privado de Contratación, por una Compañía de Seguros legalmente establecida en Colombia, así:			

Garantía de cobertura del riesgo	PRE-CONTRACTUAL	CONTRACTUAL	POST-CONTRACTUAL	Porcentaje (%)	Plazo
Cumplimiento	no	si	Si	10	Por el plazo de ejecución del mismo y seis (6) meses más
Pago de salarios y prestaciones sociales e indemnizaciones laborales.	no	si	Si	5	Por el plazo de ejecución del mismo y tres (3) años más
Calidad del servicio	no	si	Si	10	Por el plazo de ejecución del mismo y seis (6) meses más
Calidad de los bienes	no	si	Si	10	Por el plazo de ejecución del mismo y seis (6) meses más

11. RECURSOS REQUERIDOS PARA LA EJECUCIÓN

Equipos de cómputo	**SI/NO**	**CANTIDAD**	**PROPIETARIO**	**RESPONSABLE**
	No		☐ Proveedor	☐ Proveedor
			☐ Positiva	☐ Positiva
Infraestructura TI	**SI/NO**	**CANTIDAD**	**PROPIETARIO**	**RESPONSABLE**
	No		☐ Proveedor	☐ Proveedor
			☐ Positiva	☐ Positiva
Puestos de trabajo (espacio físico, muebles y enseres)	**SI/NO**	**CANTIDAD**	**PROPIETARIO**	**RESPONSABLE**
	No		☐ Proveedor	☐ Proveedor
			☐ Positiva	☐ Positiva
Cuentas de correo	**SI/NO**	**CANTIDAD**	**PROPIETARIO**	**RESPONSABLE**
	No		☐ Proveedor	☐ Proveedor
			☐ Positiva	☐ Positiva
Licenciamiento	**SI/NO**	**ESPECIFICACIÓN**	**PROPIETARIO**	**RESPONSABLE**
	No		☐ Proveedor	☐ Proveedor
			☐ Positiva	☐ Positiva
Inmuebles	**SI/NO**	**ESPECIFICACIÓN**	**PROPIETARIO**	**RESPONSABLE**
	No		☐ Proveedor	☐ Proveedor
			☐ Positiva	☐ Positiva
Papelería e impresión	**SI/NO**		**PROPIETARIO**	**RESPONSABLE**
	No		☐ Proveedor	☐ Proveedor
			☐ Positiva	☐ Positiva
Prueba de Concepto	**SI/NO**		**ESPECIFICACIÓN**	
	No			

Servicios adicionales	N/A

Actividades para solicitar, recibir y certificar los Bienes, Servicios y/o Obras	
Solicitud	Soporte telefónico, correo electrónico y en sitio.
Recepción	Validar la entrega de informes cuando se tengan incidentes y las reuniones que se deben hacer para dar seguimiento a reportes que se generen.
Certificación	Informe de seguimiento mensual hechos por el supervisor del contrato, donde se describen las actividades desarrolladas durante el mes y los soportes como evidencias adjuntas

12. ANÁLISIS DE RIESGOS			
Seguridad de la Información			
¿Es necesario el acceso a servicios tecnológicos de Positiva por parte del tercero?	Si ☒	No ☐	
Tipo de Personal tercerizado	Personal de mantenimiento y soporte de hardware y software.		
¿Qué tipo de acceso requiere?	Acceso Físico		
¿Cuál es la clasificación de la información a la que tendrá acceso el proveedor?	Pública ☐	Pública Reservada ☐	Pública Clasificada ☒
Pública Clasificada (Datos personales)	Si ☐	No ☒	
¿Requiere tiempo de reserva de la información?	Si ☐	No ☒	
Duración del tiempo de reserva de confidencialidad	N/A		
Requiere que el proveedor firma de Acuerdos de confidencialidad de la información técnica y personal del vínculo contractual.	Si ☒	No ☐	
Continuidad del Negocio			
¿El servicio a contratar apoyará labores o actividades de procesos asociados a macro proceso catalogados dentro de mapa operacional de la Compañía como misionales o de apoyo?	Si ☒	No ☐	
De acuerdo con su conocimiento respecto al servicio a contratar, en caso de presentarse indisponibilidad del mismo, usted considera que el impacto sería	Fuerte		
¿El servicio a contratar apoyará labores o actividades de procesos/subproceso catalogados como críticos dentro de la continuidad del negocio de la compañía?	Si ☒	No ☐	
¿Cuál?	Comunicación Global de Servicios Tecnológicos de Positiva		

¿El resultado del análisis de la Oficina de Gestión Integral de Riesgos ha catalogado el objeto contractual como crítico?	Si
Matriz de Riesgos Previsibles	
Requiere matriz de riesgos previsibles (Cuantías mayores a 500 SMMLV, procesos de selección por modalidad pública, y aquellos contratos que hayan presentado eventos de riesgo)	No

13. EXPERIENCIA DEL CLIENTE			
¿El proveedor va a tener contacto directo con los clientes de Positiva Compañía de Seguros?	Si ☐		No ☒
¿Qué tipo de contacto?	Presencial ☐	Telefónico ☐	Ambos ☒
Requiere protocolo de presentación personal. **(Presencial)**	Si ☐		No ☒
Requiere protocolo de comunicación y relacionamiento con el cliente. **(Presencial)**	Si ☐		No ☒
Requiere protocolo de reporte de novedades al cliente. **(Presencial)**	Si ☐		No ☒
Requiere protocolo de comportamiento por insatisfacción del cliente. **(Presencial)**	Si ☐		No ☒
Requiere protocolo de Comunicación, relacionamiento y abordaje al cliente. **(Telefónico)**	Si ☐		No ☒
Requiere protocolo de actuación inmediata frente a insatisfacción del cliente generada por el proveedor. **(Telefónico)**	Si ☐		No ☒

14. DOCUMENTOS DEL CONTRATISTA REQUERIDOS PARA CONTRATAR

REQUISITOS JURÍDICOS

1. Registro único tributario – RUT *(posterior al 12/12/2012)*
2. Certificado de Existencia y Representación Legal, **con fecha de expedición no superior a 30 días** (*El área usuaria verificará la existencia y representación legal del proveedor en el RUE http://www.rues.org.co/RUES_Web/ y anexará la impresión de la verificación, si este no anexa la Cámara de Comercio.)*
3. Copia de la cédula del representante legal.
4. Certificado de antecedentes disciplinarios del representante legal y de la persona jurídica Con fecha de **expedición no superior a 30 días** *(El área usuaria verificará el Certificado Antecedentes Disciplinarios vigente, expedido por la Procuraduría General de la Nación del representante legal, incluso si es persona jurídica en el link http://www.procuraduria.gov.co/portal/antecedentes.html)*
5. Certificación de responsabilidad fiscal del representante legal y de la persona jurídica Con fecha de **expedición no superior a 30 días** *(El área usuaria verificará el Certificado de la Contraloría General de la Nación vigente, en el sentido de que no es responsable fiscal, en el link: http://200.93.128.206/siborinternet/index.asp y selecciona la opción Persona Jurídica y Representante Legal).*
6. Certificación bancaria.
7. Original del Formulario de vinculación de proveedores y empleados de la Superintendencia Financiera de Colombia SARLAFT. *(La parte ilustrada como persona natural debe incluir los datos del representante*

legal, indicando que es Proveedor, el formulario debe diligenciarse con la misma letra llenando TODAS las casillas, además tener huella legible y firma del representante. Este formulario es un requisito indispensable para la vinculación contractual de los proveedores a Positiva, fundamentado en la circular 026 externa de 2008 de la Superintendencia financiera de Colombia.

8. Formato único de hoja de vida de la función pública *(Formato en página web de la función pública).*
9. Certificación de pago de seguridad social y aportes parafiscales. *PERSONA JURIDICA: De acuerdo a lo previsto en el Artículo 50 de la Ley 789 de 2002, se hace necesario expedir Certificación de Paz y Salvo de pago de aportes parafiscales, suscrita por el Revisor Fiscal o del Representante Legal de la entidad que esté contratando con Positiva S.A. en el sentido de que "**durante los seis meses anteriores** a la suscripción del contrato, la sociedad ha cumplido con sus obligaciones con los sistemas de salud, riesgos profesionales, pensiones y aportes a las cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje (SENA)". Debe ser coincidente el nombre de quien firma el paz y salvo con el de la persona que figura autorizada como revisor fiscal en la Cámara de Comercio ó Representante legal de la empresa que esté contratando con Positiva S.A. No debe estar firmada por el contador a menos que este sea el revisor fiscal, ni por representante de una cooperativa o temporal por la cual se efectúen los pagos.*
10. Certificación Suscrita por el representante legal de la empresa participante a través de la cual manifieste no tener multas, sanciones, apremios ni declaratorios de incumplimiento contractual.
11. Certificación suscrita por el representante legal de la empresa participante por medio del cual indique que el contratista mantiene y ejecuta buenas prácticas en sus procesos, dirigidas a evitar que sus operaciones puedan ser utilizadas como instrumento para el ocultamiento, manejo, inversión o aprovechamiento en cualquier forma de dinero u otros bienes provenientes de actividades de lavado de activos, la financiación del terrorismo y/o sus delitos conexos. (Certificación "Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo").
12. Declaración bajo la gravedad de juramento de no estar en causales de inhabilidad y/o incompatibilidad ni conflictos de interés para contratar, expedida por el representante legal de EL CONTRATISTA.
13. Poder por el cual se confiere representación por parte del oferente cuando concurra por intermedio de un apoderado.
14. Certificación de composición accionaria debidamente firmada por su revisor fiscal, o su contador y representante legal, con fecha de **expedición no mayor a 30 días**

REQUISITOS EN CALIDAD, SEGURIDAD, SALUD EN EL TRABAJO, Y AMBIENTE Y/O NORMATIVIDAD ESPECIAL

TEMA	DOCUMENTO QUE APORTARA EL OFERENTE/PROVEEDOR	Periodicidad de seguimiento etapa contractual	TIPO B Prestación servicios fuera Positiva
			PJ
CALIDAD	Hojas de vida con soportes del perfil de cada persona vinculada en donde acredite la Educación, Formación, Habilidades y Experiencia	Una vez	x
SST	Constancia o certificación de la implementación del sistema de Seguridad y Salud en el trabajo, expedida por el representante legal tanto para personas naturales (al registrar empleados) y jurídicos. Esta constancia se presenta **única vez y no tiene vencimiento.**	Una vez	X
	Certificado Aportes Parafiscales vigente	Mensual	x

REQUISITOS TÉCNICOS

1. Carta de presentación de la oferta, que incluya el valor total, especificando IVA y si no aplica indicarlo.
2. Propuesta técnica a desarrollar para este contrato; incluyendo el servicio a prestar o bien a suministrar por el proveedor, así como las especificaciones técnicas del bien o el servicio.
3. Un (1) certificado de Experiencia del proponente, relacionada con el objeto del contrato, por un valor no inferior al de este proceso y que su fecha de inicio de ejecución no haya sido anterior a cuatro (4) años.

REQUISITOS FINANCIEROS

El oferente deberá demostrar que cuenta con la capacidad financiera adecuada para ejecutar el Contrato. Para ello, el Oferente o cada uno de los integrantes del oferente deben presentar:

1. Estados financieros comparativos de los dos (2) años anteriores al trámite contractual a 31 de diciembre de 2019 y 2020: (Balance General, Estado de Resultados, Notas a los Estados Financieros) y certificación expedida por el Representante Legal, el Contador Público y el Revisor Fiscal en los casos en que este último aplique, en donde se detallen cada uno de los indicadores.
2. Tarjeta Profesional del Contador y del Revisor Fiscal: Se debe presentar fotocopia legible de la Tarjeta Profesional del Contador y Revisor Fiscal expedida por la Junta Central de Contadores.
3. Certificado de Vigencia de la Inscripción del Contador y del Revisor Fiscal: Se debe presentar fotocopia legible del Certificado de Vigencia de la Inscripción y de antecedentes disciplinarios del Contador y el Revisor Fiscal, expedido por la Junta Central de Contadores, con no más de tres (3) meses de su expedición.
4. Condiciones de los Dictámenes: Se debe presentar fotocopia legible del dictamen, si EL OFERENTE legalmente está obligado a tener revisor fiscal.

Teniendo en cuenta que se trata de un proceso de selección bajo la modalidad de "invitación directa", en el que prima la necesidad de garantizar la prestación de servicios y que el proveedor está en capacidad de prestar, dada la experiencia e idoneidad que acredita tener, para el presente proceso no se hace necesario adelantar un análisis de indicadores financieros.

15. FACTORES DE ESCOGENCIA PONDERACIÓN

N/A

JEFE DE OFICINA O GERENTE RESPONSABLE AREA USUARIA			
NOMBRE: SILVERIO CARMONA LOZANO			
CARGO: JEFE OFICINA DE TECNOLOGIA DE LA INFORMACION			
FIRMA:			
PROFESIONAL RESPONSABLE REVISIÓN			
NOMBRE: JESÚS ALFREDO VARGAS CARVAJAL			
CARGO: Profesional Especializado – OTI – Líder Infraestructura			
FIRMA:			
PROFESIONAL RESPONSABLE ELABORACIÓN			
NOMBRE: LEONARDO ESTRADA CASTRO			
CARGO: PROFESIONAL ESPECIALIZADO - OTI			
FIRMA:			
Vo.Bo. RESPONSABLE GERENCIA DE ABASTECIMIENTO ESTRATEGICO:			
NOMBRE: PAULA ANDREA GÓMEZ MOLANO			
CARGO: CONTRATISTA			
FIRMA:			
FECHA DE APROBACIÓN ESTUDIOS PREVIOS GERENCIA DE ABASTECIMIENTO ESTRATÉGICO			

RESPONSABLE AVAL OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN (Cuando aplique)
NOMBRE:
CARGO:
FIRMA:
RESPONSABLE AVAL OFICINA DE ESTRATEGIA Y DESARROLLO (Ambiente y calidad) / GERENCIA DE TALENTO HUMANO (Seguridad y Salud en el Trabajo) (Cuando aplique)
NOMBRE:
CARGO:
FIRMA:
RESPONSABLE AVAL OFICINA DE GESTIÓN INTEGRAL DE RIESGOS (Continuidad del Negocio) (Cuando aplique)
NOMBRE:
CARGO:
FIRMA: