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	C05372021 y C06082021	
Nombre de Proveedor y NIT(Si Aplica)	GLOBALTEK SECURITY S.A.S. - 830.001.516-4	
Objeto	Suministro y renovación de licenciamiento Forcepoint Web security en solución híbrida, cambio de appliance por obsolescencia tecnológica y servicio de soporte por 3 años, que realizará EL CONTRATISTA para POSITIVA, de acuerdo con las condiciones previstas en el contrato.	
Plazo y/o vigencia del contrato	EL CONTRATISTA a partir de la fecha de firma del acta de inicio, tendrá para realizar par POSITIVA un (1) mes para el suministro de los entregables y renovación del licenciamiento, así como tres (3) años para prestarles el soporte técnico, previa perfeccionamiento y legalización del contrato.	
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 Tecnologías de la Información	
Código de las Naciones Unidas (UNSPSC)	43233205 - Software de seguridad de transacciones y de protección contra virus 43222604: Equipo de red de entrega de contenido	
¿El contrato requiere acta de inicio?	Si ☒	No ☐
¿El contrato requiere Interventoría?	Si ☐	No ☒
Interventoría del contrato	Nombre: N/A	
	Razón Social: N/A	
	Correo Electrónico: N/A	
Alcance de la interventoría	N/A	
Clase de contrato	Suministro	

¿El contrato se encuentra incluido dentro de un acuerdo comercial?	Si ☐	No ☒
2. CONDICIONES DEL CONTRATO A CELEBRAR		
Forma de Pago	POSITIVA le pagará al CONTRATISTA el valor total del contrato en un (1) sólo pago vencido, una vez aprobada por el supervisor del contrato el acta de entrega por parte del CONTRATISTA del appliance y de la certificación de licenciamiento por los tres años adquiridos, previa aceptación de la factura por Positiva. 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. **PARÁGRAFO SEGUNDO.-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) Acta de entrega aprobada por el supervisor del contrato, con los entregables respectivos. **PARÁGRAFO TERCERO.-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 COMPAÑÍA DE SEGUROS S.A. 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 ☐

<table>
<tr><td>¿Se contratará un servicio especializado con alto contenido de trabajo intelectual?</td><td colspan="2">Si ☐</td><td>No ☒</td></tr>
<tr><td>Instrumentos de Agregación de Demanda: ¿Hará uso de Acuerdo Marco para la Contratación?</td><td>Si ☐</td><td>No ☒</td><td>NA ☐</td></tr>
<tr><td>Describa la Justificación, Si se aparta de los Instrumentos de Agregación Demanda “Acuerdo Marco” para la contratación.</td><td colspan="3">Se consultó el servicio de renovación de licenciamiento de Forcepoint PROXY y cambio del appliance en los acuerdos marco de TI que se encuentran disponibles en la Tienda Virtual del Estado Colombiano (TVEC) abril 2021. Como resultado de la búsqueda No se encuentra el producto específico.</td></tr>
<tr><td>¿Se aplicará alguna de las causales para invitación directa?</td><td colspan="2">Si ☒</td><td>No ☐</td></tr>
<tr><td>Tipo de invitación</td><td colspan="3">Invitación Directa</td></tr>
<tr><td>Describa la Justificación de la modalidad de contratación de acuerdo con el Manual para la Gestión de Abastecimiento</td><td colspan="3">La contratación se realiza con base en el Manual para la Gestión de Abastecimiento Versión 4:

Capítulo 9, numeral 9.4, ítem n)
“Cuando se trate de ampliación, actualización o modificación de software ya instalado, o del soporte del mismo, respecto del cual el proveedor tenga legalmente registrados tales derechos o se trate de quien implementó el software”.

Capítulo 9, numeral 9.4, 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.
<table>
<tr><td colspan="5">3 años</td></tr>
<tr><td>PROVEEDOR</td><td>VALOR</td><td>IVA</td><td>TOTAL</td><td>Diferencia % Con Respecto al mas bajo</td></tr>
<tr><td>GMS SEGURIDAD</td><td>$ 614,000,000</td><td>$ 116,660,000</td><td>$ 730,660,000</td><td>46.23%</td></tr>
<tr><td>Nemesis</td><td>$ 636,000,000</td><td>$ 120,840,000</td><td>$ 756,840,000</td><td>48.09%</td></tr>
<tr><td>GLOBALTEK</td><td>$ 330,138,000</td><td>$ 62,726,220</td><td>$ 392,864,220</td><td></td></tr>
</table>

El proveedor GLOBALTEK nos brindó el servicio de implementación de esta herramienta y desde entonces nos ha ofrecido el servicio de mantenimiento con niveles especializados óptimos. Esta firma es autorizada por el fabricante ForcePoint, para darnos la atención y el mejor descuento ofrecido teniendo en cuenta la certificación del fabricante donde se identifica el proveedor como el registrado para Positiva, por lo tanto, consideramos viable hacer nuevamente la contratación con este proveedor.</td></tr>
</table>

	Adicionalmente la herramienta está catalogada por Gartner como una de las mejores apareciendo como líder al menos una vez en los últimos 3 años.	
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	14. Contar con una infraestructura tecnológica flexible e integrada	
Describa la necesidad, que genera la solicitud de la contratación	POSITIVA COMPAÑÍA DE SEGUROS con el propósito de dar cumplimiento a los requisitos de seguridad informática para sus sistemas de información y atendiendo a la necesidad de proteger los activos de información, requiere la renovación de la suscripción de la herramienta ForcePoint Web Security para 1100 licencias, renovar el soporte Essential de fabricante que permite tener actualizaciones constantes y parches de seguridad, renovar el mantenimiento de proveedor con un acuerdo de servicios 5x8. Lo anterior con el fin de poder proteger a la compañía frente a amenazas avanzadas, robo de datos y poder tener control frente a la navegación hacia internet de los usuarios, permitiendo niveles de productividad que ofrezcan mejora continua para la organización.	
Describa los beneficios que obtendrá la Compañía, con la contratación	Positiva, al renovar el licenciamiento de la solución Forcepoint web Security, podrá obtener el adecuado soporte y mantenimiento, para contar con un control de protección de los activos de información y en especial en los activos catalogados como confidenciales, de esta forma prestar un servicio eficiente al usuario interno enfocado en la mejora de la gestión de la información. A nivel técnico la solución de Seguridad Web detiene el ingreso de las amenazas avanzadas persistentes (ATP por sus siglas en inglés) así como también protege a los usuarios del uso inadecuado en la navegación Web, sin importar la ubicación física de acceso de los usuarios dentro de la compañía. A nivel de riesgo contar con esta herramienta permite a la compañía tener control de la navegación de los usuarios, mitigando el riesgo de ingreso a paginas maliciosas donde pueden generarse descargas que pueden comprometer la seguridad de la información, abrir sitios de contenidos inapropiados, disminuir la productividad y por ende se podrían ver afectada la disponibilidad, la integridad y la confidencialidad de	

	la información lo cual causaría una pérdida económica incalculable.

7. FICHA TÉCNICA DEL BIEN, SERVICIO Y/O OBRA	
Nombre del Producto	ForcePoint Web Security y appliance Forcepoint V5000 G4R2 con garantía por 3 años
Especificaciones Técnicas	El licenciamiento de la solución para control de acceso a sitios web y de aplicaciones, debe tener los siguientes términos: **ForcePoint Web Security** Renovación de 1100 licencias por tres (3) años. La solución debe contar con las siguientes características: 1. La solución debe ser un proxy para HTTP, HTTPS, FTP, FTP sobre HTTP y SOCKS 2. La solución debe poseer tecnología de web caching para proveer mejoras adicionales en el desempeño de la red mediante el uso de contenido que sea reusable y de almacenamiento local. 3. La solución proxy deberá tener la facultad adicionalmente instalarse en hardware de servidores abiertos y soportar virtualización tanto en sistemas como Hyper-V o VMWare. 4. La solución debe soportar diversos modos de implementación. Se espera que la solución pueda configurarse como proxy explícito y como proxy transparente. 5. El modo de operación proxy transparente debe incluir: Soporte para usar WCCP (Web Cache Content Protocol) y PBR (Policy Based Routing) . 6. El modo de operación proxy explicito debe incluir lo siguiente: configuración manual de browser y/o soporte para auto configuración del proxy mediante el uso de PAC, WPAC y políticas de Active Directory. 7. El equipamiento provisto debe tener CPU y memoria dedicada a cada uno de los siguientes componentes: • Componente Proxy • Componente de Filtrado de Contenido • Componente de Análisis de Protocolos de red Se deberá especificar que recursos dedicados en términos de CPU y memoria están disponibles para cada componente. 8. La solución debe poseer la capacidad de ser implementada en modo clúster, con soporte para políticas y configuración unificada para todos los componentes del arreglo lógico que hacen parte del clúster. Debe soportar configuraciones Activo-Activo y Activo-Pasivo para poseer alta disponibilidad para el servicio de acceso web con el uso de failover que puede involucrar a 2 o más nodos. 9. La solución debe hacer uso de las siguientes tecnologías para alta disponibilidad: Virtual IP, DNS Round Robin, y clustering administrado. 10. La solución debe soportar WCCP (Web Cache Content Protocol) para ser usado en conjunto con un router para proveer alta disponibilidad, adicionalmente debe soportar el uso de balanceadores de carga para resiliencia y escalabilidad. 11. La solución deberá proveer autenticación selectiva utilizando diferentes tipos de autenticación que podrán ser usados de manera simultánea en un mismo ambiente. Los administradores podrán especificar ciertos usuarios para ser autenticados de manera transparente (no login)

		mientras que otros usuarios deberán autenticarse de manera manual (login required) de forma tal que se puedan usar y aplicar políticas apropiadas en ambientes donde se tengan PC compartidos, PC para uso del público y PC para uso de empleados corporativos 12. Debe soportar integración con servicios de Active Directory, NTLM, Novell eDirectory (LDAP), Oracle Sun Java System Directory 13. Debe usar tecnología líder que permita desencriptación on-box de tráfico HTTPS para inspección profunda de dicho tráfico y aplicación de políticas en el mismo appliance 14. Debe permitir la administración de certificados digitales con el uso de una consola web desde donde también se debe permitir el uso de políticas globales y generación de reportes con el fin de disminuir las tareas administrativas. 15. La solución debe prevenir ataques encriptados mediante la capacidad de realizar desencriptación de SSL en el Gateway. Una vez abierto el túnel, debe aplicar análisis de motor antivirus basado en la misma caja, análisis de contenido en tiempo real en la misma caja y detección de aplicaciones mediante fingerprint en la misma caja. No se aceptarán soluciones que utilicen mecanismos mediante ICAP o Secure ICAP para realizar dichas funciones 16. La solución deberá soportar integración con soluciones DLP líder del mercado (Data Leak Prevention) para realizar escaneo de HTTPS (SSL) sobre contenido saliente con el fin de prevenir pérdidas o fugas de información vitales para la organización. El producto deberá tener un motor de políticas de DLP integrado en el mismo Appliance para minimizar los efectos de latencia y no se aceptarán soluciones que utilicen ICAP o Secure ICAP para realizar dicha integración 17. La solución debe proveer clasificación en tiempo real en más de 120 categorías de filtro de contenido (Viajes, deportes, contenido adulto, etc) mediante la extracción de elementos (lenguaje natural, palabras clave, colores, fuentes, títulos, fondos) y clasificar este contenido en tiempo real usando algoritmos propietarios de la solución y base de datos de categorías propietaria del fabricante de la solución. Todo este análisis debe ser realizado on-box (en la misma caja) sin requerir consultas de reputación en la nube o técnicas de categorización dinámica en la nube. 18. Debe proveer análisis de seguridad en tiempo real con el fin de identificar y evitar que amenazas como spyware, phishing, malware, entre otros, lleguen a comprometer los usuarios del servicio de navegación, la solución debe contar con la capacidad de extraer componentes activos (scripts, exploits, código binario, imágenes, entre otros) que se encuentren dentro del contenido web que pueda activar cualquier actividad malintencionada. Este análisis debe ser realizado on-box (en la misma caja). No se aceptarán soluciones que requieran Appliance adicionales para dichos trabajos ni que requieran ICAP o Secure ICAP para tal tarea o que requieran conectividad a servicios en la nube para dichas tareas 19. La solución debe tener la capacidad de categorizar dinámicamente sitios web emergentes o sitios web desconocidos con contenido malicioso sin	

		necesidad de consultar EN LA NUBE por dicha categoría por servicios de rating o similar. El análisis debe ser hecho ON BOX (En la misma caja). Debe demostrar cómo se realiza el análisis de los analíticos* en más de 120 categorías mediante un ejemplo. (Analíticos se define como un conjunto de algoritmos que mediante técnicas de peso y estadística de contenido determina valores porcentuales a los componentes de una página web) 20. Debe bloquear aplicaciones para Windows maliciosas mediante el uso de Reconocimiento de Aplicaciones, Detección Avanzada de Aplicaciones y Análisis de Seguridad en Tiempo Real. Este debe ser un motor de seguridad adicional que permita identificar ciertos archivos binarios como herramientas de hacking renombradas entre otros. Este análisis debe ser realizado ON BOX (en la caja) 21. La tecnología de Reconocimiento de Aplicaciones deberá usar firmas, hashes de aplicaciones y fingerprints para comparar contra una base de datos local antes de descargar archivos ejecutables; este análisis lo debe utilizar en tiempo real y también en sitios con contenido estático y deberá ser realizado ON BOX (en la misma caja) 22. La solución deberá tener la capacidad de entender los sitios web, contenido web, aplicaciones y malware, más allá de la reputación misma del sitio considerando el uso y el contexto del mismo en Internet de manera que se logre un análisis del riesgo del sitio en tiempo real. Aun si un sitio confiable que goce de buena reputación es comprometido la solución deberá poder prevenir la amenaza. 23. Actividad de Red Sospechosa: Deberá tener un mapa que geolocalice las infecciones derivadas de descargas entrantes o datos salientes. El mapa deberá localizar los siguientes grados de complejidad de la infección basándose en los siguientes grados: • Severidad Crítica: Agrupa a incidentes relacionados con Categorías de Control y Comando, Payloads avanzados de Malware y Datos encriptados criminales salientes • Severidad Media: Sitios Web Maliciosos, Malware Móvil, Phishing y otros Fraudes • Severidad Alta: Redes Bot, keyloggers • Severidad Baja: Hacking, Proxy Avoidance 24. Los eventos de seguridad deberán mostrase bajo la siguiente modalidad: • Usuario • Dispositivo o Equipo • Categoría • Ultimo Acceso • País • Incidente 25. Deberá tener las siguientes categorías avanzadas de detección de datos: • Subidas de Archivos en Formato Criminal • Archivos que contienen Password Estas categorías deberán vigilar por los datos detectados y que sean encriptados en formatos desconocidos utilizados por redes bots y	

también aquellos datos que conlleven password tipo SAM (Security Account Manager)

26. Servicios de Investigación en línea: Deberá tener vinculado la URL detectada como maliciosa hacia un servicio en Internet gratuito que pueda dar más información de las características del sitio entre las que debe ofrecer:
    - IP
    - País de donde se hospeda
    - Bytes Recibidos
    - Código de estado HTTP
    - Identificación de Seguridad en Tiempo Real
    - Extracto del análisis de JS Ofuscado
    - Detección de link de URL
    - Historial de Seguridad
27. Debe realizar actualizaciones diarias, con descargas incrementales con opción de actualizaciones dinámicas y desatendidas.
28. Debe tener categorías separadas para sitios web que afectan el tiempo de productividad de los empleados y sitios que afecta el ancho de banda del acceso a internet
29. Debe tener categoría separada para Seguridad: Allí debe estar contenidos sitios web que presentan amenazas como:
    - Bot networks
    - Keyloggers,
    - Malicious Embedded iFrame
    - Malicious Embedded Link
    - Malicious Web Sites
    - Phishing and Others Frauds
    - Potencially Unwanted Software
    - Spyware
    - Suspicious Embedded Link

    No se consideran soluciones que no cuenten con estas categorías mínimas exigidas
30. Debe tener los siguientes controles para el manejo de Facebook:
    - Facebook Friends
    - Facebook Photo Upload
    - Facebook Mail
    - Facebook Events
    - Facebook Apps
    - Facebook Chat
    - Facebook Questions
    - Facebook Video Upload
    - Facebook Groups
    - Facebook Games
31. Debe tener los siguientes controles para el manejo de Linkedin:
    - LinkedIn Connections
    - LinkedIn Jobs
    - LinkedIn Mail
    - LinkedIn Updates

		32. Debe tener los siguientes controles para YouTube • YouTube Commenting • Youtube Sharing • Youtube video Upload 33. Deberá garantizar que nuevas páginas cuyo contenido represente riesgos a la seguridad sean agregadas automáticamente a la lista de URL's máximo cinco minutos después de haber sido descubiertas por el fabricante de la solución, durante el transcurso del día y de manera automatizada aparte de la clasificación que ya realiza en forma dinámica con motores analíticos locales 34. Si un sitio se encuentra infectado con códigos móviles maliciosos o el nombre y la URL utilizada en ataques de phishing, ataques fraudulentos u otros ataques maliciosos, notificar a la organización con detalles del ataque de modo que se puedan tomar medidas. 35. Deberá permitir la reclasificación manual de cualquier página Web según las necesidades de la empresa, bien como permitir que ciertas páginas puedan ser accedidas a cualquier momento, aunque pertenezcan a categorías bloqueadas 36. Deberá permitir el bloqueo de páginas que pertenezcan a categorías permitidas, pero cuya URL posea ciertas palabras-clave 37. Deberá permitir el acceso a páginas de ciertas categorías, pero bloquear el intento de ciertos tipos de archivo (tales como video, audio, archivos comprimidos, ejecutables, documentos, etc.) desde dichas páginas 38. Deberá permitir la definición de políticas por IP, rangos de IP's, usuarios y grupos de los siguientes servicios de directorio para HTTP(S)/FTP sobre HTTP: • Dominios del Microsoft Windows NT (NTLM) • Dominios del Microsoft Active Directory • Directorios LDAP 39. Deberá permitir diferentes tipos de bloqueo por horarios del día y días de la semana para cualquiera de las políticas definidas 40. Deberá permitir la definición de montos de cuotas de tiempo distintos para usuarios de grupos distintos, para usuarios específicos y para los usuarios generales 41. Deberá exhibir una página HTML personalizable cada vez que un usuario intentar acceder a una página bloqueada 42. Deberá enviar una alerta administrativa por e-mail, popup o SNMP caso haya un número (configurable) accesos a páginas de las categorías deseadas durante el día 43. Deber tener listas personalizables donde el acceso a los sitios contenidos allí es de acceso libre para todos los usuarios del servicio de navegación 44. La solución debe tener la capacidad de asignar umbrales de ancho de banda para varias URL, categorías de URL, protocolos y categorías de protocolos. 45. Debe permitir aplicar políticas de ancho de banda para usuarios y grupos. 46. Los empleados deben ser notificados cuando sobrepasen los límites de ancho de banda configurados en las políticas.	

47. La solución debe contar con reportes tipo drill down que se puedan generar y consultar desde la consola web. Estos reportes deben proveer datos históricos y deben tener al menos 80 plantillas predefinidas que puedan ser utilizadas
48. Debe tener la capacidad de delegar la generación de reportes y debe permitir que el delegatario tenga capacidad de generar los reportes para un grupo específico de usuarios.
49. Deberá poseer interfaz de generación de reportes basados en templates predefinidos, los cuales deberán permitirse el filtrado por usuarios, grupos de usuarios, categorías, clases de riesgos, acción tomada por el sistema, fechas y rangos de fechas
50. La interfaz de generación de reportes deberá permitir la generación de resúmenes, reportes detallados, gráficas y tablas sencillas
51. La interfaz de generación de reportes deberá permitir la programación de múltiples tareas de generación de reportes predeterminados, en horarios y días de la emanas predefinidos, y deberá:
    - Enviar los reportes generados por correo electrónico hacia los recipientes deseados
52. Se podrá generar reportes de Riesgos de Seguridad presentes, como que usuarios/IP han sido atacados con Spyware, Phising, Adware, Keyloggers, etc
53. Se generarán reportes en función de cuanto ancho de banda consumen estas clases de riegos (bytes Enviados/Recibidos/Total).
54. Se podrá configurar que se manden alertas en tiempo real, a correo electrónico o en pantalla, sobre estos riegos, a detalle, con información sobre Usuario/IP, Categoría accedida, Sitio/URL, IP del Sitio, la disposición (si fue bloqueada o permitida de acuerdo a las políticas), hora y fecha
55. La interfaz de acceso directo a los registros de log deberá permitir que cada criterio de datos se pueda expandir según otro criterio, generando informes de múltiples niveles
56. Debe tener la capacidad de delegar la generación de reportes y debe permitir que el delegatario tenga capacidad de generar los reportes para un grupo específico de usuarios.

Compatibilidad IPv6 Convivencia con IPv4

El servicio contratado debe estar en capacidad de poder resolver direccionamiento IPV6 y debe ser capaz de convivir con los dos protocolos IPv6 e IPv4, es decir debe ser capaz de integrarse con estos protocolos en todas sus funcionalidades, operación, servicios y en general en todo.

<u>Soporte de Fabricante</u>

Incluye Soporte Essential con el fabricante por tres (3) años en modalidad 7x24 el cual contempla las siguientes características:

- Soporte en línea las 24 horas del día, los 7 días de la semana, los 365 días del año: Soporte
- La base de conocimientos y la documentación
- El Foro de Clientes
- Suscripción a Tech Alerts

		▪ Descargar actualizaciones de software y parches ▪ Enviar y hacer un seguimiento de los casos de soporte ▪ Soporte 24/7 para problemas de Severidad Uno ▪ Los temas de Gravedad Dos, Gravedad Tres y Gravedad Cuatro se trabajarán únicamente durante el horario laboral habitual de Forcepoint. ▪ Asignar un número de caso de problema utilizado para rastrear el estado y como referencia para las consultas de los suscriptores ▪ Comunicar el estado de los casos abiertos ▪ Registrar la actividad de soporte y proporcionar actualizaciones de estado **<u>Appliance Forcepoint V5000 G4R2</u>** ▪ Procesador: x Intel Xeon E-2144G ▪ Memoria RAM: 16GB ▪ HDD: Capacidad 1TB (2 x 1TB, RAID-1) ▪ NIC: 4x 10/100/1000Mb RJ-45 Puertos ethernet ▪ Fuente de poder: Single 250W (100V-240V) ▪ MISC: iDRAC 9 *Enterprise card for light's out mgmt.* ▪ Dimensiones: U form factor, 23.5" D x 17.1" W x 1.69" H (595.6cm D x 43.4cm W x 4.28cm H) ▪ Soporte de hardware: global disponible 24/7 por teléfono; siguiente día hábil o 4hrs en sitio, garantía por 36 meses; 60 meses en sitio opcional. ▪ Regulación y cumplimiento normativo: FCC / ICES / EN55022 / VCCI / BIS / BSMI / C-Tick / SABS / CCC / MIC Class A y UL60950-1 / Verificado para cumplir con la directiva RoHS / Consumo energético y emisión de ruido acorde a ISO 9299	
	Requisitos de Calidad y Oportunidad	La solución de ForcePoint Web Security posee las siguientes características de calidad: 1. Contar con ATP para mitigar el ingreso de amenazas avanzadas persistentes. 2. Haber sido líder en el cuadrante mágico de Gartner al menos una vez durante los últimos 2 años. 3. Ser líder en IDC marketScape 4. Contar con soporte de fabricante en modalidad 7x24 5. El fabricante de la solución debe tener su propio Laboratorio de Seguridad cuyo foco sea hacer minería de información en internet en búsqueda de sitios que presenta amenazas conocidas y amenazas emergentes de seguridad. 6. Las actualizaciones de seguridad que se realizan en tiempo real deben tener capacidad de ser entregadas durante las 24 horas del día. 7. El proveedor debe presentar al menos 3 certificaciones en los últimos 5 años con experiencia en implementaciones de Web Security en más de 1000 usuarios. 8. El contratista deberá asegurar la continuidad y permanencia de un Ingeniero de Sistemas, Electrónico o de Telecomunicaciones, certificado por el fabricante en al menos 3 de las siguientes certificaciones: System	

	Engineer; Administrator, Web Olympian, DLP, asignado al proyecto, durante la vigencia del soporte y la garantía. 9. El proveedor debe tener un profesional universitario en ingeniería electrónica, de sistemas o de telecomunicaciones con experiencia de mínimo 4 años en soporte y mantenimiento de soluciones de Proxy Enterprise (Web Security), y certificación CISM O certificación líder Auditor 27001, debe contar con una experiencia no inferior a un (1) año en atención de incidentes de seguridad. Debe haber participado en un ciento por ciento en mínimo dos (2) proyectos relacionados con Seguridad de la Información, uno de los cuales debió estar relacionados con Web Security. con el fin de recomendar las mejores prácticas de implementación de políticas de seguridad.
Cantidad	1100 licencias y 1 appliance
Condiciones de Conservación	El chasis para el appliance debe ser de materiales duraderos y cumpliendo con estándares medioambientales.
Dimensiones	Appliance: U form factor, 23.5" D x 17.1" W x 1.69" H (595.6cm D x 43.4cm W x 4.28cm H)
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

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

Estimación del presupuesto oficial: El valor estimado del contrato con IVA en NÚMERO	$392.864.220 incluido IVA
Estimación del presupuesto oficial: El valor estimado del contrato con IVA en LETRAS	TRESCIENTOS NOVENTA Y DOS MILLONES OCHOCIENTOS SESENTA Y CUATRO MIL DOSCIENTOS VEINTE PESOS M/CTE, incluido IVA

9. RECURSOS FINANCIEROS DEL CONTRATO

Fuente de los recursos	Código de Orden

VIGENCIA ACTUAL	
Número Código de Orden	C05372021
Fecha de expedición	16 de septiembre de 2021
Rubro/Ramo	Amortización programas de computadores
Valor	$370,016,220

VIGENCIA ACTUAL	
Número Código de Orden	C06082021
Fecha de expedición	16 de septiembre de 2021
Rubro/Ramo	Depreciaciones
Valor	$22,848,000

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. Atender todos los eventos o incidentes relacionados con la operación, servicio y/o funcionalidad de la herramienta, reportados por POSITIVA 2. Tramitar los eventos, incidentes, garantías y/o toda la gestión con el fabricante en caso de que así lo requiera. 3. Suministrar a POSITIVA, 1.100 licencias, que permita controlar la navegación a internet de los usuarios de la compañía, protegiéndolos frente a amenazas avanzadas y el robo de datos con capacidad de adaptar la protección web a las necesidades requeridas, incluir soporte de fabricante Essential 7x24 que permita tener actualizaciones constantes con apoyo técnico de fabricante y mantenimiento de proveedor 8x5 para resolución de problemas, fallas, eventos incidentes y cualquier requerimiento que positiva solicite para apoyar la correcta operación de los servicios contratados. 4. Cumplir con las condiciones técnicas, de calidad, oportunidad, cantidad y todas las demás previstas en el capítulo 7 "**FICHA TÉCNICA DEL BIEN, SERVICIO Y/O OBRA**", de los estudios previos, así como las condiciones ofrecidas por el CONTRATISTA en su propuesta de servicios de fecha 19 de agosto del 2021, documentos que forman parte del contrato
Entregables del proveedor	**EL CONTRATISTA en desarrollo del contrato, deberá cumplir las siguientes actividades:** **A. ENTREGABLES DEL PROVEEDOR PARA LA ADMINISTRACION DELEGADA**

	1. Entregar informes por demanda, es decir se deben entregar informes de las labores realizadas por cada solicitud que se haga por parte de Positiva o por tareas que el proveedor defina se deben hacer mediante el monitoreo constante de la plataforma de TI definida por la Compañía. Para estos últimos informes el proveedor debe entregar la documentación máximo 5 días hábiles después de realizada la tarea. 2. Entregar información adicional que se requiera de arquitectura de la solución durante la ejecución del contrato. 3. Entregar información de mejores prácticas de operación cuando se requiera durante el contrato 4. Desarrollar un mantenimiento preventivo al año y entregar el informe realizado. 5. Entregar informes de planes de acciones realizados por actualizaciones, parches y demás de la plataforma. **B. ENTREGABLES PARA EL APPLIANCE** 1. Un (1) equipo appliance Forcepoint V5000 G4R2 con las características descritas en las especificaciones técnicas definidas por POSITIVA. 2. Plan de trabajo para la instalación, configuración migración y puesta en producción del nuevo equipo appliance V5000 G4R2. 3. Documentación técnica sobre instalación, configuración y migración del equipo appliance V5000 G4R2. 4. Resultados de pruebas de funcionalidad.
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	1. Coordinar a través del supervisor del contrato, la entrega del equipo, el plan del trabajo y las demás actividades necesarias para el cumplimiento del objeto del contrato.

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	N/A	☐ 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. ilimitado.
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	N/A		
¿Qué tipo de acceso requiere?	N/A		
¿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	Importante		
¿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?	N/A		
¿El resultado del análisis de la Oficina de Gestión Integral de Riesgos ha catalogado el objeto contractual como crítico?	No		
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	TIPO B Prestación servicios dentro de Positiva
		PJ
SEGURIDAD Y SALUD EN EL TRABAJO	Certificado emitido por la empresa (ARL) sobre la implementación del SG-SST, porcentaje de cumplimiento Estándares Mínimos (autoevaluación), cuenta con un plan de capacitación en SST, un plan de emergencias, reporte de accidentes de trabajo y Enfermedad Laboral del año anterior. Este documento ser firmado por el Representante Legal de la empresa o Especialista en SST que maneja el sistema.	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 (Invitación Pública, Méritos y Cerrada)
N/A

JEFE DE OFICINA O GERENTE RESPONSABLE AREA USUARIA
NOMBRE: SILVERIO CARMONA LOZANO
CARGO: Jefe Oficina de Tecnologías de la Información
FIRMA:
PROFESIONAL RESPONSABLE ELABORACIÓN
NOMBRE: ANDRÉS IVÁN ANTURI FIGUEROA
CARGO: Técnico Administrativo nivel 3 - OTI
FIRMA:
PROFESIONAL RESPONSABLE REVISIÓN
NOMBRE: JESÚS ALFREDO VARGAS CARVAJAL
CARGO: Profesional Especializado – Líder Infraestructura - OTI
FIRMA:
Vo.Bo. RESPONSABLE GERENCIA DE ABASTECIMIENTO ESTRATEGICO:
NOMBRE: LINA MARIA PANTOJA FERNÁNDEZ
CARGO: Profesional Especializada
FIRMA:

FECHA DE APROBACIÓN ESTUDIOS PREVIOS GERENCIA DE ABASTECIMIENTO ESTRATÉGICO	21	09	2021

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: