FORMULACIÓN DE INQUIETUDES

RFP Prestación de los servicios de gestión, administración y monitoreo integral de la infraestructura central tecnológica y del centro de operaciones de seguridad de la Caja para los componentes de servidores, bases de datos, almacenamiento, copias de respaldo, cintas para custodia de medios y equipos de telecomunicaciones y de Seguridad

Pregunta	Anexo al que corresponde	Numeral del Anexo	Respuesta
Se solicita atentamente a la entidad compartir la minuta del contrato para análisis por parte del proveedor	RFP-Servicio-Soc-y-Noc	RFP-Servicio-Soc-y-Noc	La minuta del contrato se comparte únicamente con el proveedor seleccionado.
Se solicita comedidamente a la entidad confirmar que el filtro para el tiempo de las certificaciones de experiencia, indicado en 4 años, se tomara con base en la fecha de terminación del contrato.	RFP-Servicio-Soc-y-Noc	Términos de negociación RFP	Contratos que este en curso o que hayan finalizado en los últimos 4 años
Se solicita respetuosamente a la entidad confirmar si para este proceso se deberá constituir una póliza de ciberseguridad y riesgos digitales a favor de COMFENALCO o no, ya que este costo es elevado y es importante para el proveedor tenerlo contemplado en el modelo financiero del proyecto. De no ser contestada la observación, se entenderá que no se va a pedir y no se agregara posteriormente el costo.	RFP-Servicio-Soc-y-Noc	Términos de negociación RFP	Frente a la determinación de las garantías, la Caja indicará cuáles serán las que se tendrán en la suscripción y ejecución del contrato una vez se haya seleccionado el proveedor. Sin embargo, dado el riesgo que representa la operación del SOC y el NOC, sí se requiere de la protección de los datos, por lo que probablemente esta sea una de las pólizas requeridas.
Se solicita cordialmente a la entidad confirmar que el periodo de las experiencias especificas de los perfiles solicitados en el ANEXO 1 FICHA TÉCNICA NOC Y ANEXO 2. FICHA TÉCNICA SOC, refieren a que debe demostrar con certificaciones laborales y de clientes que desempeño o desempeña el rol para el que se perfilo en periodos anteriores a Septiembre de 2020, 2021, 2022 o 2023 según los años de experiencia que se solicite para el perfil (5,4,3 o 2 años)	Anexo 1 Ficha técnica NOC Anexo 2 Fichas Técnicas SOC	Perfiles Requeridos	Se esta solicitando que se adjunte las hojas de vida, la caja podrá solicitar los certificados que acrediten la experiencia, la formación profesional y las certificaciones.
Para el numeral 9 Finalización del servicio y empalme del Anexo 1 Ficha técnica NOC se indica que se deberá incluir 1 mes para empalme al finalizar el contrato, pero en el numeral 9 Finalización del servicio y empalme del Anexo 2 Fichas Técnicas SOC indican que deben ser 2 meses. Por favor establecer para las 2 fichas un tiempo de 1 mes. Lo anterior teniendo en cuenta que el servicio de NOC y SOC será prestado por el mismo oferente adjudicado.	Anexo 1 Ficha técnica NOC Anexo 2 Fichas Técnicas SOC	Numeral 9	NOC Y SOC son servicios con condiciones diferentes por la criticidad , parametrización y demás configuraciones. La caja considera que el proceso del SOC requiere un mayor tiempo de empalme. Por ejemplo el SIEM es un producto que su implementación es responsabilidad del contrato.
Para el requerimiento de **Valores Agregados** en cualquiera de las opciones de calificación, se sugiere que el oferente cuente con la experiencia especifica en la formulación de DRP, tanto a nivel metodológico como técnico, adicional el recurso que desempeñe el rol para el acompañamiento en la construcción del DRP, cuente con las capacidades y certificaciones correspondientes. Derivado a esta sugerencia se solicita respetuosamente a la entidad que pondere de forma diferencial la evaluación y entrega de puntaje para valor agregado, teniendo en cuenta los criterios mencionados anteriormente.	RFP-Servicio-Soc-y-Noc	7.2.2 Valores agregados (100 puntos adicionales)	La entidad agradece la sugerencia presentada; sin embargo, se aclara que no se aceptará la modificación solicitada. El criterio de evaluación definido en los pliegos ya establece la forma de asignación de puntaje para el valor agregado relacionado con el acompañamiento en la construcción del DRP, de manera objetiva y medible a través de la dedicación de horas. En este sentido, no se incorporarán ponderaciones adicionales relacionadas con experiencia específica o certificaciones del recurso, dado que dichos requisitos no fueron previstos en los términos de referencia y su inclusión alteraría las condiciones de participación previamente establecidas para todos los oferentes. La caja solicita un acompañamiento especializado para la implementación del Plan de recuperación ante desastres (DRP), por lo cual se solicitarán certificaciones, experiencia y formación, la cual permita comprobar su idoneidad en la formulación de DRP, esto tendrá un impacto en la calificación.
En cuanto a las actividades de empalme se tienen estimadas 320 horas en coordinación con el proveedor actual, ¿en caso de requerirse más horas se tendrá esta disponibilidad?	Anexo-3-Actividades-Empalme-NOC	Actividades Empalme	La cantidad de horas esta definida, de igual manera el equipo técnico de la caja acompañará el proceso para que se cumpla con lo definido en los anexos.
Teniendo en cuenta la cantidad de servidores tanto Linux, Windows, AIX y en general la línea base de infraestructura, bases de datos, servicio de monitoreo, es posible que los ANS de diagnóstico ante fallas sea superior a los 20 minutos solicitados?, esto por la cantidad de servidores en plataformas que se encuentran fuera de soporte y los niveles de escalamiento que pueden requerirse.	Anexo-1-Ficha-tecnica-NOC	3.2 Requisitos Generales	20 Minutos son los que actualmente se tienen comprometidos para el diagnostico y la Caja desea mantener y/o mejorar estos tiempos.

FORMULACIÓN DE INQUIETUDES

RFP Prestación de los servicios de gestión, administración y monitoreo integral de la infraestructura central tecnológica y del centro de operaciones de seguridad de la Caja para los componentes de servidores, bases de datos, almacenamiento, copias de respaldo, cintas para custodia de medios y equipos de telecomunicaciones y de Seguridad

Pregunta	Anexo al que corresponde	Numeral del Anexo	Respuesta
Para el requerimiento "Soporte en sitio de nivel 1, 2 y 3 cuando se requiera en la sede administrativa Palace, IDC de UNE y a futuro un sitio alterno. Se solicita amablemente a la entidad confirmar que las siguientes actividades: Mantenimientos programados, Incidente, actualización de microcódigo, y solicitudes de cambio, deben ser prestadas en sitio.	Anexo-1-Ficha-tecnica-NOC	1.5 y 1.6 Requisitos Generales	El proveedor debe disponer de personal para prestar asistencia en Sitio. Las partes de acuerdo a la criticidad y a los riesgos determinarán para cada caso como debe ser la atención si en sitio o remoto.
Para el requerimiento Debe tener un recurso en sitio por demanda para la administración y gestión de BD, Virtualización, plataforma Intel, Servidores AIX, copias de respaldo, almacenamiento y seguimiento a los diferentes servicios prestados(Comités), es posible se permita sea 100% remoto?	Anexo-1-Ficha-tecnica-NOC	Requisitos Generales - Operación - 1.7	El proveedor debe disponer de personal para prestar asistencia en Sitio. Las partes de acuerdo a la criticidad y a los riesgos determinarán para cada caso como debe ser la atención si en sitio o remoto.
Con respecto al requerimiento: Ofrece El 20% de variación permisible por encima y por debajo de la línea base entregada, de acuerdo a los inventarios entregados en los anexos de este proceso y a los componentes que se presenten adicionales con el crecimiento normal de la organización. ¿Es posible considerar bajar el porcentaje al 10% teniendo en cuenta la cantidad de elementos y servicios a soportar y administrar?	Anexo-1-Ficha-tecnica-NOC	Requisitos Generales - ANS Generales - 3.4	20% es el porcentaje definido por La Caja.
Para el requerimiento: El servicio se prestará de forma presencial y/o remota en horario no hábil de lunes a domingo, garantizando que haya personal disponible para atender cualquier necesidad fuera del horario laboral estándar. Se entiende que la modalidad puede ser 100% remota?	Anexo-1-Ficha-tecnica-NOC	Fecha_Tecnica_NOC - 2 Modalidad de la prestación del servicio - 2.3	El proveedor debe disponer de personal para prestar asistencia en Sitio. Las partes de acuerdo a la criticidad y a los riesgos determinarán para cada caso como debe ser la atención si en sitio o remoto. Algunas actividades del contrato podrán ejecutarse de manera remota
Se solicita aclarar si el servicio de THALES esta en clúster o es individual.	Anexo-2-Ficha-tecnica-SOC	Fecha_Tecnica_SOC 12 Administración de THALES - 12.1	Esta en Azure y esta en Clúster.
El pliego solicita:- - Certificación del fabricante de las soluciones de seguridad : el oferente o su subcontratista debe presentar una certificación del fabricante de las soluciones de seguridad que posee la entidad, donde se evidencie que el oferente cuenta con el máximo nivel de membresía y adicionalmente que cuenta con las especialización de: SECURITY OPERATION. Se solicita a la entidad tener en cuenta que el objeto de la renovación actual de licenciamiento hace parte del Core de seguridad de Comfenalco, en este sentido se recomienda respetuosamente complementar solicitando a los oferentes aporten esta carta sea dirigida a la entidad y emitida máximo 30 días antes de la presentación de la oferta.	RFP-Servicio-Soc-y-Noc	7.1.2 Habilitación Técnica	Comfenalco se apoyará con el fabricante para la evaluación de las certificaciones.
El pliego solicita: Debe Incluir el acompañamiento a la migración e implementación a nuevas herramientas, en caso de que Comfenalco renueve Se solicita a Comfenalco Aclarar el alcance de este ítem	Anexo 2 Ficha técnica SOC	Requisitos Generales_Migración 2.1.	Esto aplica para cuando la caja adquiera una nueva solución y esta requiera interacción con algunas de las soluciones de este contrato.
Debe incluir la administración y gestión de los servidores de aplicaciones, de acuerdo al inventario entregado en los anexos de este proceso y a los componentes que se presenten adicionales con el crecimiento normal de la organización Se solicita a Comfenalco Aclarar el alcance de este ítem, ya que el servicio se limita a administrar la línea base de seguridad Fortinet objeto del presente RFP, en el enunciado se expone servidores de aplicaciones que no hacen parte de la arquitectura de seguridad.	Anexo 2 Ficha técnica SOC	Requisitos Generales_Migración 2.2.	La administración y gestión de los servidores de aplicaciones hace parte del NOC, no obstante desde el SOC se debe realizar el monitoreo y la gestión de seguridad de esta infraestructura.
El oferente debe incluir un servicio de pruebas de penetración que simule las acciones de un atacante desde redes externas e internas, ejecutando dichas pruebas en al menos doscientos (200) activos de información en caja blanca, negra y gris y realizarlas al menos tres (3) veces durante el año? Es de nuestro entendimiento que las pruebas de penetración se realizaran sobre un total de línea base de 200 activos de información.	Anexo 2 Ficha técnica SOC	Ficha técnica SOC_ 13. Pruebas de Penetración	Comfenalco definirá cuales son los 200 activos en el plan de trabajo. Puede variar el recurso al cual se le ejecutará la prueba. Las 200 activos de información se distribuyen en 3 momentos durante el año.
El servicio de escaneo de vulnerabilidades se ejecutará al menos tres (3) veces durante el año, con el primer escaneo a los 3 meses luego del inicio de la operación. Teniendo en cuenta que las pruebas de penetración se realizaran sobre 200 activos de información, por favor aclarar si serán las mismos 200 activos de información para el servicio de pruebas de vulnerabilidades.	Anexo 2 Ficha técnica SOC	Ficha técnica SOC_ 14. Escaneo de Vulnerabilidades	Comfenalco definirá cuales son los 200 activos en el plan de trabajo. Puede variar el recurso al cual se le ejecutará la prueba.
el pliego solicita en: 9.1.155Servicio de Administración del DLP Se solicita realizar el cambio en el enunciado ya que este ítem corresponde en la ficha técnica a Servicio de Administración de SOAR	Anexo 2 Ficha técnica SOC	9.1.155Servicio de Administración del DLP	La administración del DLP hace parte también de las fichas técnicas del SOC en el punto 8.2

FORMULACIÓN DE INQUIETUDES

RFP Prestación de los servicios de gestión, administración y monitoreo integral de la infraestructura central tecnológica y del centro de operaciones de seguridad de la Caja para los componentes de servidores, bases de datos, almacenamiento, copias de respaldo, cintas para custodia de medios y equipos de telecomunicaciones y de Seguridad

Pregunta	Anexo al que corresponde	Numeral del Anexo	Respuesta
El pliego solicita: en el anexo Anexo-10-Inventario-Servidores-SegPerimetral_SOC pestaña inventario de seguridad perimetral Se solicita aclarar si se debe administrar además, el NAC, Autenticator, DLP, SOAR	Anexo-10-Inventario-Servidores-SegPerimetral_SOC pestaña Inventario seguridad perimetral	Anexo-10-Inventario-Servidores-SegPerimetral_SOC pestaña Inventario seguridad perimetral	Si, es necesaria la administración de las plataformas referenciadas
Teniendo en cuenta el panorama actual del mercado respecto a la gestión de vulnerabilidades , la cual cambia a diario con nuevos CVE, parches, nuevas lo que representa un entorno de vulnerabilidades muy dinámico es necesario realizar Detección Continúa de las mismas, por ende, se solicita que el escaneo de vulnerabilidades sea continuo y que como mínimo se permita de forma mensualmente durante la vigencia del contrato para los 200 activos de red mencionados en la ficha. Este cambio le dará un panorama real y actual a la entidad para categorizar y priorizar las vulnerabilidades, lo que permite que las pruebas de penetración se realicen enfocadas a los activos más críticos en cuanto a vulnerabilidades identificadas.	Anexo 2 Ficha técnica SOC	Ficha técnica SOC_ 14. Escaneo de Vulnerabilidades Pruebas de Penetración	El análisis continuo de vulnerabilidades se consigue con el SIEM y las diferentes herramientas que actualmente tiene la caja y que van a hacer implementadas en este contrato. Comfenalco definirá cuales son los 200 activos en el plan de trabajo. Es variable el recurso al cual se le ejecutará la prueba.
Con respecto a las pruebas de penetración, se requiere por buena practica ejecutarla sobre los activos mas atacados o vulnerables de ser atacados por esto, se solicita amablemente a la entidad acotar el alcance para que sean máximo 2 pruebas de penetración por año a máximo el 10% del total de activos evaluados en vulnerabilidades, normalmente los que estén en el top de los mas vulnerables.	Anexo 2 Ficha técnica SOC	Ficha técnica SOC_ 14. Escaneo de Vulnerabilidades Pruebas de Penetración	Las partes dentro de la planeación definirán cuales serán los 200 activos de información para las pruebas y estas se distribuirán en tres momentos del año.
Se solicita amablemente a la entidad confirmar si lo enunciado en los términos del RFP COMO "Se estará en la modalidad de siete (7) días por veinticuatro (24) horas diarias en el horario laboral de la República de Colombia." se refiere a que el servicio debe ser prestado de forma integral en modalidad 7X24 a nivel de disponibilidad, primera respuesta y solución de incidentes, requerimientos, problemas y en general todos los procesos de buenas practicas a nivel de gestión, administración y monitoreo y que no se refiere a solamente el horario laboral como cobertura inicial del servicio.	RFP-Servicio-Soc-y-Noc	Términos de negociación RFP	La modalidad 7x24 establecida en los términos del RFP sí implica la prestación integral del servicio de gestión, administración y monitoreo de la infraestructura tecnológica y de seguridad, durante las 24 horas del día, los 7 días de la semana, sin limitarse exclusivamente al horario laboral colombiano. Esto incluye, pero no se limita a: *Disponibilidad continua del servicio *Primera respuesta y atención de incidentes *Gestión de cambios, problemas y eventos
Solicitamos a la entidad realizar la ampliación de la presentación de la oferta en al menos 8 días adicionales, debido a que se deben considerar temas con fabricantes.	Ficha General		La entidad agradece la solicitud presentada; sin embargo, se aclara que no se otorgará la ampliación solicitada. El cronograma definido para la presentación de ofertas se mantiene en los términos inicialmente establecidos, por lo cual no habrá modificaciones en las fechas publicadas.
Solicitamos a la entidad confirmar si se debe presentar oferta para el proceso completo o se puede presentar solo oferta de NOC o solo oferta de SOC	Ficha General		La entidad aclara que la propuesta debe presentarse de manera integral para la totalidad del proceso, por lo cual no se aceptarán ofertas parciales únicamente para NOC o únicamente para SOC.
¿La entidad permite que un mismo candidato cumpla con más de un perfil requerido, siempre y cuando se demuestre el cumplimiento de la experiencia y certificaciones exigidas para cada uno?	Anexo-1-Ficha-tecnica-NOC.xlsx / Anexo-2-Fichas-tecnica-SOC.xlsx	Perfiles Requeridos	No se admite que una sola persona consolide mas de dos perfiles, deben ser independientes.
¿La entidad garantiza que cuenta actualmente con los contratos de soporte y atención vigentes con los fabricantes, para asegurar el correcto escalamiento de incidentes y requerimientos según lo estipulado en los pliegos?	anexo-1-ficha-tecnica-NOC	2,8	Comfenalco es responsable de los contratos de soporte de hardware y software de la infraestructura que es de su propiedad.
¿Se confirma que dentro del alcance del servicio se deben incluir tanto las licencias de IBM Instana como su puesta en marcha, de acuerdo con los requerimientos técnicos del anexo correspondiente?	anexo-1-ficha-tecnica-NOC	23	Si, se debe incluir el licenciamiento, la implementación y administración.
¿Se entiende que el periodo de empalme entre el proveedor saliente y el entrante será asumido por el adjudicatario, sin generar costos adicionales para la entidad?	anexo-1-ficha-tecnica-NOC	7,4	En las ficha técnicas se indica que el empalme arranca antes del inicio de operación, en ese periodo la caja estará pagando por la operación al operador actual y no causara ningún pago al proveedor entrante. Una vez inicie la fase de operación del nuevo contrato la Caja pagará por la operación al nuevo contratista durante los tiempos definidos en las fichas técnicas.
¿La entidad acepta que las herramientas de monitoreo y de gestión de servicios (ITSM) propuestas sean soluciones open source, siempre que cumplan con los requerimientos funcionales y técnicos establecidos?	Anexo-1-Ficha-tecnica-NOC.xlsx	Ficha_Tecnica_NOC, ítem 5 y 1.5	Para la herramienta de monitoreo se puede implementar open source, para la herramienta ITSM se debe utilizar la suministrada por la Caja.

FORMULACIÓN DE INQUIETUDES

RFP Prestación de los servicios de gestión, administración y monitoreo integral de la infraestructura central tecnológica y del centro de operaciones de seguridad de la Caja para los componentes de servidores, bases de datos, almacenamiento, copias de respaldo, cintas para custodia de medios y equipos de telecomunicaciones y de Seguridad

Pregunta	Anexo al que corresponde	Numeral del Anexo	Respuesta
Dentro de los servicios se requiere gestión sobre la infraestructura monitoreada por el SOC exclusivamente para los equipos de seguridad. Por tal motivo se solicita el inventario de equipos incluyendo marca, modelo, características funcionales activas, y parámetros base para administración como pueden ser entre otras: tipo y cantidad de licenciamiento actual, cantidad de reglas de FW configuradas, cantidad de VPNs S to S o C to S, servicios como Antix, filtrado de contenido, protección de correo, cantidad de zonas, dominios configurados, reglas de filtrado, cantidad de eventos procesados, cantidad de data o capacidad de almacenamiento a analizar. en general una descripción de cada dispositivo, crecimiento proyectado durante la vigencia del contrato, igualmente una descripción de que hace, como esta configurado y que se esta monitoreando actualmente a nivel de SOC. en los posible tener arquitecturas generales o diagramas que reflejen la topología actual.	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	1.1	Esta información será entregada al proveedor seleccionado con mayor detalle. Parte de está información está incluida en los anexos de este RFP.
aclarar la infraestructura o esquema de virtualización que se tiene actualmente, ya que el valor actual de eventos y dispositivos monitoreados se encuentra en el limite entre las bandas de licenciamiento y el posible crecimiento implicaría posibles cambios de configuración o esquema de virtualización adicionales.	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	2.2	Actualmente se utiliza VMware y Virtual Machine de IBM
como se encuentra respaldada la infraestructura sobre la cual residen las aplicaciones actualmente, que niveles de disponibilidad se tienen establecidos en este moneto con la infraestructura dispuesta ? Por favor especificar que se espera del concepto de optimo desempeño ? igualmente que se espera del concepto continuidad de las aplicaciones ? lo anterior teniendo en cuenta que el SOC prestara esencialmente el servicio de monitoreo, análisis reportaje y manejo de incidentes.	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	2.5	Un ataque puede afectar el desempeño, la disponibilidad y continuidad del servicio. Por eso es necesario que el proveedor disponga de recurso humano para poder mitigar los riesgos. Comfenalco cuenta con diferentes estrategias para respaldar la información , mucha de esta se puede encontrar en los inventarios y en las fichas técnicas.
ítem para las BDs como para las aplicaciones ?	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	2.6	La pregunta no es clara
por favor incluir lo requerido en el numeral 1.1	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	2.10	La pregunta no es clara
por favor entregar información sobre la capacidad actual del fortianalizer, almacenamiento, nivel de procesamiento, arquitectura , colectores incluidos en caso de que existan.	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	2.12	Esta información será entregada al proveedor seleccionado con mayor detalle.
Con el objetivo de aclara el entendimiento, el proceso Manejo de incidentes de seguridad será realizado por el cliente ? Y la información solicitada será entregada por el SOC, o el proceso hace parte de alguno de los requerimientos del pliego y lo debe generar y gestionar el proveedor seleccionado, de tal forma que el SOC llegue hasta la remediación de los mismos como parte de su labor. en tal caso la gestión del SOC debería trabajar en conjunto con las áreas de TI del cliente que se encarguen de operar los ambientes.	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	2.14	Si, es un trabajo en conjunto con las áreas interesadas , se debe tener en cuenta que el NOC es un actor principal en el proceso.
complementando el punto anterior, existe un servicio de ticketing o mesa de servicio del cliente para registrar estos casos, o el proveedor seleccionado deberá tener un sistema propio y se evaluara la interacción de los dos servicios (cliente/proveedor) ?	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	2.15	Comfenalco tiene una herramienta de gestión de tickets la cual debe ser utilizada por el proveedor.
por favor darnos a conocer de forma general el modelo de clasificación de incidentes actual, sobre todo en cuanto a tiempos de atención, priorización y solución o remediación.	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	2.16	En los requisitos generales de las fichas técnicas se encuentran documentados los ANS. Parte de información será entregada al proveedor seleccionado con mayor detalle. Adicionalmente en contratos de operación del servicio, el proveedor debo construir en conjunto con la Caja el modelo de clasificación y priorización de incidentes. Basado en su promesa de valor, sus capacidades técnicas y tecnologías y alineado con los procesos técnicos y gestión de la caja.
estará supeditado a los tiempos informados por el cliente, en el punto anterior ?	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	2.17	En los requisitos generales de las fichas técnicas se encuentran documentados los ANS. Parte de información será entregada al proveedor seleccionado con mayor detalle. Adicionalmente en contratos de operación del servicio, el proveedor debo construir en conjunto con la Caja el modelo de clasificación y priorización de incidentes. Basado en su promesa de valor, sus capacidades técnicas y tecnologías y alineado con los procesos técnicos y gestión de la caja.

FORMULACIÓN DE INQUIETUDES

RFP Prestación de los servicios de gestión, administración y monitoreo integral de la infraestructura central tecnológica y del centro de operaciones de seguridad de la Caja para los componentes de servidores, bases de datos, almacenamiento, copias de respaldo, cintas para custodia de medios y equipos de telecomunicaciones y de Seguridad

Pregunta	Anexo al que corresponde	Numeral del Anexo	Respuesta
se puede entregar una vista con privilegios de visualización exclusivamente ?	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	2.19	Si
a manera de aclaración, se puede brindar el servicio a manera de acompañamiento para aclarar procesos o procedimientos realizados por el servicio de SOC. es correcto ?	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	2.20	El proveedor deberá colaborar activamente en la entrega de información técnica, trazabilidad, evidencias y cualquier otro requerimiento que sea solicitado por dichas entidades, garantizando la confidencialidad, integridad y disponibilidad de la información involucrada. Esto incluye asistencia a sitio para las evaluaciones y pruebas solicitadas por los auditores. Esto incluye el desarrollo de los entregables que soliciten los auditores o entes de control para la infraestructura que sea de gestión y/o administración por parte del proveedor.
se entiende como pruebas de rendimiento a las pruebas de estrés/carga en el dispositivo ? O informes de rendimiento a nivel de carga de procesamiento, memoria entre otras... Por favor aclarar.	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	3.8	Se entiende como pruebas de rendimiento a las pruebas de estrés/carga en el dispositivo, adicionalmente el proveedor deberá entregar informes de rendimiento a nivel de carga de procesamiento, memoria entre otras.
por favor entregar capacidad de almacenamiento actual del fortianalizer, esquema de respaldo y duración del mismo.	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	4.6	Esta información será entregada al proveedor seleccionado con mayor detalle
estas pruebas hacen parte del set solicitado en el numeral 14 de los presentes requerimientos o deben ser adicionales ?	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	5.11	Las pruebas de WAF son adicionales
por favor informar con que tipo de solución NAC cuenta el cliente, marca, modelo, funcionalidades activas, si existen configuraciones de línea base para el acceso. Si tiene un modelo de postura actualmente.	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	7.1.1	Se tiene FortiNAC en implementación.
Se requiere un monitoreo permanente de marca o por consultas programadas durante la vigencia	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	8.1.2	Este ya no es un requerimiento de este RFP
Este licenciamiento se solicita para personal del cliente, o hace parte del personal que el servicio de SOC considera para su operación interna ?	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE	10.1.83	Estas licencias son requeridas para el componente de SOAR que entra a hacer parte del servicio del SOC.
se puede utilizar una herramienta que automatice las pruebas ? Los 200 activos solicitados serán los mismos evaluados siempre y se realizaran pruebas sobre ellos 3 veces durante el año ? O se realizaran pruebas al azar sobre un universo de 200 activos del total de activos ? de tal forma que pueden llegar a ser 600 evaluaciones sobre diferentes activos al año, corriéndolo una sola vez por activo ?	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	14,1	El proveedor debe garantizar la calidad de las pruebas. Comfenalco definirá cuales son los 200 activos en el plan de trabajo. Puede variar el recurso al cual se le ejecutará la prueba.
cual es el alcance a nivel de cantidad de Ips, tipos de dispositivos, o tipo evaluación, a considerar en este servicio ?	Ficha técnica SOC-ADMINISTRACION , MONITOREO Y GESTIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD	15,1	Entendemos que hace referencia al punto 14.1 Escaneo de vulnerabilidades. Comfenalco definirá cuales son los 200 activos en el plan de trabajo. Puede variar el recurso al cual se le ejecutará la prueba.
Dado que se solicita - Certificado de Fabrica IBM: El oferente debe presentar certificación del fabricante, en la categoría Gold o superior de las soluciones de IBM que posee la Entidad, donde se evidencia que el oferente cuente con el conocimiento y experticia para prestar los servicios., amablemente solicitamos omitir todas certificaciones especificas IBM del personal puesto limita la pluralidad de proponente pues este requerimiento favorece al actual proveedor de servicios.	RFP Servicio SOC Y NOC – TÉRMINOS DE NEGOCIACIÓN	7,1,2	IBM cuenta con múltiples canales certificados en Colombia y es necesario para la Caja comprobar la idoneidad del personal que intervendrá las plataformas Core de la Caja, varias de las cuales están soportadas sobre plataformas IBM.
Certificación del fabricante de la solución SIEM: El oferente debe presentar una certificación del fabricante de la solución SIEM que posee la Entidad, donde se evidencia que el oferente es Distribuidor Autorizado en los 3 primeros niveles	RFP Servicio SOC Y NOC – TÉRMINOS DE NEGOCIACIÓN		"Certificación del fabricante de la solución SIEM" no hace parte de este RFP.
Certificado de Fabrica IBM: El oferente debe presentar certificación de Distribuidor Autorizado del fabricante de las soluciones de IBM	RFP Servicio SOC Y NOC – TÉRMINOS DE NEGOCIACIÓN		La pregunta no es clara, no obstante IBM cuenta con múltiples canales certificados en Colombia y es necesario para la Caja comprobar la idoneidad del personal que intervendrá las plataformas Core de la Caja, varias de las cuales están soportadas sobre plataformas IBM.