**RESPUESTA A OBSERVACIONES**

FIDUPREVISORA S.A. en cumplimiento a las actividades del cronograma establecido en la invitación a cotizar No. 002 de 2021, se permite dar respuesta a cada una de las observaciones presentadas, en relación a

(…) *“una solución que preste los servicios de SOC (Centro de Operaciones de Seguridad), apoyados en la tecnología de correlación de eventos de seguridad, con personal experto, en horario 7\*24 durante la vigencia del contrato, esto con el fin de monitorear y dar respuesta a los incidentes de seguridad de la infraestructura tecnológica en cumplimiento a los dispuesto en la circular Externa 007 de 2018 de la Superintendencia Financiera de Colombia.”*

**FIDUPREVISORA S.A.**

**INVITACION A COTIZAR No. 002 de 2021**

**RESPUESTA A OBSERVACIONES**

Fiduprevisora S.A. en respuesta a observaciones a la Invitación a cotizar número 002 de 2021 se procede a responder las observaciones, de la siguiente manera:

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 12 | 14-01-2021 | Correo Electrónico | **PWC** |

1. En cuanto a la experiencia específica, respetuosamente solicitamos a la compañía permitir la inclusión de contratos en ejecución dado la naturaleza del servicio
2. Dentro del alcance la compañía indica que “El servicio de monitoreo y correlación de eventos de la infraestructura tecnológica de la Entidad incluye el monitoreo de la plataforma de servidores alojados en los diferentes Data Center de la entidad como también las nubes públicas y privadas, aplicaciones, bases de datos, plataforma de correo electrónico, seguridad informática y de la información, Redes LAN, WLAN y WAN y servicios conexos”. Respetuosamente solicitamos a la compañía ampliar la información, esto con el propósito de acotar nuestra propuesta y para ello nos permitimos remitir un formato anexo Hoja de alcance SOC con la información requerida:



1. De acuerdo a lo relacionado dentro del alcance y que indica “El servicio de Gestión apoyo y colaboración en la infraestructura tecnológica de la Entidad comprende las acciones de soporte en sus diferentes niveles del servicio requeridos por la Vicepresidencia de Tecnología de la Información”, respetuosamente solicitamos a la DC1 - Información de uso interno compañía aclarar a qué hacen referencia o cuál es el alcance de las acciones de soporte?
2. En el requerimiento #6 se indica que “El servicio de monitoreo y correlación de eventos debe monitorear todos los eventos recolectados a través del SIEM y brindar respuesta a incidentes de seguridad de la información 7\*24 durante la vigencia del contrato, con una capacidad máxima de mil (1.000) dispositivos (servidores, dispositivos de red, dispositivos de seguridad y/0 equipos de escritorio, etc.)” dicho esto el manager del Correlacionador puede ser cloud y se podría colocar un receptor en el Data Center de la Fiduprevisora para la recolección de los logs?
3. En el requerimiento #7 se indica que el proponente debe “Suministrar en modalidad de servicio un correlacionador para soportar 1000 dispositivos con un rango de 700 hasta 1000 eventos por segundo que permita colectar, retener y correlacionar los eventos de seguridad de la Infraestructura TI”. Solicitamos comedidamente que sea proporcionado el listado de los 1.0000 dispositivos a correlacionar con su respectivo rol para acotar la propuesta y sea beneficioso para la compañía.
4. En el requerimiento #16 se solicita que “El correlacionador y el equipo de SOC deberá monitorear interfaces de red de 1GB y 10 GB y ancho de banda de 150 MB a 200MB”. para este punto a que se hace referencia, a ¿monitoreo de red como análisis de comportamiento y modelaje de red? , para este punto a que hace referencia, a monitoreo de red como análisis de comportamiento y modelaje de red; por favor aclarar.
5. En el requerimiento #17 se solicita capacitación en las funcionalidades de la solución y dicho entrenamiento debe ser certificable, por favor aclarar si la certificación debe ser expedida directamente por el fabricante de la solución e indicar para cuántas personas se requieres el entrenamiento.
6. El requerimiento #48 indica “La solución debe permitir definir correlaciones estáticas y dinámicas” por favor aclarar a qué se hace referencia.
7. En el requerimiento #52 se indica que “la solución de correlación de eventos debe soportar mecanismos nativos para tomar acciones sobre endpoint (Ej., bloqueo de IP, bloqueo de usuarios) en casos de incidentes críticos”, por favor aclarar si se requiere incluir dentro de la solución tecnologías SOAR.
8. Por favor aclarar si el alcance para el análisis de vulnerabilidades y pruebas de ethical hacking corresponde a la infraestructura que será monitoreada por el SOC más la página web, hasta 10 aplicaciones y hasta 10 portales web.
9. De acuerdo a los requerimientos, entendemos que ¿se solicita un (1) análisis de vulnerabilidades por semestre, es correcta nuestra apreciación?
10. Respetuosamente solicitamos no limitar la solución únicamente de tipo appliance permitir la opción de una solución tipo software para el análisis de vulnerabilidades y la cual también este homologada con el CVE.

diana.p.aguirre@pwc.com

**RESPUESTA DE FIDUPREVISORA:**

1. Si se permite.
2. Se entrega archivo adjunto diligenciado.
3. Se aclara este punto, el servicio requerido es de monitoreo y reporte oportuno de alarmas derivadas de este y recomendaciones y sugerencias de cómo se pueden mitigar. El soporte indicado hace referencia a que el servicio opere 7\*24 y cualquier incidente relacionado con indisponibilidad se resuelva en el menor tiempo posible.
4. Puede ser cloud? Rta: Si, siempre y cuando el ancho de banda utilizado para subir los logs a la nube sea responsabilidad de proveedor y no se consuma el ancho de banda de la Entidad.

Se podría colocar un receptor en el Data Center de la Fiduprevisora para la recolección de los logs? Rta: Si

1. En la invitación para cotización en el numeral 4.1 Generalidades se incluyó esta información, adicional se brindó más detalle en el documento adjunto denominado PWC Hoja de alcance SOC.
2. Es para análisis de comportamiento e identificación de anomalías y a su vez correlacionarlas.
3. La certificación no necesariamente debe ser del fabricante de la herramienta, en cuanto a las personas son cinco.
4. Hace referencia a la capacidad de la solución de permitir correlacionar fuentes de datos estáticos o dinámicos y de generar nuevas reglas de correlación, para lograr su afinamiento.
5. Si.
6. Sí, teniendo en cuenta que puede haber crecimiento en la infraestructura tecnológica. Estimarlo en un 10% máximo.
7. Si.
8. No se acepta la solicitud.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 2 | 14-01-2021 | Correo Electrónico | **New Net S.A.** |

1. La entidad solicita: Correlacionador que permita soportar 1000 dispositivos con un rango de 700 hasta 1000 eventos por segundo que permita colectar, retener y correlacionar los eventos de seguridad de la Infraestructura TI. Solicitamos saber qu√© tipo de dispositivos son los que har√°n parte del servicio de monitoreo.
2. ¿La solución debe ser Cloud u On Premise?

**RESPUESTA DE FIDUPREVISORA:**

1. Son lo que están relacionados en el pliego de invitación a cotizar. Relacionados con servidores se distribuyen en un 90% de máquinas virtuales y 10% de máquinas físicas.
2. Puede ser de cualquier tipo para el servicio de SOC y Ethical Hacking, para vulnerabilidades On premise.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 2 | 15-01-2021 | Correo Electrónico | **Softline** |

1. En el numeral 51 de las especificaciones solución SOC, el cual dice "El Servicio de vulnerabilidades debe estar integrado con el monitoreo y correlación y se deben declarar incidentes ante vulnerabilidades detectadas.", por favor especificar qué nivel de vulnerabilidades es considerado incidente.
2. En el numeral 1 de análisis de vulnerabilidades, el cual dice "Proveer un sistema de análisis de vulnerabilidades de propósito específico -appliance- instalado y configurado en las instalaciones de Fiduprevisora, soportado por el proveedor y licenciado por un a√±o a nombre del cliente.", nos gustaría validar si este Appliance puede ser virtual y estar licenciado a la compañía que presta el servicio o necesariamente al cliente.

**RESPUESTA DE FIDUPREVISORA:**

1. Las vulnerabilidades que se identificaron y se lograron aprovechar lo que deriva en la materialización de un incidente.
2. Tal cual como se indica en el pliego.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 6 | 15-01-2021 | Correo Electrónico | **Digiware** |

1. De acuerdo al numeral 8) Para el servicio de monitoreo y correlación, por favor confirmar si es posible ofértalo como servicio en la nube o si se requiere que se implemente en sitio.
2. Con relación al requerimiento 16) por favor ampliar el alcance deseado. Así mismo confirmar si lo que se requiere es el monitoreo de disponibilidad de las interfaces de red o si lo que se requiere es aprender acerca del comportamiento del tráfico e identificar anomalías. Adicionalmente, ¿Cuantas interfaces de 1GB y de 10GB?
3. Con relación al numeral 18) por favor informar si las aplicaciones y la nube que se requiere monitorear cuenta con registros de auditoria que permita conocer las actividades de los administradores de la nube y el servicio de nube permita accederlos a través de API u otro tipo de mecanismo.
4. Con relación al numeral 45) por favor indicar con cuantas aplicaciones propietarias cuenta la organización.
5. Con relación al numeral 55) Por favor confirmar si la entidad cuenta con una solución firewall de bases de datos o auditoria habilitada sobre las bases de datos que permita el monitoreo sobre las mismas.
6. Para el numeral 4.2 análisis de vulnerabilidades. Por favor confirmar la cantidad de direcciones IP a las que se debe hacer el análisis de vulnerabilidades

**RESPUESTA DE FIDUPREVISORA:**

1. Si es posible en la nube, siempre y cuando se propongan los conectores necesarios y se utilice un canal independiente al del cliente.
2. Se requiere aprender acerca del comportamiento del tráfico e identificar anomalías y a su vez correlacionarlas.
3. Las aplicaciones y los servicios en nube cuenta con registros de auditoria pero no permite accederlos a través de API.
4. Alrededor de 32 aplicaciones.
5. Se cuenta con tablas de auditoría habilitadas.
6. Son alrededor de 224 direcciones IP aproximadamente, con un margen de crecimiento del 5%.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 8 | 15-01-2021 | Correo Electrónico | **Sonda** |

1. REQUERIMIENTO: Numeral 1.8 Experiencia Especifica - “El interesado debe relacionar experiencia de ejecución de contratos cuyo objeto contemple las actividades citadas en el objeto de esta invitación. En caso, de que el (los) interesado(s) tenga(n) experiencia con entidades del sector financiero, favor relacionarlas de forma adicional”

OBSERVACION: Solicitamos a la entidad muy amablemente indicar la cantidad de contratos mínimo se requieren certificar y el monto mínimo a certificar.

1. Agradecemos a la entidad indicar si no es requerido por parte de la entidad un plazo de ejecución de contratos mínimos a certificar.
2. Agradecemos a la entidad si el documento invitación a cotizar corresponde a una invitación de estudio de mercado o es un RFP.

**RESPUESTA FIDUPREVISORA:** El documento de invitación a cotizar en mención corresponde a un estudio de mercado tal como se indica en el acápite 1. INFORMACIÓN GENERAL de la misma invitación:

*(…) “la presente solicitud de cotización no se puede considerar como una oferta para celebrar contrato; por lo tanto, no podrá deducirse relación contractual alguna.*

*En consecuencia, la finalidad de la presente solicitud es analizar las condiciones del mercado” (…)*

1. Agradecemos a la entidad indicar la fecha de adjudicación del proceso.
2. Agradecemos por favor indicar la fecha de inicio de ejecución del servicio SOC.
3. La entidad dentro del documento de invitación 002, especifica que se requiere una oferta a 12, 24 y 36 meses, solicitamos por favor aclarar si una vez presentada la oferta la duración del servicio será acordada con el proveedor.
4. Solicitamos a la entidad aclara si la calificación del proceso será únicamente precio o si existen valores agregados y calificables a tener en cuenta.
5. Se sugiere que la entidad incluya y especifique que la infraestructura a proponer en modalidad IaaS para prestar el servicio solicitado deba ser Nueva, no remanufacturada y de uso exclusivo para la entidad, dado la criticidad de las aplicaciones que corren dentro de la infraestructura actual de tal forma que con el proyecto que se encuentra visible para toda la entidad no afecte o deteriore la latencia y performance de las aplicaciones.

**RESPUESTA DE FIDUPREVISORA:**

1. No se estableció un mínimo en este punto, solo que es un aspecto deseable sobre todo si la experiencia es en el sector financiero.
2. No es requerido por parte de la entidad un plazo de ejecución de contratos mínimos a certificar.
3. Es una invitación de estudio de mercado.
4. La fecha de adjudicación del proceso, después de la ampliación de fechas aprobada, se dará entre febrero. y marzo, dado que hasta el 1 de febrero de 2021 se recibirán las cotizaciones o propuestas comerciales.
5. Se espera poder contar con el servicio operativo iniciando abril.
6. Si.
7. Existen valores agregados y calificables a tener en cuenta.
8. El equipo solicitado en el numeral 4.2 no debe ser no remanufacturada y debe ser de uso exclusivo para la entidad, dado la criticidad de las aplicaciones que corren dentro de la infraestructura actual de tal forma que con el proyecto que se encuentra visible para toda la entidad no afecte o deteriore la latencia y performance de las aplicaciones.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 10 | 15-01-2021 | Correo Electrónico | **Entelgy** |

1. REQUERIMIENTO: Numeral 1.8 Experiencia Especifica - “El interesado debe relacionar experiencia de ejecución de contratos cuyo objeto contemple las actividades citadas en el objeto de esta invitación. En caso, de que el (los) interesado(s) tenga(n) experiencia con entidades del sector financiero, favor relacionarlas de forma adicional”
2. Al listar los dispositivos, Se solicita a la Entidad indicar si al referirse a “incluir” se trata del servicio de monitoreo y correlación de eventos y no del “suministro” de los elementos mencionados en este numeral.
3. Se solicita a la Entidad confirmar la cantidad de páginas Web para las cuales se solicita el servicio ya que no se menciona la cantidad de dichos activos de información. El tipo de aplicaciones incluidas, si son Web, móviles
4. Se solicita a la Entidad confirmar: El tipo de aplicaciones incluidas, si son Web, móviles
5. 4) Se debe vigilar que los elementos bajo contrato estén funcionando durante todo el tiempo necesario y, en caso de que algún equipo se inhabilite o trabaje inadecuadamente sin causa aparente, el SOC tomará las medidas acordadas en los niveles de servicio, en conjunto con el cliente, para reactivar/restaurar el servicio lo antes posible.

Se solicita a la Entidad ampliar el entendimiento de este numeral, ya que no es claro si los “elementos” mencionados son aquellos suministrados propiamente por el proveedor o se refiere al listado de elementos anteriormente mencionados por FIDUPREVISORA S.A. como parte del inventario de equipos a monitorear.

1. Se solicita a la Entidad confirmar la cantidad de interfaces de red de 1GB y 10GB requeridos y si el ancho de banda de 150 a 200 Mbps se mide por interfaz o por la sumatoria de los anchos de banda que serán conectados al correlacionador.
2. Se solicita a la Entidad indicar el porcentaje de disponibilidad requerido, ya que se menciona que debe estar soportado sobre una infraestructura de un TIER 3
3. Se solicita a la Entidad indicar la cantidad de IPs que serán objeto de las pruebas de análisis de vulnerabilidades.
4. Se solicita a la Entidad informar la cantidad y tipo de activos de información sobre los cuales se desea ejecutar el test de penetración.
5. Se solicita a la Entidad confirmar la cantidad total de usuarios de correo electrónico.

**RESPUESTA DE FIDUPREVISORA:**

1. No entendemos la observación, se citó textualmente lo contenido en la invitación a cotizar.
2. Se trata del servicio de monitoreo y correlación de eventos.
3. En la invitación se especifica que son hasta 10 portales WEB, no son APIs.
4. Son WEB, en su gran mayoría, muy pocas son cliente/servidor.
5. Se aclara que es el inventario suministrado de equipos a monitorear.
6. Son hasta 10 interfaces, 2 de las cuáles deberían ser a 10 GB. El ancho de banda es un promedio del tráfico por cada interfaz.
7. 99.8%
8. Son alrededor de 224 direcciones IP aproximadamente, con un margen de crecimiento del 5%.
9. La idea es realizarlo sobre la plataforma descrita, pero se definirían alcances acordados previamente con nosotros.
10. Alrededor de 1200 usuarios.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 7 | 14-01-2021 | Correo Electrónico | **SoftwareOne** |

1. Por favor confirmar si el estimado de entre 700 a 1.000 eventos por segundo, es la totalidad de eventos generados estimados para los 1.000 dispositivos a integrar en el sistema de correlación.
2. Para el servicio de análisis de vulnerabilidades y ethical hacking, ¿se debe incluir retest?
3. Para el servicio de análisis de vulnerabilidades y ethical hacking, ¿cuántos portales son informativos y cuantos son transaccionales?
4. Para el servicio de análisis de vulnerabilidades y ethical hacking, ¿cuántos portales son internos y cuantos son públicos?
5. Para el servicio de análisis de vulnerabilidades y ethical hacking, ¿el alcance especifico es a 10 aplicaciones y a 10 portales web?, por favor especificar nombre, tipo y función de las 10 aplicaciones.
6. En el requerimiento "1) Proveer un sistema de análisis de vulnerabilidades de propósito específico –appliance- instalado y configurado en las instalaciones de Fiduprevisora, soportado por el proveedor y licenciado por un año a nombre del cliente.", es posible presentar una solución basada en software instalada en servidor
7. ¿Es posible ampliar el plazo para presentar ofertas 5 días hábiles más posteriores a la fecha estimada?

**RESPUESTA DE FIDUPREVISORA:**

1. Es un estimado, pero seguramente pueden ser muchos más, la cantidad de dispositivos es la detallada, pero no es la totalidad actual, solo estamos previendo un posible crecimiento.
2. Si y la fecha de realización debe acordarse previamente con Fiduprevisora.
3. No se cuenta con portales transaccionales.
4. Todos son públicos.
5. En la oferta se indica hasta 10 portales, previendo un crecimiento. La información solicitada en cuánto a nombre, tipo y función de las 10 aplicaciones solo se suministrará en caso de ser el oferente contratado.
6. No, definitivamente debe ser un appliance.
7. Sí, el plazo se amplió hasta el 1 de febrero del año en curso.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 10 | 14-01-2021 | Correo Electrónico | **Multisoft** |

1. ¿Cuántas interfaces se deben monitorear y en cuantos activos?
2. Se solicita por favor nombrar los servicios en la nube con los fabricantes a integrar.
3. ¿El licenciamiento y el hardware debe quedar a nombre de Fiduprevisora?
4. Fiduprevisora dispondrá de recurso o infraestructura (ambientes virtuales, canales de comunicación) para instalar los corrrelacionador y/o componentes necesarios?
5. Solicitamos a la FIDUPREVISORA que la alianza directa para combatir el cibercrimen como ICSPA y FIRST o equivalentes sea válida para cumplir este punto (23) y punto (24), ya que cubren objetivos en común para combatir el cibercrimen.
6. Solicitamos a la FIDUPREVISORA que la alianza directa para combatir el cibercrimen como ICSPA o equivalentes sea válida para cumplir este punto (24), ya que cubren objetivos en común con los grupos de respuesta a incidentes de seguridad.
7. Fiduprevisora exige personal dedicado para la atención exclusiva para la prestación del servicio para la entidad?
8. Por favor confirmar cuantas aplicaciones propietarias generaran este tipo de logs.
9. Se solicita a la entidad evaluar este punto (52) ya que la integración nativa y automatización se dará siempre y cuando las tecnologías sean del mismo fabricante. La solución de correlación soportara un mecanismo nativo y realizara acciones, siempre y cuando sean del mismo fabricante.
10. ¿Cuántos host se deben escanear?

**RESPUESTA DE FIDUPREVISORA:**

1. Son hasta 10 interfaces, 2 de las cuáles deberían ser a 10 GB. El ancho de banda es un promedio del tráfico por cada interfaz.
2. Microsoft, Nube Pública de infraestructura de servidores Claro.
3. Solo el licenciamiento del appliance.
4. Toda infraestructura interna la suministra Fiduprevisora, pero cualquier integración con servicios de nube el proponente debe contemplar la infraestructura necesaria.
5. Si es válido.
6. Si es válido.
7. No es necesario, siempre que se cumpla los niveles de servicio pactados y el reporte de alertas sea oportuno y hayan sido analizadas para disminuir falsos positivos.
8. Alrededor de 10 aplicaciones, 10 portales WEB y cambios sobre la página WEB.
9. Se mantiene el ítem 52 sin modificaciones.
10. Son alrededor de 224 direcciones host, con un margen de crecimiento del 5%.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 14 | 14-01-2021 | Correo Electrónico | **A3sec** |

1. En el punto 1.8 Experiencia Específica por favor precisar si se debe adjuntar certificados emitidos por el cliente final o solo la información contenida en la tabla.
2. En el punto 2.0 OBJETO por favor aclarar si es válido para la entidad un modelo de operación del servicio donde el alertamiento de los incidentes sea 7x24 pero los analistas están con disponibilidad 5x8.
3. En el punto 2.0 OBJETO por favor aclarar si en lo referente a la Circular Externa 042 de 2012 numeral 7.1 Análisis de vulnerabilidades, cual de las 3 arquitecturas es válida para la entidad para implementar un “hardware de propósito específico” para el análisis de vulnerabilidades: On-premises, Cloud o hibrido (on-premieses + Cloud).
4. En el punto 4.1 Generalidades por favor especificar la versión de la solucion NAC, para validar si se encuentra soportada nativamente dentro de los conectores soportados de la solución o si se requieren servicios profesionales para su desarrollo.
5. En el punto 4.1 Generalidades por favor confirmar si son en total 2 las pruebas anuales a realizar por cada tipo de prueba (análisis de vulnerabilidades y Ethical Hacking) durante la vigencia del contrato.
6. En el punto 4.1 Especificaciones Solución SOC item 16 el cliente solicita “monitorear interfaces de red de 1GB y 10 GB y ancho de banda de 150 MB a 200MB.”. Para esto el cliente cuenta con un IDS o IPS que piensa integrar al SIEM o espera que el SIEM tenga la capacidad de monitorizar tráfico con una función de IDS integrada.
7. En el punto 4.1 Especificaciones Solución SOC item 47 el cliente solicita que “El servicio debe permitir correlacionar la información de accesos a nivel perimetral (Firewalls), junto con las vulnerabilidades detectadas a nivel de equipos, esto con el fin de simular propagaciones de malware y explotaciones de vulnerabilidades.”, sin embargo en el listado de fuentes a incluir no especifica ningun escaner de vulnerabilidades a integrar, se solicita amablemente se considere omitir este punto como criterio de evaluación dentro de la propuesta.
8. En el punto 4.1 Especificaciones Solución SOC item 47 el cliente solicita que “El servicio debe permitir correlacionar la información de accesos a nivel perimetral (Firewalls), junto con las vulnerabilidades detectadas a nivel de equipos, esto con el fin de simular propagaciones de malware y explotaciones de vulnerabilidades.”, sin embargo en el listado de fuentes a incluir no especifica ningun escaner de vulnerabilidades a integrar, se solicita amablemente se considere omitir este punto como criterio de evaluación dentro de la propuesta.
9. En el punto 4.1 Especificaciones Solución SOC no se especifica funcionalidades de analítica avanzada que permitan la cacería de amenazas, ni tampoco capacidades de big data lo que mejora sustantivamente la velocidad de acceso a los datos, el análisis de información y la capacidad de respuesta ante incidentes, esas son características importantes mencionadas por analistas independientes como Gardner

(<https://www.exclusive-networks.com/se/wp-content/uploads/sites/18/2020/03/Gartner-Critical-capabilities-for-SIEM-2020.pdf>) adicionalmente, tampoco se especifica que la solución sea reconocida como líder en el mercado por Gartner u otro analista independiente, consideran importantes estas observaciones como para incluirlas dentro del pliego de requerimientos?.

**RESPUESTA DE FIDUPREVISORA:**

1. Es mejor anexarlos para evidenciar la experiencia informada.
2. Si es posible
3. On premise.
4. Clear Pass Versión 6.9.4
5. Si son dos de cada una, las cuales tendrán un alcance diferente dependiendo de nuestras necesidades (no se realizará sobre el 100% de los dispositivos relacionados en la invitación), adicional estos deben contar con su respectivos retest, los cuales también deben realizarse también de común acuerdo con la Entidad.
6. Esperamos que el SIEM tenga la capacidad de monitorizar tráfico con una función de IDS integrada.
7. El escáner o appliance de vulnerabilidades lo debe proveer el oferente de acuerdo a lo especificado en la invitación a cotizar.
8. Ítem repetido, respondido en el punto anterior.
9. Se incluyen en los requerimientos de la solución de la invitación a cotizar, lo siguiente:

La solución debe contar con funcionalidades de analítica avanzada que permitan la cacería de amenazas, y capacidades de big data lo que mejora sustantivamente la velocidad de acceso a los datos, el análisis de

información y la capacidad de respuesta ante incidentes, esas son características importantes mencionadas por analistas independientes como Gartner.

La solución debe ser reconocida como líder en el mercado por Gartner u otro analista independiente.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 3 | 14-01-2021 | Correo Electrónico | **HEON Health online** |

1. En el sub item 4.5.1 "Obligaciones Específicas - SIEM", en su literal A "Suministrar en modalidad de servicio un SIEM para soportar 1500 dispositivos con un rango de 1000 hasta 1500 eventos por segundo que permita colectar, retener y correlacionar los eventos de seguridad de la infraestructura TI de la entidad. ¿Se puede contar con una arquitectura distribuida multimarca?
2. ¿Para certificaciones de seguridad de del equipo profesional a cargo, Son válidas las certificaciones de la entidad Mile2?
3. Es factible contar con un SIEM multitenan o debe ser dedicado.

**RESPUESTA DE FIDUPREVISORA:**

1. Preferiblemente toda la solución debería ser de una sola marca.
2. Sí.
3. Puede ser multitenan.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 20 | 14-01-2021 | Correo Electrónico | **SecureSoft** |

 En el ítem 4 se listan los dispositivos que se deben incluir en la solución. Solicitamos a FIDUPREVISORA:

1. Indicar la cantidad y referencia de los Firewalls Fortinet.
2. Indicar la cantidad de usuarios de Antivirus
3. Indicar la cantidad de buzones de Office 365 a Monitorear.
4. Marca de NAC
5. Indicar si los logs de todos los dispositivos listados se pueden centralizar en un único punto para su monitoreo.

En el Ítem 4.1 Especificaciones solución SOC se solicita información a FIDUPREVISORA referente a:

1. Por favor confirmar si el correlacionador como servicio debe estar en las instalaciones de la FIDUPREVISORA o puede estar en la nube del proveedor.
2. Por favor indicar si el correlacionador implementado como servicio debe contar con alta disponibilidad.
3. “El correlacionador y el equipo de SOC deberá monitorear interfaces de red de 1GB y 10 GB y ancho de banda de 150 MB a 200MB.” Por favor indicar si lo que se busca es que el correlacionador, adicional al monitoreo de eventos, también deba realizar monitoreo de flujos de red.
4. “El correlacionador y el equipo de SOC deberá monitorear interfaces de red de 1GB y 10 GB y ancho de banda de 150 MB a 200MB.” Solicitamos mayor información del alcance del monitoreo de estas interfaces
5. “Los centros de cómputo que alojan la infraestructura de TIC del servicio de SOC se encuentren acreditados en su mayoría como TIER 3 o su respectivo equivalente. (Deseable). Especificar” Por favor confirmar que se debe garantizar que la acreditación del centro de cómputo TIER3 o equivalente no solamente sea en diseño, también debe cumplir con acreditación en construcción.
6. “El motor analítico de la solución de correlación debe permitir identificar patrones anómalos de comportamiento por usuario y/o IP.” Por favor indicar si desean que el correlacionador usado como servicio debe tener activo el módulo de UBA, con el fin de monitorear el comportamiento de los usuarios.
7. “El motor analítico de la solución de correlación debe permitir identificar patrones anómalos de comportamiento por usuario y/o IP.” Por favor indicar la cantidad de usuarios a monitorear.
8. “52) La solución de correlación de eventos debe soportar mecanismos nativos para tomar acciones sobre endpoint (Ej., bloqueo de IP, bloqueo de usuarios) en casos de incidentes críticos.” Por favor indicar si se refiere a que la solución de SIEM debe tener las capacidades nativas de integrarse con soluciones SOAR que permitan automatizar las acciones sobre los diferentes dispositivos incluyendo Endpoint, más no debe incluirse dentro del proceso actual un servicio de automatización de incidentes SOAR.
9. “55) Monitoreo permanente de los motores de bases de datos (SQL, Oracle), garantizando y asegurando disponibilidad, integridad, consistencia, seguridad, control de las bases de datos dando continuidad a la operación en los ambientes productivos.” Debido a que esta funcionalidad no es base de una solución de correlación SIEM y con el fin de garantizar la pluralidad de los oferentes se solicita cambiar este punto a: 55) Monitoreo permanente de los motores de bases de datos (SQL, Oracle), garantizando seguridad y monitoreo de las bases de datos dando continuidad a la operación de los ambientes productivos.
10. Por favor confirmar la cantidad de usuarios a monitorear de FIDUPREVISORA.
11. En el primer punto del ítem 4.2 se solicita lo siguiente:

Las tecnologías de Análisis de vulnerabilidades por lo general son soluciones de software que requieren de un servidor local para instalar su consola de administración. Solicitamos a FIDUPREVISORA aceptar la instalación de un servidor local bar metal que solo tenga la consola de administración de la solución de análisis de vulnerabilidades la cual será de propósito especifico y cumplirá con el ítem solicitado. Secure Soft incluirá en su oferta el hardware necesario para el correcto funcionamiento de la solución.

1. Para poder dimensionar la solución de Análisis de vulnerabilidades, solicitamos a FIDUPREVISORA que nos informe de la cantidad de activos (estaciones o nodos) que deberán ser analizados recurrentemente. Para esto agradecemos indicar: Cantidad de servidores, cantidad de estaciones de trabajo e indicar a que otros activos (descripción y cantidad) deben ser analizados.

3. En el primer punto del ítem 4.3 se solicita:

1. Solicitamos a FIDUPREVISORA indicar la cantidad de objetivos (direcciones IP) a las que se les debe ejecutar las pruebas de Ethical hacking

En el segundo punto del Ítem 4.3 se solicita:

1. Solicitamos a FIDUPREVISORA indicar la cantidad de objetivos (direcciones IP o activos) a los que se les debe ejecutar las pruebas de penetración

En el tercer punto del ítem 4.3 se solicita:

1. Solicitamos a FIDUPREVISORA aclarar cuantas veces al año se deben ejecutar las pruebas de ingeniería social.

**RESPUESTA DE FIDUPREVISORA:**

1. Firewall Fortigate 200D (1)
2. 1250
3. 1200
4. Clear Pass Versión 6.9.4
5. Sí, pero se debe recolectar la información de distintas VLANS (varias interfaces de red).
6. Puede estar en la nube del proveedor, y los recursos necesarios para su operación, dependen del mismo (canal de datos).
7. Sí.
8. La idea es que se analice también tráfico y comportamiento en la red.
9. Son hasta 10 interfaces, 2 de las cuáles deberían ser a 10 GB. El ancho de banda es un promedio del tráfico por cada interfaz.
10. Garantizar que la acreditación del centro de cómputo TIER3 o equivalente no solamente sea en diseño, también debe cumplir con acreditación en construcción. Deseable.
11. Sí debe tener activo el módulo de UBA.
12. Alrededor de 1200.
13. No es necesario.
14. Se cambia el requerimiento 55 por:

Monitoreo permanente de los motores de bases de datos (SQL, Oracle), garantizando seguridad y monitoreo de las bases de datos dando continuidad a la operación de los ambientes productivos.

1. Alrededor de 1000.
2. No.
3. Se indicó dentro de la invitación a cotizar, pero el alcance será definido acorde a las necesidades que se vayan presentando en Fiduprevisora, puede que se solicite en su totalidad, o parcialmente.
4. Son alrededor de 10 aplicaciones, 10 aplicaciones WEB y la página WEB, en conjunto con su infraestructura tecnológica, con un margen de crecimiento del 5%. El alcance puede variar dependiendo de necesidades de la entidad (menor cantidad).
5. Son alrededor de 224 direcciones IP aproximadamente, con un margen de crecimiento del 5%. El alcance puede variar dependiendo de necesidades de la entidad (menor cantidad).
6. Por lo menos una vez al año.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 20 | 14-01-2021 | Correo Electrónico | **Olimpia IT** |

1. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.1 Generalidades. Actualmente la entidad cuenta los dispositivos listados en la invitación, que se deben incluir en la solución.

Se solicita a la entidad indicar si los dispositivos indicados hacen parte para la integración

en la solución SIEM, o son los dispositivos que hacen parte del análisis de vulnerabilidades. Se solicita también indicar, tipo, marca y modelo de estos dispositivos, en el caso de los Windows server indicar el rol que tienen, para el Firewall Fortinet indicar si es perimetral o interno.

Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.1 Generalidades.

Para los servicios de análisis de vulnerabilidades y Ethical Hacking se tiene adicional:

- Página WEB

- Hasta 10 aplicaciones

- Hasta 10 portales WEB

1. Se solicita a la entidad indicar la cantidad de dispositivos o IP´S, a los cuales se les debe realizar los análisis de vulnerabilidades.
2. Se solicita a la entidad indicar la cantidad de análisis de vulnerabilidades que se requieren realizar en un año y si estos requieren retest.
3. Se solicita a la entidad indicar la cantidad de las IPS, URL o sitios web a los cuales se les debe realizar Ethical Hacking.
4. Se solicita a la entidad indicar la cantidad de ethical hacking que se requieren realizar en un año y si estos requieren retest.
5. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.1 Especificaciones Solución SOC. 3) Las tareas de prevención, detección, contención y recuperación de ataques, entre otras, deberán estar incluidas dentro del proceso de manejo de incidentes de seguridad de la metodología de atención del SOC.

Se solicita a la entidad indicar cuántos incidentes de seguridad se presentan en Fiduprevisora en un mes.

1. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.1 Especificaciones Solución SOC. 7) Suministrar en modalidad de servicio un correlacionador para soportar 1000 dispositivos con un rango de 700 hasta 1000 eventos por segundo que permita colectar, retener y correlacionar los eventos de seguridad de la Infraestructura TI.

Se solicita a la entidad aclarar si los dispositivos mencionados son los que aparecen en el ítem anterior del documento Inv 002 SOC NOC V04, por favor indicar de los 1000 dispositivos a soportar tipo, marca, modelo y rol de estos dispositivos. Se solicita a la entidad aclarar si requiere que la solucion SIEM del SOC, soporte 1000 dispositivos o soporte entre 700 y 1000 EPS, cual de las dos opciones, dado que por la experiencia podemos indicar que 1000 dispositivos de una entidad normalmente no envían esa cantidad de EPS, la cantidad de EPS para 1000 dispositivos esta por encima de los 1000 EPS.

1. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.1 Especificaciones Solución SOC. 16 El correlacionador y el equipo de SOC deberá monitorear interfaces de red de 1GB y 10GB y ancho de banda de 150 MB a 200MB.

Se solicita a la entidad indicar cantidad, marca y modelo de los equipos a los cuales se les deben monitorear las interfaces de red.

1. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.1 Especificaciones Solución SOC. 17 EL proveedor deberá brindar capacitación en las funcionalidades de la solución, en relación al entendimiento del dashboard, la generación de informes, y la visualización y entendimiento de las reglas del correlacionador de eventos. Este entrenamiento debe ser certificable por parte del proveedor.

Se solicita a la entidad indicar cantidad de participantes e intensidad horaria para la transferencia de conocimiento

1. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.1 Especificaciones Solución SOC. 18 El correlacionador deberá poder monitorear las aplicaciones en la nube de la entidad, utilizando como detección de una combinación de DNS, proxy web y registros de firewalls integrándose directamente con los principales servicios en la nube, para proporcionar un solo panel, que permita revisar: inicios de sesión en los servicios en la nube, donde se registran los usuarios (incluso fuera de la red corporativa), qué actividad realizan los administradores de servicios en la nube, usuarios retirados que continúen autenticándose en los servicios

Se solicita a la entidad indicar las aplicaciones y servicios que tienen en la nube y especificar en cuál nube.

1. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.1 Especificaciones Solución SOC. Los centros de cómputo que alojan la infraestructura de TIC del servicio de SOC se encuentren acreditados en su mayoría como TIER 3 o su respectivo equivalente. (Deseable). Especificar

Se solicita la entidad que requiere que el datacenter principal que aloja la infraestructura de TIC del servicio de SOC se encuentre acreditado como TIER IV y datacenter de contingencia como TIER 3.

1. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.1 Especificaciones Solución SOC. 40. Especificar la marca de la solución de correlacionador de eventos con la que trabaja el SOC.

Se solicita la entidad incluir dentro de los requerimientos que la solución SIEM a utilizar dentro del servicio, se encuentre como líder en el cuadrante Garther, esto garantiza que se cuente con una solución robusta, con grandes capacidades, de alto nivel, capaz de cubrir todos los requerimientos solicitados.

1. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.1 Especificaciones Solución SOC. 42. El servicio debe contar con un mecanismo que permita obtener inteligencia de amenazas tanto en el contexto externo como interno de la organización. Se solicita la entidad indicar si requiere adicional el servicio de inteligencia artificial, o por favor explicar detalladamente qué quiere o entiende por inteligencia de amenazas.
2. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.1 Especificaciones Solución SOC. 51. El Servicio de vulnerabilidades debe estar integrado con el monitoreo y correlación y se deben declarar incidentes ante vulnerabilidades detectadas.

Se solicita a la entidad aclarar si en el servicio de análisis de vulnerabilidades requieren estos análisis en tiempos establecidos bajo demanda o requieren una solucion de gestión de vulnerabilidades que siempre este revisando los dispositivos en tiempo real.

1. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.1 Especificaciones Solución SOC. 52. La solución de correlación de eventos debe soportar mecanismos nativos para tomar acciones sobre endpoint (Ej., bloqueo de IP, bloqueo de usuarios) en casos de incidentes críticos. Se solicita aclarar a la entidad este requerimiento, dado que la solucion SIEM, integra, correlaciona, alerta, pero no toma acciones sobre dispositivos, lo solicitados para toma de acciones se refiere a un SOAR.
2. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4. Especificaciones Solución SOC. 55. Monitoreo permanente de los motores de bases de datos (SQL, Oracle), garantizando y asegurando disponibilidad, integridad, consistencia, seguridad, control de las bases de datos dando continuidad a la operación en los ambientes productivos. Se solicita a la entidad si requieren el monitoreo de los servidores de bases de datos, si lo que requieren es monitorear las bases de datos, se requiere una solucion tipo DAM, si es así por favor indicar cantidad de servidores de bases de datos, cuántos de estos tienen menos de 8 corres y más de 8 cores, si están configurados en clúster y en qué esquema, activo- activo o activo pasivo, y en cuántas ubicaciones o datacenter están estos servidores.
3. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.2 Análisis de Vulnerabilidades. 1. Proveer un sistema de análisis de vulnerabilidades de propósito específico –appliance instalado y configurado en las instalaciones de Fiduprevisora, soportado por el proveedor y licenciado por un año a nombre del cliente. Se solicita a la entidad aclarar si requiere un apliance con la solución de escaner de vulnerabilidades para realizar programaciones de los análisis de vulnerabilidades, o requieren una solución que incluya en escaner de vulnerabilidades pero además que realice gestión de vulnerabilidades todo el tiempo, para esto por favor indicar actividad de ip o dispositivos que se requiere analizar o gestionar.
4. Según el documento Inv 002 SOC NOC V4, numeral 4 CONDICIONES DEL SERVICIO REQUERIDO, 4.3 Ethical Hacking. 1.Realizar dos pruebas de Ethical Hacking externas (caja negra), donde se valide como mínimo: SQL Injection

- Cross Site Scripting

- CSRF

- Blind SQL

- Ataques de directorio transversal

Ataques por referencia directa a objetos

Se solicita a la entidad indicar la cantidad de IP públicas, sitios web o URL a las que se requiere realizar el Ethical hacking y si se requiere retest.

1. Se solicita a la entidad indicar la cantidad de datacenter, o las ubicaciones donde se encuentran los dispositivos a monitorizar
2. Se solicita a la entidad indicar si requiere un tiempo estimado de almacenamiento de los logs durante la vigencia del contrato, ejemplo los últimos 3 o 6 meses.

**RESPUESTA DE FIDUPREVISORA:**

1. Los dispositivos listado se deben incluir en la propuesta para la solución de SOC y Análisis de vulnerabilidades, este último puede presentar alcance variable (no incluir todos los activos en la prueba), para el caso de Ethical Hacking se debe realizar a las aplicaciones, portales y página WEB indicados, más su infraestructura de TI en esta caso el alcance también puede variar.

Los datos como tipo, marca, modelo y rol de estos dispositivos, solo se suministrará al oferente seleccionado una vez suscrito el contrato, para el caso del el Firewall Fortinet es perimetral.

1. Son alrededor de 224 direcciones IP aproximadamente, con un margen de crecimiento del 5%. El alcance puede variar dependiendo de necesidades de la entidad (menor cantidad).
2. Son dos análisis de vulnerabilidades al año, con su respectivo retest.
3. Son alrededor de 10 aplicaciones, 10 aplicaciones WEB y la página WEB, en conjunto con su infraestructura tecnológica, con un margen de crecimiento del 5%. El alcance puede variar dependiendo de necesidades de la entidad (menor cantidad).
4. Son dos análisis de Ethical Hacking, con su respectivo retest.
5. Entre 10 y 15 máximo, incluyendo reportes de usuarios finales y los solicitados por la plataforma de gestión de casos de mesa de ayuda (disponibilidad de infraestructura).
6. Realmente son menos de 700, se indicó esto previendo un crecimiento importante en la infraestructura pero esto puede ser un escenario remoto. Son alrededor de 400 dispositivos. Por favor cotizar entre 400 y 700 y de 700 a 1000, por si se determina que se deben monitorear equipos de usuario final.
7. La cantidad está dentro de la invitación a cotizar y los demás datos solo serán suministrados al oferente seleccionado.
8. Cantidad 5 funcionarios y la intensidad horaria depende de las definiciones realizadas por el oferente para lograr la certificación y la complejidad de la solución.
9. Office 365 correo electrónico y herramienta corporativas y acceso a servidores de nube pública Claro.
10. El Datacenter es triara de Claro.
11. Punto incluido.
12. Lo que se requiere es registro, identificación, detección y prevención de amenazas y que la solución se encuentre actualizada en la aparición de nuevas amenazas y vectores de ataques.
13. Se requiere una solución de gestión de vulnerabilidades que siempre este revisando los dispositivos en tiempo real.
14. Por favor incluir en la solución el costo de integrar el SOAR e internamente se tomará la decisión de tomar esta opción o irnos sin este servicio.
15. Son alrededor de 10 servidores de bases de datos de máximo dos cores cada uno y al igual que el punto anterior realizar la cotización con y sin este módulo.
16. Solo lo indicado en la invitación a cotizar.
17. Son alrededor de 10 aplicaciones, 10 aplicaciones WEB y la página WEB, en conjunto con su infraestructura tecnológica, con un margen de crecimiento del 5%. El alcance puede variar dependiendo de necesidades de la entidad (menor cantidad). Y si se requiere retest.
18. Dos Data center.
19. Almacenamiento por la vigencia del contrato y al finalizar entregar los logs.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 1 | 14-01-2021 | Correo Electrónico | **Seidor** |

1. Queríamos solicitar una extensión en la fecha de presentación de la cotización para este estudio de mercado, si es posible que sea entregada el día Lunes 25 de Enero.

**RESPUESTA DE FIDUPREVISORA:** XXX

1. Se emitió la respuesta de esta observación el pasado viernes 22, para que el ofertante tuviera oportunidad en la repuesta.



|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 7 | 14-01-2021 | Correo Electrónico | **Alinatech** |

1. Respecto al punto 12: Dice el documento: El correlacionador debe almacenar datos relacionados con los incidentes y eventos, incluidos el comportamiento de los usuarios y activos asociados durante el período de vigencia del contrato, en forma de búsqueda para un estándar de 90 d√≠as y custodia durante 12 meses.

Pregunta: ¿Se espera que la solución incluya capacidades de UEBA? de ser así cuál es el máximo de entidades y usuarios de la entidad?

1. Respecto al punto 18: El correlacionador deberá poder monitorear las aplicaciones en la nube de la entidad, utilizando como detección de una combinación de DNS, proxy web y registros de firewalls integrándose directamente con los principales servicios en la nube, para proporcionar un solo panel, que permita revisar: inicios de sesión en los servicios en la nube, donde se registran los usuarios (incluso fuera de la red corporativa), qué actividad realizan los administradores de servicios en la nube, usuarios retirados que continúan autenticándose en los servicios.
2. Pregunta: Agradecemos por favor nos indiquen los servicios y aplicaciones en la nube utiliza actualmente la entidad y que hacen parte del alcance a monitorear?
3. Pregunta: En el alcance que se define en el punto 7 de Eventos por segundo, se incluyen los de estos servicios y aplicaciones en la nube?
4. Respecto al punto 48. La solución debe permitir definir correlaciones estáticas y dinámicas. Pregunta: Agradecemos nos indiquen a que hacen referencia con correlación estática y dinámica.
5. Respecto al punto 53. La solución de correlación de eventos debe ser también alimentada por fuentes de inteligencia externas de amenazas que contengan listas de reputación (IP) y/o dominios catalogados como sospechosos para la generación de indicadores de compromiso.

Pregunta: Agradecemos nos indiquen si existe alguna restricción respecto al uso de fuentes públicas?

Análisis de Vulnerabilidades

1. Respecto al punto 1: Proveer un sistema de análisis de vulnerabilidades de propósito específico –appliance- instalado y configurado en las instalaciones de Fiduprevisora, soportado por el proveedor y licenciado por un año a nombre del cliente.

Pregunta: Agradecemos confirmar si el requerimiento está enfocado en realizar análisis de vulnerabilidades sobre aplicaciones (portales web, servicios web, app móviles, cliente servidor y código fuente o si también hace referencia a vulnerabilidades a nivel de infraestructura?

**RESPUESTA DE FIDUPREVISORA:**

1. Por favor cotizar las dos opciones, son alrededor de 1200 usuarios.
2. No vemos cuál es la observación, se copió el requerimiento de la invitación a cotizar textualmente.
3. Microsoft, Nube Pública de infraestructura de servidores Claro.
4. Sí, pero podríamos estar entregando cifras muy pequeñas, no se tiene bien dimensionada la cantidad de eventos por segundo actualmente, era una cifra anterior, pero dado los cambios implementados puede haber aumentado considerablemente.
5. Hace referencia a la capacidad de la solución de permitir correlacionar fuentes de datos estáticos o dinámicos y de generar nuevas reglas de correlación, para lograr su afinamiento.
6. No existe restricción.
7. Hace referencia también a la infraestructura.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 26 | 14-01-2021 | SECOP | **Evolution IT** |

1. Numeral 3. Alcance, respetuosamente solicitamos a la entidad por favor Indicar con cuántos Datacenter cuenta desde donde se deba extraer datos e información para el monitoreo solicitado.
2. Numeral 3. Alcance, respetuosamente solicitamos a la entidad por favor listar las Nubes Públicas y Privadas en las cuales tiene infraestructura a monitorear para poder realizar un adecuado dimensionamiento.
3. Numeral 3. Alcance, respetuosamente solicitamos a la entidad por favor indicar la plataforma de correo electrónico con la cual cuenta, y si esta esta en la nube o es una instalación on premise.
4. Numeral 3. Alcance, respetuosamente solicitamos a la entidad por favor listar los servicios conexos que deberán ser monitoreados.
5. Numeral 3. Alcance, respetuosamente solicitamos a la entidad por favor aclarar que espera como “Servicio de Gestión de Apoyo y Colaboración en la infraestructura tecnológica de la Entidad” y que responsabilidades tendrá el proponente sobre la infraestructura de Fiduprevisora.
6. Numeral 3. Alcance, respetuosamente solicitamos a la entidad por favor indicar en el “Servicio de Gestión de Apoyo y Colaboración en la infraestructura tecnológica de la Entidad” cuales son los niveles de servicio requeridos.
7. Numeral 4.1, generalidades, respetuosamente solicitamos a la entidad indicar la Volumetría de eventos y/o incidentes de seguridad generados en los últimos meses.
8. Numeral 4.1, generalidades, respetuosamente solicitamos a la entidad indicar si cuenta con un equipo de respuesta a incidentes (Interno).
9. Numeral 4.1, generalidades, respetuosamente solicitamos a la entidad exigir como requisito al proveedor del servicio este certificado en ISO 27001, con el fin de evidenciar experiencia y calidad en el servicio suministrado.
10. Numeral 4.1, ítem 6, respetuosamente solicitamos a la entidad por favor detallar los dispositivos red (tecnología, marca, etc.) y motores de bases de datos.
11. . Numeral 4.1, ítem 6, respetuosamente solicitamos a la entidad por favor indicar la cantidad de aplicaciones y servidores WEB (Tipos) requeridos en el servicio de monitoreo.
12. Numeral 4.1, ítem 6, respetuosamente solicitamos a la entidad por favor indicar si cuenta con más de un dominio.
13. 3. Numeral 4.1, ítem 8, respetuosamente solicitamos a la entidad por favor especificar las marcas y modelos requeridos.
14. Numeral 4.1, ítem 10, respetuosamente solicitamos a la entidad por favor indicar si cuenta con espacio en el Datacenter (2U) y/o en un entorno Virtual (VMWare o Hyper-V) para instalar un servidor de captura de logs “connector” o “sensor”.
15. Numeral 4.1, ítem 11, respetuosamente solicitamos a la entidad por favor indicar si actualmente cuenta con reglas de correlación personalizadas que deberá considerar el proveedor en su implementación.
16. Numeral 4.1, ítem 17, respetuosamente solicitamos a la entidad y de acuerdo con la situación nacional ocasionada por el COVID-19 y las medidas decretadas por el gobierno nacional, que las capacitaciones puedan ser brindadas vía virtual con el fin de proteger el personal de Fiduprevisora S.A. y del proponente.
17. Numeral 4.1, ítem 18, respetuosamente solicitamos a la entidad especificar los proveedores de nube.
18. Numeral 4.1, ítem 41, respetuosamente solicitamos a la entidad especificar la versión de Aranda (bus).
19. Numeral 4.2 Análisis de Vulnerabilidades, respetuosamente solicitamos a la entidad por favor indicar el número de direcciones IP que serán alcance del servicio.
20. Numeral 4.2 Análisis de Vulnerabilidades, respetuosamente solicitamos a la entidad por favor aclarar si el Appliance es requerido físico o si Fiduprevisora proveerá la infraestructura de virtualización para instalar un virtual Appliance.
21. Numeral 4.2 Análisis de Vulnerabilidades, respetuosamente solicitamos a la entidad por favor aclarar si el servicio requerido de análisis de vulnerabilidades es continuo y con informes mensuales como lo indica el numeral 4) o si solo es requerido dos análisis con sus respectivos informes durante el año de servicio como lo indican los numerales 2) y 3).
22. Numeral 4.3 Ethical Hacking, Ítem 1), respetuosamente solicitamos a la entidad por favor indicar el número de objetivos y el alcance del servicio por cada una de las pruebas expresado en cantidad de direcciones IP a evaluar.
23. Numeral 4.3 Ethical Hacking, Ítem 2), respetuosamente solicitamos a la entidad por favor aclarar el alcance del test de penetración interno y que espera de la ejecución de estas pruebas.
24. Numeral 4.3 Ethical Hacking, Ítem 2), respetuosamente solicitamos a la entidad por favor indicar el número de objetivos y el alcance del servicio por cada una de las pruebas expresado en cantidad de direcciones IP a evaluar
25. Numeral 4.3 Ethical Hacking, Ítem 3), respetuosamente solicitamos a la entidad por favor aclarar si se requiere una (1) sola prueba por cada año de ejecución del contrato.
26. Numeral 5. Duración, respetuosamente solicitamos a la entidad por favor aclarar si se requiere por cada año de servicios pruebas adicionales de Ethical hacking, es decir:
	1. Para doce (12) meses dos (2) pruebas de Hacking Ético, una (1) Prueba interna y una (1) de Ingeniería social.
	2. Para veinticuatro (24) meses cuatro (4) pruebas de Hacking Ético, dos (2) Pruebas internas y dos (2) de Ingeniería social.
	3. Para treinta y seis (36) meses ocho (8) pruebas de Hacking Ético, cuatro (4) Pruebas internas y cuatro (4) de Ingeniería social.

**RESPUESTA DE FIDUPREVISORA:**

1. 2 datacenter
2. Microsoft, Nube Pública de infraestructura de servidores Claro.
3. Microsoft Office 365, nube
4. Servicio Internet, de impresión, wifi.
5. Se requiere la actividad de monitoreo y alertamiento oportuno de los verdaderos positivos identificados (se solicita se afinen las reglas para que se filtren adecuadamente los falsos negativos) y adicional las recomendaciones de cómo se podría solucionar acorde a su base de conocimiento.

|  |  |  |
| --- | --- | --- |
| **Nivel de prioridad** | **Tiempo para Generar Alerta**  | **Impacto** |
| Inferior | 1 horas | Leve |
| Bajo | 30 minutos | Inferior |
| Medio | 15 minutos | Moderado |
| Alto | 5 minutos | Superior |
| Superior | 3 minutos | Extremo |

1. Entre 10 y 15 máximo al mes, incluyendo reportes de usuarios finales y los solicitados por la plataforma de gestión de casos de mesa de ayuda (disponibilidad de infraestructura).
2. Sí señor, pero son los mismo funcionales de seguridad y TI.
3. Se incluirá dentro de la invitación a cotizar.
4. Esta información solo se suministrará al oferente seleccionado.
5. Alrededor de 10 aplicaciones WEB y 10 servidores WEB.
6. Solo un dominio.
7. Esto se entregó en la incitación a cotizar.
8. Sí.
9. No.
10. De acuerdo, de igual manera estamos trabajando en casa actualmente.
11. Microsoft y Claro.
12. Versión de Aranda: 8.0.59
13. Son alrededor de 224 direcciones IP aproximadamente, con un margen de crecimiento del 5%. El alcance puede variar dependiendo de necesidades de la entidad (menor cantidad).
14. Debe ser físico.
15. Debe ser dos al año con sus respectivos retest y los resultados debe correlacionarse en el SIEM del SOC para identificar posibles ataques.
16. Alrededor de 10 aplicaciones, 10portales WEB y la página más la infraestructura tecnológica que los soporta.
17. El alcance está acotado por la cantidad de vulnerabilidades identificadas y cuáles de ellas podrían ser aprovechadas por usuarios internos y cómo, se quiere identificar los incidentes que pueden ser perpetrados por funcionarios de la Fiduprevisora, teniendo activos los controles actuales.
18. Numeral repetido, respuesta 22.
19. Se requiere dos pruebas al año con sus respectivos retest, los alcances serían diferentes para cubrir la totalidad del alcance ya expresado.
20. No, son las mismas cantidades para cada año de servicio, es decir dos pruebas al año con su retest y una prueba de ingeniería social.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 4 | 14-01-2021 | Correo Electrónico | **IT Security Services IT-SS** |

1. El ítem 3 indica lo siguiente “Las tareas de prevención, detección, contención y recuperación de ataques, entre otras, deberán estar incluidas dentro del proceso de manejo de incidentes de seguridad de la metodología de atención del SOC.” Solicitamos amablemente aclarar el alcance esperado para la contención y erradicación de los posibles incidentes identificados.
2. El ítem 18 indica lo siguiente “El correlacionador deberá poder monitorear las aplicaciones en la nube de la entidad…”, adicional a esto el pliego menciona a Office 365; solicitamos amablemente aclarar si la entidad cuenta con otras plataformas o aplicaciones en la nube que estarán incluidas en el alcance de este proceso; en caso de contar con aplicaciones adicionales, por favor indicarlas e incluir el número de usuarios de estas.
3. El ítem 55 indica lo siguiente “Monitoreo permanente de los motores de bases de datos (SQL, Oracle), garantizando y asegurando disponibilidad, integridad, consistencia, seguridad, control de las bases de datos dando continuidad a la operación en los ambientes productivos.”, solicitamos amablemente aclarar el alcance esperado para esta solicitud, asimismo solicitamos amablemente indicar el número de bases de datos o instancias a monitorear.
4. Para la operación del servicio ofertado se requieren 2 servidores virtualizados con las siguientes características:

Servidor 1:

o 8 Cores de procesamiento a 2,6 GHZ.

o 48 GB de RAM.

o 100 GB de disco duro.

Servidor 2:

o 6 Cores de procesamiento a 2,6 GHZ.

o 24 GB de RAM.

o 50 GB de disco duro.

Con la finalidad de disminuir costos operativos del servicio, solicitamos amablemente que Fiduprevisora pueda disponer y entregar al proveedor la infraestructura mencionada.

**RESPUESTA DE FIDUPREVISORA:**

1. Favor cotizar el servicio con SOAR y sin SOAR, a fin de validar si es viable que la tarea de contención en caso de identificarse incidentes críticos quede del lado del proveedor, ya la erradicación sería una actividad nuestra.
2. Solo Microsoft y la mayor parte de la Infraestructura TI se encuentra en la Nube Pública de Claro.
3. Se solicita que el servicio esté en la capacidad de recolectar los logs de diferentes bases de datos y correlacionarlos. A su vez también por favor cotizar con y sin el módulo DAM activo, para tomar decisiones sobre su viabilidad.
4. Se debe especificar qué rol cumplirán los servidores solicitados.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 3 | 15-01-2021 | Correo Electrónico | **ETB** |

1. Debe contar con alianzas directas y activas para combatir el cibercrimen a nivel nacional o mundial como ICSPA o equivalente. Especificar cuáles y contactos para revalidar alianzas.

Por favor aclarar si las alianzas directas deben ser del proveedor o en su defecto se aceptan alianzas del proveedor con sus respectivos aliados estratégicos.

1. Debe tener una vinculación directa y activa con grupos de respuesta a incidentes de seguridad informática como FIRST por ejemplo. Especificar con cuáles.

Por favor aclarar si permiten cumplir con este requisito mediante alianzas del Proveedor con sus aliados estratégicos.

1. El proponente deberá tener un SOC propio.

Por favor aclarar si permiten cumplir con este requisito mediante alianzas del Proveedor con sus aliados estratégicos.

**RESPUESTA DE FIDUPREVISORA:**

1. Principalemnet con ICSPA, pero si cuentan con alianzas con organizaciones de igual reconocimiento por favor indicarlas y si se aceptan alianzas del proveedor con sus respectivos aliados estratégicos, siempre que se cuente con información actualizada para identificar nuevos vectores de ataque a nivel mundial en el servicio.
2. Adicional a FIRST, está el CSIRT y COLCERT, por ejemplo.
3. No, el SOC si debe ser propio para no afectar los tiempos en los ANS.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 14 | 15-01-2021 | SECOP | **AXITY** |

1. Actualmente la entidad cuenta con los siguientes dispositivos, que se deben incluir en la solución. Agradecemos indicarnos las cantidades y modelos de los dispositivos
2. "Para los servicios de análisis de vulnerabilidades y Ethical Hacking se tiene adicional:

- Página WEB

- Hasta 10 aplicaciones

- Hasta 10 portales WEB"

Respetuosamente solicitamos nos indiquen la cantidad de dispositivos a los que se les va a hacer Análisis de Vulnerabilidades y la cantidad a los que se les va a hacer Ethical Hacking

1. Por favor indicarnos el alcance del Ethical Hacking esperado, si este va a ser caja negra, caja blanca o caja gris
2. 3) Las tareas de prevención, detección, contención y recuperación de ataques, entre otras, deberán estar incluidas dentro del proceso de manejo de incidentes de seguridad de la metodología de atención del SOC solicitamos aclarar este requerimiento, lo esperado por parte de Fiduprevisora es la documentación de estas tareas? O esperan que se ejecuten como parte del servicio de SOC? Esto teniendo en cuenta que las tareas de contención y recuperación se ejecuta directamente en los dispositivos y desde el sic no se tendría acceso a esos dispositivos
3. 4) Se debe vigilar que los elementos bajo contrato estén funcionando durante todo el tiempo necesario y, en caso de que algún equipo se inhabilite o trabaje inadecuadamente sin causa aparente, el SOC tomará las medidas acordadas en los niveles de servicio, en conjunto con el cliente, para reactivar/restaurar el servicio lo antes posible. Respetuosamente solicitamos aclarar el alcance esperado en "reactivar/restaurar el servicio lo antes posible", esto teniendo cuenta que desde el SOC no tendríamos administración o soporte sobre los dispositivos afectados
4. 9) El correlacionador debe proporcionar una arquitectura escalable donde la capacidad de procesamiento, memoria y almacenamiento se puede aumentar o disminuir de acuerdo con la carga real en producción El dispositivo de correlación puede estar en Nube?
5. 9) El correlacionador debe proporcionar una arquitectura escalable donde la capacidad de procesamiento, memoria y almacenamiento se puede aumentar o disminuir de acuerdo con la carga real en producción La entidad puede proveer un servidor en premisa que actuará como collector?
6. 26) Los centros de cómputo que alojan la infraestructura de TIC del servicio de SOC se encuentren acreditados en su mayoría como TIER 3 o su respectivo equivalente. (Deseable). Especificar En caso que la entidad permita el servicio ubicado en Nube, este punto se cumpliría con las características provistas por el proveedor de nube
7. 34) El proponente deberá desarrollar estrategias que permitan hacer inteligencia de ataques y detección de nuevo malware y APTs y establecer procedimientos de contención y erradicación de los mismos. Agradecemos confirmar si el alcance del servicio para este punto es hasta documentar las actividades de contención y erradicación mas no ejecutarlas, esto teniendo en cuenta que no se tiene administración de la plataforma TI que puede llegar a ser afectada
8. 52) La solución de correlación de eventos debe soportar mecanismos nativos para tomar acciones sobre endpoint (Ej., bloqueo de IP, bloqueo de usuarios) en casos de incidentes críticos.

Solicitamos aclarar si lo esperado en este punto cuando indican que se requiere mecanismos nativos para tomar acciones sobre endpoint, es una herramienta de respuesta automática (SOAR), en caso que no agradecemos aclarar lo esperado en ese punto

1. 53) La solución de correlación de eventos debe ser también alimentada por fuentes de inteligencia externas de amenazas que contengan listas de reputación (IP) y/o dominios catalogados como sospechosos para la generación de indicadores de compromiso. los eventos generados por esas fuentes de inteligencia externas de amenazas, harían parte de los 700-1000 EPS indicados anteriormente como la capacidad requerida? o debe contemplarse capacidad adicional para estos logs
2. 55) Monitoreo permanente de los motores de bases de datos (SQL, Oracle), garantizando y asegurando disponibilidad, integridad, consistencia, seguridad, control de las bases de datos dando continuidad a la operación en los ambientes productivos El monitoreo a los motores de bases de datos hacen parte de los 700-1000 EPS indicados anteriormente como la capacidad requerida? o debe contemplarse capacidad adicional para estos logs
3. 1) Proveer un sistema de análisis de vulnerabilidades de propósito específico –appliance- instalado y configurado en las instalaciones de Fiduprevisora, soportado por el proveedor y licenciado por un año a nombre del cliente. Por favor indicarnos si puede ser un servidor con el software de gestión de vulnerabilidades exclusivo para ese propósito
4. "1) Realizar dos pruebas de Ethical Hacking externas (caja negra), donde se valide como mínimo:

- SQL Injection

- Cross Site Scripting

- CSRF

- Blind SQL

- Ataques de directorio transversal

- Ataques por referencia directa a objetos"

Por favor indicarnos la cantidad de objetivos a los que se les haría Ethical Hacking

**RESPUESTA DE FIDUPREVISORA:**

1. Es lo indicado en la invitación a cotizar
2. Para análisis de vulnerabilidades son alrededor de 224 direcciones IP aproximadamente, con un margen de crecimiento del 5%. El alcance puede variar dependiendo de necesidades de la entidad (menor cantidad).

Para Ethical Hacking son alrededor de 10 aplicaciones, 10 aplicaciones WEB y la página WEB, en conjunto con su infraestructura tecnológica, con un margen de crecimiento del 5%. El alcance puede variar dependiendo de necesidades de la entidad (menor cantidad).

1. Por favor cotizar el costo de cada tipo de prueba, la idea es realizar de diferentes tipos y con diferente alcance, cubriendo la totalidad de activos en el año.
2. Favor cotizar el servicio con SOAR y sin SOAR, a fin de validar si es viable que la tarea de contención en caso de identificarse incidentes críticos quede del lado del proveedor, ya la erradicación sería una actividad nuestra.
3. Misma aclaración anterior.
4. Si es posible en la nube, siempre y cuando se propongan los conectores necesarios y se utilice un canal independiente al del cliente.
5. Si contamos con uno, pero es necesario se valide su funcionamiento (no soporte), por favor cotizar con y sin este dispositivo.
6. Sí.
7. Mismo punto tratado anteriormente con el SOAR y documentación de recomendaciones para poder tratar el incidente.
8. Sí, favor cotizar con y sin SOAR para la toma de decisiones.
9. Se encuentra contemplado en la capacidad requerida.
10. Se encuentra contemplado en la capacidad requerida.
11. Debe ser un appliance de vulnerabilidades.
12. Se respondió en el ítem 2.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 9 | 15-01-2021 | Correo Electrónico | **American Inteligencie Group** |

1. 10) Los recursos necesarios para la instalación y operación de la solución con relación a la memoria, procesamiento y almacenamiento, deberán ser proporcionados por el contratista. Esto indica que los recursos anteriormente nombrados, ordenadores a nivel de hardware, ¿Deben ser ofertados por el mismo proveedor de SOC?
2. 17) EL proveedor deberá brindar capacitación en las funcionalidades de la solución, con relación al entendimiento del dashboard, la generación de informes, y la visualización y entendimiento de las reglas del correlacionador de eventos. Este entrenamiento debe ser certificable por parte del proveedor. Esta formación que requieren, ¿Es un tema de manejo y entendimiento o con un enfoque técnico? y ¿Para que número de usuarios seria la formación?
3. 24) Debe tener una vinculación directa y activa con grupos de respuesta a incidentes de seguridad informática como FIRST, por ejemplo. Especificar con cuáles. Si el servicio lo presta el SOC propio del ofertante, ¿Por qué es de tan alto interés esa vinculación directa?
4. 28) Debe contar con protecciones físicas contra daño por: Incendio, inundación, terremoto, explosión, manifestaciones sociales, otras formas de desastre natural o artificial. No queda muy claro este alcance, pues se puede contar con planes de contingencia y respuesta ante incidentes, pero ¿Protección contra desastres naturales, como terremotos?, es todo un esquema que no tiene cobertura realista.
5. 32) Las instalaciones del SOC deberán tener periódicamente información de indicadores sobre plataforma monitoreada. No se entiende el requerimiento, de forma es un requerimiento que ya esta hecho en otro punto, en tal caso de no ser así, ¿Podrían ser un poco más específicos?
6. 55) Monitoreo permanente de los motores de bases de datos (SQL, Oracle), garantizando y asegurando disponibilidad, integridad, consistencia, seguridad, control de las bases de datos dando continuidad a la operación en los ambientes productivos. ¿Esta garantía es parte del esquema de la monitorización continua, la orquestación y autorización de procesos (SOAR)? o ¿qué enfoque se le da?, pues al detectarse una amenaza inminente o anomalía ya podría hablarse de que la seguridad se vio comprometida
7. 1) Proveer un sistema de análisis de vulnerabilidades de Propósito específico –appliance instalado y configurado en las instalaciones de Fiduprevisora, soportado por el proveedor y licenciado por un año a nombre del cliente ¿En tal caso sería la adquisición de la tecnología como canal de frente a Fiduprevisora como cliente final?, se quiere dar total entendimiento de esta sección. A su vez se amplia la consulta a lo siguiente: ¿los costes de instalación y configuración que conllevan el despliegue inicial de las tecnologías se cotizaran en un esquema aparte de lo concerniente al servicio mensual? o ¿cómo se procederá en este contexto?
8. 5) Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual del inmediatamente anterior ¿Esto es mensualmente en cada informe?
9. Queda un punto que no se ve cubierto y nuestro centro de operaciones hace énfasis en que es importante darle cobertura.

El análisis del tráfico cifrado que viaja vía HTTPS o por aplicaciones que utilizan protocolos de encriptación punto a punto, no estaría siendo monitorizado realmente pues la lectura de las cabeceras de los paquetes cifrados no dan entrada al payload, con lo cual, plataformas basadas en IA como DarkTrace, te indica que “puede realizar análisis de esta forma” sin embargo el perfilar el cifrado de un payload e identificarlo con un tipo de cabecera en concreto no te asegura la fidelidad de ese contenido, por eso AIG recomienda encarecidamente utilizar un sistema de Descifrado SSL que funciona como túnel, el cual desencripta los datos, hace la lectura del payload y en la salida de la función vuelve a cifrarlos, para que viajen totalmente seguros permitiendo analizar ese 80% del actual tráfico Web que viaja de forma cifrada.

**RESPUESTA DE FIDUPREVISORA:**

1. Los recursos que requieren para poner en funcionamiento el servicio, sí.
2. Sí y sería para máximo 5 funcionarios.
3. Como por ejemplo CSIRT y COLCERT, para tener en el radar los incidentes que se reportan a estas entidades y vincularlos al correlacionador y a su vez de nuestra parte hacer el reporte si se amerita.
4. Estas necesidades se solicitan siempre para garantizar la continuidad del servicio prestado, por favor proporcionar el plan de continuidad para el servicio a contratar.
5. Se solicita se lleven estadísticas sobre el funcionamiento del SOC, cantidades en cuanto a los servicios o aplicaciones monitorizadas, cantidad de eventos identificados, cuáles son verdaderos positivos y demás indicadores que nos permitan establecer la efectividad del servicio prestado.
6. Entregar cotización con SOAR y Sin SOAR y a su vez con DAM y sin él, para este ítem.
7. Sí, es un appliance que se instale en Fiduprevisora y la licencia este a nombre nuestro por un año o por el tiempo de la vigencia del contrato, la cotización debe ser a nivel general detallando todos estos aspectos en ella.
8. No, son solo dos pruebas al año con sus respectivos retest y el análisis diferencial se debe hacer del informe generado VS. retest y luego VS. nueva prueba desarrollada si tiene alcances homogéneos.
9. Se incluye esta recomendación dentro de la invitación a cotizar.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 13 | 15-01-2021 | Correo Electrónico | **American Intelligence Group** |

1. En el documento “Invitación a cotizar”, en el Numeral 4.1 Generalidades se mencionan los diferentes dispositivos que se deben incluir dentro de la solución, entre los cuales se menciona:

• Firewall Fortinet

• Suite Trend Micro

• Office 365

Para dimensionar los servicios a ser prestados se solicita a FIDUPREVISORA

complementar la información, mencionando:

-La cantidad de firewalls y de ser posible el modelo

-Trend Micro mencionar, para cuantos usuarios esta licenciada

-Office 365 cantidad de usuarios

1. En el documento “Invitación a cotizar”, en el Numeral 4.1 Especificaciones Solución SOC FIDUPREVISORA solicita:

“4)-Se debe vigilar que los elementos bajo contrato estén funcionando durante todo el tiempo necesario y, en caso de que algún equipo se inhabilite o trabaje inadecuadamente sin causa aparente, el SOC tomará las medidas acordadas en los niveles de servicio, en conjunto con el cliente, para reactivar/restaurar el servicio lo antes posible.” Se solicita a la entidad aclarar que este requerimiento, solo aplica a los equipos suministrados como parte del servicio y no para la infraestructura propia de FIDUPREVISORA.

1. En el documento “Invitación a cotizar”, en el Numeral 4.1 Especificaciones Solución SOC FIDUPREVISORA solicita:

“6)-El servicio de monitoreo y correlación de eventos debe monitorear todos los eventos recolectados a través del SIEM y brindar respuesta a incidentes de seguridad de la información 7\*24 durante la vigencia del contrato, con una capacidad máxima de mil (1.000) dispositivos (servidores, dispositivos de red, dispositivos de seguridad y/0 equipos de escritorio, etc.)

Se solicita favor aclarar si FIDUPREVISORA requiere que la solución reciba lo eventos generados por cada uno de los equipos de escritorio, de ser afirmativo favor entregar la cantidad de equipos de escritorio que requieren este servicio.

1. En el documento “Invitación a cotizar”, en el Numeral 4.1 Especificaciones Solución SOC FIDUPREVISORA solicita

“7) Suministrar en modalidad de servicio un correlacionador para soportar 1000dispositivos con un rango de 700 hasta 1000 eventos por segundo que permita colectar, retener y correlacionar los eventos de seguridad de la Infraestructura TI.”

Se solicita a la entidad aclarar si esta es una capacidad de crecimiento a futuro, teniendo en cuenta que el listado de dispositivos entregado en el presente documento no alcanza los 1000 dispositivos o si hace falta relacionar más dispositivos, como por ejemplo estaciones de trabajo.

1. En el documento “Invitación a cotizar”, en el Numeral 4.1 Especificaciones Solución SOC FIDUPREVISORA solicita “9) El correlacionador debe proporcionar una arquitectura escalable donde la capacidad de procesamiento, memoria y almacenamiento se puede aumentar o disminuir de acuerdo con la carga real en producción.”

Se solicita a la entidad favor aclarar si FIDUPREVISORA puede suministrar un servidor físico o virtual, el cual pueda ir creciendo de acuerdo con los parámetros que los proponentes entreguen como prerrequisitos en la propuesta, esta opción ayudaría a la entidad en optimizar los costos del proyecto.

1. En el documento “Invitación a cotizar”, en el Numeral 4.1 Especificaciones Solución SOC FIDUPREVISORA solicita

“11) La implementación de las reglas del SIEM deberán hacerse al momento de la entrega del funcionamiento correcto y evidenciable de la herramienta y su ajuste deberá realizarse a más tardar en el primer mes de la operación de la herramienta.” Se solicita a la entidad ampliar este plazo, teniendo en cuenta que la integración de todas las fuentes puede tomar mucho más de un mes y posterior a esta integración se deben crear las REGLAS del SIEM y casos de uso, los cuales dependiendo de las necesidades de FIDUPREVISORA pueden tomar otros meses, se sugiere solicitar que cada proponente entre un cronograma especificando los tiempos que les tomaría realizar esta actividad.

1. En el documento “Invitación a cotizar”, en el Numeral 4.1 Especificaciones Solución SOC FIDUPREVISORA solicita “16) El correlacionador y el equipo de SOC deberá monitorear interfaces de red de 1GB y 10 GB y ancho de banda de 150 MB a 200MB.”

Se solicita a FIDUPRESISORA aclarar si lo que están solicitando es que el equipo suministrado por el proveedor cuente con interfaces de 1GB y 10 GB o si lo que se requiere es que la solución de SIEM, pueda monitorear flujos de tráfico, para realizar análisis de comportamiento, mediante la configuración de port mirror.

1. En el documento “Invitación a cotizar”, en el Numeral 4.1 Especificaciones Solución SOC FIDUPREVISORA solicita “20) El equipo del SOC o especialista encargado deberá realizar las labores correspondientes a la instalación, configuración, parametrización y administración del correlacionador dispuesto para la ejecución del servicio, que debe incluir la creación de los conectores necesarios para un correcto monitoreo/correlación de las plataformas que se requieran“ Se solicita a la entidad tener en cuenta que el esfuerzo y los costos del desarrollo de los conectores, solo se puede dimensionar si FIDUPREVISORA menciona en detalle cada una de las plataformas a ser incluidas, especialmente si estas corresponden a aplicaciones desarrolladas por la misma FIDUPREVISORA. Solicitamos a la entidad eliminar este requisito o cambiarlo por bancos de horas de soporte para la creación de conectores.
2. En el documento “Invitación a cotizar”, en el Numeral 4.1 Especificaciones Solución SOC FIDUPREVISORA solicita “23) Debe contar con alianzas directas y activas para combatir el cibercrimen a nivel nacional o mundial como ICSPA o equivalente. Especificar cuáles y contactos para revalidar alianzas.” “24) Debe tener una vinculación directa y activa con grupos de respuesta a incidentes de seguridad informática como FIRST, por ejemplo. Especificar con cuáles. “Se solicita a la entidad integrar este requerimiento en un solo ítem, en donde se pida que los proveedores cuenten con una de las dos membresías, mas no las dos, teniendo en cuenta que las dos membresías cumplen el mismo fin y la mayoría de proponentes solo cuentan con membresía en una de las dos, lo cual limitaría la participación de proponentes.
3. En el documento “Invitación a cotizar”, en el Numeral 4.1 Especificaciones Solución SOC FIDUPREVISORA solicita “5) Monitoreo permanente de los motores de bases de datos (SQL, Oracle), garantizando y asegurando disponibilidad, integridad, consistencia, seguridad, control de las bases de datos dando continuidad a la operación en los ambientes productivos. “ Se solicita a la entidad eliminar este requerimiento, teniendo en cuenta que esta funcionalidad no hace parte de las características entregadas por las soluciones SIEM, las cuales detectan comportamientos anómalos, más no están dedicadas a garantizar disponibilidad, integridad, consistencia de las bases de datos.
4. . En el documento “Invitación a cotizar”, en el Numeral 4.2 Análisis de Vulnerabilidades FIDUPREVISORA solicita: “1) Proveer un sistema de análisis de vulnerabilidades de propósito específico – Appliance- instalado y configurado en las instalaciones de Fiduprevisora, soportado por el proveedor y licenciado por un año a nombre del cliente. “ Se solicita a la entidad ampliar este requerimiento y permitir la instalación de la solución como una máquina virtual, la cual cumple con los mismos requerimientos que el appliance.
5. En el documento “Invitación a cotizar”, en el Numeral 4.2 Análisis de Vulnerabilidades No se detalla la cantidad de direcciones IP a las cuales se les deba realizar este servicio, se solicita a FIDUPREVISORA entregar el número de direcciones IP a las que se les debe realizar el escaneo, teniendo en cuenta que los fabricantes dimensionan los precios con base en este parámetro.
6. En el documento “Invitación a cotizar”, en el Numeral 4. Ethical Hacking Se mencionan los tipos de pruebas a ser realizadas, pero no se detallan a cuantos dispositivos ni qué tipo de dispositivo se les debe realizar este servicio, se solicita a la entidad entregar un detalle del número de dispositivos a los que se les debe realizar estas pruebas relacionando su función (Base de datos, servidor WEB, sistema operativo, etc.).

**RESPUESTA DE FIDUPREVISORA:**

1. La cantidad de firewalls y de ser posible el modelo: Firewall Fortigate 200D (1)

Trend Micro mencionar, para cuantos usuarios esta licenciada: 1250.

Office 365 cantidad de usuarios: Alrededor de 1200

1. Solo aplica a los equipos suministrados como parte del servicio
2. No es necesario, favor cotizar de 700 a 1000 y de 400 a 700.
3. Se proyecta un crecimiento del 5 al 10%, pero de igual manera favor hacer las cotizaciones solicitadas en el ítem 3.
4. Es viable.
5. Ítem incluido en la invitación a cotizar
6. Se requiere que la solución pueda monitorear flujos de tráfico, para realizar análisis de comportamiento, mediante la configuración de port mirror.
7. Las aplicaciones están construidas sobre plataformas estándar que permiten fácil integración con el correlacionador.
8. Este ítem se agregó para que los oferentes nos coticen el servicio entregado con un DAM y se analizará validando costos sobre la viabilidad de contar con este servicio activo.
9. No, definitivamente debe ser un appliance.
10. Son alrededor de 224 direcciones IP aproximadamente, con un margen de crecimiento del 5%.
11. Para Ethical Hacking son alrededor de 10 aplicaciones, 10 aplicaciones WEB y la página WEB, en conjunto con su infraestructura tecnológica, con un margen de crecimiento del 5%. El alcance puede variar dependiendo de necesidades de la entidad (menor cantidad).

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 12 | 15-01-2021 | SECOP | **INSITEL** |

1. Alertamiento temprano de nuevas amenazas o vulnerabilidades (monitoreo de riesgos emergentes). Este enfoque es mejor llevarlo a un tema de Inteligencia de amenazas cibernéticas
2. Envío de información de las alertas gestionadas, tiempos de respuesta y demás estadísticas del servicio (integración con Elastic para que puedan ser consultadas en vivo en la plataforma, enviados desde el software de gestión de incidentes de ITSS). Definir el software aquí nombrado y referenciar si este ya este operativo en las instalaciones de la FIdu.
3. El servicio es 7x24, debe usar el SIEM de Colpensiones. ¿Colpensiones requiere el equipo de analistas en sitio, o de forma remota?
4. Alertamiento temprano de nuevas amenazas o nuevas vulnerabilidades (monitoreo de riesgos emergentes). Pregunta>> Se seguirá llevando este esquema desde la trinchera de respuestas de incidentes (CSIRT) o podemos migrarlo a un esquema del proceso del centro de operaciones de seguridad (SOC), desde el enfoque de inteligencia de amenazas cibernéticas, basado en el equipo de trabajo de THREAT HUNTING
5. En el punto 7 es importante aclarar la cantidad de eventos por segundo colectados en tasa sostenida el retener, no esta claro el tiempo de retención.
6. En el punto 9, habla del correlacionador o del SIEM completo?
7. Punto 12 debido a que es un correciolanador, no guarda datos, por favor aclarar este punto.
8. Punto 15, Se le solicita muy amablemente a la entidad modificar dicho punto ya que es posible usar el algoritmo un script para hacer de hashing
9. Punto16, es posible aclarar dicho punto, debido a que por los tamaños expresados, no tiene equidad en el servicio, solicitan una solución grande para un ancho de banda pequeño?
10. ¿cuantas interfaces de red son? ¿que quieren monitorear? es Full packet capture o si se maneja por NetFlow, la diferencia de costos es grande
11. En el punto 18, ¿Es posible aclarar dicho solicitud? ¿Esta relacionado con el punto de "hasta 10 aplicaciones”? ¿Es proxy web, DNS o los registros del firewall?, o son otras aplicaciones
12. En el punto 23, es importante validar el tipo de alianza, ICSPA o FIRST, OTX de alíen vault, si se maneja una alianza técnica, se realiza una integración de manera optima porque se integra la fuente, por lo que se sugiere este tipo de alianza e integración.

**RESPUESTA DE FIDUPREVISORA:**

1. Se toma la recomendación suministrada.
2. No entendemos la observación
3. Colpensiones? De forma remota
4. Favor cotizar las dos opciones
5. Tiempo de retención durante la vigencia del contrato y al finalizar nos deben entregar los logs.
6. SIEM completo
7. Es un SIEM
8. Se toma la recomendación.
9. EL ancho de banda para el adecuado funcionamiento del servicio lo debe proveer el oferente.
10. Son hasta 10 interfaces, 2 de las cuáles deberían ser a 10 GB. El ancho de banda es un promedio del tráfico por cada interfaz. No es por Full packet capture.
11. Esos elementos deben incluirse adicional a la infraestructura detallada en la invitación a cotizar
12. Se tendrá en cuanta la recomendación.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 11 | 15-01-2021 | SECOP | **WEXLER** |

1. Se solicita muy amablemente a la entidad especificar la integración que se requiere en cada uno de los casos para verificar los requerimientos necesarios para hacer cada una de las integraciones.

▪ AIX 5.3 (1)

▪ AIX 6.1 (1)

▪ Fresad Pre-11 versions (64-bit) (2)

▪ Linux Centos 4/5 (2)

▪ Linux Centos 6 (5)

▪ Linux Centos 7 (1)

▪ Linux Redhat 6/7 (32)

▪ Linux Solaris 10/11 (34)

▪ Vmware ESXI 5.5 (1)

▪ Windows 2003 Server (20)

▪ Windows 2008 Server (3)

▪ Windows 2008 Server R2 (28)

▪ Windows 2012 Server (22)

▪ Windows 2012 Server R2 (2)

▪ Windows Server Estándar 2016 (4)

▪ Windows 2019 Server (3)

▪ Firewall fortinent

▪ Suite Trend Micro (antinirus, antimalware, DLP, device control)

▪ Office 365

▪ Switches Aruba (60)

▪ NAC

▪ Directorio Activo

1. Se solicita muy amablemente a la entidad especificar la cantidad de dispositivos por que la lista de equipos enviados es alrededor de 300, pero se solicita un equipo de mínimo 700 dispositivos, por eso es necesario que se especifique la cantidad requerida. “El servicio de monitoreo y correlación de eventos debe monitorear todos los eventos recolectados a través del SIEM y brindar respuesta a incidentes de seguridad de la información 7\*24 durante la vigencia del contrato, con una capacidad máxima de mil (1.000) dispositivos (servidores, dispositivos de red, dispositivos de seguridad y/0 equipos de escritorio, etc.)”
2. Se solicita muy amablemente a la entidad y especificar cuáles son los grupos de respuesta o si hay una cantidad o requisito mínimo. “Debe tener una vinculación directa y activa con grupos de respuesta a incidentes de seguridad informática como FIRST por ejemplo. Especificar con cuáles.”
3. Se solicita muy amablemente a la entidad aclarar si la ubicación de las herramientas del SOC debe tener características tipo TIER 3 o se debe tener una certificación vigente. “Los centros de cómputo que alojan la infraestructura de TIC del servicio de SOC se encuentren acreditados en su mayoría como TIER 3 o su respectivo equivalente. (Deseable). Especificar”
4. Se solicita muy amablemente a la entidad aclarar, ya que la infraestructura de TIC debe estar en una instalación con características tipo TIER 3, es posible colocar un equipo tipo colector en las instalaciones donde están los dispositivos para tener una mejor sincronía con los dispositivos.
5. Se solicita muy amablemente a la entidad aclarar si todas las herramientas del SOC se pueden colocar en las instalaciones de la entidad y desde las instalaciones donde estará el personal del SOC se realizará el acceso a las herramientas por un canal seguro tipo VPN Ipsec. Si es afirmativo, por favor indicar si las herramientas se pueden virtualizar en la infraestructura de la entidad o si por el contrario pueden dar un espacio de 2 unidades de rack para su instalación.
6. Se solicita muy amablemente a la entidad aclarar a cuantas maquinas se le van hacer el análisis de vulnerabilidad ya que estas herramientas se dimensionan por cantidad de dispositivos, adicionalmente se solicita que la opción de appliance se pueda dejar opcional y se puedan ofrecer soluciones virtualizadas o en cloud. “Proveer un sistema de análisis de vulnerabilidades de propósito específico –appliance- instalado y configurado en las instalaciones de Fiduprevisora, soportado por el proveedor y licenciado por un año a nombre del cliente.”
7. Se solicita muy amablemente a la entidad para la parte de Ethical Hacking y Análisis de Vulnerabilidades se pida como mínimo 5 años de experiencia para el oferente para garantizar un óptimo ejercicio, adicionalmente para el oferente se soliciten certificaciones CISSP, CISM, auditor Lider ISO 27001:2013, CEH y CISA. Así se garanticen que se van a realizar las mejores prácticas.
8. Se solicita dentro de las generalidades, “el interesado debe contar con la certificación ISO 27001 vigente o certificar la implementación de buenas prácticas de reconocimiento mundial a nivel de seguridad y ciberseguridad de la información, para esto el proponente deberá presentar el certificado emitido por una entidad certificadora.”. Solicitamos amablemente a la entidad que, con el fin de permitir la pluralidad de oferentes, se modifique el requerimiento permitiendo que se sustente el cumplimiento por medio de un documento firmado por el representante legal, donde se mencione que la compañía se encuentra en proceso de certificación.
9. Teniendo en cuenta la criticidad del servicio que prestara el contratista, la alta prioridad y nivel de especialización requeridos, sugerimos amablemente a la entidad que para garantizar que el personal asignado al proyecto cuente con las capacidades técnicas y profesionales mínimas necesarias se solicite dentro de los requerimientos adjuntar documentos que soporten las Especialidades del personal que prestara los servicios, dentro del mismo, sugerimos se considere un LÍDER DE SOC, se cuente con las siguientes capacitaciones certificadas y un 20% de dedicación en la ejecución del contrato

Un profesional en Ingeniería de sistemas, o telemática, electrónica, comunicaciones o afines según SNIES.

* + Debe tener especialización seguridad de la información o administración de riesgos informáticos
1. Y las siguientes certificaciones:

o CISM – Certified Information Security Management

o ISO/IEC 27035-1/2:2016 Incident Manager

o ISO/IEC 27041 / 27043:2015 Incident Analyst

o CEH – Certified Ethical Hacker

o CPTE (CERTIFIED PENETRATION TESTING ENGINEER)

o Debe estar certificado como Auditor líder de ISO27001:2013.

o Certificado Itil Foundation v4

o Certificado Digital Forensics Examiner (CDFE)

**RESPUESTA DE FIDUPREVISORA:**

1. Captura de logs, análisis de vulnerabilidades y correlación de eventos.
2. Se requiere nos brinden en la cotización el valor de la solución para los elemento entregados con un porcentaje de crecimiento del 5% al 10% y otra por hasta mil dispositivos, esto para validar si se toma la decisión de integrar los equipos de usuario final.
3. CSIRT y COLCERT por ejemplo.
4. Deben contar con dicha certificación sobre el servicio prestado, pero esto es algo deseable, no es un requisito obligatorio.
5. Sí es posible.
6. La herramientas si se pueden ubicar en las instalaciones de la Entidad y la VPN se puede configurar sin problema.
7. Para análisis de vulnerabilidades son alrededor de 224 direcciones IP aproximadamente, con un margen de crecimiento del 5%. El alcance puede variar dependiendo de necesidades de la entidad (menor cantidad). Debe ser appliance necesariamente.
8. Se tendrá en cuenta la recomendación.
9. No, necesariamente se requiere de dicha certificación o equivalentes.
10. Esto se espera sea propuesto por el oferente y validaremos opciones de acuerdo también al costo y especialización que presentan del talento humano relacionado.
11. Lo indicado en el punto anterior.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 18 | 15-01-2021 | Correo Electrónico | **CLARO – COMCEL S.A.** |

1. En cuanto al punto que dice: "(…) deben presentar sus cotizaciones por medio de correo electrónico" Se solicita por favor aclarar si la cotización deberá ser presentada por correo electrónico o a través del proceso publicado en la plataforma SECOP II, o si es necesario realizarlo por los dos medios.
2. En cuanto al punto que dice:"(…) relacionar experiencia de ejecución de contratos cuyo objeto contemple las actividades citadas en el objeto de esta invitación" Teniendo en cuenta que el objeto de la invitación hace referencia al término "servicios de SOC (Centro de Operaciones de Seguridad)", se solicita a la entidad considerar que los contratos cuyo alcance contempla la Gestión de Incidentes de Seguridad, Correlación de Eventos, así como la Provisión en modalidad de servicio, Administración, Soporte, Gestión, Operación, entre otras actividades relacionadas, de plataformas y servicios de seguridad, de manera implícita contemplan la existencia de un SOC, se solicita considerar la validez de este tipo de experiencias mientras el proponente pueda certificar que dispone de un SOC propio.
3. En cuanto al punto que dice:"4.1 Generalidades (…) " "Se sugiere a la entidad dentro de las generalidades del requerimiento incluir que el proponente pueda certificar que dispone de un SOC propio en Colombia.

Adicionalmente, con la finalidad de validar las capacidades del SOC, se sugiere contemplar que éste deba ser miembro activo del FIRST (Forum of Incident Response and Security Teams)."

1. En cuanto al punto que dice:"10) Los recursos necesarios para la instalación y operación de la solución en relación a la memoria, procesamiento y almacenamiento, deberán ser proporcionados por el contratista." "Se solicita por favor confirmar si el correlacionador de eventos deberá estar físicamente en una ubicación dispuesta por Fiduprevisora o si este podrá estar en instalaciones del proveedor.

En el evento en que el correlacionador deba estar ubicado en un sitio determinado por Fiduprevisora, por favor confirmar si la entidad facilitará los recursos a nivel de espacio y energía o si estos deberán ser contemplados por el proponente.

Así mismo, según la ubicación del dispositivo, por favor confirmar si la conectividad, sea LAN, Cross conexiones y/o enlaces WAN o hacia Internet debe ser contemplada por el proponente o si Fiduprevisora proporcionará estos recursos."

1. En cuanto al punto que dice:"16) El correlacionador y el equipo de SOC deberá monitorear interfaces de red de 1GB y 10 GB y ancho de banda de 150 MB a 200MB." "Se solicita por favor precisar el inventario de interfaces a monitorear y discriminar si estas pertenecen a redes públicas o privadas, así como la ubicación física de las mismas.

Adicionalmente, se solicita confirmar si los enlaces, sean canales MPLS o VPNS, para el monitoreo de dichas interfaces serán provistos por Fiduprevisora o si deben ser contemplados por el proponente en su oferta."

1. En cuanto al punto que dice:"(…) nubes públicas y privadas, aplicaciones, bases de datos, plataforma de correo electrónico, seguridad informática y de la información, Redes LAN, WLAN y WAN y servicios conexos"

Teniendo en cuenta la cobertura que debe tener el servicio a nivel de nubes, redes, aplicaciones, entre otros, se solicita por favor ampliar y detallar la información del inventario establecido en la sección 4.1 Generalidades, ya que en la parte de infraestructura IT se limita a indicar número de servidores y sistema operativo, pero no se referencian los componentes de aplicación, bases de datos, etc.

1. En cuanto al punto que dice:36) El proponente deberá contar con personal especializado para el seguimiento al cumplimiento del servicio contratado, una gerencia de servicio.

Se solicita a la entidad confirmar los roles, perfiles, actividades, dedicación y ubicación de cada uno de los miembros requeridos para el equipo de trabajo de esta solución.

1. En cuanto al punto que dice:6) El servicio de monitoreo y correlación de eventos debe monitorear (…), con una capacidad máxima de mil (1.000) dispositivos (servidores, dispositivos de red, dispositivos de seguridad y/0 equipos de escritorio, etc.) Se solicita a la entidad aclarar cuál es el alcance del ítem No 6 del cuadro de Especificaciones Solución SOC, dado que además de los dispositivos de red y Datacenter, se incluyen equipos de usuario final (terminales) los cuales no hacen parte del alcance de un SOC. Favor aclarar su alcance y requerimientos a cumplir al igual que actividades a realizar por parte del oferente en este contrato.
2. Confirmar si para el punto anterior la entidad requiere que se incluyan endpoints para los equipos finales, de ser así indicar por favor: cantidades, Sistemas operativos, características de las máquinas y alcance del servicio.
3. En cuanto al punto que dice:7) Suministrar en modalidad de servicio un correlacionador para soportar 1000 dispositivos con un rango de 700 hasta 1000 eventos (…) Se solicita a la entidad aclarar del ítem No 7 del cuadro de Especificaciones Solución SOC, si la entidad lo que espera es un servicio o que el oferente disponga de un equipo dedicado para la entidad con capacidad de almacenamiento local durante el tiempo del contrato. En caso de que la expectativa sea la de un appliance dedicado, de propósito específico, se sugiere a la entidad incluir dentro de las especificaciones que la infraestructura debe ser nueva, de última tecnología.
4. En cuanto al punto que dice:9) El correlacionador debe proporcionar una arquitectura escalable donde la capacidad de procesamiento, memoria y almacenamiento se puede aumentar o disminuir de acuerdo con la carga real en producción. Se solicita a la entidad confirmar el porcentaje de crecimiento esperado durante el tiempo de contratación de la solución.
5. En cuanto al punto que dice:7) Suministrar en modalidad de servicio un correlacionador para soportar 1000 dispositivos con un rango de 700 hasta 1000 eventos (…) Se solicita a la entidad confirmar si la administración de la solución estará a cargo de la Fiduciaria o del oferente.
6. En cuanto al punto que dice:12) El correlacionador debe almacenar datos relacionados con los incidentes y eventos, incluidos el comportamiento de los usuarios y activo asociados durante el período de vigencia del contrato, en forma de búsqueda para un estándar de 90 días y custodia durante 12 meses. Se solicita a la entidad confirmar si nuestro entendimiento es correcto con respecto a lo indicado en el ítem No 12 del cuadro de Especificaciones Solución SOC,? se deberá habilitar un usuario de consulta sobre el repositorio de logs de la solución ofertada? (Esta pregunta aplica, en el caso de que la administración sea del proveedor)
7. En cuanto al punto que dice:13) La plataforma deberá tener una consola tipo dashboard en la cual se pueda personalizar varios tipos de gráficas, tablas y reportes, para permitir tener una visión global de los eventos, incidentes de seguridad y reglas implementadas en la herramienta. Se solicita a la entidad confirmar si nuestro entendimiento es correcto con respecto a lo indicado en el ítem No 13 del cuadro de Especificaciones Solución SOC,  además de monitorear en el SOC del proveedor lo dispositivos de la Fiduciaria y gestionar el servicio ofertada en este proceso, la entidad requiere contar con una vista de consulta o dashboard tipo web para el equipo de TI?, en caso positivo favor indicar si es válido entregar un usuario de consulta para el equipo. (Esta pregunta aplica, en el caso de que la administración sea del proveedor)
8. En cuanto al punto que dice:14) El correlacionador deberá proporcionar información en tiempo real de los eventos generados por los dispositivos de seguridad administrada, así como las alarmas que permitan identificar los eventos relevantes y que puedan afectar la integridad, confidencialidad o disponibilidad de los servicios protegidos de FIDUPREVISORA S.A. Se solicita a la entidad aclarar cuál es el alcance del ítem No 14 del cuadro de Especificaciones Solución SOC, dado que usualmente las soluciones de SOC manejan unos parámetros y umbrales de configuración que permiten optimizar la operación de los dispositivos sin incurrir en sobrecostos por dimensionamientos innecesarios, dando cumplimiento a su función de manera adecuada y eficiente, esto considerando además la cantidad de componentes que la Fiduciaria requiere monitorear. Se sugiere a la entidad requerir tiempos de actualización en unidades de minutos, no en tiempo real.
9. En cuanto al punto que dice:7) Suministrar en modalidad de servicio un correlacionador para soportar 1000 dispositivos con un rango de 700 hasta 1000 eventos (…) Se solicita a la entidad confirmar, solo en caso de que la solución sea dedicada, en qué Centros de Datos requiere su aprovisionamiento y si se requiere en stand alone.
10. En cuanto al punto que dice:55) Monitoreo permanente de los motores de bases de datos (SQL, Oracle), garantizando y asegurando disponibilidad, integridad, consistencia, seguridad, control de las bases de datos dando continuidad a la operación en los ambientes productivos. Se solicita a la entidad aclarar cuál es el alcance del ítem No 55 del cuadro de Especificaciones Solución SOC, favor indicar cantidad de Bases de datos a monitorear, cantidad de instancias, Fabricante y versión de los motores manejados.
11. Se solicita a la entidad especificar el alcance, cantidad de activos y entregable de los ítems No 1, 2 y 3 del cuadro de especificaciones 4.3 Ethical Hacking.

**RESPUESTA DE FIDUPREVISORA:**

1. Por correo electrónico, como se indica en la invitación.
2. De acuerdo.
3. Se tendrá en cuenta la recomendación.
4. Podrá estar donde el proveedor pero el canal de transimisión de logs y demás debe ser colocado por el proveedor. La conectividad, sea LAN, Crossconexiones y/o enlaces WAN o hacia Internet debe ser contemplada por el proponente.
5. Son hasta 10 interfaces, 2 de las cuáles deberían ser a 10 GB. El ancho de banda es un promedio del tráfico por cada interfaz.
6. Es a es la información que podemos entregar por ahora, el detalle se le proporcionará al oferente seleccionado.
7. Eseramos que este equipo no lo proponga el oferente, de acuerdo al servicio dimensionado, no queremos volver esto una camisa de fuerza y eso también nos permite analizar los costos por talento humano de los diferentes proveedores.
8. Son alrededor de 400 dispositivos, por lo que se solicita una cotización de 400 a 700 y 700 a 1000, basados en esto se determinará la posibilidad de integrar equipos de usuario final.
9. Por ahora, favor no incluir.
10. Esperamos un servicio, pero que si tengan capacidad de almacenamiento de logs durante la vigencia del contrato y estos sean entregados al culminar el mismo.
11. Del 5% al 10%
12. Del oferente.
13. Sí para las dos preguntas, esto en caso de tener requerimientos por investigaciones.
14. Sí y se requieren dos usuarios uno para TI y otro para seguridad de la información.
15. Se tendrá en cuenta la sugerencia.
16. En caso que sea dedicada debe ser en el centro de datos claro (Triara).
17. Favor cotizar con y sin DAM. Bases de Datos alrededor de 10, Motores de bases de datos alrededor de 10, 24 instancias, Oracle.
18. Para Ethical Hacking son alrededor de 10 aplicaciones, 10 aplicaciones WEB y la página WEB, en conjunto con su infraestructura tecnológica, con un margen de crecimiento del 5%. El alcance puede variar dependiendo de necesidades de la entidad (menor cantidad).

Se trata de dos pruebas de ethical hacking al año de caja negra para determinar el estado de la seguridad de la entidad a nivel de posibles atacantes externos, dentro de una de estas pruebas se puede incluir la de caja blanca para poder identificar también vulnerabilidades internas y si fue posible realizar algún ataque, para evaluar a la Entidad a nivel de controles ante atacantes internos (en ambos casos no se levantará ningún control de los existentes ya en la entidad), por otra parte se requiere al menos una prueba de ingeniería social para medir el nivel de cultura en seguridad de la información de los funcionarios, se pueden hacer al mismo tiempo con estas dos pruebas o programarlo en otro período.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 5 | 15-01-2021 | SECOP | **COMPAÑÍA INTERNACIONAL DE INTEGRACIÓN** |

Cordial saludo, para e punto 4. SW – SIEM solicitamos por favor su apoyo con la información solicitada en el archivo adjunto “Plantilla Dimensionamiento” y también con las siguientes inquietudes:

 

1. Específicamente qué se requiere monitorear
2. En cuántas Vlans están estos dispositivos
3. Qué tipos de escaneos requieren, si con autenticación o sin autenticación. Cuando nos referimos a tipos de escáner nos referimos por ejemplo: Hay un escáner que es por fuera de donde el agente recolecta solo y el otro si tienen dispositivos a los que hay que conectarles el escáner directo.
4. Requieren algún tipo de reporte definido, ¿dashboards?
5. Qué requieren o esperan tener con Tenable en cuánto a las frecuencias de reportes: semanal, quincenal, mensual.

**RESPUESTA DE FIDUPREVISORA:**

1. La infraestructura de TI de la Entidad.
2. En 10 Vlans.
3. No se entiende la observación.
4. Sí Dashboards, además de los reportes que por defecto traen este tipo de soluciones, que se posible también la parametrización de unos nuevos, en caso de requerirse.
5. Mensual a nivel de reportes para SOC, para vulnerabilidades lo descrito en la invitación.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 7 | 15-01-2021 | Correo Electrónico | **04IT** |

De acuerdo a la invitación a cotizar, solicitamos con el mayor respeto a la Entidad responder las siguientes observaciones:

1. 4.1. SOC: ¿Monitorear interfaces de red? ¿qué quieren decir? ¿eventos de red o la integración al SOC con estas interfaces?
2. ¿La solución de SOC cuenta con herramienta de gestión de tickets, es de obligatorio cumplimiento que se integre con Aranda?
3. ¿Qué es estático y dinámico? ¿cómo los definen?
4. En cuanto al punto 52. Lo hacemos con Resilient, necesitamos el detalle de los endpionts para validar
5. ¿Cuál sería el alcance (bases de datos, infraestructura sobre la que están, otros)? Sería con Guardium
6. En cuanto al punto que establece: El correlacionador y el equipo de SOC deberá monitorear interfaces de red de 1GB y 10 GB y ancho de banda de 150 MB a 200MB. Se solicita a la entidad informar si las interfaces a las que hacen referencia son externas o internas, se tendrá acceso al monitoreo de las interfaces.
7. En cuanto al punto que dice: EL proveedor deberá brindar capacitación en las funcionalidades de la solución, en relación al entendimiento del dashboard, la generación de informes, y la visualización y entendimiento de las reglas del correlacionador de eventos. Este entrenamiento debe ser certificable por parte del proveedor. Se solicita a la entidad aclarar si se deberá entregar usuario de lectura a Fiduprevisora.

**RESPUESTA DE FIDUPREVISORA:**

1. Es para análisis de comportamiento e identificación de anomalías y a su vez correlacionarlas.
2. Sí, para quitar el reproceso de radicar ticket cuando nos hagan un reporte.
3. Hace referencia a la capacidad de la solución de permitir correlacionar fuentes de datos estáticos o dinámicos y de generar nuevas reglas de correlación, para lograr su afinamiento.
4. De acuerdo al inventario suministrado.
5. Las dos, Guardium está bien.
6. Si se tiene acceso y son interna y externas.
7. Sí se requiere mínimo dos usuarios de lectura.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 1 | 15-01-2021 | Correo Electrónico | **Cipher** |

De acuerdo con el cronograma de actividades y encontrándonos interesados en el proceso de la referencia,

nos permitimos enviar nuestras inquietudes para que sean evaluadas. De antemano muchas gracias por su

gentileza.

1. Proveer un sistema de análisis de vulnerabilidades de propósito específico –appliance- instalado y configurado en las instalaciones de Fiduprevisora, soportado por el proveedor y licenciado por un año a nombre del cliente.

No tenemos la visibilidad de cuales son su total de activos (IP), su segmentación de red (cuántas redes segmentadas tienen). Solicitamos aclaración.

**RESPUESTA DE FIDUPREVISORA:**

1. Son alrededor de 224 direcciones IP aproximadamente, con un margen de crecimiento del 5%. Y 10 Vlans.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 8 | 15-01-2021 | Correo Electrónico | **Deloitte** |

1. Por favor confirmar si como respuesta a esta invitación a cotizar únicamente se espera que el proponente diligencie los cuadros de especificaciones, indicando el cumplimiento del requisito y el cuadro de valor de cotización, o si también se espera contenido de nuestro servicio, metodología y demás aspectos de nuestra propuesta.

**Especificaciones Solución SOC**

1. En la pregunta 40 del apartado 4.1 Especificaciones Solución SOC, se debe especificar “la marca de la solución de correlacionador de eventos con la que trabaja el SOC”. ¿Fiduprevisora tiene alguna preferencia en cuanto a la elección de la herramienta SIEM (teniendo en cuenta que Deloitte apostará por la solución líder del mercado que mejor se adapte a Fiduprevisora, dada nuestra visión agnóstica en cuanto a tecnología)?
2. En la pregunta 42 del apartado 4.1 Especificaciones Solución SOC, se especifica que “El servicio debe contar con un mecanismo que permita obtener inteligencia de amenazas tanto en el contexto externo como interno de la organización”. ¿Se está solicitando un monitoreo y reporte en 24/7 de inteligencia general y específica para Fiduprevisora? ¿Cuántos dominios y/o marcas estarán sujetas al servicio? ¿Se requiere cierre de sitios?

**Análisis de Vulnerabilidades**

1. ¿Por favor confirmar si se debe cotizar el valor del appliance o este va ser provisto por Fiduprevisoa?
2. Por favor confirmar que se espera realizar únicamente dos análisis de vulnerabilidades en el año (uno por semestre) de los cuales se generará un informe técnico y posteriormente, mes a mes se generará un informe de seguimiento de remediación de las vulnerabilidades identificadas en cada semestre. En caso no ser adecuado nuestro entendimiento, por favor aclarar.

**Ethical Hacking**

1. Por favor confirmar el número y tipo de objetivos sobre los que se realizará las pruebas de ethical hacking externas
2. Por favor confirmar el número y tipo de objetivos sobre los que se realizará las pruebas de ethical hacking internas tipo caja blanca.
3. Por favor confirmar para la prueba de ingeniería social si se espera dos cotizaciones, una para una prueba para 20 funciones y otra para una prueba de pshising para la totalidad de usuarios. Indicar el número total de usuarios de correo electrónico

**RESPUESTA DE FIDUPREVISORA:**

1. También se espera contenido de nuestro servicio, metodología y demás aspectos de nuestra propuesta.
2. No tenemos preferencia.
3. Sí, por favor cotizar la posibilidad de integrar el servicio que permita el cierre de sitios y presentarlo independiente para analizar los costos. Solo contamos con un dominio local, favor realizar la cotización con el inventario de activos suministrado en la invitación.
4. Cotizar valor appliance, lo deseable es que el proveedor ya cuente con él y nos incluyan el licenciamiento por la duración del contrato.
5. Si es adecuado el entendimiento
6. Alrededor de 10m portales WEB y página WEB más su infraestrutura.
7. Alrededor de 10 aplicaciones, más us infarestructura tecnológica.
8. Por favor cotizar las dos opciones de manera independiente para la toma de decisiones.

|  |  |  |  |
| --- | --- | --- | --- |
| **N° DE OBSERVACIONES** | **FECHA DE RECIBO** | **MEDIO DE RECIBO** | **OBSERVANTE** |
| 7 | 15-01-2021 | Correo Electrónico | **Adsum** |

1. Acorde al numeral 4.1 Generalidades, se requiere contar con la certificación ISO 27001vigente. Con el fin de brindar mayor oportunidad de participación a los ofertantes, sugerimos que tal requerimiento pueda ser omitido o modificado, indicando que el SOC ofrecido esté alineado con la normativa ISO 27001 aún cuando no se encuentre aun certificado

Con respecto al item 4.1 relacionamos las siguientes observaciones:

1. En cuanto al punto 7) Suministrar en modalidad de servicio un correlacionador para soportar 1000 dispositivos con un rango de 700 hasta 1000 eventospor segundo que permita colectar, retener y correlacionar los eventos de seguridad de la Infraestructura T. Se solicita amablemente a la entidad acotar la cantidad de dispositivos a monitorear teniendo en cuenta que en el listado de equipos se relacionan aproximadamente alrededor de 260 Equipos y dentro de las condiciones se solicita un máximo de 1000. Lo anterior teniendo en cuenta que este es un insumo primordial para realizar el correcto dimensionamiento de la solución
2. 11) La implementación de las reglas del SIEM deberán hacerse al momento de la entrega del funcionamiento correcto y evidenciable de la herramienta y su ajuste deberá realizarse a más tardar en el primer mes de la operación de la herramienta. Se recomienda a la entidad ampliar el plazo de entrada a producción de la herramienta SIEM ya que este tipo de herramientas tienen varias etapas en su correcta puesta en marcha, y funcionamiento a su máxima capacidad, por lo cual se solicita ampliar el plazo de implementación a 2 meses, lo que garantiza a la entidad tener una plataforma estable y perfectamente funcional.
3. El correlacionador debe proteger la integridad y confidencialidad de la información almacenada con algoritmos de hashing fuertes mínimo SHA256. Se solicita a la entidad aclarar el alcance de este punto, ¿en relación con si se requiere un doble factor de autenticación?, o si esta protección debe estar relacionada en los log que están embebidos en la plataforma.
4. Cambios directos sobre las bases de datos. Se recomienda a la entidad tener en cuenta que las protecciones de modificación sobre las bases de datos las realiza una herramienta especializada de propósito especifico como lo es un DAM, o firewall de bases de datos, la capacidad del SIEM puede estar limitada a correlacionar las alertas emitidas por la propia base de datos o una herramienta de protección de estas bases de datos.
5. Suplantación de identidad (correos electrónicos sospechosos, phishing) Se solicita a la entidad tener en cuenta que este tipo protección las realiza un Gateway de correo electrónico, como lo es la solución de TrendMicro, el siem tiene la capacidad de correlacionar las alertas que pueda recibir de esta herramienta. Y no esta basada en la protección del SIEM.
6. Respecto al numeral 4.2 Análisis de vulnerabilidades, solicitamos aclarar:

 Solicitamos indicar la cantidad de equipos que van a estar sometidos al análisis de vulnerabilidades durante el desarrollo del contrato.

**RESPUESTA DE FIDUPREVISORA:**

1. Debe contar con la certificación.
2. Por favor dimensionar de 400 a 700 y otra para de 700 a 1000, para tomar la decisión de si se monitorean eventos en equipos finales de usuario o no.
3. Se tendrá en cuenta la recomendación.
4. Esta protección debe estar relacionada en los log que están embebidos en la plataforma.
5. Favor realizar la cotización con y sin DAM o firewall de bases de datos, para la toma de decisiones.
6. Se requiere que el servicio tenga la capacidad de correlacionar las alertas que pueda recibir de esta herramienta.
7. Son alrededor de 224 direcciones IP aproximadamente, con un margen de crecimiento del 5%.

**Fiduprevisora S.A**

 **“Defensoría del Consumidor Financiero**: Dr. JOSÉ FEDERICO USTÁRIZ GÓNZALEZ. Carrera 11 A No 96-51 - Oficina 203, Edificio Oficity en la ciudad de Bogotá D.C. PBX 6108161 / 6108164, Fax: Ext. 500. E-mail: defensoriafiduprevisora@ustarizabogados.com de 8:00 am - 6:00 pm, lunes a viernes en jornada continua”. Las funciones del Defensor del Consumidor son: Dar trámite a las quejas contra las entidades vigiladas en forma objetiva y gratuita. Ser vocero de los consumidores financieros ante la institución. Usted puede formular sus quejas contra la entidad con destino al Defensor del Consumidor en cualquiera agencia, sucursal, oficina de corresponsalía u oficina de atención al público de la entidad, asimismo tiene la posibilidad de dirigirse al Defensor con el ánimo de que éste formule recomendaciones y propuestas en aquellos aspectos que puedan favorecer las buenas relaciones entre la Fiduciaria y sus Consumidores. Para la presentación de quejas ante el Defensor del Consumidor no se exige ninguna formalidad, se sugiere que la misma contenga como mínimo los siguientes datos del reclamante: 1. Nombres y apellidos completos 2. Identificación 3. Domicilio (dirección y ciudad) 4. Descripción de los hechos y/o derechos que considere que le han sido vulnerados. De igual forma puede hacer uso del App "Defensoría del Consumidor Financiero" disponible para su descarga desde cualquier smartphone, por Play Store o por App Store.

Play Store o por App Store.