INVITACIÓN ABIERTA 005-2021

27 de abril de 2021

RESPUESTA A OBSERVACIONES PRESENTADAS AL PLIEGO DE CONDICIONES:

"Prestar servicios profesionales especializados en seguridad informática y SOC Nivel 2, para la protección de la infraestructura y los activos tecnológicos que soportan los procesos de LA PREVISORA S.A. e implementar las mejoras requeridas para el fortalecimiento de la seguridad informática."

Agradecemos a todos los oferentes por su interés en el proceso y sus observaciones, a continuación, daremos respuesta o aclaraciones a las mismos.

I. OBSERVACIONES GENERALES

En esta sección se brinda respuesta sobre algunas inquietudes u observaciones que se presentan de manera reiterada entre los proponentes

1. Cronograma de la Invitación Abierta

La Previsora ajustó el numeral 1.21 CRONOGRAMA DE LA INVITACIÓN ABIERTA mediante Adenda N°2 publicada el 25 de mayo de 2021 en la página web de La Previsora.

2. Tiempo de experiencia del Proponente

La Previsora se mantiene en que los contratos certificados deben haber iniciado durante los últimos cinco (5) años contados a partir del inicio de la presente invitación, como está establecido en el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE del pliego de condiciones.

3. Número de certificaciones de experiencia general

La Previsora realiza ajuste sobre el pliego de condiciones mediante Adenda N°3 para ampliar a hasta cuatro (4) el número de certificaciones de experiencia general. Esta modificación se puede apreciar en el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE del pliego de condiciones.

4. Certificaciones del Recurso Humano calificable

La Previsora realiza ajuste sobre el pliego de condiciones mediante Adenda N°3 en el ANEXO No. 2 RECURSO HUMANO CALIFICABLE para adicionar algunas de las certificaciones observadas por los proponentes según la necesidad del recurso humano calificable.

5. Capacidad Financiera

La Previsora mantiene los indicadores financieros establecidos en el numeral 3.2. CAPACIDAD FINANCIERA del pliego de condiciones.

II. OBSERVACIONES PRESENTADAS POR LA EMPRESA NEOSECURE

Observación No. 1 Agradecemos ampliar el plazo para el envío de observaciones y entrega de propuesta.

Respuesta: De manera atenta se informa que su observación fue tenía en cuenta y se ajustó el numeral 1.21 CRONOGRAMA DE LA INVITACIÓN ABIERTA mediante Adenda N° 1 publicada el 18 de mayo de 2021 y Adenda N°2 publica el 25 de mayo de 2021 en la página web de La Previsora.

Observación No. 2. 3.2 CAPACIDAD FINANCIERA

Nivel de Endeudamiento (Pasivo Total/Activo Total): Menor o igual al 70%.

Solicitamos que el Nivel de Endeudamiento sea menor o igual al (<= 0,73).

Al modificar este indicador la entidad no pondrá en riesgo el proceso de contratación ya que el mismo estaría respaldado por:

* Garantía de Seriedad de la propuesta

* Garantías del contrato

* La entidad no hará anticipo, para este proceso la entidad efectuará el pago bajo la modalidad de mensualidades vencidas, mediante treinta y seis (36) pagos iguales cada uno con un valor fijo mensual, valor que se determinará de acuerdo con el valor de la propuesta seleccionada. Estos pagos deben venir acompañados de los entregables que se definan en las obligaciones y el acta de recibo a satisfacción por parte del supervisor del contrato.

Respuesta: Al respecto, nos permitimos informar que la Capacidad Financiera definida por Previsora se basó en el estudio de mercado que se realizó en el cual se contemplaron aspectos como: objeto del contrato, tiempo del contrato, valor del contrato, complejidad y forma de pago del mismo, buscando así que el proveedor tenga la liquidez y solidez necesarias para llevar a cabo el desarrollo del contrato, por lo cual los niveles solicitados para los indicadores establecidos permiten evaluar dicha condición. Adicionalmente, se tuvo en cuenta la información financiera registrada en Superintendencia de Sociedades de empresas dedicadas a actividades relacionadas con el objeto del contrato.

Así mismo, para la definición de estos indicadores se tuvo en cuenta lo señalado en la forma de pago del contrato y plazo de ejecución del contrato del pliego, ya que los proponentes deberán contar con una capacidad financiera mínima para cumplir con el desarrollo de las actividades que deberán ser asumidas por ellos por el tiempo de ejecución del contrato.

Por lo tanto y con el fin de garantizar los fines de la contratación, se establecieron los indicadores financieros solicitados en la invitación, buscando así una idoneidad financiera de los proponentes, a través de la evaluación de varias dimensiones como lo son capital de trabajo, nivel de endeudamiento y patrimonio, los cuales evalúan aspectos diferentes que en conjunto garanticen liquidez para la ejecución satisfactoria del objeto del contrato.

Teniendo en cuenta lo anterior y considerando que los indicadores solicitados se ajustan a las necesidades de Previsora, se mantiene la capacidad financiera definida inicialmente.

Observación 3: SERVICIOS DE SOC. ¿Qué SIEM utiliza actualmente para el servicio de SOC de la entidad?

Respuesta: Nos permitimos indicar que el servicio de SIEM es tercerizado y el proveedor actual nos proporciona un FortiSIEM y un Alien Vault Ossim.

Observación 4: SERVICIOS DE SOC ¿Cuál es la plataforma de gestión de incidentes que utiliza la Entidad?

Respuesta: La plataforma de gestión de incidentes que actualmente tenemos es Aranda.

Observación 5: SERVICIOS DE SOC ¿Para el servicio de manejo de incidentes que alcance espera la Entidad tener con el servicio de SOC?

Respuesta: El servicio para el manejo de incidentes que se espera alcanzar es de un nivel 2 de seguridad “análisis exhaustivo y de respuesta”, así mismo les indicamos que la información se encuentra detallada en el numeral 3.3.7.1 SERVICIOS DE SOC del pliego de condiciones.

Observación 6: SERVICIOS DE SOC. Para la recolección de los eventos de las diferentes fuentes el servicio requiere la integración de un componente en las instalaciones de la Entidad ¿La Entidad puede proveer los recursos de infraestructura necesarios para instalar el software del colector o se debe contemplar un servidor como parte del servicio?

Respuesta: Nos permitimos aclarar que para un mayor entendimiento se ajusta numeral 3.3.7.5. HERRAMIENTAS DE GESTIÓN DE LA SOLUCIÓN donde se detalla la información de los parámetros de las plataformas y software a instalar, la cual se verá reflejada sobre Adenda N°3.

Observación 7: SERVICIOS DE SOC. ¿Los respaldos a los que se hacen referencia en este punto se enfocan en las tecnologías que soportan el servicio o alguna solución tecnológica en especial?

Respuesta: Los respaldos corresponden a las tecnologías que soportan el servicio y que deben tener como mínimo una retención de 12 meses, el cual puede contemplar esquemas de backup incrementales full, mensuales periódicos y anuales, los backup pueden ser entregados a la Previsora para custodia, y una vez el log cumpla los 12 meses y este respaldado puede gestionar la sobre escritura del mismos.

Observación 8: SERVICIOS DE SOC. Para este requerimiento "Contener o neutralizar los ataques detectados en caso de presencia de amenazas, para estos eventos se deberá contar con una matriz de incidencias y deberá estar avalada por LA PREVISORA S.A." ¿El contener o neutralizar los ataques detectados requiere que se tenga gestión de las diferentes soluciones tecnológicas (Controles), es así como se tiene contemplado el servicio?
¿En caso de ser así, ¿cuáles serían las soluciones tecnológicas que serían foco de esta gestión?

Respuesta: Nos permitimos aclarar que su entendimiento es adecuado, como se describe en el pliego de condiciones, el servicio contempla gestión de herramientas de seguridad informática con los recursos técnicos solicitados, quienes serán los encargados de administrar, operar, gestionar, mejorar las plataformas como: Firewall, antivirus, aplicaciones seguridad Office365, entre otras.

Observación 9: SERVICIOS DE SEGURIDAD ADMINISTRADA. ¿El analista de seguridad TI se debe contemplar en tiempo dedicado o parcial para el servicio? ¿Este recurso debe ser contemplado remoto o en sitio?

Respuesta: Nos permitimos aclarar que la información requerida esta descrita en el numeral 3.3.7.2. SERVICIOS DE SEGURIDAD ADMINISTRADA del pliego de condiciones, donde se indica que los dos (2) analistas de seguridad deben estar 100% dedicados a LA PREVISORA.

Adicionalmente, como se indica en el pliego de condiciones 3.3.6. RECURSO HUMANO MINIMO HABILITANTE, se estipula un recurso en sitio y el otro del remoto, los elementos tecnológicos deben ser suministrados por el proveedor.

Observación 10: SERVICIOS DE SEGURIDAD ADMINISTRADA. ¿Las líneas base se deben contemplar en todas las soluciones tecnológicas o se cuenta con un listado en específico? ¿Es posible contemplar una solución tecnológica para realizar esta evaluación? ¿Los ajustes de las líneas base se deben realizar por parte del Analista o los realizan los administradores de las diferentes tecnologías?

Respuesta: Nos permitimos aclarar que:

Punto 1: Las líneas base se manejan para los sistemas de información activos en la compañía y para los servicios nuevos a nivel de comunicaciones, seguridad, Bases de

datos, sistemas Operativos y aplicaciones Web, adicional se informa que se cuenta con una matriz o inventario.

Punto 2: Con respecto a una solución tecnológica para realizar estas evaluaciones tipo más automatizado, es posible contemplarla por parte de los oferentes, aclarando que debe estar inmersa al servicio, sin costos adicionales al servicio que debe prestar a LA PREVISORA.

Punto 3: Por último, los analistas de seguridad crean, actualizan, gestionan y evalúan las líneas base, pero los encargados de su implementación y evidencias son los administradores de cada herramienta o sistema de información de La Previsora.

Observación 11: SERVICIOS DE SEGURIDAD ADMINISTRADA. ¿Para el análisis de vulnerabilidades se debe contemplar un retest?
¿De cuantas líneas en promedio se proyectan los análisis de código requeridos para el servicio?

Respuesta: Nos permitimos indicar que:

Punto 1: Los análisis de vulnerabilidades deben contemplar los re-test junto con los informes respectivos.

Punto 2: Para los análisis de código se desconoce el número de líneas de código que pueda tener una aplicación y/o validación ya que estos se efectúan a demanda y en su mayoría son servicios nuevos.

Observación 12: TECNICO DE SEGURIDAD TI. ¿Este recurso debe estar enfocado en la gestión y atención de requerimientos de diferentes soluciones tecnológicas de la Entidad?
¿Cuántos recursos tiene dedicados a estas tareas actualmente?
¿Cuántos requerimientos se tiene actualmente registrados en la estadística de requerimientos? ¿Cuáles son las soluciones tecnológicas que deben ser administradas por el servicio? ¿Este(os) recurso(s) debe(n) ser contemplado(s) en sitio o remoto?

Respuesta: Nos permitimos aclarar que:

Punto 1: El Técnico de Seguridad está enfocado en la gestión de requerimientos e incidentes sobre las plataformas de seguridad de La Previsora

Punto 2: Se cuenta con un (1) recurso para esta labor

Punto3: El promedio de requerimientos e incidentes que atiende al mes es de 90 casos.

Punto 4: Las soluciones que se tienen actualmente son: Firewalls, Antivirus y Gestor de Identidades.

Punto 5: La información se encuentra en el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego.

Observación 13: SERVICIO. ¿Los ANS que se contemplan se deben cubrir en modalidad 7x24 o son 5x8, en relación a la gestión de incidentes?

Respuesta: Nos permitimos aclarar que su observación corresponde a 7X24, de igual forma esta se encuentra descrita en el numeral 3.3.7.4. ACUERDOS DE NIVELES DE SERVICIO del pliego de condiciones, adicionales ajustes en la Adenda N°3.

Observación 14: ENTREGABLES. ¿Los análisis y reportes de riesgos que se requieren del servicio son construidos en conjunto con la Entidad basados en sus análisis de riesgos o se deben enfocar en el análisis de riesgo desde la solución de monitoreo implementada?

Respuesta: Nos permitimos aclarar que los análisis de riesgos se efectúan en conjunto con el área de riesgos y son basados en los activos de la entidad.

Observación 15: ENTREGABLES. ¿La generación de políticas y directrices de seguridad hace parte de las funciones del equipo de Seguridad de la Información de la entidad, el servicio como complementa esta funcionalidad?

Respuesta: Nos permitimos indicar que el servicio debe efectuar los controles y hacer cumplir las políticas y lineamientos entregados por Seguridad de la Información de la entidad, así mismo, debe prevalecer por el cumplimiento de buenas prácticas de seguridad en todos los sistemas.

Observación 16: OBLIGACIONES DEL PROVEEDOR. ¿El SOC del proveedor debe cumplir con alguna ubicación física especial o puede ser contemplado en cualquier ubicación geográfica?

Respuesta: No, la Previsora no está sesgando ubicación geográfica para el servicio del SOC.

Observación 17: ANEXO No. 5 ALCANCE SOC. ¿Para los requerimientos mínimos de monitoreo, las fuentes entregan este tipo de alertas y eventos? Los controles generan los alertamientos o eventos requeridos para el monitoreo?

Respuesta: Nos permitimos aclarar que:

Punto 1: Para cada categoría las fuentes generan estos parámetros

Punto 2: Los alertamientos o eventos dependerán de la parametrización de la herramienta de correlación.

Observación 18: ANEXO No. 1 Dispositivos Monitoreo. ¿Es posible contar con un listado más específico de las fuentes? (Tipo, referencia y ubicación (Nube/On premise), esto es necesario para el dimensionamiento de la solución de monitoreo.

Respuesta: Nos permitimos aclarar que no es posible contar con información más detallada, sin embargo, se indica que las fuentes son comunes como S.O Windows, Linux Red Hat, a nivel de Base de Datos son 3 fuentes básicas de motor (SQL Server, Oracle y Sybases)

Los sistemas de información de la compañía se alojarán en nube privada y otros estarán en modalidad on-premise.

Observación 19: RECURSO HUMANO MINIMO HABILITANTE. ¿El servicio requiere de los siguientes recursos para la operación:
1 Gerente de Servicio.
4 Analistas SOC
2 Analistas de Seguridad
1 Técnico de seguridad
Es correcto el entendimiento del requerimiento?

Respuesta: Nos permitimos aclarar que su entendimiento es correcto.

Observación 20: CAPACIDAD FINANCIERA. Nivel de Endeudamiento (Pasivo Total/Activo Total): Menor o igual al 70%.
Solicitamos que el Nivel de Endeudamiento sea menor o igual al (<= 0,73).
Al modificar este indicador la entidad no pondrá en riesgo el proceso de contratación ya que el mismo estaría respaldado por:
* Garantía de Seriedad de la propuesta
* Garantías del contrato
* La entidad no hará anticipo, para este proceso la entidad efectuará el pago bajo la modalidad de mensualidades vencidas, mediante treinta y seis (36) pagos iguales cada uno con un valor fijo mensual, valor que se determinará de acuerdo con el valor de la propuesta seleccionada. Estos pagos deben venir acompañados de los entregables que se definan en las obligaciones y el acta de recibo a satisfacción por parte del supervisor del contrato.

Respuesta: Al respecto, nos permitimos informar que la Capacidad Financiera definida por Previsora se basó en el estudio de mercado que se realizó en el cual se contemplaron aspectos como: objeto del contrato, tiempo del contrato, valor del contrato, complejidad y forma de pago del mismo, buscando así que el proveedor tenga la liquidez y solidez necesarias para llevar a cabo el desarrollo del contrato, por lo cual los niveles solicitados para los indicadores establecidos permiten evaluar dicha condición. Adicionalmente, se tuvo en cuenta la información financiera registrada en Superintendencia de Sociedades de empresas dedicadas a actividades relacionadas con el objeto del contrato.

Así mismo, para la definición de estos indicadores se tuvo en cuenta lo señalado en la forma de pago del contrato y plazo de ejecución del contrato del pliego, ya que los proponentes deberán contar con una capacidad financiera mínima para cumplir con el desarrollo de las actividades que deberán ser asumidas por ellos por el tiempo de ejecución del contrato.

Por lo tanto y con el fin de garantizar los fines de la contratación, se establecieron los indicadores financieros solicitados en la invitación, buscando así una idoneidad financiera

de los proponentes, a través de la evaluación de varias dimensiones como lo son capital de trabajo, nivel de endeudamiento y patrimonio, los cuales evalúan aspectos diferentes que en conjunto garanticen liquidez para la ejecución satisfactoria del objeto del contrato.

Teniendo en cuenta lo anterior y considerando que los indicadores solicitados se ajustan a las necesidades de Previsora, se mantiene la capacidad financiera definida inicialmente.

Observación 21: EXPERIENCIA DEL PROPONENTE. Agradecemos considerar lo siguiente: Los contratos certificados deben haber iniciado durante los últimos 10 años a la presentación de la presente invitación. Esto demuestra alta experiencia en la ejecución de este tipo de proyectos.

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta, remitirse al numeral I. OBSERVACIONES GENERALES ítem 2 “Tiempo de experiencia del Proponente” del presente documento.

Observación 22: EXPERIENCIA DEL PROPONENTE. Agradecemos considerar lo siguiente: Con el fin de cumplir con la experiencia mínima habilitante, EL PROPONENTE deberá adjuntar con su propuesta mínimo (3) máximo cinco (5) certificaciones de contratos suscritos con empresas públicas o privadas nacionales en las que se acredite experiencia de la siguiente forma:

Respuesta: Nos permitimos indicar que el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE del pliego de condiciones se ajustará mediante Adenda N°3, remitirse al numeral OBSERVACIONES GENERALES ítem 3 “Número de certificaciones de experiencia general” del presente documento.

III. OBSERVACIONES PRESENTADAS POR LA EMPRESA REALTIME CONSULTING & SERVICES SAS

Observación: De manera atenta solicitamos a la Entidad no limitar la experiencia general del proceso a los últimos Parcia; lo anterior obedece a que los proyectos del tipo requerido en esta licitación normalmente son con duración a tres y cinco años y la gran mayoría se encuentran en ejecución. Con el ánimo de permitir pluralidad de ofertas, solicitamos que la misma se amplié a los últimos 8 años. Tiempo en el cual se puede demostrar mayor experiencia del proponente, más aún, cuando es de gran importancia para la Entidad contar con proveedores con un mayor conocimiento que se recoge a lo largo del camino; lo que adquiere mayor relevancia, que cuando es menor el tiempo de experiencia en este tipo de proyectos. Esto podrá garantizar una ejecución del contrato sin contratiempos.

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta, remitirse al numeral I. OBSERVACIONES GENERALES ítem 2 “Tiempo de experiencia del Proponente” del presente documento.

IV. OBSERVACIONES PRESENTADAS POR LA EMPRESA ITBP SOLUCIONES

Observación 1: CAPACIDAD FINANCIERA. - REQUISITOS FINANCIEROS

Solicitamos respetuosamente a la entidad replanteé los requerimientos del pliego de condiciones, acerca de los indicadores financieros para este proceso licitatorio, se podrá evidenciar el soporte de nuestra solicitud; y de esta manera las compañías que se presenten darán un mejor respaldo financiero y garantía de cumplimiento económico a la posible ejecución del contrato, por ello puntualmente sugerimos:

Nivel de Endeudamiento se solicitaba menor o igual al 60%.

Respuesta: Al respecto, nos permitimos informar que la Capacidad Financiera definida por Previsora se basó en el estudio de mercado que se realizó en el cual se contemplaron aspectos como: objeto del contrato, tiempo del contrato, valor del contrato, complejidad y forma de pago del mismo, buscando así que el proveedor tenga la liquidez y solidez necesarias para llevar a cabo el desarrollo del contrato, por lo cual los niveles solicitados para los indicadores establecidos permiten evaluar dicha condición. Adicionalmente, se tuvo en cuenta la información financiera registrada en Superintendencia de Sociedades de empresas dedicadas a actividades relacionadas con el objeto del contrato.

Así mismo, para la definición de estos indicadores se tuvo en cuenta lo señalado en la forma de pago del contrato y plazo de ejecución del contrato del pliego, ya que los proponentes deberán contar con una capacidad financiera mínima para cumplir con el desarrollo de las actividades que deberán ser asumidas por ellos por el tiempo de ejecución del contrato.

Por lo tanto y con el fin de garantizar los fines de la contratación, se establecieron los indicadores financieros solicitados en la invitación, buscando así una idoneidad financiera de los proponentes, a través de la evaluación de varias dimensiones como lo son capital de trabajo, nivel de endeudamiento y patrimonio, los cuales evalúan aspectos diferentes que en conjunto garanticen liquidez para la ejecución satisfactoria del objeto del contrato.

Teniendo en cuenta lo anterior y considerando que los indicadores solicitados se ajustan a las necesidades de Previsora, se mantiene la capacidad financiera definida inicialmente.

Observación 2: EQUIPO MÍNIMO REQUERIDO

- De manera atenta nos permitimos solicitar a la entidad que dos (2) Analistas SOC Dedicados con 3 años de experiencia: sea modificado y se solicite En pliego definitivo 4 Analistas SOC con menos años de experiencia (2 años). Recursos DEDICADOS.
- Se solicita amablemente a la entidad que para el cargo de Gerente de Proyecto o Gerente de Servicio: Se solicita que la Dedicación sea de forma PARCIAL y no de forma por porcentaje, ya que de esta forma no se estaría realizando un seguimiento más efectivo al cargo solicitado. Y adicionalmente se solicita que las certificaciones sean en control de cambios en documentos.
- De igual forma para el roll Técnico de Seguridad se solicita se pueda modificar y el recurso sea dedicado.

- Solicitamos amablemente que los dos (2) Analistas de Seguridad TI con 5 años de experiencia esta sea modificada a dos (2) años de experiencia y que estos a su vez para la ejecución del mismo sea una de forma remota y otro en forma presencial.

Respuesta: Nos permitimos informar que su observación no será tenida en cuenta, pero se aclaran los siguientes puntos:

Punto 1: La definición de los recursos están descritos en el pliego de condiciones numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE, así mismo se indica que estos son los mínimos requerido para el servició, el oferente debe disponer del recurso necesario que considere necesario para el cumplimiento de los ANS sin ningún costo adicional para la entidad, por lo tanto, no es necesario ni se está solicitando dedicación a la entidad para el servicio de SOC.

Punto 2: Nos permitimos indicar que su observación será tenida en cuenta y se ajustará el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE mediante Adenda N°3.

Sin embargo, su observación " que las certificaciones sean en control de cambios en documentos" no fue entendida, por lo que no será tenida en cuenta.

Punto 3: El rol de Técnico de seguridad TI, se hace la aclaración y confirmación que es dedicado, de igual forma se realizara aclaración en el numeral 3.3.7.2.2. TECNICO DE SEGURIDAD TI mediante Adenda N°3

Punto 4: Solicitamos remitirse al numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE ítem DOS (2) ANALISTAS DE SEGURIDAD TI donde se confirma la información respectiva de los recursos.

Observación 3: EVALUACION ECONOMICA

Solicitamos respetuosamente a la entidad replanteé y se deje este requerimiento como MEDIA GEOMETRIA CON PRESUPUESTO OFICIAL, ya que se busca ampliar el espectro de participación favoreciendo la pluralidad de los oferentes que se alinea con el principio de la libre concurrencia el cual permiten el acceso y participación efectiva de todos los posibles interesados

Respuesta: Agradecemos su observación, pero la misma no será tenida en cuenta, a razón de que la entidad busca siembre el mejor costo beneficio, garantizando la reducción de costos.

Observación 4: CERTIFICADO POR FABRICANTE

De manera atenta solicitamos a la entidad retirar el requerimiento habilitante de presentación, toda vez que tal como este requerimiento limita efectivamente la libre concurrencia de proponentes y solo beneficia a un número reducido de proponentes.

Respuesta: Agradecemos su observación, pero la misma no será tenida en cuenta, debido a que los proponentes deberán contar con soporte y acreditación del producto respectivo,

por parte de los fabricantes, por temas de soporte y mantenimiento de las mismas herramientas, así mismo es importante para la entidad saber que cuenta con respaldo de fábrica de las herramientas que utilizará para la prestación del servicio.

Observación 5: RECURSO HUMANO CALIFICABLE

Solicitamos respetuosamente a la entidad replanteé los siguientes requerimientos:

- Para el Especialista de Seguridad: que para la dedicación de este sea de forma parcial para un mayor eficacia y mejor seguimiento.
- Director del SOC: solicitamos adicional mínimo de 10 años de experiencia 10 años de experiencia profesional de los cuales al menos OCHO (8) años sean en Gerencia de proyectos o consultoría de seguridad de la información. Con maestría y/o especialización en seguridad de la información.

Y adicional que este cuente con al menos 06 de la siguientes certificaciones o acreditaciones técnicas

- -Togaf 9
- -ECIH “Certified Incident Handler”
- -Auditor Líder ISO 22301 del 2012.
- -Auditor Líder de Implementación ISO 27001 del 2013
- -Líder de implementación ISO 270032 del 2017
- -Auditor Líder ISO 27001 del 2013.
- -ISO 27032 del 2017
- -ISO 31000 del 2018

Respuesta: Nos permitimos aclarar lo siguiente:

Punto 1: Con respecto al Especialista de Seguridad la observación no será tenida en cuenta.

Punto 2: Con respecto a la modificación solicitada para el director SOC, le informamos que su observación no será tenida en cuenta.

Punto 3: Se ajustara ANEXO No. 2 RECURSO HUMANO CALIFICABLE del pliego de condiciones, mediante Adenda N°3, de igual forma se especifica el detalle el numeral OBSERVACIONES GENERALES ítem 3 “Certificaciones del Recurso Humano calificable“ del presente documento.

V. OBSERVACIONES PRESENTADAS POR LA EMPRESA CIPHER

Observación 1:

PLAZO DE EJECICION DEL CONTRATO	Solicitamos a la Previsora revaluar el no pago del proceso de transición, esta fase es importante y no exime al contratista de costos laborares y técnicos.

Respuesta: De manera atenta informamos que La Previsora no puede asumir un doble gasto por la ejecución de un mismo servicio, por lo cual, el proceso de transición entre el

proveedor saliente y el proponente seleccionado continuará como se encuentra descrito en el pliego de condiciones.

Así mismo, se aclara que en esta etapa el proponente seleccionado deberá iniciar labores de implementación, configuración, parametrización, pruebas, estabilización y entrenamiento de los recursos. En la etapa de transición el servicio de SOC es responsabilidad del proveedor actual. Una vez se finalice el tiempo de transición, el nuevo proponente asumirá la operación ya deberá contar con operación y deberá cumplir los ANS descritos en el pliego de condiciones.

Observación 2:

CIERRE DEL PROCESO y PLAZO PARA PRESENTAR PROPUESTAS	Solicitamos a la Previsora ampliar el plazo de cierre, esta es muy corto para hacer el diseño de la solución y mas cuando hubo un festivo. Solcitamos el cierre para la primera semana de julio.

Respuesta: De manera atenta se informa que su observación fue tenía en cuenta y se ajustó el numeral 1.21 CRONOGRAMA DE LA INVITACIÓN ABIERTA mediante Adenda N° 1 publicada el 18 de mayo de 2021 y Adenda N°2 publica el 25 de mayo de 2021 en la página web de La Previsora.

Observación 3:

PRESENTACIÓN DE LAS PROPUESTAS	Solicitamos a la Previsora hacer mayor claridad sobre las intuiciones del punto 2.

Respuesta: Nos permitimos informar que para la presentación de las propuestas deberá contener el detalle de todo el Capítulo IV “Aspectos calificables” del pliego de condiciones en un documento con clave, la cual deberá suministrarse en la audiencia de cierre para publicidad del mismo.

Observación 4:

CAPACIDAD FINANCIERA	¿Solicitamos a la Previsora aclarar porque una sociedad extrajera deba tener RUP actualizado? De acuerdo con la normativa que rige el sistema de compras y contratación pública, las personas naturales o jurídicas extranjeras sin domicilio o sucursal en Colombia no están obligadas a estar inscritas en el Registro único de Proponentes – RUP, razón por las cual las Entidades Estatales deben verificar directamente el cumplimiento de los requisitos habilitantes. Ahora bien, que el proponente extranjero sin domicilio o sucursal en Colombia no esté obligado a estar inscrito en el RUP no presenta ninguna desventaja ni limita su participación en los Prpcesos de Contratación, toda vez que las Entidades Estatales deben exigir en igualdad de condiciones la acreditación de los requisitos habilitantes, se trate de proponente nacional o extranjero. Lo único que varía cuando se trata de proponente extranjero sin domicilio o sucursal en Colombia es la forma de verificación de los requisitos habilitantes, tal y cómo se anotó en precedencia.

Respuesta: Agradecemos su observación, la cual será tenida en cuenta remitirse al numeral I. OBSERVACIONES GENERALES ítem 5 “Capacidad Financiera” y ajuste mediante Adenda N°3.

Observación 5:

EXPERIENCIA DEL PROPONENTE	Solicitamos a la Previsora modificar el requerimiento, solicitando hasta 3 certificaciones de contratos.

Respuesta: Nos permitimos indicar que el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE del pliego de condiciones se ajustará mediante Adenda N°3, remitirse al numeral OBSERVACIONES GENERALES ítem 3 “Número de certificaciones de experiencia general” del presente documento.

Observación 6:

RECURSO HUMANO MINIMO HABILITANTE.	Solicitamos a la Previsora que se modifique el requerimiento y que mediante carta del Representate Legal se haga compromiso de entregar en 05 días hábiles las hojas de vida del personal solicitado.

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta, sin embargo, se efectúa modificación sobre el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE mediante Adenda N°3.

Observación 7:

c. Realizar análisis del software libre, entregando un informe con la recomendación de uso. Este se manejará a demanda.	Se solicita a la entidad por favor detallar más lo requerido o esperado en el ítem en referencia. Adicionalmente, cuales son las aplicaciones de software libre que utiliza la previsora, y sobre cuales distribuciones de software libre se encuentran desarrolladas.

Respuesta: Nos permitimos aclarar que los análisis de software se solicitan a demanda y estos dependerán de la necesidad de La Previsora, de igual forma el análisis solicitado es para confirmar si el software puede llegar a generar alguna vulnerabilidad a nivel interno, mala reputación, limitaciones o incumplimiento normativo de derechos de autor.

Observación 8:

o. Aseguramiento y gestión de vulnerabilidades: Anualmente se deberán generar dos (2) análisis de vulnerabilidad, Ethical Hacking y penetración a la plataforma tecnológica, a los que se deberá elaborar una matriz de seguimiento de los hallazgos encontrados y los planes de remediación y/o mitigación, el cual deberá ser gestionado por EL PROVEEDOR. Para cada uno de los análisis se debe contemplar todos los dispositivos activos de LA PREVISORA S.A los cuales se estiman en un promedio de 600 objetivos. Por otra parte, se debe contemplar análisis de vulnerabilidades a demanda adicionales para nuevas aplicaciones y/o solicitudes internas. Se solicita contemplar por lo menos 2 análisis de código por año y el respectivo Re-test de cada uno de los análisis efectuados, los análisis de penetración a las herramientas se solicita estimación de por lo menos 3 por año.	Se consulta a la entidad si es posible cambiar la modalidad de los análisis de código de caja blanca a caja gris, lo anterior con el fin de no tener acceso directo al código de las aplicaciones.

Respuesta: Nos permitimos aclarar que La Previsora no está sesgando la modalidad de los análisis de código, el proponente puede proponer su esquema de análisis bajo el modelo de caja conveniente.

Observación 9:

j. Generar informes diarios y/o a demanda de eventos sobre los dispositivos de seguridad.	Se consulta a la entidad si es completamente obligatorio la entrega de informes diarios, dado que esto se traduce en la dedicación tanto del proveedor como del personal de TI y seguridad de la previsora. Se propone que se consulte la información en los dashboards que serán parte de la solución ofertada

Respuesta: Nos permitimos aclarar que para un mayor entendimiento se realiza ajuste al numeral 3.3.7.2.2. TECNICO DE SEGURIDAD TI del pliego de condiciones mediante Adenda N°3

Observación 10:

LA PREVISORA S.A actualmente cuenta con un SOC tercerizado tradicional nivel 1, que monitoriza y analiza eventos de la infraestructura tecnológica core de negocio y busca fortalecer la seguridad con los nuevos desafíos, por lo que se contempla la evaluación de nivel 1 a nivel 2 "Análisis exhaustivo y de respuesta".	Se consulta a la entidad por el promedio de EPS (Eventos por segundo) en promedio que maneja con el actual proveedor.

Respuesta: Nos permitimos informar que el promedio de EPS actual es de 1500, pero es de aclarar que esta información solo es una parte de lo que se requiere monitorear. Para mayor claridad por favor remitirse al ANEXO No. 1 DISPOSITIVOS MONITOREO

Observación 11:

LA PREVISORA S.A actualmente cuenta con un SOC tercerizado tradicional nivel 1, que monitoriza y analiza eventos de la infraestructura tecnológica core de negocio y busca fortalecer la seguridad con los nuevos desafíos, por lo que se contempla la evaluación de nivel 1 a nivel 2 "Análisis exhaustivo y de respuesta".	Se consulta a la entidad por el tráfico gigadía en promedio que maneja con el actual proveedor.

Respuesta: Nos permitimos indicar que el tráfico promedio por día es de 4 Gigas, pero es de aclarar que esta información es del monitoreo actual que no contempla lo requerido para el nuevo proceso. Para mayor claridad por favor remitirse al ANEXO No. 1 DISPOSITIVOS MONITOREO

Observación 12:

LA PREVISORA S.A actualmente cuenta con un SOC tercerizado tradicional nivel 1, que monitoriza y analiza eventos de la infraestructura tecnológica core de negocio y busca fortalecer la seguridad con los nuevos desafíos, por lo que se contempla la evaluación de nivel 1 a nivel 2 "Análisis exhaustivo y de respuesta".	Se consulta a la entidad si con el actual proveedor cuenta con conectores personalizados, cuantos y cuales son?

Respuesta: Nos permitimos aclarar que con el proveedor actual no se cuentan con conectores personalizados.

Observación 13:

LA PREVISORA S.A actualmente cuenta con un SOC tercerizado tradicional nivel 1, que monitoriza y analiza eventos de la infraestructura tecnológica core de negocio y busca fortalecer la seguridad con los nuevos desafíos, por lo que se contempla la evaluación de nivel 1 a nivel 2 "Análisis exhaustivo y de respuesta".	Se consulta a la entidad si con el actual proveedor cuenta con reglas de correlación personalizadas, cuantas y cuales son?

Respuesta: Nos permitimos informar que, si se cuenta con reglas de correlación personalizadas, el detalle de la información se entregara al proveedor seleccionado.

Observación 14:

LA PREVISORA S.A actualmente cuenta con un SOC tercerizado tradicional nivel 1, que monitoriza y analiza eventos de la infraestructura tecnológica core de negocio y busca fortalecer la seguridad con los nuevos desafíos, por lo que se contempla la evaluación de nivel 1 a nivel 2 "Análisis exhaustivo y de respuesta".	Se consulta a la entidad si actualmente cuenta con servicios de Microsoft Azure y si es posible compartir el presupuesto anual para estos servicios

Respuesta: Nos permitimos indicar que La Previsora si cuenta con servicios de Microsoft Azure, pero teniendo en cuenta que la información presupuestal no es relevante para el presente proceso, no se considera necesario suministrar la información requerida.

Observación 15:

LA PREVISORA S.A actualmente cuenta con un SOC tercerizado tradicional nivel 1, que monitoriza y analiza eventos de la infraestructura tecnológica core de negocio y busca fortalecer la seguridad con los nuevos desafíos, por lo que se contempla la evaluación de nivel 1 a nivel 2 "Análisis exhaustivo y de respuesta".	Se consulta a la entidad si es posible asociar el licenciamiento del SIEM a la previsora

Respuesta: Nos permitimos informar que no es posible asociar el licenciamiento del SIEM a La Previsora teniendo en cuenta que este se solicita como servicio.

Observación 16:

LA PREVISORA S.A actualmente cuenta con un SOC tercerizado tradicional nivel 1, que monitoriza y analiza eventos de la infraestructura tecnológica core de negocio y busca fortalecer la seguridad con los nuevos desafíos, por lo que se contempla la evaluación de nivel 1 a nivel 2 "Análisis exhaustivo y de respuesta".	Se consulta a la entidad si cuenta con alguna restricción sobre la geolocalización de los servicios de SIEM y UBA, es decir si por ejemplo puede estar ubicada en la nube del proveedor en Estados Unidos u otro país.

Respuesta: Nos permitimos indicar que no existe restricción de geolocalización con respecto a los servicios solicitados ya que se entiende que por ser nube puede estarán localizadas en otro país, sin embargo, debe cumplir con la regulación colombiana sobre reposo de información alojada en nube definido por la Superintendencia Financiera de Colombia

Observación 17:

CONDICIONES TÉCNICAS OBLIGATORIAS MÍNIMAS	Se consulta a la entidad si se enviarán a todas las respuestas a las preguntas realizadas por todos los participantes del proceso

Respuesta: Nos permitimos informar que las respuestas a las observaciones serán publicadas en la página de La Previsora.

Observación 18:

o. Contener o neutralizar los ataques detectados en caso de presencia de amenazas, para estos eventos se deberá contar con una matriz de incidencias y deberá estar avalada por LA PREVISORA S.A.	Se consulta a la entidad si dentro del alcance del servicio, espera que el proveedor acceda a los dispositivos involucrados en un evento de seguridad para su contención o neutralización, lo anterior debido a que representa un riesgo para la entidad que un proveedor modifique o altere cualquier regla o parámetro que afecte el funcionamiento de los servicios de la Previsora

Respuesta: Nos permitimos aclarar que el servicio solicitado requiere respuesta sobre eventos, por lo cual para temas de ataques se deberán tomar las acciones pertinentes. Así mismo el servicio cuenta con personal que administrara las plataformas respectivas por lo cual se podría manejar un nivel de configuración especifico. Si los dispositivos involucrados hacen parte de la gestión del servicio de seguridad de TI, el recurso Técnico de Seguridad TI deberá estar en capacidad de solventar, contener o neutralizar los eventos en las plataformas definidas en su gestión, si las plataformas involucradas no hacen parte del servicio contratado La Previsora es la responsable de ejecutar las acciones, configuración recomendadas por el Grupo de SOC o Analistas de Seguridad TI.

Observación 19:

b. Apoyar la implementación segura de los sistemas de información.	Se consulta a la entidad cuantos y cuales son estos sistemas de información a los que hace referencia el ítem

Respuesta: Nos permitimos indicar que el ítem hace alusión a todos los sistemas de información (aplicaciones y demás) con los que cuente La Previsora, el detalle de la información se entregara al oferente seleccionado junto.

Observación 20:

Identificar y establecer el nivel de madurez de seguridad informática y de ciberseguridad en LA PREVISORA S.A teniendo en cuenta el estándar ISO 27001 y/o NIST 800-53 (GAP).	Se consulta a la entidad si debería realizarse la evaluación de la madurez de la seguridad de la información en las áreas de negocio de la empresa? Si es así, por favor, ¿es posible enumerarlos?

Respuesta: Nos permitimos aclarar que el análisis de la madurez de la seguridad se realiza de manera transversal sobre los procesos de la entidad, alineado con el MSPI (El Modelo de Seguridad y Privacidad de la Información).

Observación 21:

Identificar y establecer el nivel de madurez de seguridad informática y de ciberseguridad en LA PREVISORA S.A teniendo en cuenta el estándar ISO 27001 y/o NIST 800-53 (GAP).	Se consulta a la entidad si actualmente cuenta con un equipo interno dedicado a la Seguridad de la Información?

Respuesta: Nos permitimos informar que actualmente La Previsora S.A cuenta con un equipo de Seguridad de la información en el área de la Gerencia de Riesgos.

Observación 22:

Identificar y establecer el nivel de madurez de seguridad informática y de ciberseguridad en LA PREVISORA S.A teniendo en cuenta el estándar ISO 27001 y/o NIST 800-53 (GAP).	Se consulta a la entidad si se ha realizado antes la Evaluación de Madurez?

Respuesta: Nos permitimos informar que la entidad si ha realizado evaluación de madurez con periodicidad anual, el cual es socializado ante el Comité de Seguridad de la Información y Riesgos y es de cumplimiento por medición de los entes externos como la Superintendencia Financiera de Colombia.

Observación 23:

Identificar y establecer el nivel de madurez de seguridad informática y de ciberseguridad en LA PREVISORA S.A teniendo en cuenta el estándar ISO 27001 y/o NIST 800-53 (GAP).	Se consulta a la entidad si cuenta con otros procesos de cumplimiento de la seguridad de la información en curso?

Respuesta: Nos permitimos informar que La Previsora al ser una entidad pública/privado debe cumplir con otros procesos de cumplimiento de la Seguridad de la Información que están a cargo de otra área Gerencia de Riesgos. Así mismo hay procesos para cumplimiento de ítems sobre seguridad de la información.

Observación 24:

Identificar y establecer el nivel de madurez de seguridad informática y de ciberseguridad en LA PREVISORA S.A teniendo en cuenta el estándar ISO 27001 y/o NIST 800-53 (GAP).	Se consulta a la entidad si cuenta con un equipo para realizar la gestión de riesgos?

Respuesta: Nos permitimos indicar que La Previsora si cuenta con un equipo de la gestión de Riesgos a cargo de la Gerencia de Riesgos de la entidad.

Observación 25:

m. Complementar la documentación relacionada con los aspectos de ciberseguridad e incluidos en la revisión de la documentación existente, de los procesos de la Gerencia de TI.	Se consulta a la entidad si actualmente utiliza alguna herramienta de gestión de riesgos?

Respuesta: Nos permitimos aclarar que La Previsora S.A si cuenta con una herramienta de Gestión de Riesgos y está a cargo de otro proceso diferente a TI.

Observación 26:

m. Complementar la documentación relacionada con los aspectos de ciberseguridad e incluidos en la revisión de la documentación existente, de los procesos de la Gerencia de TI.	Se consulta a la entidad si cuenta con un equipo con las capacidades de de implementar y mantener un SGSI de acuerdo con los requisitos de la ISO 27001?

Respuesta: La Previsora S.A cuenta con un equipo de la gestión de seguridad de la Información alineado a todos los procesos de la norma ISO27001.

Observación 27:

m. Complementar la documentación relacionada con los aspectos de ciberseguridad e incluidos en la revisión de la documentación existente, de los procesos de la Gerencia de TI.	Se consulta a la entidad si cuenta con un proyecto de implementación de SGSI (si no se implementó)?

Respuesta: La Previsora S.A a través de su área de Seguridad de la Información gestiona y cuenta con un proyecto de SGSI como buena práctica de seguridad.

Observación 28:

m. Complementar la documentación relacionada con los aspectos de ciberseguridad e incluidos en la revisión de la documentación existente, de los procesos de la Gerencia de TI.	Se consulta a la entidad si tiene un alcance definido para su SGSI?

Respuesta: Nos permitimos indicar que La Previsora S. A si cuenta con un alcance definido del SGSI y es liderado por el área de Seguridad de la Información de la compañía.

Observación 29:

m. Complementar la documentación relacionada con los aspectos de ciberseguridad e incluidos en la revisión de la documentación existente, de los procesos de la Gerencia de TI.	Se consulta a la entidad si cuenta con la documentación del SGSI?

Respuesta: Nos permitimos indicar que La Previsora S. A si cuenta con un documento definido del SGSI y es liderado por el área de Seguridad de la Información de la compañía.

Observación 30:

m. Complementar la documentación relacionada con los aspectos de ciberseguridad e incluidos en la revisión de la documentación existente, de los procesos de la Gerencia de TI.	Se consulta a la entidad si en el último año ha llevado a cabo un análisis de riesgos dentro del alcance del SGSI, incluida la evaluación de riesgos, los planes de tratamiento y la reevaluación de riesgos?

Respuesta: Nos permitimos indicar que La Previsora S.A ha realizado análisis de riesgos sobre dispositivos críticos de la compañía, pero no se ha realizado la reevaluación de este. Esto está a cargo del área de Seguridad de la Información de la Compañía.

Observación 31:

m. Complementar la documentación relacionada con los aspectos de ciberseguridad e incluidos en la revisión de la documentación existente, de los procesos de la Gerencia de TI.	Se consulta a la entidad si cuenta con todas las políticas y estándares de SGSI, como políticas de seguridad de la información, clasificación de la información, gestión de acceso, respuesta a incidentes, etc.?

Respuesta: Nos permitimos indicar que La Previsora S.A cuenta con políticas de seguridad de la información, y tiene definido y documentos la clasificación de la información, la gestión de accesos, así como la respuesta a incidentes alineado a la taxonomía definida por la Superintendencia Financiera de Colombia, el cual está a cargo del área de Seguridad de la Información de la Compañía.

Observación 32:

m. Complementar la documentación relacionada con los aspectos de ciberseguridad e incluidos en la revisión de la documentación existente, de los procesos de la Gerencia de TI.	Se consulta a la entidad si en el último año ha tenido una auditoría interna o externa del funcionamiento de su SGSI

Respuesta: Nos permitimos indicar que La Previsora S.A en el último año ha tenido auditorías internas y externas del funcionamiento del SGSI.

Observación 33:

m. Complementar la documentación relacionada con los aspectos de ciberseguridad e incluidos en la revisión de la documentación existente, de los procesos de la Gerencia de TI.	Se consulta a la entidad si cuenta con toda la documentación de los controles implementados y sus indicadores de desempeño?

Respuesta: Nos permitimos indicar que La Previsora S.A cuenta con documentación de controles e indicadores de desempeño, es de aclarar que este proceso se actualiza según sea requerido.

Observación 34:

o. Aseguramiento y gestión de vulnerabilidades: Anualmente se deberán generar dos (2) análisis de vulnerabilidad, Ethical Hacking y penetración a la plataforma tecnológica, a los que se deberá elaborar una matriz de seguimiento de los hallazgos encontrados y los planes de remediación y/o mitigación, el cual deberá ser gestionado por EL PROVEEDOR. Para cada uno de los análisis se debe contemplar todos los dispositivos activos de LA PREVISORA S.A los cuales se estiman en un promedio de 600 objetivos. Por otra parte, se debe contemplar análisis de vulnerabilidades a demanda adicionales para nuevas aplicaciones y/o solicitudes internas. Se solicita contemplar por lo menos 2 análisis de código por año y el respectivo Re-test de cada uno de los análisis efectuados, los análisis de penetración a las herramientas se solicita estimación de por lo menos 3 por año.	Se consulta a la entidad si es posible cambiar la modalidad de los análisis de código de caja blanca a caja gris, lo anterior con el fin de no tener acceso directo al código de las aplicaciones.

Respuesta: Nos permitimos aclarar que La Previsora no está sesgando la modalidad de los análisis de código, el proponente puede proponer su esquema de análisis bajo el modelo de caja conveniente.

Observación 35:

c. Conocimientos mínimos para ejecución de troubleshooting en la administración de plataformas de antivirus, firewall, redes, controladores de dominio, sistemas operativos y aplicaciones genéricas como filezilla, ftp, entre otras para la correcta solución de un incidente y/o requerimiento.	Se solicita a la entidad aclarar si el alcance del servicio incluye administración de dispositivos de TI, dado que no es parte de los servicios de gestión de seguridad de la información

Respuesta: Nos permitimos aclarar que para el técnico de seguridad el alcance se encuentra descrito en el numeral 3.3.7.2.2. TECNICO DE SEGURIDAD TI y deberá cumplir con la totalidad de las obligaciones del servicio

Observación 36:

a. Gestionar el desarrollo e implementación de nuevas políticas, normas, directrices, procedimientos e instructivos de seguridad y ciberseguridad para el óptimo cumplimiento de los controles de seguridad descritos y manejados en cada una de las plataformas.	Se consulta a la entidad cuáles son las políticas de seguridad de la información ya desarrolladas por la previsora

Respuesta: Esta información será entregada al proponente seleccionado, en caso de requerirlo.

Observación 37:

j. Generar informes diarios y/o a demanda de eventos sobre los dispositivos de seguridad.	Se consulta a la entidad si es completamente obligatorio la entrega de informes diarios, dado que esto se traduce en la dedicación tanto del proveedor como del personal de TI y seguridad de la previsora. Se propone que se consulte la información en los dashboards que serán parte de la solución ofertada

Respuesta: Agradecemos su observación y se informa que se ajustará el numeral 3.3.7.2.2. TECNICO DE SEGURIDAD TI del pliego de condiciones mediante Adenda N°3.

Observación 38:

k. Contar con disponibilidad y participación en las pruebas de DRP y unitarias que establezca LA PREVISORA S.A y generar las acciones respectivas si lo amerita para el cumplimiento adecuado de la actividad a nivel de seguridad.	Se consulta a la entidad en que consisten las pruebas DRP y unitarias, así como su duración y cantidad de tiempo estimado que se debe dedicar en la duración del contrato

Respuesta: Nos permitimos aclarar que las pruebas unitarias y/o DRP hace referencia a las actividades que se deban realizar en las herramientas de seguridad para garantizar la continuidad de los servicios a nivel de seguridad, las cuales se ejecutan con una periodicidad de una vez al año o a demanda según se requiera, por cumplimiento normativo o por afectación de algún servicio. No se puede indicar el tiempo estimado que debe dedicar en la duración, ya que esto depende del evento o incidente que se presente, es por esto que se indica que debe estar disponible para la entidad del 100% en caso de requerirse.

Observación 39:

Acuerdos de Niveles de Servicio (ANS) de Gestión de Incidentes de Servicio	Se consulta a la entidad si para los niveles de criticidad el porcentaje de cumplimiento en el tiempo de atención y solución es mensual o cual es el período de tiempo a evaluar.

Respuesta: Nos permitimos indicar que el tiempo de medición se realiza de manera mensual.

Observación 40:

Acuerdos de Niveles de Servicio (ANS) de Gestión de Requerimientos de Servicio	Se consulta a la entidad si para los niveles de criticidad el porcentaje de cumplimiento en el tiempo de atención y solución es mensual o cual es el período de tiempo a evaluar.

Respuesta: Nos permitimos indicar que el tiempo de medición se realiza de manera mensual.

Observación 41:

Acuerdos de Niveles de Servicio (ANS) de Gestión de Requerimientos de Servicio	Se solicita a la entidad especificar los dispositivos del Anexo 1 que hacen parte de la infraestructura de seguridad dentro del alcance del servicio

Respuesta: Nos permitimos aclarar que no es posible especificar el detalle de la información, esta será entregada al proponente seleccionado.

Observación 42:

Acuerdos de Niveles de Servicio (ANS) de Gestión de Incidentes de Servicio	Se consulta a la entidad si es posible proponer otros ANS

Respuesta: Nos permitimos indicar que en esta etapa el proponente podía indicar en su observación la propuesta de indicador para análisis, sin embargo, no la visualizamos. Por otro lado, se indica que el proveedor seleccionado podrá proponer o adicionar otros ANS si así lo considera en conceso y/o aprobación con la entidad. Referente al ANS de Gestión de Incidentes de Servicios si no se reciben observaciones se mantiene como está definido en el pliego de condiciones.

Observación 43:

Acuerdos de Niveles de Servicio (ANS) de Gestión de Requerimientos de Servicio	Se consulta a la entidad si es posible proponer otros ANS

Respuesta: Nos permitimos indicar que en esta etapa el proponente podía indicar en su observación la propuesta de indicador para análisis, sin embargo, no la visualizamos. Por otro lado, se indica que el proveedor seleccionado podrá proponer o adicionar otros ANS si así lo considera en conceso y/o aprobación con la entidad. Referente al ANS de Gestión de Requerimientos de Servicios si no se reciben observaciones se mantiene como está definido en el pliego de condiciones.

Observación 44:

Acuerdos de Niveles de Servicio (ANS) de Gestión de Incidentes de Servicio	Se consulta a la entidad si una notificación automatizada es aprobada para cumplir con el tiempo de atención requerido

Respuesta: Nos permitimos aclarar que estas automatizaciones son aprobadas para cumplir con estos tiempos.

Observación 45:

Acuerdos de Niveles de Servicio (ANS) de Gestión de Requerimientos de Servicio	Se consulta a la entidad si una notificación automatizada es aprobada para cumplir con el tiempo de atención requerido

Respuesta: Nos permitimos aclarar que estas automatizaciones son aprobadas para cumplir con estos tiempos.

Observación 46:

Acuerdos de Niveles de Servicio (ANS) de Gestión de Incidentes de Servicio	Se consulta a la entidad si en caso de requerir gestión por parte de la previsora para atender un incidente, la alteración de los tiempos de respuesta no represente un incumplimiento sobre los ANS y por ende una penalidad sobre el servicio

Respuesta: Nos permitimos aclarar que los ANS solo aplican para la infraestructura y gestión por el proponente. En caso de escalamiento a La Previsora S.A el cual debe realizar a través de la herramienta de gestión de casos, será responsabilidad de gestión del nuevo resolutor por lo que no aplicará penalidad. Sin embargo, esto debe estar identificado y documentado.

Observación 47:

Acuerdos de Niveles de Servicio (ANS) de Gestión de Requerimientos de Servicio	Se consulta a la entidad si en caso de requerir gestión por parte de la previsora para atender un incidente, la alteración de los tiempos de respuesta no represente un incumplimiento sobre los ANS y por ende una penalidad sobre el servicio

Respuesta: Nos permitimos aclarar que los ANS solo aplican para la infraestructura y gestión por el proponente. En caso de escalamiento a La Previsora S.A el cual debe realizar a través de la herramienta de gestión de casos, será responsabilidad de gestión del nuevo resolutor por lo que no aplicará penalidad. Sin embargo, esto debe estar identificado y documentado.

Observación 48:

Acuerdos de Niveles de Servicio (ANS) de Gestión de Incidentes de Servicio	Se consulta a la entidad si las penalidades son acumulativas?

Respuesta: Nos permitimos indicar que las penalidades no son acumulativas ya que la medición es mensual contra factura del mes de servicio medido.

Observación 49:

Acuerdos de Niveles de Servicio (ANS) de Gestión de Requerimientos de Servicio	Se consulta a la entidad si las penalidades son acumulativas?

Respuesta: Nos permitimos indicar que las penalidades no son acumulativas ya que la medición es mensual contra factura del mes de servicio medido.

Observación 50:

5. Informe del análisis del estado de ciberseguridad en LA PREVISORA S.A. (Assessment inicial) y plan de acción respectivo para la mejora continua. Se deberán contemplar las herramientas de seguridad que se gestionarán.	Se solicita a la entidad informar el estado actual de los equipos que hacen parte del alcance del presente proceso incluyendo el estado del soporte, garantías, vida útil, últimos mantenimientos preventivos y correctivos realizados.

Respuesta: Nos permitimos informar que el estado actual de los equipos es el siguiente:

DISPOSITIVO	VIDA UTIL /GARANTIAS	ULTIMO MANTENIMIENTO
Firewall	2023 /soporte fabrica	Febrero 2021
Antivirus (nube)	N/A / soporte fabrica y proveedor	Semanal
OIM	N/A / soporte fabrica y proveedor	Abril 2021
Office365 (seguridad en nube)	N/a / soporte fabrica	N/A

Observación 51:

OBLIGACIONES DEL PROVEEDOR	Solicitamos a la Previsora exija y de puntaje al OFERENTE tenga SOC propio en el territorio colombiano y al menos uno (1) fuera del país (LATAM) esto con el fin de garantizar la calidad y la alta disponibilidad del servicio.

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta ya que este requerimiento limitaría la pluralidad de oferentes.

Observación 52:

CRITERIOS CALIFICABLES QUE OTORGAN PUNTAJE – CRITERIOS DE EVALUACIÓN:	Solicitamos a la Previsora que modifique este cuadro de puntaje agregando mas puntaje al oferente que cuente con las normas ISO 20000 e ISO 27000, que como lo refiere la fila anterior los beneficios para la aseguradora son importantes.

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta a razón de que la certificación ISO 270001 es un requisito habilitante al proceso, sin embargo, el numeral 4.1.4. CERTIFICACIONES ADICIONALES (30) PUNTOS será modificado mediante Adenda N°3.

Observación 53:

CRITERIOS CALIFICABLES QUE OTORGAN PUNTAJE – CRITERIOS DE EVALUACIÓN:	Solicitamos a la Previsora que el Oferente este certificado en ISO 20000; la norma ISO 27001 y la ISO 20000 en su conjunto son herramientas perfectas para disponer de la protección adecuada frente a la gestión de los servicios TI y la seguridad de la información y los datos que maneje una empresa del sector financiero.

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta a razón de que la certificación ISO 270001 es un requisito habilitante al proceso, sin embargo, el numeral 4.1.4. CERTIFICACIONES ADICIONALES (30) PUNTOS será modificado mediante Adenda N°3.

Observación 54:

ANEXO No. 1 DISPOSITIVOS MONITOREO	Se solicita a la entidad incluir en la documentación, las marcas, referencias o modelos de los equipos que hacen parte del alcance del servicio

Respuesta: Nos permitimos aclarar que no es posible especificar el detalle de la información, esta será entregada al proponente seleccionado.

Observación 55:

ANEXO No. 1 DISPOSITIVOS MONITOREO	Se solicita a la entidad especificar cuales de los dispositivos son te tipo appliance on premise, virtuales en cloud público o privado, si se incluyen servicios tipo PaaS o SaaS, etc.

Respuesta: Nos permitimos aclarar que el detalle de los dispositivos a monitorear será entregado al proponente seleccionado. Sin embargo, se informa que el core de negocio es op premise, los demás componentes de la compañía son virtuales en modalidad cloud privada.

VI. OBSERVACIONES PRESENTADAS POR LA EMPRESA EVOLUTION TECHNOLOGIES GROUP

Observación 1: Numeral 1.1 objeto solicitamos a la Entidad aclarar si el servicio SOC NIVEL 2 es solo para prestar servicios profesionales especializados en seguridad informática y SOC "…para la protección de la infraestructura y los activos tecnológicos que soportan los procesos de LA PREVISORA S.A. e implementar las mejoras requeridas para el fortalecimiento de la seguridad informática...", y el SIEM será provisto por la entidad o el SIEM deberá ser provisto por el proponente.

Respuesta: Nos permitimos informar que el SIEM deberá ser provisto por el proponente. Para mayor claridad remítase al numeral 3.3.7.1 desde la pagina 45, donde se explica el alcance del SOC y se incluye en el literal h. la herramienta SIEM.

Observación 2: Numeral 1.9 solicitamos a la entidad por favor aclarar que servicios a nivel nacional tiene, cantidades, fabricantes y Eventos por Segundo generados desde esas ubicaciones.

Respuesta: Nos permitimos informar que la información solicitada se encuentra en el Anexo No 1 pagina 77. Se cuenta con un promedio EPS (Eventos por Segundo) de 1500. El fabricante a nivel de servidores es HP y puede cambiar, a nivel LAN es HP y a nivel WLAN es Cisco.

Observación 3: Numeral 1.9 solicitamos a la entidad por favor aclarar que servicios en nubes privadas tiene, cantidades, fabricantes y Eventos por Segundo generados desde esas ubicaciones.

Respuesta: Nos permitimos informar que próximamente, se tendrán los servicios de IaaS y collocation en nube privada para toda la infraestructura de Datacenter. Se cuenta con un

promedio EPS (Eventos por Segundo) de 1500 sobre las herramientas de seguridad actuales (Firewall, antivirus, proxy, anti-spam, entre otras).

Observación 4: Numeral 1.9 solicitamos a la entidad por favor aclarar que servicios en nubes públicas tiene, cantidades, fabricantes y Eventos por Segundo generados desde esas ubicaciones.

Respuesta: Nos permitimos aclarar que se tienen servicios de nube publica con Salesforce, Litisoft, y Office 365 de Microsoft. Se cuenta con un promedio EPS (Eventos por Segundo) de 1500 sobre las herramientas de seguridad actuales (Firewall, antivirus, proxy, anti-spam, entre otras).

Observación 5: Numeral 3.3.6 solicitamos a la entidad por favor aclarar si para el perfil de Analistas SOC hay que presentar las 4 hojas de vida o solo con una es suficiente.

Respuesta: Nos permitimos aclarar que para un mayor entendimiento se realiza ajuste sobre numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE mediante Adenda N°3

Observación 6: Numeral 3.3.6 solicitamos a la entidad para el rol de Gerente de Servicio incluir las siguientes certificaciones:

a) Cobit 5 Foundation
b) ISO 27001:2013 Certificación Internacional Auditor Interno
c) Certificado a la Protección de Datos Personales

Respuesta: Nos permitimos indicar que se ajusta el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones y este se verá reflejado mediante Adenda N°3

Observación 7: Numeral 3.3.6 solicitamos a la entidad por favor para los Roles de Analistas SOC incluir las siguientes certificaciones para no limitar los recursos que apoyarán la operación:

a) EC-COUNCIL CERTIFIED INCIDENT HANDLER - CIH
b) (CISM) Certified Information Security Manager – ISACA
c) ISO 27001:2013 Certificación Internacional Auditor Líder
d) Auditor interno ISO 20000
e) Itil v3 Foundation
f) Cobit 5 Foundation
g) Implementador Líder ISO 27001:2013
h) Auditor Interno ISO 22301:2019
i) Certificados de Fabricante de la Solución SIEM Propuesta
j) Certificado a la Protección de Datos Personales

Respuesta: Nos permitimos indicar que se ajustó el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones y este se verá reflejado mediante Adenda N°3

Observación 8: Numeral 3.3.6 solicitamos a la entidad por favor para los Roles de Analistas de Seguridad de TI incluir las siguientes certificaciones para no limitar los recursos que apoyarán la operación:

a. EC-COUNCIL CERTIFIED INCIDENT HANDLER - CIH
b. (CISM) Certified Information Security Manager – ISACA
c. ISO 27001:2013 Certificación Internacional Auditor Líder
d. Auditor interno ISO 20000
e. Itil v3 Foundation
f. Cobit 5 Foundation
g. Implementador Líder ISO 27001:2013
h. Auditor Interno ISO 22301:2019
i. Certificados de Fabricante de la Solución SIEM Propuesta
j. Certificado a la Protección de Datos Personales

Respuesta: Nos permitimos indicar que se ajustó el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones y este se verá reflejado mediante Adenda N°3.

Observación 9: Numeral 3.3.6 solicitamos a la entidad por favor para los Roles de Técnico de Seguridad de TI incluir las siguientes certificaciones para no limitar los recursos que apoyarán la operación:

a) NSE 1: Network security Associate
b) ET01 - sophos central overview
c) ET40 - sophos email Potection
d) Scrum Foundation
e) Security Operations Technical Certification (ArcSight)
f) EC-COUNCIL CERTIFIED INCIDENT HANDLER – CIH
g) McAfee ESM 11 Essentials
h) Sophos ET-15
i) McAfee ePo
j) Certificate Endpoint McAfee
k) Nessus Certificate of Proficiency
l) AWS Security Fundamentals
m) AWS Security , Identity and Compliance
n) (CISM) Certified Information Security Manager – ISACA
o) ISO 27001:2013 Certificación Internacional Auditor Líder
p) Auditor interno ISO 20000
q) Itil v3 Foundation
r) Cobit 5 Foundation
s) Implementador Líder ISO 27001:2013

t) Auditor Interno ISO 22301:2019
u) Certificados de Fabricante de la Solución SIEM Propuesta
v) Certificado a la Protección de Datos Personales

Respuesta: Nos permitimos indicar que se ajustó el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones y este se verá reflejado mediante Adenda N°3.

Observación 10: Numeral 3.3.7.1 SERVICIOS DE SOC, ítem h, solicitamos a la entidad por favor aclarar si es posible presentar soluciones que no sean necesariamente en la nube o se encuentra limitado únicamente a soluciones de nube.

Respuesta: Nos permitimos aclarar que la solución puede ser on premise, siempre y cuando el oferente asuma todos los costos de collocotión e interconexión al DataCenter de la entidad, sin ningún recargo al servicio o costo adicional a la entidad. La infraestructura no será provista por la entidad.

Observación 11: Numeral 3.3.7.1 SERVICIOS DE SOC, ítem h, solicitamos a la entidad por favor aclarar si La Previsora proveerá los canales de conexión con el servicio.

Respuesta: Nos permitimos aclarar que el proponente debe proveer absolutamente todo lo necesario para la prestación del servicio.

Observación 12: Numeral 3.3.7.1, ítem a, solicitamos a la entidad por favor indicar el nombre de la herramienta para la gestión de incidentes la cual será suministrada por la entidad, igualmente solicitamos indicar si durante la transición del servicio la entidad realizara capacitación de esta herramienta al personal del contratista.

Respuesta: La herramienta de gestión de incidentes es Aranda, así mismo se indica que es posible realizar trasferencia de conocimiento de uso de la herramienta.

Observación 13: Numeral 3.3.7.1, SERVICIOS DE SOC, ítem h, solicitamos a la entidad indicar si cuenta con licenciamiento en la nube para habilitar API´s para la integración con el SIEM.

Respuesta: Nos permitimos aclarar que el proponente debe proveer absolutamente todo lo necesario para la prestación del servicio en nube.

Observación 14: Numeral 3.3.7.1, ítem j, solicitamos a la entidad aclarar si el almacenamiento solicitado es solo para las configuraciones de las herramientas provistas por el contratista (Backups).

Respuesta: Nos permitimos aclarar que el entendimiento es correcto.

Observación 15: Numeral 3.3.7.1, ítem j, solicitamos a la entidad aclarar el tiempo que requiere de retención de Logs y eventos.

Respuesta: Los respaldos corresponden a las tecnologías que soportan el servicio y que este debe tener como mínimo una retención de mínimo 12 meses, puede contemplar esquemas de backup incrementales full, mensuales periódicos y anuales, los backup puede ser entregados a la entidad para custodia, y una vez el log cumpla los 12 meses y está respaldado puede gestionar la sobre escritura del mismos.

Observación 16: Numeral 3.3.7.1, ítem k, solicitamos a la entidad indicar la cantidad de dominios/LDAP con los que cuenta la entidad.

Respuesta: De manera atenta se informa que se tiene un único dominio.

Observación 17: Numeral 3.3.7.1, ítem c, solicitamos a la entidad indicar si cuenta con un equipo de respuesta a incidentes (Interno).

Respuesta: Nos permitimos aclarar que no se tiene un equipo interno para manejo de respuesta a incidentes interno.

Observación 18: Anexo No. 1, DISPOSITIVOS MONITOREO, solicitamos a la entidad indicar los eventos por Segundo (EPS) que actualmente consume la plataforma.

Respuesta: El promedio de EPS actual es de 1500, pero es de aclarar que esta información solo es una parte de lo que se requiere monitorear. Para mayor claridad por favor remitirse al ANEXO No. 1 DISPOSITIVOS MONITOREO.

Observación 19: Numeral 3.3.7.1 SERVICIOS DE SOC, solicitamos a la Entidad aclarar si la entidad cuenta con un SIEM propio durante la prestación del servicio el cual se deberá integrar con el SIEM brindado por el proponente, en caso de ser así indicar la marca del SIEM de la entidad.

Respuesta: La Previsora S.A no tiene SIEM propio, este es del proveedor saliente y no debe haber integración entre estos.

Observación 20: Numeral 3.3.7.1 SERVICIOS DE SOC, ítem h, solicitamos a la Entidad indicar si cuenta con espacio en el Data Center de la Entidad para ubicar los sensores requeridos por el SIEM del proveedor para el monitoreo o cuentan con espacio en entornos virtuales (Vmware, Hyper V, etc) para implementar los sensores como appliance virtuales.

Respuesta: Nos permitimos aclarar que para un mayor entendimiento se ajusta el numeral 3.3.7.5. HERRAMIENTAS DE GESTIÓN DE LA SOLUCIÓN del pliego de condiciones donde se detalla la información de los parámetros de las plataformas y software a instalar, la cual se verá reflejada mediante Adenda N°3.

Observación 21: Numeral 3.3.7.2, solicitamos a la entidad aclarar si requiere servicios de administración tercerizada de los equipos y servicios de seguridad que posee LA PREVISORA.

Respuesta: Nos permitimos aclarar que el numeral 3.3.7.2 SERVICIOS DE SEGURIDAD ADMINISTRADA completo el alcance en funciones del analista y del técnico de Seguridad TI. Allí se menciona las actividades, integrables, el soporte y gestión de las plataformas de seguridad que posee La Previsora.

Observación 22: Numeral 3.3.7.2.1, numeral i, solicitamos aclarar cuál va a ser el alcance de la revisión del nivel de madurez vs el estándar ISO27001:2013 o NIST800-53, se realizará transversalmente a toda la organización? ¿Solo al área de TI?
a. ¿La Previsora cuenta con un SGSI – ¿Sistema de Gestión de la Seguridad, implementado y operativo?

Respuesta: El alcance es transversal a todos los procesos la organización basado en los lineamientos definidos por el MSPI (El Modelo de Seguridad y Privacidad de la Información) y La Previsora S.A. cuenta con un SGSI implementado y en proceso de mejoramiento a cargo de la Gerencia de Riesgos quien gestiona la Seguridad de la Información.

Observación 23: Numeral 3.3.7.2.1, numeral j, solicitamos aclarar cuál va a ser el alcance de las pruebas a realizar y que tipo de pruebas y resultados esperan obtener.

Respuesta: Nos permitimos aclarar que el alcance de las pruebas y demás factores relacionados a este ítem se definirán en común acuerdo entre La Previsora S.A. y el proponente seleccionado ya que dependen de los controles y reglas que defina para la detección de eventos.

Observación 24: Numeral 3.3.7.2.1, numeral m, solicitamos indicar cuantos documentos tiene como documentación existente y cuál es el esperado de documentos a revisar/actualizar.

Respuesta: Nos permitimos aclarar este ítem será acordado entre las partes cuando quede adjudicado el proceso, sin embargo, algunos de los documentos existentes son: MSPI, Manuales de seguridad, Documentos internos de gestión de contraseñas seguras, entre otros que son requeridos para la seguridad informática de La Previsora.

Observación 25: Numeral 3.3.7.2.1, numeral n, solicitamos aclarar cuantas líneas base tiene desarrolladas e implementadas

Respuesta: Nos permitimos aclarar que se tienen implementadas veintiocho (28) líneas base las cuales pueden incrementar, la implementación actual es sobre el 100% de los sistemas de información productivos de la entidad. Las cantidades y documentos base serán entregados al oferente seleccionado.

Observación 26: Numeral 3.3.7.2.1, numeral n, solicitamos aclarar cuál va a ser el alcance de la medición de cumplimiento de las líneas base.

Respuesta: Nos permitimos aclarar que el alcance está escrito en el mismo literal: "realizar un aseguramiento o medición del cumplimiento de cada una de ellas y entregar informe respectivo de la medición, así como el apoyar a los administradores de TI en la implementación de los parámetros de línea base."

Observación 27: Numeral 3.3.7.2.1, numeral o, solicitamos indicar el alcance de las pruebas de Vulnerabilidad y Hacking Ético, es decir confirmar a cuantas direcciones IP se les realizará Pruebas de Vulnerabilidad (600?) y a cuantas Direcciones IP se les va a realizar Hacking Ético (600?).

Respuesta: Nos permitimos aclarar que la definición detallada de los 600 objetivos se realizara en conjunto con el proveedor seleccionado, el escaneo de vulnerabilidades será sobre los 600 objetivos así como su correspondiente re-test, con una periodicidad de 2 veces al año (primer semestre escaneo de vulnerabilidades, segundo semestre el re-test), para el caso del ethical hacking se efectúa sobre los sistemas de información CORE de negocio que promedian en 20 aplicaciones o según defina la prioridad la Gerencia de Riesgos con una periodicidad de 1 vez al año.

Observación 28: Numeral 3.3.7.2.1, numeral r, solicitamos aclarar cuantos indicadores y métricas de seguridad informática y de ciberseguridad se tienen implementados a los cuales deba realizarse seguimiento:
a. Por favor aclarar la periodicidad de la medición de cada uno.

Respuesta: Nos permitimos aclarar que se tienen alrededor de quince (15) indicadores y su periodicidad de medición es mensual.

Observación 29: Numeral 3.3.7.2.2, solicitamos indicar las plataformas de seguridad que posea la compañía que serán alcance de la operación y soporte por parte del oferente:

a) Tipo de Plataforma
b) Cantidad por cada plataforma
c) Fabricante de cada plataforma
d) Indicar si la plataforma cuenta con licenciamiento y soportes vigentes por parte del fabricante

Respuesta: Nos permitimos aclarar la siguiente información, todas cuentan con licenciamiento vigente, y soporte pode proveedores y directamente con fabricante.

DISPOSITIVO	CANTIDAD	VIDA UTIL /GARANTIAS	FABICANTE
Firewall	4	2023 /soporte fabrica	Fortinet
Antivirus (nube)	1	N/a / soporte fabrica y proveedor	Sophos
OIM	2	N/a / soporte fabrica y proveedor	Oracle

Office365 (seguridad en nube)	1	N/a / soporte fabrica	Microsoft

Observación 30: Numeral 3.3.7.2.2, solicitamos aclarar si serán entregados usuarios administradores de las plataformas de seguridad al oferente para realizar las actividades solicitadas.

Respuesta: Nos permitimos aclarar que efectivamente se entregaran los usuarios con el nivel de permisos necesarios para la gestión en cada plataforma.

Observación 31: Numeral 3.3.7.2.2, solicitamos aclarar si la responsabilidad de las plataformas de seguridad pasará a ser del proveedor o si la responsabilidad de las plataformas será de La Previsora.

Respuesta: Nos permitimos aclarar que la responsabilidad de las plataformas de seguridad a nivel de soporte y gestión pasara a ser responsabilidad del proponente seleccionado.

Observación 32: Numeral 3.3.7.2.2, numeral e, solicitamos aclarar cuantas validaciones de línea base (cantidades) serán parte del servicio.

Respuesta: Nos permitimos aclarar que se debe validar cada línea base con un muestreo aleatorio por cada línea, según el número de sistemas de información productivos en el periodo de medición coordinado en el cronograma.

Observación 33: Numeral 3.3.7.4.1, ítem ACUERDO DE NIVELES DE SERVICIO (ANS) DE GESTION DE INCIDENTES DE SERVICIO solicitamos a la entidad por favor indicar la Volumetría de eventos y/o incidentes de seguridad generados en los últimos 6 meses.

Respuesta: Nos permitimos informar que en promedio mensual se han registrado veinte 20 incidentes de criticidad alta.

Observación 34: Numeral 3.3.7.4.2, ítem ACUERDO DE NIVELES DE SERVICIO (ANS) DE GESTION DE INCIDENTES DE SERVICIO solicitamos a la entidad por favor indicar la Volumetría de requerimientos de servicio generados en los últimos 6 meses.

Respuesta: Nos permitimos informar que en promedio mensual se han registrado noventa (90) requerimientos.

Observación 35: Numeral 3.3.7.5., solicitamos aclarar si la herramienta de monitoreo será provista por La Previsora

Respuesta: Nos permitimos informar que claramente en el numeral 3.3.7.5. se indica que el proponente las debe suministrar, haciendo alusión al objeto de la presente invitación.

Observación 36: Numeral 3.3.8.1, numeral 2, solicitamos aclarar si adicional a los servicios solicitados en el pliego se deben proveer servicios de monitoreo tipo NOC para poder entregar informes de disponibilidad y capacidad de las plataformas de seguridad.

a. Si la respuesta es afirmativa por favor entregar la información detallada de las plataformas para poder realizar un adecuado dimensionamiento de los servicios (Cantidades, Fabricantes, función, etc.)

Respuesta: Nos permitimos informar que La Previsora para este proceso no está solicitando servicios de NOC, por lo que no requiere que se monitoree la disponibilidad o capacidades sobre los sistemas de información, el servicio requerido es de monitoreo de eventos o incidentes de seguridad.

Observación 37: Numeral 3.3.8.1, numeral 4, solicitamos aclarar si el proponente debe proveer una herramienta de Gestión de Usuarios y roles tipo IAM y/o tipo PAM o si la herramienta será provista por La Previsora

Respuesta: Nos permitimos informar que se requiere un informe con acciones, relacionadas a usuarios privilegiados o monitoreo del directorio activo o la plataforma de Gestión de identidades de la entidad.

Observación 38: Numeral 3.3.8.1, numeral 4, solicitamos aclarar la cantidad de usuarios por cada una de las plataformas a monitorear.

Respuesta: Nos permitimos aclarar que los usuarios privilegiados solicitados a monitorear están definidos en el numeral 3.3.7.1 SERVICIOS DE SOC literal “k” están sobre los doscientos (200).

Observación 39: Numeral 3.3.8.2, numeral 22, solicitamos aclarar el alcance de las pruebas de Ingeniería Social solicitadas, cantidad de usuarios y tipos de pruebas esperadas.

Respuesta: Nos permitimos aclarar que el alcance y demás factores relacionados a este ítem se definirán en común acuerdo entre La Previsora S.A. y el proponente seleccionado en las reuniones iniciales.

Observación 40: Numeral 3.3.8.2, numeral 23, solicitamos aclarar la cantidad de usuarios que harán parte de las capacitaciones, y definir la periodicidad de dichas capacitaciones.

Respuesta: Nos permitimos aclarar que la periodicidad esta descrita en el numeral 3.3.8. ENTREGABLES y que la cantidad de usuarios de planta es de setecientos cincuenta y cuatro (754), sin embargo, dependerá de la estrategia de capacitación que se defino ejemplo tipo Webinar, Charla, Video, entre otros.

Observación 41: Numeral 4.1.3.2, para obtener los cincuenta (50) puntos calificables se relaciona el numeral “O” del ítem 3.3.6. 2.1, el numeral 3.3.6 es el Recurso Humano Mínimo Habilitante y no tiene Numeral “O” y el numeral 2.1. es la Presentación de las Propuestas. Por favor aclarar contra que ítem se obtendrán los puntos adicionales.

Respuesta: Nos permitimos aclarar que el numeral correcto es 3.3.7.2.1. para mayor claridad se modificará el numeral 4.1.3.2. con dicha corrección mediante Adenda N°3.

Observación 42. Numeral 4.1.4, solicitamos confirmar si los treinta (30) puntos adicionales se obtienen comprando a nombre de la entidad y entregando a La Previsora las Normas ISO27002:2013, ISO27017 e ISO27018 (diez puntos por cada norma entregada).

Respuesta: Nos permitimos indicar que su entendimiento no es correcto, sin embargo, le informo que el numeral 4.1.4. CERTIFICACIONES ADICIONALES (30) PUNTOS del pliego de condiciones será ajustará mediante Adenda N°3.

Observación 43: Anexo 2 – Recurso Humano Calificable, solicitamos a la entidad por favor para el Rol de Director y/o Coordinador SOC incluir las siguientes certificaciones para no limitar los recursos que apoyarán la operación:

a) EC-COUNCIL CERTIFIED INCIDENT HANDLER - CIH
b) ISO 27001:2013 Certificación Internacional Auditor Líder
c) Auditor interno ISO 20000
d) Itil v3 Foundation
e) Cobit 5 Foundation
f) Implementador Líder ISO 27001:2013
g) Auditor Interno ISO 22301:2019
h) Certificados de Fabricante de la Solución SIEM Propuesta
i) Certificado a la Protección de Datos Personales

Respuesta: Nos permitimos indicar que se ajustó el ANEXO No. 2 RECURSO HUMANO CALIFICABLE del pliego de condiciones, el cual se verá reflejado mediante Adenda N°3, de igual forma se especifica el detalle el numeral OBSERVACIONES GENERALES ítem 3 “Certificaciones del Recurso Humano calificable“ del presente documento.

Observación 44: Anexo 2 – Recurso Humano Calificable, solicitamos a la entidad por favor para el Rol de Experto Coordinador de Grupo de Respuestas a Incidentes incluir las siguientes certificaciones para no limitar los recursos que apoyarán la operación:

a. Auditor interno ISO 20000
b. Itil v3 Foundation
c. Cobit 5 Foundation
d. Implementador Líder ISO 27001:2013
e. Auditor Interno ISO 22301:2019
f. Certificados de Fabricante de la Solución SIEM Propuesta
g. Certificado a la Protección de Datos Personales

Respuesta: Nos permitimos indicar que se ajustó el ANEXO No. 2 RECURSO HUMANO CALIFICABLE del pliego de condiciones, el cual se verá reflejado mediante Adenda N°3, de igual forma se especifica el detalle el numeral OBSERVACIONES GENERALES ítem 3 “Certificaciones del Recurso Humano calificable“ del presente documento.

Observación 45: Anexo 9 - Aspectos Ambientales, solicitamos a la entidad por favor verificar estos aspectos calificables. De acuerdo con nuestra actividad económica no se genera ningún tipo de residuo ambiental, igualmente se realizan conferencias de sensibilización con respecto al medio ambiente.

Respuesta: Se aclara al proponente que todas las compañías de cualquier actividad económica (grandes, medianas, pequeñas, unipersonales, personales, otras) generan algún tipo de impacto al medio ambiente (manejo y disposición de Raees, manejo y disposición adecuada de tóner, ahorro y uso eficiente del agua, ahorro y uso eficiente de energía, uso eficiente de papel, entre otros), razón por la cual son objeto de regulación de las autoridades ambientales. Por lo anterior, Previsora Seguros es una entidad comprometida con el medio ambiente y busca que sus proveedores estén alineados a nuestro sistema como parte interesada.

VII. OBSERVACIONES PRESENTADAS POR LA EMPRESA TIVIT

Observación 1: Solicitamos a la entidad considerar un aplazamiento en el mayor tiempo posible para la entrega de las ofertas en aras de entregar la mejor oferta posible a LA PREVISORA

Respuesta: De manera atenta se informa que su observación fue tenía en cuenta y se ajustó el numeral 1.21 CRONOGRAMA DE LA INVITACIÓN ABIERTA mediante Adenda N° 1 publicada el 18 de mayo de 2021 y Adenda N°2 publica el 25 de mayo de 2021 en la página web de La Previsora.

Observación 2: En el numeral 3.3.2 Experiencia del Proponente en el literal la entidad solicita que se aporte experiencia de contratos que se hayan ejecutado en su totalidad. Solicitamos a la entidad considerar que se pueda aportar experiencia de contratos en ejecución, esta solicitud se realiza teniendo en cuenta que hay contratos que tienen una duración superior a 5 años y se estarían dejando por fuera experiencias de clientes los cuales pueden ofrecer una mejor calificación porque los servicios se están prestando en la actualidad

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE del pliego de condiciones se modificó mediante Adenda N°3.

Observación 3: En el numeral 3.3.2 Experiencia del Proponente en el literal la entidad solicita que se aporte experiencia de contratos que se hayan iniciado durante los últimos 5

años a la presentación de la presente invitación. Solicitamos a la entidad considerar que se pueda aportar experiencia de contratos que hayan iniciado o ejecutado durante los últimos 5 años, lo que va a permitir la pluralidad de oferentes en el presente proceso de contratación.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE del pliego de condiciones se modificó mediante Adenda N°3

Observación 4: - Solicitamos a la entidad considerar un aplazamiento en el mayor tiempo posible para la entrega de las ofertas en aras de entregar la mejor oferta posible a LA PREVISORA

Respuesta: De manera atenta se informa que su observación fue tenía en cuenta y se ajustó el numeral 1.21 CRONOGRAMA DE LA INVITACIÓN ABIERTA mediante Adenda N° 1 publicada el 18 de mayo de 2021 y Adenda N°2 publica el 25 de mayo de 2021 en la página web de La Previsora.

Observación 5: En el numeral 3.3.2 Experiencia del Proponente en el literal la entidad solicita que se aporte experiencia de contratos que se hayan ejecutado en su totalidad. Solicitamos a la entidad considerar que se pueda aportar experiencia de contratos en ejecución, esta solicitud se realiza teniendo en cuenta que hay contratos que tienen una duración superior a 5 años y se estarían dejando por fuera experiencias de clientes los cuales pueden ofrecer una mejor calificación porque los servicios se están prestando en la actualidad

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE del pliego de condiciones se modificó mediante Adenda N°3.

Observación 6: En el numeral 3.3.2 Experiencia del Proponente en el literal la entidad solicita que se aporte experiencia de contratos que se hayan iniciado durante los últimos 5 años a la presentación de la presente invitación. Solicitamos a la entidad considerar que se pueda aportar experiencia de contratos que hayan iniciado o ejecutado durante los últimos 5 años, lo que va a permitir la pluralidad de oferentes en el presente proceso de contratación.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE del pliego de condiciones se modificó mediante Adenda N°3.

Observación 7: Solicitamos a la entidad permitir que las hojas de vida sean aportados únicamente por el proponente adjudicado, lo anterior debido a que al ser perfiles especializados los mismos son requeridos de acuerdo a los contratos firmados para

prestación de este tipo de servicios y no se encuentran normalmente en la nómina de las compañías.

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta, sin embargo, se efectúa modificación sobre el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones mediante Adenda N°3.

Observación 8: Solicitamos a la entidad no solicitar carta de compromiso por parte de los funcionarios que el proponente está postulando en los perfiles, si no una carta de compromiso por parte del Proponente firmada por el Representante Legal de colocar los perfiles en caso de salir favorecidos.

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta, a razón de que el ANEXO No. 4 CARTA DE COMPROMISO es solicitado únicamente para el RECURSO HUMANO CALIFICABLE.

Observación 9: En el numeral 4.1.4 Certificaciones Adicionales, solicitamos a la entidad considerar la eliminación de este requerimiento como calificable debido a que no se estaría presentando una pluralidad de oferentes, al no poderse obtener la totalidad de puntos y haciendo que los oferentes presenten una oferta económica con riesgos financieros para poder cubrir la perdida de este puntaje.

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta, sin embargo, el numeral 4.1.4. CERTIFICACIONES ADICIONALES (30) PUNTOS será modificado mediante Adenda N°3.

Observación 10: - AMBIENTAL

En el Anexo 9 correspondiente a los puntajes otorgados por aspectos ambientales, solicitamos a la entidad que se pueda presentar los certificados de la empresa del grupo del oferente que realiza estos procesos para poder obtener el total de los puntos**.**

Respuesta: Aclaramos al proponente que es viable esta solicitud en caso de presentarse en Unión temporal o en consorcio y no cuando se presenta de manera individual así pertenezca a un grupo empresarial.

Observación 11: -- Se solicita muy cordialmente que sean consideradas válidas las certificaciones otorgadas a cualquiera de las sociedades que hacen parte de un Grupo Empresarial. Nuestra compañía ejecuta este tipo de proyectos con una vista regional. Esto favorece sin lugar a dudas a LA PREVISORA, pues estaría contratando una empresa que aportaría su experiencia y conocimiento global a nivel LATAM (no sólo Colombia). Al limitar la experiencia a empresas nacionales no existiría pluralidad de oferentes

Respuesta: Nos permitimos aclarar que su observación será tenida en cuenta y se modificará en el numeral 3.3.2 EXPERIENCA DEL PROPONENTE del pliego de condiciones mediante Adenda N°3.

VIII. OBSERVACIONES PRESENTADAS POR LA EMPRESA XDC

Observación 1: 3.3.2. EXPERIENCIA DEL PROPONENTE

Con el fin de cumplir con la experiencia mínima habilitante, EL PROPONENTE deberá adjuntar con su propuesta tres (3) certificaciones de contratos suscritos con empresas públicas o privadas nacionales en las que se acredite experiencia de la siguiente forma:

Solicitamos modificar el requerimiento de la siguiente forma:

"Con el fin de cumplir con la experiencia mínima habilitante, EL PROPONENTE deberá adjuntar con su propuesta ***máximo*** *tres (3) certificaciones de contratos suscritos con empresas públicas o privadas nacionales en las que se acredite experiencia de la siguiente forma"*

Respuesta: Nos permitimos indicar que el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE del pliego de condiciones se ajustará mediante Adenda N°3, remitirse al numeral OBSERVACIONES GENERALES ítem 3 "Número de certificaciones de experiencia general" del presente documento.

Observación 2: 5. Los contratos certificados deben haberse ejecutado en su totalidad; no se aceptarán certificaciones de contratos en ejecución

Solicitamos modificar el Numera 5 de la siguiente forma:

5. Los contratos certificados deben haberse ejecutado en su totalidad ***y/o estar en ejecución con mínimo doce (12) meses de ejecución***

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y esta será modificada mediante Adenda N°3

Observación 3: 6. Los contratos certificados deben haber iniciado durante los últimos 5 años a la presentación de la presente invitación.

Solicitamos modificar el Numera 6 de la siguiente forma:

6. Los contratos certificados deben haber iniciado durante los ***últimos 8 años*** a la presentación de la presente invitación

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta, remitirse al numeral I. OBSERVACIONES GENERALES ítem 2 "Tiempo de experiencia del Proponente" del presente documento.

IX. OBSERVACIONES PRESENTADAS POR LA EMPRESA TIGO-UNE

Observación 1: GARANTÍAS DEL CONTRATO: Cumplimiento del contrato, calidad del servicio y responsabilidad civil extracontractual Valor/Porcentaje: Veinte por ciento (20%) del valor del contrato

Se solicita amablemente a la entidad bajar los porcentajes de las pólizas de esta manera: Cumplimiento: 10%, Calidad del Servicio: 10%, Responsabilidad civil extracontractual: 10%, estos son los porcentajes utilizados en el mercado para esta clase de contratos y un mayor cubrimiento acarrearía un mayor costo que elevaría el valor de las ofertas que recibiría su entidad

Respuesta: Las garantías exigidas para el proceso, los amparos y valores, fueron definidas con base en al objeto, valor y naturaleza del contrato, así como en las normas que rigen la materia y a las políticas internas de LA PREVISORA S.A.

Observación 2: GARANTÍAS DEL CONTRATO: Cumplimiento del contrato, calidad del servicio, salarios, prestaciones sociales e indemnizaciones y responsabilidad civil extracontractual

Se solicita respetuosamente al CLIENTE no exigir la firma del representante legal o apoderado de UNE de las pólizas, el certificado y/anexos que hacen parte de la misma que se constituye a favor del CLIENTE (Beneficiario) en la medida que conforme a lo dispuesto en los Artículos 1036 y 1046 del Código de Comercio el contrato de seguro es consensual, bilateral, oneroso, aleatorio y de ejecución sucesiva, por lo cual para su perfeccionamiento solo se requiere del acuerdo de voluntades entre las partes (Tomador y Asegurador) y de manera expresa solamente la firma del Asegurador.

Respuesta: Agradecemos su observación, la misma no será tenida en cuenta ya que si bien el contrato de seguro es consensual, para temas probatorios es necesario que el seguro conste por escrito en una póliza como se establece en el artículo 1046 del Código de Comercio, primordial para este tipo de procesos contar con la prueba de cada actuación que se realice en el mismo.

Observación 3: 1. Una certificación firmada por el Representante Legal del proponente, en la que se indique que cuenta con el Sistema de Gestión de Seguridad y Salud en el Trabajo, de acuerdo con los criterios de valoración dispuestos en la Resolución No. 0312 de 2019 del Ministerio del Trabajo, la que lo modifique o sustituya.

Se solicita amablemente a la entidad permitir que dicha certificación sea presentada con la firma del Responsable del SG-SST.

Respuesta: La certificación del Sistema de Gestión de Seguridad y Salud en el Trabajo de acuerdo con la Resolución 0312 de 2019 solo puede ser firmada por el empleador como lo indica el pliego de condiciones, esto debido a que de conformidad con el Decreto 1072 de 2015 que establece las responsabilidades que tiene el funcionario responsable de Sg-SST

son entre otras, las que se relacionan a continuación y no se encuentra autorizado en firma dicho documento:

O Artículo 2.2.4.6.8., Numeral 3. - El responsable del SG-SST está en la obligación de rendir cuentas internamente de acuerdo a su desempeño como mínimo una vez al año. Esta rendición de cuentas es obligatoria para todos aquellos que tengan responsabilidades en el SG-SST. Además, la rendición se podrá realizar a través de medios escritos, electrónicos, verbales o aquellos que sean considerados por los responsables.

O Artículo 2.2.4.6.8., Numeral 10. El perfil del responsable del SG-SST deberá ser acorde con los establecido con la normatividad vigente y los estándares mínimos que determine el Ministerio del Trabajo. En este caso el responsable deberá,

O Artículo 2.2.4.6.8., Numeral 10.1. - Planear, organizar, dirigir, desarrollar y aplicar el SG-SST y realizar, como mínimo, una vez al año su respectiva evaluación

O Artículo 2.2.4.6.8., Numeral 10.2. - Mantener informada a la alta dirección de la empresa sobre el funcionamiento y los resultados del SG-SST.

O Artículo 2.2.4.6.8., Numeral 10.3. - Promover la participación de todos los miembros de la empresa en la implementación del SG-SST.

O Artículo 2.2.4.6.12., Numeral 5 -El responsable del SG-SST también tiene como obligación, junto al empleador, la firma del plan de trabajo anual en seguridad y salud en el trabajo.

O Artículo 2.2.4.6.29. Parágrafo. y Artículo 2.2.4.6.31. Parágrafo -El responsable del SG-SST debe ser notificado sobre la auditoría de cumplimiento del SG-SST y los resultados de la revisión por la alta dirección para adelantar las medidas preventivas, correctivas o de mejora en la empresa.

O Artículo 2.2.4.6.32., Parágrafo 2 -En la investigación de incidentes, accidentes de trabajo y enfermedades laborales el empleador deberá formar un equipo investigador. Éste estará compuesto por el responsable del SG-SST, el jefe inmediato o supervisor del trabajador accidentado, un representante del Comité Paritario o Vigía de Seguridad y Salud en el Trabajo, quienes deberán realizar todo lo correspondiente a la investigación del suceso.

Observación 4: Copia de la política de Seguridad y Salud en el Trabajo firmada por el Gerente o Representante Legal del proponente

Se solicita amablemente a la entidad permitir que dicha Política sea presentada con la firma del Responsable del SG-SST.

Respuesta: La política de SST solo puede ser firmada por el representante legal como lo indica el pliego de condiciones, esto por ser un requisito normativo del Decreto 1072 de 2015 (Decreto único del Sector Trabajo) en su artículo 2.2.4.6.12. – Inciso 1 que dice textualmente “la política y los objetivos de la empresa en materia de seguridad y salud en el trabajo SST, deben ser firmados por el empleador.”

Observación 5: Indicadores que se deben acreditar

La Entidad debe tener en cuenta que, de no procederse con la modificación, se estaría restringiendo la participación de proponentes que cuentan con la solidez financiera suficiente, seriedad y reconocimiento en el sector para ejecutar el contrato, vulnerando así el principio de la libre concurrencia y no permitiendo que la Entidad obtenga ofertas favorables para el servicio a prestar.

INDICADORES SOLICITADOS EN EL PLIEGO DE CONDICIONES PROCESO

INDICADORES EXIGIDOS	
Índice de Liquidez (Razón Corriente)	Mayor o igual a 1
Capital de Trabajo	Mayor o igual al 30% del presupuesto oficial de la contratación.

OBSERVACIÓN: Se pide respetuosamente a la Entidad la modificación de estos indicadores financieros para que sean establecidos de la siguiente forma:

INDICADORES EXIGIDOS	
Índice de Liquidez (Razón Corriente)	Mayor o Igual a 0.9
Capital de trabajo	No solicitar este indicador

Solicitamos tener en cuenta que, de acuerdo con lo establecido por el Manual de Requisitos Habilitantes de Colombia Compra Eficiente, el indicador de capital de trabajo no se considera un indicador principal de la capacidad financiera, es decir, es un indicador adicional y utilizado excepcionalmente. Las Entidades Estatales pueden establecer indicadores adicionales a los establecidos en el numeral 3 del artículo 10 del Decreto 1510 de 2013, **solo en aquellos casos en que sea necesario por las características del objeto a contratar, la naturaleza o complejidad del Proceso de Contratación.** (resaltado fuera de texto)

Como verificación de los Requisitos Habilitantes en los procesos de contratación que para el efecto ha expedido la Entidad Colombia Compra Eficiente se ha indicado que: "La capacidad Financiera requerida en un proceso de contratación debe ser adecuada y proporcional a la naturaleza y al valor del contrato. En consecuencia, la Entidad Estatal debe establecer los requisitos de Capacidad Financiera con base en su conocimiento del sector relativo al objeto del Proceso de Contratación y de los posibles Oferentes" para lo cual y teniendo en cuenta que Colombia Compra eficiente a partir del estudio del sector ha identificado los indicadores financieros que serían aplicables, por ejemplo en los acuerdos marco de precios de BPO, nube privada, nube pública o conectividad no se ha solicitado el capital de trabajo como indicador financiero, amablemente solicitamos la eliminación del capital de trabajo como indicador y requisito habilitante.

Es importante anotar que la modificación expuesta no genera riesgos para la Entidad y permite la participación de proponentes que cuentan con la experiencia y capacidad financiera suficiente para dar cumplimiento a las obligaciones contractuales, garantizando la seguridad y la continuidad del servicio a la Entidad, garantizado además por la experiencia en el mercado y en el cumplimiento de aquella exigida para el proceso, lo cual da seguridad técnica, jurídica y operacional en la ejecución del contrato. Tal es el Caso de UNE EPM TELECOMUNICACIONES ha venido ejecutando el contrato cumpliendo con todas las obligaciones de él derivadas.

Adicionalmente, en el sector particular de operadores de telecomunicaciones, si se observa el comportamiento de las grandes empresas, que pudieran llegar a ser proveedores y que lo han sido en proyectos similares, se evidencia que su capacidad financiera y organizacional obedece a una realidad del sector que implica la inversión en proyectos e infraestructura que podrán llegar a afectar sus indicadores, pero que en ningún momento comportan su falta de capacidad para cumplir con sus obligaciones.

Como referente al establecer indicadores financieros se puede tomar en cuenta que Colombia Compra Eficiente como la entidad encargada de "diseñar, organizar y celebrar los acuerdos marco de precios y demás mecanismos de agregación de demanda" definió dentro de los acuerdos marco para los Servicios de conectividad, nube privada y nube pública los siguientes indicadores, los cuales reflejan de la manera más acertada la realidad del sector.

Conectividad

Indicador	Índice requerido
Índice de liquidez	Mayor o igual a 0,6
Índice de endeudamiento	Menor o igual a 86%
Razón de cobertura de intereses	Mayor o igual a 0
Utilidad operacional sobre activos	Mayor o igual a 0%
Utilidad operacional sobre patrimonio	Mayor o igual a 0%

Fuente: Colombia Compra Eficiente - Tablas del acuerdo marco de precios para los servicios de conectividad.

Nube Publica 2019

Indicador	Índice requerido
Índice de liquidez	Mayor o igual a 0,55
Índice de endeudamiento	Menor o igual a 0,85
Razón de cobertura de intereses	Mayor o igual a 0
Utilidad operacional sobre activos	Mayor o igual a 0%
Utilidad operacional sobre patrimonio	Mayor o igual a 0%

Fuente: Colombia Compra Eficiente - Tablas del acuerdo marco de precios para los servicios de Nube Publica.

Nube Privada 2019

Indicador	Índice requerido
Índice de liquidez	Mayor o igual a 0,55
Índice de endeudamiento	Menor o igual a 0,82
Razón de cobertura de intereses	Mayor o igual a 0
Utilidad operacional sobre activos	Mayor o igual a 0%
Utilidad operacional sobre patrimonio	Mayor o igual a 0%

Fuente: Colombia Compra Eficiente - Tablas del acuerdo marco de precios para los servicios de Nube Privada.

Frente a nuestra solicitud vale la pena tener en cuenta lo indicado por la Corte Constitucional en sentencia C-713/09, según la cual:

El derecho a la igualdad de oportunidades, aplicado a la contratación de la administración pública, se plasma en el derecho a la libre concurrencia u oposición, según el cual, se garantiza la facultad de participar en el trámite concursal a todos los posibles proponentes que tengan la real posibilidad de ofrecer lo que demanda la administración. La libre concurrencia, entraña, la no discriminación para el acceso en la participación dentro del proceso de selección, a la vez que posibilita la competencia y oposición entre los interesados en la contratación. Consecuencia de este principio es el deber de abstención para la administración de imponer condiciones restrictivas que impidan el acceso al procedimiento de selección, ...puesto que ellas impiden la más amplia oportunidad de concurrencia y atentan contra los intereses económicos de la entidad contratante, en razón a que no permiten la consecución de las ventajas económicas que la libre competencia del mercado puede aparejar en la celebración del contrato. (...)

En el mismo sentido, el Consejo de Estado se ha pronunciado sobre el principio de transparencia, la igualdad y la libre concurrencia, estableciendo que las condiciones y previsiones de las entidades en los procesos de contratación no deben conducir a la exclusión de potenciales oferentes y deben garantizar la selección objetiva con el fin de no restringir la participación y obtener la mejor oferta para el servicio a contratar.[1]

De acuerdo con lo señalado, solicitamos la modificación de los indicadores financieros en el proyecto de pliego de condiciones.

Respuesta: Al respecto, nos permitimos informar que la Capacidad Financiera definida por Previsora se basó en el estudio de mercado que se realizó en el cual se contemplaron aspectos como: objeto del contrato, tiempo del contrato, valor del contrato, complejidad y forma de pago del mismo, buscando así que el proveedor tenga la liquidez y solidez necesarias para llevar a cabo el desarrollo del contrato, por lo cual los niveles solicitados para los indicadores establecidos permiten evaluar dicha condición. Adicionalmente, se tuvo en cuenta la información financiera registrada en SuperSociedades de empresas dedicadas a actividades relacionadas con el objeto del contrato.

Así mismo, para la definición de estos indicadores se tuvo en cuenta lo señalado en la forma de pago del contrato y plazo de ejecución del contrato del pliego, ya que los proponentes deberán contar con una capacidad financiera mínima para cumplir con el desarrollo de las actividades que deberán ser asumidas por ellos por el tiempo de ejecución del contrato.

Por lo tanto y con el fin de garantizar los fines de la contratación, se establecieron los indicadores financieros solicitados en la invitación, buscando así una idoneidad financiera de los proponentes, a través de la evaluación de varias dimensiones como lo son capital de trabajo, nivel de endeudamiento y patrimonio, los cuales evalúan aspectos diferentes que en conjunto garanticen liquidez para la ejecución satisfactoria del objeto del contrato.

Teniendo en cuenta lo anterior y considerando que los indicadores solicitados se ajustan a las necesidades de Previsora, se mantiene la capacidad financiera definida inicialmente.

Observación 6: Negociación entre las partes al ANEXO 11 MODELO MINUTA DEL CONTRATO

Teniendo en cuenta el principio de buena fe contractual y la conmutatividad que debe existir entre las partes, se solicita que, en caso de ser beneficiado con la adjudicación, las

condiciones contractuales puedan ser revisadas y negociadas entre ambas partes con el fin de buscar acuerdos que favorezcan a ambos contratantes.

Respuesta: Teniendo en cuenta que en efecto es un contrato consensual, donde prima la buena fe contractual entre las partes, sin embargo, se deben tener en cuenta las reglas y condiciones del proceso establecidas en el pliego de condiciones, las cuales se constituyen en ley para las partes y que son formalizadas con la suscripción del contrato.

Observación 7: Inclusión de cláusula al ANEXO 11 MODELO MINUTA DEL CONTRATO

De suscribirse un contrato se solicita incluir la siguiente cláusula por tratarse de un contrato negociado entre empresas: Inaplicación del Régimen de Protección de Usuarios y Régimen de Calidad. Al presente contrato, no le es aplicable el régimen de Protección de Usuarios consagrado en la Resolución de la Comisión de Regulación de Comunicaciones –CRC-5111 de 2017, ni el régimen de calidad para los servicios de telecomunicaciones establecido en la Resolución de la Comisión de Regulación de Comunicaciones - CRC 5165 de 2017 de, ni demás normas que modifiquen o sustituyan las citadas resoluciones; dado que las características del servicio y la red y la totalidad de las condiciones técnicas, económicas y jurídicas han sido negociadas y pactadas por mutuo acuerdo y así lo declaramos las partes.

Respuesta: Agradecemos su observación, sin embargo, la solicitud de incluir la cláusula en los términos propuestos no resulta pertinente, por cuanto no es posible que las partes acuerden no cumplir con normativas que establecen requisitos legales para la prestación de este tipo de servicios.

Observación 8: Modificación a la CLÁUSULA NOVENA. TERMINACIÓN Y CAUSALES DE TERMINACIÓN ANTICIPADA

Se solicita que, en la causal de terminación por parte de la Previsora de manera unilateral, se reconozca al contratista el valor de la inversión realizada para la prestación del servicio para el tiempo inicialmente contratado, y los demás costos en que deba incurrir el contratista como causa de la terminación anticipada de la relación contractual.

Respuesta: Agradecemos su observación, pero la misma no será tenida en cuenta

Observación 9: Modificación a la CLÁUSULA DÉCIMA CUARTA. CESIÓN Y SUBCONTRATACIÓN

Se solicita amablemente darle alcance bilateral a esta cláusula en el sentido de indicar que el contrato no podrá cederse por ninguna de las partes sin la autorización previa y escrita de la otra parte

Respuesta: No se acepta la solicitud de modificación de las cláusulas de la minuta publicada, teniendo en cuenta que la minuta publicada es un formato que contiene las principales estipulaciones contractuales que se pactan con nuestros proveedores, y que cualquier tipo de modificación, será concertada de manera directa con el proveedor seleccionado.

Observación 10: Eliminación o modificación de la CLÁUSULA TRIGÉSIMA PRIMERA. CLÁUSULA PENAL

Se solicita amablemente la eliminación de ésta cláusula pues los servicios incluyen un anexo que prevé el cumplimiento de ANS, se solicita revisar conjuntamente este punto pues en el caso que los eventos contarían con penalidades especificas por incumplimiento de ANS. De no ser posible su eliminación les solicitamos que nos informen los criterios objetivos para la determinación del valor de 20%, toda vez que, consideramos que el valor es excesivo y por dicha razón solicitamos la disminución de este a un valor objetivo, por otro lado la aplicación de las presentes disposiciones debe ser sometida a decisión jurisdiccional, su imposición no debe ser a través de un procedimiento impuesto por una de las partes ya que no es equilibrado paar el contrato que una parte se reserve la facultad de determinar si existe o no un incumplimiento, pues su imposición de manera unilateral vulnera el principio de igualdad.

Respuesta: Agradecemos su observación, pero la misma no será tenida en cuenta, y la cláusula trigésima primera se mantiene sin modificación. Los ANS están diseñados para sancionar algunas de las operaciones y servicios específicos del contrato, en tanto, la cláusula penal surge del incumplimiento general o de cualquier condición del contrato. El valor del 20% es el establecido por las políticas internas de LA PREVISORA S.A. para este tipo de procesos, y el proceso lo que busca es generar espacios de arreglo directo, antes de someter la controversia a la jurisdicción correspondiente., Sin embargo, el procedimiento señalado en la cláusula puede ser sujeto de revisión de las partes.

Observación 11: Modificación a la CLÁUSULA TRIGÉSIMA CUARTA. INDEMNIDAD

Se solicita amablemente modificar en el sentido de indicar que todo daño o perjuicio debe ser plenamente probado, en la vía judicial, además todo tipo de responsabilidad objetiva se encuentra proscrita. Adicionalmente se solicita que se limite la indemnidad al 10% del valor del contrato y al plazo del mismo.

Respuesta: No se aceptan las solicitudes de modificación de las cláusulas de la minuta publicada, teniendo en cuenta que la minuta publicada es un formato que contiene las principales estipulaciones contractuales que se pactan con nuestros proveedores, y que cualquier tipo de modificación, será concertada de manera directa con el proveedor seleccionado. Adicionalmente, no se aceptan limitaciones a la responsabilidad.

Observación 12: 3.1.4 GARANTÍA DE SERIEDAD DE LA PROPUESTA "Deberá estar firmado por quien expide la garantía y por el representante legal del proponente."

Se solicita respetuosamente a la entidad no exigir la firma del representante legal o apoderado de UNE de las pólizas, el certificados y/anexos que hacen parte de la misma que se constituye a favor de la Previsora en la medida que conforme a lo dispuesto en los Artículos 1036 y 1046 del Código de Comercio, el contrato de seguro es consensual, bilateral, oneroso, aleatorio y de ejecución sucesiva, por lo cual para su perfeccionamiento solo se requiere del acuerdo de voluntades entre las partes (Tomador y Asegurador) y de manera expresa solamente la firma del Asegurador.

Respuesta: Agradecemos su observación, la misma no será tenida en cuenta ya que si bien el contrato de seguro es consensual, para temas probatorios es necesario que el seguro conste por escrito en una póliza como se establece en el artículo 1046 del Código de Comercio, primordial para este tipo de procesos contar con la prueba de cada actuación que se realice en el mismo.

Observación 13: RECURSO HUMANO MINIMO HABILITANTE. Un (1) Gerente de Servicio que estará durante el tiempo total del contrato (Implementación y operación)

Teniendo en cuenta la duración del contrato y las variaciones que puede tener la compañía con respecto a su personal, solicitamos respetuosamente se eliminación de la obligación de permanencia, toda vez que el oferente lo que debe garantizar es la prestación del servicio bajo las condiciones contratadas más allá de la permanencia o no de una persona en la ejecución del mismo.

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta a razón de que la entidad no limita ni solicito que el recurso o una persona especifico permaneciera o no durante todo la ejecución del servicio, ya que es un factor que no se puede controlar, lo que se solicita es que el ROL de Gerente de Servicio este durante el tiempo de ejecución del servicio, ya que es el rol responsable de gerenciar, atender al cliente, hacer seguimientos al servicio y ANS pactado, independientemente si hay cambio a futuro del recurso por otro.

X. OBSERVACIONES PRESENTADAS POR LA EMPRESA SOFTTEK

Observación 1:

1. **Según Solicitud en el Numeral RECURSO HUMANO** CALIFICABLE Solicitamos que el Requerimiento sea Modificado así;

* Un (1) Especialista de Seguridad: Solicitamos ***DEDICACIÓN NO PORCENTUAL***, pero **SI PARCIAL.**

* Un (1) Director del SOC: Solicitamos dedicación **NO PORCENTUAL**, pero **SI PARCIAL.** Adicional se considere tener en cuenta importante requerir como Mínimo 8 años de experiencia profesional de los cuales al menos Seis (6) años sean en Gerencia de proyectos y/o consultoría de seguridad de la información. Especialización o Maestría en seguridad de la información y al menos cinco (5) de las siguientes certificaciones y/o acreditaciones técnicas:

- -ABCP (Associate business Continuity Professional)
- -Auditor Líder ISO 22301 del 2012.
- -Auditor Líder de Implementación ISO 27001 del 2013
- -Certified Data Provacy Solutiones Engineer
- -Certified Archimate 3 Foundation
- -CISM "Certified Information Security Management"
- -COBIT Foundation
- -ISO 27032 del 2017
- -ISO 31000 del 2018
- -ITIL Fundation Version 3 o 4.

* Un (1) EXPERTO COORDINADOR DE GRUPO DE RESPUESTAS A INCIDENTES: Solicitamos dedicación **NO PORCENTUAL**, pero **SI PARCIAL**

Respuesta: Nos permitimos aclarar que:

Punto 1: Con respecto al Especialista SOC confirmamos que su observación no será tenida en cuenta

Punto 2: Para el recurso director SOC se confirma que se modificará la dedicación en Adenda N°3, por otro lado, a nivel de experiencia por ser un calificable no se efectuaran cambios.

Punto 3: Para el recurso experto coordinador de grupo de respuestas confirmamos que su observación será tenida en cuenta y este se verá modificado en Adenda N°3

Observación 2:

2. En la Solicitud de **HOJAS DE VIDA Según Numeral *EQUIPO MINIMO* - Solicitamos que el Requerimiento sea Modificado así;**

*En la Solicitud del Gerente de Proyecto o Gerente de Servicio: sea modificada la Dedicación a **PARCIAL Y que no sea PORCENTUAL**. Y en relación a las certificaciones sugeridas sean allegadas en documentos de control de cambios.

*En la Solicitud en el perfil de los dos (2) Analistas SOC Dedicados con 3 años de experiencia: Solicitamos a la entidad que Dichos Analistas cuenten con al menos dos (2) años de experiencia

* En la Solicitud en el perfil de los dos (2) Analistas de Seguridad TI con 5 años de experiencia: solicitamos que Dichos Analistas cuenten con al menos con un (1) años de experiencia, Adicional se Considere que los perfiles sea Uno remoto, y el otro recurso de forma presencial.

Respuesta: Nos permitimos aclarar que:

Punto 1: Para el gerente de servicio se tiene en cuenta la observación y se efectúa modificación al pliego de condiciones mediante Adenda N°3

Punto 2: Para los analistas de SOC se confirma que su observación no será tenida en cuenta a razón de que este parámetro se encuentra descrito sobre el pliego de condiciones en el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE

Punto 3: Para los analistas de seguridad se confirma que su observación no será tenida en cuenta, sin embargo, se solicita validar el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE para mayor claridad.

Observación 3:

3. En Solicitud Referente A Certificado Por Parte Del Fabricante Solicitamos Modificar O Ampliar El Texto Así: (Incluir Y/O Su Mayorista)

CERTIFICADO POR PARTE DEL FABRICANTE

EL PROPONENTE deberá adjuntar con su propuesta la certificación del producto (SIEM) como canal autorizado o expedida por el fabricante y/o su mayorista o su representante en Colombia. Esta certificación deberá estar vigente al momento de la presentación de la oferta y firma del contrato.

Respuesta: Agradecemos su observación y se ajustará el numeral 3.3.4. del pliego de condiciones mediante Adenda N°3

Observación 4: FINANCIERA

4. En solicitud de INDICADORES FINANCIEROS Y MÉTODO DE EVALUACIÓN. Solicitamos A la Entidad Considere Modificar los Indicadores Financieros y el Procedimiento de Evaluación de ofertas.

*Nivel de Endeudamiento se solicitaba menor o igual al 59%.

Respuesta: Al respecto, nos permitimos informar que la Capacidad Financiera definida por Previsora se basó en el estudio de mercado que se realizó en el cual se contemplaron aspectos como: objeto del contrato, tiempo del contrato, valor del contrato, complejidad y forma de pago del mismo, buscando así que el proveedor tenga la liquidez y solidez necesarias para llevar a cabo el desarrollo del contrato, por lo cual los niveles solicitados para los indicadores establecidos permiten evaluar dicha condición. Adicionalmente, se tuvo en cuenta la información financiera registrada en SuperSociedades de empresas dedicadas a actividades relacionadas con el objeto del contrato.

Así mismo, para la definición de estos indicadores se tuvo en cuenta lo señalado en la forma de pago del contrato y plazo de ejecución del contrato del pliego, ya que los proponentes deberán contar con una capacidad financiera mínima para cumplir con el desarrollo de las actividades que deberán ser asumidas por ellos por el tiempo de ejecución del contrato.

Por lo tanto y con el fin de garantizar los fines de la contratación, se establecieron los indicadores financieros solicitados en la invitación, buscando así una idoneidad financiera de los proponentes, a través de la evaluación de varias dimensiones como lo son capital de

trabajo, nivel de endeudamiento y patrimonio, los cuales evalúan aspectos diferentes que en conjunto garanticen liquidez para la ejecución satisfactoria del objeto del contrato.

Teniendo en cuenta lo anterior y considerando que los indicadores solicitados se ajustan a las necesidades de Previsora, se mantiene la capacidad financiera definida inicialmente.

Observación 5:

5. En solicitud al PUNTO REFERENTE A MEMBRESIA FIRST.

Solicitamos a la entidad considerar retirar dicha Membresía o solicitar como opción ISO 27001, y que esta se habilitada para obtener los mismos puntos por MEMBRESIA FIRST o POR ISO27001.

"CERTIFICACIÓN o MEMBRESIA (30 Puntos)

Se asignarán el puntaje de 30 puntos, a la propuesta que allegue la membresía de FIRST

(Forum of Incident Response and Security Teams) como empresa ó acreditar mediante certificación ISO 27001 donde se especifique el alcance de esta certificación enfocada a la administración del servicio de correlación de eventos de seguridad, comprendiendo su detección, análisis, clasificación, reporte, y recomendación de acción inmediata, a través de la solución SIEM gestionada por el centro de operaciones de seguridad SOC."

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta a razón de:

1. La certificación ISO27001 es un requisito habilítate al presente proceso solicitado en el numeral 3.3.3 CERTIFICACIONES PROVEEDOR
2. La membresía first es un deseable para la entidad generando un nivel de confianza ya que les permite a los proveedores contar con un apoyo adicional para dar respuesta de manera más efectiva ante los riesgos que se puedan presentar, tendrían acceso a un banco de información y buenas prácticas, herramientas, comunicaciones, noticias y tendencias de seguridad y ciberseguridad.

Observación 6:

6. En solicitud de MÉTODO DE EVALUACIÓN. Solicitamos A la Entidad Considere Modificar los el Procedimiento de Evaluación de ofertas.

*Forma de calificación económica: Solicitamos a la Entidad Considerar como Procedimiento de Evaluación Económica: **Media Geométrica con presupuesto oficial** y NO por regla de tres inversas (que solo busca dar puntaje al menor valor) ...

Respuesta: Agradecemos su observación pero la misma no será tenida en cuenta.

XI. OBSERVACIONES PRESENTADAS POR LA EMPRESA SINERGY & LOWELLS

Observación 1. En solicitud de INDICADORES FINANCIEROS Y MÉTODO DE EVALUACIÓN. Solicitamos A la Entidad Considere Modificar los Indicadores Financieros y el Procedimiento de Evaluación de ofertas.

Observación: Se Solicita Comedidamente a la entidad sea Considerado Disminuir el Valor de este a Menor o igual a 0.57 % Teniendo en cuenta que este indicador es el cual determina el GRADO DE ENDEUDAMIENTO en la estructura de FINANCIACIÓN del proponente. A mayor índice de endeudamiento, mayor es la probabilidad del proponente de NO PODER CUMPLIR CON

SUS PASIVOS, sugerimos ajustar este indicador de acuerdo con los indicadores de las empresas de este sector que contiene el SIREM.

Respuesta: Al respecto, nos permitimos informar que la Capacidad Financiera definida por Previsora se basó en el estudio de mercado que se realizó en el cual se contemplaron aspectos como: objeto del contrato, tiempo del contrato, valor del contrato, complejidad y forma de pago del mismo, buscando así que el proveedor tenga la liquidez y solidez necesarias para llevar a cabo el desarrollo del contrato, por lo cual los niveles solicitados para los indicadores establecidos permiten evaluar dicha condición. Adicionalmente, se tuvo en cuenta la información financiera registrada en SuperSociedades de empresas dedicadas a actividades relacionadas con el objeto del contrato.

Así mismo, para la definición de estos indicadores se tuvo en cuenta lo señalado en la forma de pago del contrato y plazo de ejecución del contrato del pliego, ya que los proponentes deberán contar con una capacidad financiera mínima para cumplir con el desarrollo de las actividades que deberán ser asumidas por ellos por el tiempo de ejecución del contrato.

Por lo tanto y con el fin de garantizar los fines de la contratación, se establecieron los indicadores financieros solicitados en la invitación, buscando así una idoneidad financiera de los proponentes, a través de la evaluación de varias dimensiones como lo son capital de trabajo, nivel de endeudamiento y patrimonio, los cuales evalúan aspectos diferentes que en conjunto garanticen liquidez para la ejecución satisfactoria del objeto del contrato.

Teniendo en cuenta lo anterior y considerando que los indicadores solicitados se ajustan a las necesidades de Previsora, se mantiene la capacidad financiera definida inicialmente

Observación 2. en el Tema de Ponderacion Solicitamos a la Entidad Considere la asignación de los 30 puntos, a la propuesta que allegue la membresía de FIRST (Forum of Incident Response and Security Teams) como empresa ó acreditar mediante certificación ISO 27001 donde se especifique el alcance de esta certificación enfocada a la administración del servicio de correlación de eventos de seguridad, comprendiendo su detección, análisis, clasificación, reporte, y recomendación de acción inmediata, a través de la solución SIEM gestionada por el centro de operaciones de seguridad SOC."

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta a razón de:

1. La certificación ISO27001 es un requisito habilítate al presente proceso solicitado en el numeral 3.3.3 CERTIFICACIONES PROVEEDOR
2. La membresía first es un deseable para la entidad generando un nivel de confianza ya que les permite a los proveedores contar con un apoyo adicional para dar respuesta de manera más efectiva ante los riesgos que se puedan presentar, tendrían acceso a un banco de información y buenas prácticas, herramientas, comunicaciones, noticias y tendencias de seguridad y ciberseguridad.

Observación 3. Según solicitud de HOJAS DE VIDA Según Numeral 4.1. EQUIPO MINIMO - Solicitamos que el Requerimiento sea Modificado así;

Observación: En la Solicitud de Un (1) Gerente de Proyecto o Gerente de Servicio: Solicítanos sea considerado modificar el tema de la Dedicación a PARCIAL Y que este NO sea requerido como PORCENTUAL. Adicional que este cuente con certificaciones en documentos control de cambios.

En la Solicitud de los dos (2) Analistas de Seguridad TI con 5 años de experiencia: Solicitamos a la Entidad considerar solicitar con dos (2) años de experiencia; adicional considerar Requerir que un Recurso sea en modalidad REMOTA y el Otro en Forma PRESENCIAL

Respuesta: Nos permitimos indicar que:

Punto 1: Con respecto al Gerente de servicio su observación será tenida en cuenta y el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE será modificará mediante Adenda N°3

Punto 2: Para los analistas de seguridad se está solicitando dos años de experiencia y en el detalle descrito en el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE DOS (2) ANALISTAS DE SEGURIDAD TI se encuentra el detalle de la experiencia y la forma de operación.

Observación 4. Según solicitud en Referencia a MEMBRESIA FIRST.

Observación: Solicitamos a la entidad considerar modificar dicha Membresía o solicitar Ampliar el Requerimiento a MEMBRESIA FIRST Y/O ISO 27001, y que esta misma se considerada para obtener los mismos puntos por MEMBRESIA FIRST o POR ISO27001. “CERTIFICACIÓN o MEMBRESIA (30 Puntos)

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta a razón de:

1. La certificación ISO27001 es un requisito habilítate al presente proceso solicitado en el numeral 3.3.3 CERTIFICACIONES PROVEEDOR
2. La membresía first es un deseable para la entidad generando un nivel de confianza ya que les permite a los proveedores contar con un apoyo adicional para dar respuesta de manera más efectiva ante los riesgos que se puedan presentar,

tendrían acceso a un banco de información y buenas prácticas, herramientas, comunicaciones, noticias y tendencias de seguridad y ciberseguridad.

Observación 5. Según Solicitud en el Numeral 1. 4.2. RECURSO HUMANO CALIFICABLE Solicitamos que el Requerimiento sea Modificado asi;

* Un (1) Especialista de Seguridad: Solicítanos sea considerado modificar el tema de la Dedicación a PARCIAL Y que este NO sea requerido como PORCENTUAL.

* Un (1) Director del SOC: Solicítanos sea considerado modificar el tema de la Dedicación a PARCIAL Y que este NO sea requerido como PORCENTUAL

Adicional se considere tener en cuenta requerir como HABILITACION como Mínimo 9 años de experiencia profesional de los cuales al menos 7 años sean en Gerencia de proyectos y/o consultoría de seguridad de la información. Especialización o Maestría en seguridad de la información

- -Auditor Líder ISO 27001 del 2013.
- Auditor Líder de Implementación ISO 27001 del 2013
- COBIT Foundation
- Líder de implementación ISO 270032 del 2017
- ISO 27032 del 2017
- ISO 31000 del 2018
- ITIL Fundation Version 3 o 4.
- ITIL Expert V3

* Un (1) EXPERTO COORDINADOR DE GRUPO DE RESPUESTAS A INCIDENTES: Solicítanos sea considerado modificar el tema de la Dedicación a PARCIAL Y que la Dedicación no La Requieran como PORCENTUAL

Respuesta: Nos permitimos aclarar que:

Punto 1: Para el Especialista de Seguridad se aclarar que su observación no será tenida en cuenta.

Punto 2: Para el director del SOC se ajustará numeral ANEXO No. 2 RECURSO HUMANO CALIFICABLE del pliego de condiciones y este se verá modificado en Adenda N°3

Punto 3: Para el Experto Coordinador de Grupo de Respuestas a Incidentes se ajustará numeral ANEXO No. 2 RECURSO HUMANO CALIFICABLE del pliego de condiciones y este se verá modificado en Adenda N°3

Observación 6. sobre solicitud de Certificado Por Parte Del Fabricante Solicitamos Considerar Modificar O Ampliar El Requerimiento Así: Y/O Su Mayorista

CERTIFICADO POR PARTE DEL FABRICANTE

EL PROPONENTE deberá adjuntar con su propuesta la certificación del producto (SIEM) como canal autorizado o expedida por el fabricante y/o su mayorista o su representante en Colombia. Esta certificación deberá estar vigente al momento de la presentación de la oferta y firma del contrato.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.4. CERTIFICADO POR PARTE DEL FABRICANTE será modificado mediante Adenda N°3

Observación 7. En solicitud de MÉTODO DE EVALUACIÓN. Solicitamos A la Entidad Considere Modificar el Procedimiento de Evaluación de ofertas.

*Forma de calificación económica: Solicitamos a la Entidad Considerar como Procedimiento de Evaluación Económica: Media Geométrica con presupuesto oficial y NO por regla de tresinversa (que solo busca dar puntaje al menor valor

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta a razón de que la entidad busca siembre el mejor costo beneficio, garantizando la reducción de costos.

XII. OBSERVACIONES PRESENTADAS POR LA EMPRESA NEWNET SA

Observación 1: Solicitamos a la entidad aclarar en el numeral 3.3.4. CERTIFICADO POR PARTE DEL FABRICANTE; si la certificación del producto SIEM, como canal autorizado, es válida que sea emitida a través del mayorista quien certifica al proveedor o es el proveedor quien debe ser partner directo de la marca/producto

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.4. CERTIFICADO POR PARTE DEL FABRICANTE del pliego de condiciones será modificado mediante Adenda N°3

Observación 2: En el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE, se menciona que el proponente deberá adjuntar con su propuesta las hojas de vida y las certificaciones de experiencia del equipo de trabajo; pero más adelante en este mismo numeral también se menciona que el proponente seleccionado deberá allegar a la PREVISORA S.A cinco (5) días después de la publicación del acta de adjudicación las hojas de vida, las certificaciones de experiencia y certificaciones de estudio de los recursos mínimos con los cuales ejecutará el servicio.

Por lo anterior no es claro si la documentación del equipo de trabajo mínimo habilitante se debe presentar junto con la presente propuesta o esta documentación se deberá entregar después de adjudicado el contrato, agradecemos a la entidad realizar esta aclaración

Respuesta: Nos permitimos aclarar que para mayor entendimiento se realizara ajuste del numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones mediante Adenda N°3

Observación 3: En el numeral 3.3.7.1 SERVICIOS DE SOC ítem a, se menciona que la gestión de incidentes se debe realizar a través de la herramienta entregada por LA PREVISORA S.A., solicitamos a entidad informar cual es la herramienta con la cuentan y si se realizará transferencia de conocimiento al personal de parte del proveedor para el manejo de la misma.

Respuesta: Nos permitimos indicar que actualmente contamos con Aranda. Así mismo es posible realizar trasferencia de conocimiento al personal que está en el servicio.

Observación 4: En el numeral 3.3.7.1 SERVICIOS DE SOC ítem e, solicitamos a la entidad informar sobre cuantos dominios se deberá realizar el monitoreo de marca que se solicita en este ítem, a fin de realizar un correcto dimensionamiento para este requerimiento.

Respuesta: Nos permitimos indicar que la cantidad de marcas (1), dominios web (hasta 5), dominios de correo (1), Aplicaciones (las comunes tipo WEB), Presencia en redes sociales (Las más reconocidad en el mercado Facebook, Instagram, Twitter, etc).

Observación 5: Se permitirá la instalación/implementación de hardware o software en los centros de datos de la entidad, en caso de que el servicio propuesto por el futuro proveedor sea en modalidad on-premise o hibrida y requiera el despliegue de un equipo servidor/sensor para la recolección de los Logs?

Respuesta: Nos permitimos aclarar que se permitirá la implementación e instalación respectiva, sin embargo, para un mayor entendimiento se adiciona sobre el numeral 3.3.7.5. HERRAMIENTAS DE GESTIÓN DE LA SOLUCIÓN el detalle de este parámetro el cual se verá reflejado sobre Adenda N°3.

Observación 6: En el numeral 3.3.7.2.1. ANALISTAS DE SEGURIDAD TI. ítem c: Realizar análisis del software libre a demanda, solicitamos a la entidad estimar cuantos análisis promedio se deberán realizar anualmente

Respuesta: Nos permitimos aclarar que los análisis de software se solicitan a demanda y estos dependerán de la necesidad de La Previsora, de igual forma el análisis solicitado es para confirmar si el software puede llegar a generar alguna vulnerabilidad a nivel interno, mala reputación, limitaciones o incumplimiento normativo de derechos de autor.

Observación 7: En el numeral 3.3.7.2.1. ANALISTAS DE SEGURIDAD TI ítem j: Se requiere aclarar a qué tipo de pruebas se hace referencia en este ítem, solicitamos a la entidad ampliar la información de este requerimiento

Respuesta: Nos permitimos aclarar que el alcance de las pruebas y demás factores relacionados a este ítem se definirán en común acuerdo entre La Previsora S.A. y el proponente seleccionado ya que dependen de los controles y reglas que defina para la detección de eventos.

Observación 8: En el numeral 3.3.7.2.1. ANALISTAS DE SEGURIDAD TI ítem ítem o: Aseguramiento y gestión de vulnerabilidades: Solicitamos informar a la entidad ¿A cuántas aplicaciones se debe realizar el análisis de código aquí solicitado?

Respuesta: Nos permitimos indicar que el análisis de código se solicita a demanda y estos dependerán de la necesidad de La Previsora. En el numeral descrito se solicita un mínimo de 2 análisis por año.

Observación 9: En el numeral 3.3.7.2.2. TECNICO DE SEGURIDAD TI: ítem a: Se solicita a la entidad aclarar qué tipo de políticas, normas o directrices están esperando que se definan e implementen en este ítem, y con base a que estándar o buena práctica o normativa.

Respuesta: Nos permitimos aclarar que el objetivo de este literal es que con la experiencia del oferente se sugieran mejoras a las políticas o procedimientos actuales de seguridad en la entidad, sobre el numeral 1.2 ALCANCE DEL OBJETO donde se nombran estándares como ISO 27001, 27002, 27017, 27018 y las regulaciones de la Superintendencia Financiera de Colombia relacionadas con seguridad Informática y ciberseguridad en Colombia vigentes y futuras.

Observación 10: En el numeral 4.1.1. RECURSO HUMANO ADICIONAL CALIFICABLE 400 PUNTOS, solicitamos a la entidad informar si estos recursos deberán prestar sus servicios desde en un esquema presencial (oficinas de la entidad), o remoto?

Respuesta: Nos permitimos aclarar que el servicio de estos recursos pueden ser remoto y dependiendo de lo ofertado **se de**finiría en reuniones iniciales con el proponente seleccionado si se requiere semipresencial, de igual forma se ajusta el ANEXO No. 2 RECURSO HUMANO CALIFICABLE del pliego de condiciones modificado en Adenda N°3

Observación 11: En el ANEXO No. 1 DISPOSITIVOS MONITOREO, solicitamos a la entidad detallar si la infraestructura tecnológica a monitorear se encuentra centralizada en su totalidad en la sede principal en la ciudad de Bogotá, a fin de entender si el dimensionamiento del servicio debe contemplar alcance de ciertos equipos en otras ciudades.

Respuesta: Nos permitimos aclarar que como se indicó en el pliego de condiciones, el alcance del monitoreo es a nivel nacional por el tema de redes y dispositivos de comunicaciones, para el tema de monitoreo de servicios de sistemas de información como servidores, bases de datos, entre otros estos están centralizados actualmente en el centro de datos de la previsora y serán trasladados a TRIARA al Datacenter de Claro S.A.

Observación 12: Pregunta del numeral 3.3.2. EXPERIENCIA DEL PROPONENTE ¿Se aceptan experiencias de contratos extranjeros?

Respuesta: Nos permitimos aclarar que su observación será tenida en cuenta y se modificara en el numeral 3.3.2 EXPERIENCA DEL PROPONENTE mediante Adenda N°3.

Observación 13: En el Anexo 1. Del documento se incluye el inventario con un total 592 dispositivos en la red física más 1,575 dispositivos conectados por VPN para un total de 2,167 (con 5% de crecimiento estimado), no obstante, se puede limitar el uso a los 592 dispositivos de la red física segmentando este número de IPs?

Respuesta: Nos permitimos indicar que no es clara su observación, pero confirmamos que todos los dispositivos descritos en el ANEXO No. 1 DISPOSITIVOS MONITOREO deberán estar contemplados en el monitoreo solicitado.

XIII. OBSERVACIONES PRESENTADAS POR LA EMPRESA MULTISOFT

Observación 1: Se solicita amablemente a la entidad que nos indique del **ANEXO No. 1 DISPOSITIVOS MONITOREO,** ¿Cuántos EPS (Eventos por Segundo) generan todas las fuentes de SIEM?

Respuesta: Nos permitimos informar que el promedio de EPS actual es de 1500, pero es de aclarar que esta información solo es una parte de lo que se requiere monitorear. Para mayor claridad por favor remitirse al ANEXO No. 1 DISPOSITIVOS MONITOREO

XIV. OBSERVACIONES PRESENTADAS POR LA EMPRESA IT-SS

Observación 1:

El Pliego de condiciones menciona en el numeral 3.3.5. CLASIFICACION DE LA SOLUCION SIEM lo siguiente: ***"EL PROPONENTE deberá adjuntar la calificación y/o certificación donde se confirme que la solución de SIEM se encuentra en el cuadrante de Gartner/Forrester o líder reconocido en aplicación de ciberseguridad para el último año referido."*** Entendemos que motores de información para el procesamiento de grandes volúmenes de datos que aparezcan en el cuadrante mágico de Garner, posicionados en alguno de los referentes del mercado de seguridad, y demuestren capacidades de analítica de datos de seguridad y Logs, correlación de eventos de seguridad e identificación de posibles incidentes, que integren funciones de Machine Learning, UBA-UEBA, como lo hace una solución SIEM; cumplen con el requerimiento mencionado.

Respuesta: Nos permitimos indicar que su entendimiento es correcto

Observación 2:

El Pliego de condiciones menciona en el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE para el GRUPO DE (4) CUATRO ANALISTAS SOC – REMOTO que se debe acreditar al menos una de las siguientes certificaciones

- CSA -Certified SOC Analyst - CompTIA
- ECIH – EC-Council Certified Incident Handler - EC-Council
- CNFE – Network Forensic Investigator - Mile2
- CHFI – Computer Hacking Forensic Investigator - EC-Council
- CEH - Certified Ethical Hacker - EC-Council
- CRISC - Certified in Risk and Information Security Control -ISACA
- CPTE – Certified Pentester Engineer - Mile2
- CPTIA – CREST Practitioner Threat Intelligence Analyst – CompTIA

Entendiendo que las certificaciones requeridas se relacionan con manejo de incidentes, investigación forense, y en general ciber seguridad, solicitamos amablemente permitir certificaciones similares como CDFE – Certified Digital Forensic Examinator, CIHE – Certified Incident Handling Engineer otorgadas por Mile2; así como la certificación CSFPC – Cyber Security Foundation Professional Certificate otorgado por Certiprof; las cual es muestran las capacidades de los analistas de SOC frente a los desafíos de seguridad y el manejo de incidentes; por lo cual sugerimos amablemente la siguiente modificación

Se debe acreditar al menos (1) de las siguientes certificaciones o su equivalente:

- CSA -Certified SOC Analyst - CompTIA
- ECIH – EC-Council Certified Incident Handler - EC-Council
- CNFE – Network Forensic Investigator - Mile2
- CHFI – Computer Hacking Forensic Investigator - EC-Council
- CEH - Certified Ethical Hacker - EC-Council
- CRISC - Certified in Risk and Information Security Control -ISACA
- CPTE – Certified Pentester Engineer - Mile2
- CPTIA – CREST Practitioner Threat Intelligence Analyst – CompTIA
- CDFE – Certified Digital Forensic Examinator - Mile2
- CIHE – Certified Incident Handling Engineer - Mile2
- CSFPC – Cyber Security Foundation Professional Certificate - Certiprof

Respuesta: Nos permitimos indicar que se ajustó el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones y este se verá modificado mediante Adenda N°3.

Observación 3:

El Pliego de condiciones menciona en el numeral 3.3.7.1 SERVICIOS DE SOC como obligaciones generales del servicio lo siguiente ***"Analizar e implementar mecanismos que permitan a la entidad verificar diferentes fuentes de información tales como sitios web, blogs y redes sociales, esto con el propósito de identificar posibles ataques cibernéticos contra la entidad."*** De lo anterior se entiende que se realizará el Monitoreo sobre la Marca de La Previsora, solicitamos amablemente aclarar cuantas marcas o dominios tiene LA PREVISORA para realizar el respectivo monitoreo.

Respuesta: Nos permitimos indicar que la cantidad de marcas (1), dominios web (hasta 5), dominios de correo (1), Aplicaciones (las comunes tipo WEB), Presencia en redes sociales (Las más reconocidas en el mercado Facebook, Instagram, Twitter, etc).

Observación 4:

El Pliego de condiciones menciona en el numeral 3.3.7.1 SERVICIOS DE SOC como obligaciones generales del servicio lo siguiente ***"Notificación proactiva de amenazas proporcionando soluciones y estrategias de mitigación, tomar medidas para proteger los sistemas y redes afectados o amenazados por la actividad de intrusos y desarrollar otras estrategias de respuesta o solución alternativa, con escenarios de crisis contra ataques dirigidos como DDoS o amenazas avanzadas"*** Solicitamos amablemente aclarar:

- A qué se refiere La Previsora y qué espera de la frase: ***proporcionando soluciones***
- ***Tomar medidas para proteger los sistemas y redes afectados o amenazados por la actividad de intrusos y desarrollar otras estrategias de respuesta o solución alternativa, con escenarios de crisis contra ataques dirigidos como DDoS o amenazas avanzadas*** se refiere a las actividades que ejecutaría el Analista de Seguridad de TI?

Respuesta: Nos permitimos aclarar que:

Punto 1: La frase proporcionar soluciones hace referencia a buscar métodos o alternativas para la mitigación de una amenaza y/o ataque.

Punto 2: Con respecto al punto de tomar medidas sobre los sistemas, queremos aclarar que el servicio esperado por La Previsora con esta invitación es que sea un SOC nivel 2 "Análisis y respuesta", el proveedor deberá estar en la capacidad de analizar y tomar las medidas necesarias para la mitigación ante un ataque ya sea de manera manual o automatizada.

Observación 5:

El Pliego de condiciones menciona en el numeral 3.3.8. ENTREGABLES que se deberán contemplar informes durante la vigencia del contrato, entre el cual se menciona el siguiente ***"Informe con acciones, relacionadas a usuarios privilegiados, este deberá contener el resultado del monitoreo de todos los usuarios que realicen acciones de:***
a. borrado, inserción y actualización y/o modificación de la información.
b. Modificación de permisos sobre los usuarios.
c. Creación de nuevos usuarios con permisos de administrador o con altos privilegios." Solicitamos amablemente aclarar si el informe será realizado de acuerdo con el monitoreo realizado o esperan que los analistas de seguridad de TI o el Técnico de seguridad de TI ejecuten actividades sobre los usuarios privilegiados.

Respuesta: Nos permitimos aclarar que el informe solicitado deberá estar acorde a la información del monitoreo realizado, esto con el fin de validar todos los cambios a nivel de usuario privilegiados relacionados en los sistemas de información de la compañía.

Observación 6:

El Pliego de condiciones menciona en el numeral 3.3.8. ENTREGABLES que ***"Como parte de las obligaciones específicas del contrato, se deberán contemplar los siguientes documentos e informes los cuales deberán ser entregados para cumplir con auditorias,"*** Entendiendo que los profesionales adicionales tendrán una dedicación específica para el proyecto, solicitamos amablemente aclarar cuál es la disponibilidad que espera La Previsora para estos profesionales.

Respuesta: Nos permitimos aclarar que para un mayor entendimiento para el numeral 3.3.7.2 SERVICIOS DE SEGURIDAD ADMINISTRADA la disponibilidad es del 100% y dedicación 8x5 con los cuales se cumpliría el numeral 3.3.8 ENTREGABLES, para el servicio del SOC la disponibilidad es de 7X24.

Observación 7:

El Pliego de condiciones menciona en el numeral 4.1.1.2. OBLIGACIONES ESPECIALES RESPECTO DEL RECURSO HUMANO ADICIONAL CALIFICABLE que ***"deberá contar con disponibilidad de tiempo permanente cuando sea requerido por LA PREVISORA S.A para incidencias altas."*** Entendiendo que los profesionales adicionales tendrán una dedicación específica para el proyecto, solicitamos amablemente aclarar cuál es la disponibilidad que espera La Previsora para estos profesionales.

Respuesta: Nos permitimos aclarar que la dedicación mínima fue ajustada en el ANEXO No. 2 RECURSO HUMANO CALIFICABLE sobre la Adenda N°3, la disponibilidad de estos recursos dependerá del nivel de criticidad del incidente que se pueda presentar ante la materialización de un riesgo, entiéndase 7X24 ante un incidente crítico, exceptuando el recurso de Especialista de Seguridad TI que si deberá tener una disponibilidad del 50%.

Observación 8:

El Pliego de condiciones menciona en el numeral 4.1.4. CERTIFICACIONES ADICIONALES (30) PUNTOS que ***"Se asignará puntaje de diez (10) puntos por cada una de las siguientes certificaciones adicionales para un máximo de treinta (30) puntos. ISO/IEC 27002:2013, ISO27017, ISO27018"*** Entendiendo que técnicamente se certifica únicamente el estándar ISO/IEC 27001 para los Sistemas de Gestión de Seguridad de la Información, siendo los demás estándares guías para la implementación de controles; solicitamos a La Previsora revisar y modificar el requerimiento toda vez que no es posible para algún proveedor presentar las certificaciones mencionadas; en su lugar solicitamos amablemente requerir la Certificación PCI:DSS; la cual, aunque se relaciona con el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago, evidencia un alto compromiso y nivel de aseguramiento de los servicios ofertados.

Respuesta: Nos permitimos indicar que para un mayor entendimiento se realizará modificación el numeral 4.1.4 CERTIFICACION ADICIOANLES (30) PUNTOS en Adenda N° 3

Observación 9:

El ANEXO No. 2 RECURSO HUMANO CALIFICABLE indica para el DIRECTOR Y/O COORDINADOR SOC que debe acreditar ***Especialización o Maestría en Seguridad de la Información o sus equivalentes y al menos dos de las certificaciones***, solicitamos amablemente lo siguiente:

- Permitir la acreditación de posgrados en Arquitecturas de Tecnologías de Información, toda vez que se requiere experiencia en arquitectura de seguridad y los profesionales con este posgrado cuentan con excelentes en estrategias de TI que apoyan las responsabilidades del Director del SOC.
- Incluir Certificaciones como CPTE – Certified Pentester Engineer, CIHE – Certified Incident Handling Engineer otorgadas por Mile2; así como la certificación LCSPC – Lead Cybersecurity Professional Certificate otorgado por Certiprof; las cuales muestra la capacidad y conocimiento del profesional para las funciones solicitadas.

Respuesta: Nos permitimos aclarar que:

Punto 1: Su observación será tenida en cuenta sobre el Anexo N°3 RECURSO HUMANO CALIFICABLE sobre Adenda N°3

Punto 2: se ajustara ANEXO No. 2 RECURSO HUMANO CALIFICABLE del pliego de condiciones, este se verá modificado mediante Adenda N°3, de igual forma se especifica el detalle el numeral OBSERVACIONES GENERALES ítem 3 "Certificaciones del Recurso Humano calificable" del presente documento.

XV. OBSERVACIONES PRESENTADAS POR LA EMPRESA OLIMPIAIT

Observación 1:

Requerimiento: Certificación ISO 27001. Esta norma permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

Solicitud: Se solicita la entidad incluir dentro de los requerimientos que los procesos o procedimientos del SOC se encuentren certificados para esta norma, como una garantía de que se cubran las actividades propias del SOC y no otro tipo de funciones ajenas al proceso.

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta.

Observación 2:

Requerimiento: EL PROPONENTE deberá adjuntar la calificación y/o certificación donde se confirme que la solución de SIEM se encuentra en el cuadrante de Gartner/Forrester o líder reconocido en aplicación de ciberseguridad para el último año referido.

Solicitud: 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.

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta.

Observación 3:

Requerimiento: Servicio de monitorización inteligente de eventos de seguridad en modalidad 7x24. La gestión de incidentes se debe realizar a través de la herramienta entregada por LA PREVISORA S.A. El servicio ofrecido deberá alinearse a las políticas, procesos y procedimientos definidos por LA PREVISORA S.A.

Solicitud: Se solicita a la entidad indicar la cantidad de incidentes de seguridad que se presentan en un mes en la Previsora.

Respuesta: Nos permitimos aclarar que se tiene un promedio mensual de 20 incidentes, con las plataformas actuales, es de aclarar que estos en su mayoría con criticidad media y baja.

Observación 4:

Requerimiento: Analizar e implementar mecanismos que permitan a la entidad verificar diferentes fuentes de información tales como sitios web, blogs y redes sociales, esto con el propósito de identificar posibles ataques cibernéticos contra la entidad. Lo anterior alineado a la Circular Externa 008 de la Superfinanciera de Colombia.

Solicitud: Se solicita a la entidad aclarar si está solicitando en el requerimiento un servico de monitoreo de marca, si es correcto por favor indicar, cantidad de marcas, dominios web, dominios de correo, aplicaciones, presencia en redes sociales.

Respuesta: Nos permitimos indicar que es correcto su entendimiento, la cantidad de marcas (1), dominios web (hasta 5), dominios de correo (1), Aplicaciones (las comunes tipo WEB), Presencia en redes sociales (Las más reconocida en el mercado Facebook, Instagram, Twitter, etc).

Observación 5:

Requerimiento: Notificación proactiva de amenazas proporcionando soluciones y estrategias de mitigación, tomar medidas para proteger los sistemas y redes afectados o amenazados por la actividad de intrusos y desarrollar otras estrategias de respuesta o solución alternativa, con escenarios de crisis contra ataques dirigidos como DDoS o amenazas avanzadas.

Solicitud: Se solicita a la entidad indicar si cuenta con soluciones para proteccion de ataques de DDoS y amenzas avanzadas, que se integren a la solucion SIEM y asi poder establecer la estrategia de mitigacion frente a estos ataques.

Respuesta: Nos permitimos indicar que los dispositivos de seguridad con los que cuenta La Previsora como firewall y antivirus de nueva generación cuentan con protección de DDoS y amenazas avanzadas y se pueden integrar con el SIEM para la mitigación de estos ataques.

Observación 6:

Requerimiento: f. Dominio de herramientas de monitoreo tales como Nessus, Acutenix, burp suite, entre otras.

Solicitud: Se solicita a la entidad aclarar si también en el servicio se incluye solicitud de análisis de vulnerabildades, o sólo los recursos deben conocer las herramientas.

Respuesta: Nos permitimos indicar que sobre el numeral 3.3.7.2.1. ANALISTAS DE SEGURIDAD TI se detallan todas las obligaciones que deben realizar los recursos, incluidos los análisis de vulnerabilidades.

Observación 7:

Requerimiento: n. Líneas base de seguridad: Modificar, actualizar e implementar las líneas base de seguridad o buenas prácticas en los sistemas de información de LA PREVISORA S.A e identificadas por la Gerencia de TI. Adicionalmente, se deberá realizar un aseguramiento o medición del cumplimiento de cada una de ellas y entregar informe respectivo de la medición, así como el apoyar a los administradores de TI en la implementación de los parámetros de línea base. Esta ejecución de líneas base se debe realizar de manera anual. Estas deben regirse con los estándares internacionales (eje CIS) y/o de fabricantes según corresponda.

Solicitud: Se solicita a la entidad indicar si la entidad tiene una herramienta o solución para el establecimiento y configuracion de líneas bases.

Respuesta: Nos permitimos aclarar que La Previsora no cuenta con una herramienta para el establecimiento de líneas base, estas se efectúan actualmente de manera manual.

Observación 8:

Requerimiento: o. Aseguramiento y gestión de vulnerabilidades: Anualmente se deberán generar dos (2) análisis de vulnerabilidad, Ethical Hacking y penetración a la plataforma tecnológica, a los que se deberá elaborar una matriz de seguimiento de los hallazgos encontrados y los planes de remediación y/o mitigación, el cual deberá ser gestionado por EL PROVEEDOR. Para cada uno de los análisis se debe contemplar todos los dispositivos activos de LA PREVISORA S.A los cuales se estiman en un promedio de 600 objetivos. Por otra parte, se debe contemplar análisis de vulnerabilidades a demanda adicionales para nuevas aplicaciones y/o solicitudes internas. Se solicita contemplar por lo menos 2 análisis de código por año y el respectivo Re-test de cada uno de los análisis efectuados, los análisis de penetración a las herramientas se solicita estimación de por lo menos 3 por año.

Solicitud: Se solicita a la entidad indicar para el análisis de código la cantidad de líneas para cada aplicación.

Respuesta: Nos permitimos aclarar que para los análisis de código se desconoce el número de líneas de código que pueda tener una aplicación y/o validación ya que estos se efectúan a demanda y en su mayoría son servicios nuevos

Observación 9:

Requerimiento: Según el documento **ANEXO No. 1 DISPOSITIVOS MONITOREO**

Windows Servers

Network Firewalls

Solicitud: Se solicita a la entidad indicar cuántos servidores de directorio activo tienen, se solicita a la entidad indicar para los firewall la marca y modelo de estos, adicionalmente indicar cuántos son internos y cuántos perimetrales.

Solicitud: Se solicita a la entdad indicar los dispositivos a monitorear en cuántos datacenter o ubicaciones se encuentran.

Respuesta: Nos permitimos indicar que:

Punto 1: La Previsora S.A cuenta con 5 servidores de directorio activo

Punto 2: La Previsora S.A cuenta con cuatro (4) firewalls, dos perimetrales, uno contingente y uno interno y la referencia es Fortigate 500e

Punto 3: Como se indicó en el pliego de condiciones, el alcance del monitoreo es a nivel nacional por el tema de redes y dispositivos de comunicaciones, para el tema de monitoreo de servicios de sistemas de información como servidores, bases de datos, entre otros estos están centralizados actualmente en el centro de datos de la previsora y serán trasladados a TRIARA al Datacenter de Claro S.A.

Observación 10:

Recurso Humano Mínimo Habilitante

a) Respecto al (1) GERENTE DE SERVICIO, se solicita a la Entidad esa modificación: Demostrar experiencia profesional de **nueve (9) años** y específica como Gerente de Servicio de tres (3) años durante los últimos cuarenta y ocho (48) meses, mínimo en dos (2) dos proyectos de Seguridad y/o Ciberseguridad. Esta debe ser demostrada con certificaciones laborales, emitidas por la empresa en la que labora o por las empresas donde desarrollo proyectos.

b) Respecto al (1) GERENTE DE SERVICIO, se solicita a la Entidad: incluir dentro de las certificaciones adicionales la de PMP (Project Manager Professional).

c) Respecto al GRUPO DE (4) CUATRO ANALISTAS SOC – REMOTO, se solicita a la Entidad, incluir dentro de las certificaciones adicionales, las siguientes: Lead Cybersecurity Manager ISO 27032:2012 y Auditor Interno o Auditor lider en ISO 27001:2013.

d) Respecto a los DOS (2) ANALISTAS DE SEGURIDAD TI, se solicita a la Entidad, incluir dentro de las certificaciones adicionales, las siguientes: Auditor Interno o Auditor líder en ISO 27001:2013 y CCNA Security; así como, posgrado Especialización en Seguridad Informática o a fines.

Respuesta: Nos permitimos aclarar que:

Punto a) Para el Gerente de Servicio su observación no será tenida en cuenta.

Punto b) No es posible adicionar esta certificación, ya que lo que se solicita es que el Gerente de Servicio cuente con conocimientos de seguridad Informática/ Seguridad de la Información o Ciberseguridad y la PMP es una certificación de Gerencia de Proyectos a nivel general

Respuesta c) Respecto a las certificaciones, se ajustará numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones y este se verá modificado en Adenda N°3

Respuesta d) Respecto a las certificaciones, se ajustará numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones y este se verá modificado en Adenda N°3

Observación 11:

11. Recurso humano adicional calificable

a) Respecto al DIRECTOR Y/O COORDINADOR SOC, se solicita a la Entidad, incluir dentro de las certificaciones adicionales, las siguientes: Auditor Interno o Auditor Líder ISO 27032:2012, Auditor Interno o Auditor Líder en ISO 27001:2013, PMP.

b) Respecto al DIRECTOR Y/O COORDINADOR SOC, se solicita a la Entidad, permitir al menos una de las certificaciones técnicas descritas. Así como, Demostrar Mínimo seis (6) años de experiencia profesional y cuatro (4) años de experiencia especifica.

c) Respecto al EXPERTO COORDINADOR DE GRUPO DE RESPUESTAS A INCIDENTES, se solicita a la Entidad, permitir al menos **(1) una** de las certificaciones técnicas descritas.

Respuesta: Nos permitimos aclarar que:

Punto a) Respecto a las certificaciones, se ajustara ANEXO No. 2 RECURSO HUMANO CALIFICABLE del pliego de condiciones, este se verá modificado en Adenda N°3, de igual forma se especifica el detalle el numeral OBSERVACIONES GENERALES ítem 3 “Certificaciones del Recurso Humano calificable“ del presente documento
Punto b) su observación no será tenida en cuenta

Punto c) su observación no será tenida en cuenta

Observación 12:

Observaciones Generales

Solicitud: Se solicita la entidad incluir dentro de los requerimientos para evitar una indiponibilidad del servicio, se solicite que el SOC deba mantener la infraestructura para el servicio en un centro de datos principal con categoria TIER IV y su datacenter secundario o de contingencia con categoria TIER III.

Solicitud: Se solicita a la entidad que el centro de datos donde esté alojada la infraestructura se encuentre en Colombia como una forma de apoyo a la industria nacional.

Solicitud: Se solicita a la entidad incluir en los requerimientos del proceso que el proponente tenga el nivel más alto de membresía con el fabricante de la solucion SIEM dispuesta para el servicio.

Respuesta: Nos permitimos aclarar que sus observaciones no serán tenidas en cuenta, a razón de que son limitaciones y no permitiría la pluralidad de oferentes en el proceso.

XVI. OBSERVACIONES PRESENTADAS POR LA EMPRESA CBTSEC (CROSS BORDER TECHNOLOGY SAS)

Observación 1:

Observación No. 1: en el numeral **3.3.2. EXPERIENCIA DEL PROPONENTE** la entidad solicita lo siguiente:

> **3.3.2. EXPERIENCIA DEL PROPONENTE**
>
> Con el fin de cumplir con la experiencia mínima habilitante, EL PROPONENTE deberá adjuntar con su propuesta tres (3) certificaciones de contratos suscritos con empresas públicas o privadas nacionales en las que se acredite experiencia de la siguiente forma:

Solicitamos respetuosamente a la entidad que se permita acreditar la experiencia con mínimo seis (6) certificaciones de contratos.

Lo anterior garantiza la pluralidad de oferentes y no afecta la presentación del servicio.

Respuesta: Nos permitimos indicar que el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE del pliego de condiciones se ajustará mediante Adenda N°3, remitirse al numeral OBSERVACIONES GENERALES ítem 3 “Número de certificaciones de experiencia general” del presente documento.

.

Observación 2:

Observación No. 2: en el numeral **3.3.2. EXPERIENCIA DEL PROPONENTE** la entidad solicita lo siguiente:

> 1. El objeto, actividades u obligaciones sean iguales o similares al de la presente invitación. Entendiéndose por similar que consista en la prestación de servicios administrados de seguridad y/o servicios de SOC.

Solicitamos respetuosamente a la entidad aclarar si la experiencia puede también acreditarse mediante certificaciones con objeto, actividades u obligaciones similar a seguridad de la información o seguridad informática.

Lo anterior garantiza la pluralidad de oferentes y no afecta la presentación del servicio.

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta ya que dentro de los servicios administrados de seguridad está inmersa la gestión SOC de seguridad de la información, ciberseguridad y/o seguridad informática.

Observación 3:

Observación No. 3: en el numeral **3.3.2. EXPERIENCIA DEL PROPONENTE** la entidad solicita lo siguiente:

> **6.** Los contratos certificados deben haber iniciado durante los últimos 5 años a la presentación de la presente invitación.

Solicitamos respetuosamente a la entidad que los contratos puedan haber iniciado durante los últimos ocho (8) años a la presentación de la invitación.

Lo anterior garantiza la pluralidad de oferentes y no afecta la prestación del servicio.

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta, remitirse al numeral I. OBSERVACIONES GENERALES ítem 2 "Tiempo de experiencia del Proponente" del presente documento.

Observación 4:

Observación No. 4: se solicita a la entidad aclarar si las hojas de vida del equipo mínimo se deben entregar junto con la propuesta o el proponente adjudicatario debe entregarlas.

Respuesta: Nos permitimos informar que para un mayor entendimiento se realizara ajuste sobre Adenda N°3 sobre el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE.

Observación 5:

Observación No. 5: en el numeral **1.41.3. Recurso humano mínimo habilitante,** la entidad solicita lo siguiente para el perfil de gerente de servicio:

Perfil Profesional
Profesional en Ingeniería (Sistemas, Electrónico, telecomunicaciones o carreras afines), con especialización y/o maestría en Seguridad Informática, Seguridad de la información o seguridad en las TIC.

Solicitamos respetuosamente a la entidad que el profesional pueda tener especialización y/o maestría en gerencia de proyectos y/o gerencia de ingeniería.

Adicionalmente, se solicita lo siguiente para el perfil:

Experiencia
Demostrar experiencia profesional de diez (10) años y específica como Gerente de Servicio de tres (3) años durante los últimos cuarenta y ocho (48) meses, mínimo en dos (2) dos proyectos de Seguridad y/o Ciberseguridad. Esta debe ser demostrada con certificaciones laborales, emitidas por la empresa en la que labora o por las empresas donde desarrollo proyectos.

Solicitamos respetuosamente a la entidad que la experiencia específica pueda estar acreditada tambien dentro de los 10 años de experiencia profesional.

Adicionalmente, que sea en proyectos de seguridad de la información y/o ciberseguridad y/o seguridad informática.

Lo anterior garantiza la pluralidad de oferentes y no afecta la prestación del servicio.

Respuesta: Nos permitimos aclarar que:

Punto 1: Con respecto al Gerente de Servicio su observación no será tenida en cuenta ya que se requiere que el recurso tenga experiencia y conocimiento en servicios de seguridad informática, ciberseguridad o seguridad de la información.

Punto 2: Con respecto al tiempo de experiencia nos permitimos indicar que la misma se encuentra inmersa en la profesional.

Punto 3: Para lo relacionado a Proyectos de seguridad, La Previsora contempla seguridad a nivel general incluido seguridad informática y de la información.

Observación 6:

Observación No. 6: en el numeral **1.41.3. Recurso humano mínimo habilitante,** la entidad solicita lo siguiente para el perfil de analista SOC:

Perfil Profesional y Experiencia
Profesionales Titulados de Ingeniería de sistemas, telecomunicaciones o carreras afines con mínimo dos (2) años de experiencia como Analista de eventos de seguridad informática, dominio de herramientas de monitoreo y conocimiento de controles de seguridad informática, normas y regulaciones vigentes.
Certificaciones
Se debe acreditar al menos una (1) de las siguientes certificaciones o su equivalente: CSA -Certified SOC Analyst - CompTIA ECIH – EC-Council Certified Incident Handler - EC-Council CNFE – Network Forensic Investigator - Mile2 CHFI – Computer Hacking Forensic Investigator - EC-Council CEH - Certified Ethical Hacker - EC-Council CRISC - Certified in Risk and Information Security Control -ISACA CPTE – Certified Pentester Engineer - Mile2 CPTIA – CREST Practitioner Threat Intelligence Analyst - CompTIA

Solicitamos respetuosamente a la entidad adicionar que los analistas puedan ser tambien titulados como técnicos o tecnologos.

Adicionalmente, la experiencia de dos (2) años tambien pueda estar incluida en funciones de monitoreo de SOC y/o actividades de seguridad informática.

Tambien incluir como alternativas certificaciones en seguridad informática o ciberseguridad o en la solución SIEM ofrecida en la propuesta.

Lo anterior garantiza la pluralidad de oferentes y no afecta la prestación del servicio.

Respuesta: Nos permitimos aclarar que:

Respuesta 1: Con respecto al perfil profesional se confirma que su observación no será tenida en cuenta

Respuesta 2: Respecto a la Experiencia, se confirma que las mencionadas se encuentran incluidas dentro del perfil.

Respuesta 3: Se confirma que la observación no podrá ser tenía en cuenta

Observación 7:

Observación No. 7: en el numeral **1.41.3. Recurso humano mínimo habilitante,** la entidad solicita lo siguiente para el perfil de técnico de seguridad TI:

Perfil Profesional y Experiencia
Profesional, técnico o tecnólogo titulado en sistemas, telecomunicaciones o carreras afines con mínimo dos (2) años de experiencia en la administración y gestión de plataformas de seguridad como Firewall Fortinet o dispositivos de seguridad perimetral similares, contar con conocimientos en Consolas de Antivirus para endpoint, entre otros sistemas de seguridad, se requiere mantenimiento y aplicación de reglas a los servicios descritos.

Solicitamos respetuosamente a la entidad que el perfil pueda tambien tener conocimientos en **ciberseguridad o seguridad de TIC´s.**

Adicionalmente, solicitamos incluir como alternativas certificaciones en Seguridad informática o ciberseguridad, con el fin de acreditar la certificación solicitada.

Lo anterior garantiza la pluralidad de oferentes y no afecta la prestación del servicio.

Respuesta: Nos permitimos aclarar que:

Punto 1: la palabra ente otros sistemas de seguridad contempla ciberseguridad o seguridad de TIC´s

Punto 2: Se confirma que la observación no podrá ser tenía en cuenta

Observación 8:

Observación No. 8: en el anexo 2 la entidad solicita lo siguiente para el perfil de especialista de seguridad TI:

ESPECIALISTA DE SEGURIDAD TI	1	50%	Profesional en Ingeniería de sistemas, electrónica, o telecomunicaciones, con especialización en Seguridad Informática	Demostrar mínimo 5 años de experiencia profesional contados a partir de la expedición de la tarjeta o matrícula profesional	Para obtener los puntos por este concepto, es necesario que el ESPECIALISTA DE SEGURIDAD TI acredite la formación profesional y la experiencia aquí definidas.	100	100

Solicitamos respetuosamente adicionar como otra alternativa el posgrado en seguridad de la información.

Lo anterior garantiza la pluralidad de oferentes y no afecta la prestación del servicio.

Respuesta: Nos permitimos informar que para una mayor pluralidad de propuestas se acepta la observación y la misma será tenida en cuenta mediante la Adenda N°3

Observación 9:

Observación No. 9: solicitamos respetuosamente a la entidad incluir como otras alternativas la certificación como auditor líder ISO 27001:2013 y COBIT 5 para el perfil de director o coordinador SOC, relacionado en el anexo 2. Recurso humano calificable.

Respuesta: Nos permitimos indicar que se ajustara ANEXO No. 2 RECURSO HUMANO CALIFICABLE del pliego de condiciones, este se verá modificado en Adenda N°3, de igual forma se especifica el detalle el numeral OBSERVACIONES GENERALES ítem 3 “Certificaciones del Recurso Humano calificable“ del presente documento

Observación 10:

Observación No. 10: solicitamos respetuosamente a la entidad incluir como otra alternativa el posgrado en seguridad informática para el perfil de Experto coordinador de grupo de respuesta a incidentes, relacionado en el anexo 2. Recurso humano calificable.

Adicionalmente, incluir como otras alternativas la certificación CSX de ISACA o ISO 27032.

Lo anterior garantiza la pluralidad de oferentes y no afecta la prestación del servicio.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y será modificado el ANEXO No. 2 RECURSO HUMANO CALIFICABLE mediante la Adenda N°3.

Observación 11:

Observación No. 11: en el numeral 3.3.3. Certificaciones proveedor, solicitamos a la entidad aclarar este punto, dado que en caso de que se presente un proveedor en figura de consorcio o unión temporal compuesto por varias empresas, al menos uno de los miembros deba tener esta certificación.

Respuesta: Nos permitimos aclarar que, en caso de presentarse como consorcio o unión temporal, el proveedor con mayor participación deberá acreditar la certificación respectiva.

Observación 12:

Observación No. 12: en el numeral 4.1.6. Aspectos ambientales calificables, la entidad solicita aportar los documentos o evidencias descritos en el anexo 9. Solicitamos respetuosamente a la entidad aclarar este punto, dado que en caso de que se presente un proveedor en figura de consorcio o unión temporal compuesto por varias empresas, al menos uno de los miembros debe acreditar este requisito.

Respuesta: La Unión Temporal o Consorcio, es una vía que favorece la colaboración entre empresas para acometer y afrontar conjuntamente proyectos, es importante anotar que con que sólo una de las empresas que la conforman presente la documentación soporte, cumple el requisito, se otorga el puntaje del aspecto que se esté evaluando.

XVII. OBSERVACIONES PRESENTADAS POR LA EMPRESA PWC (PRICEWATERHOUSE COOPERS)

Observación 1: Numeral 3.3.2. EXPERIENCIA DEL PROPONENTE, con respecto a las experiencias exigidas se solicita a La Previsora permitir y habilitar de la siguiente manera.

• Con el fin de cumplir con la experiencia mínima habilitante, EL PROPONENTE deberá adjuntar con su propuesta **máximo seis (6)** certificaciones de contratos suscritos con empresas públicas o privadas nacionales en las que se acredite experiencia de la siguiente forma:

• El objeto, actividades u obligaciones sean iguales o similares al de la presente invitación. Entendiéndose por similar que consista en la prestación de servicios administrados de seguridad y/o servicios de SOC **y/o seguridad de la información y/o ciberseguridad y/o relacionadas con las actividades del proceso a contratar**.

• Una de las **seis** certificaciones con las cuales se pretende acreditar la experiencia mínima habilitante debe corresponder a empresas del Sector Gobierno o Sector Financiero.

• El valor de la sumatoria de las certificaciones deberá acreditar una cuantía igual o superior al **50%** del valor del presupuesto.

• El plazo de ejecución de cada contrato certificado incluidas sus prórrogas deberá ser igual o mayor a **seis (6)** meses.

• Los contratos certificados deben haber iniciado **y/o terminado** durante los últimos **10 años a la presentación de la presente invitación.**

Respuesta: Nos permitimos indicar que:

Punto 1: Con respecto a la experiencia habilitante, se indica que el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE del pliego de condiciones se ajustó mediante Adenda N°3, remitirse al numeral OBSERVACIONES GENERALES ítem 3 “Número de certificaciones de experiencia general” del presente documento. Adicionalmente, el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones se modificó mediante Adenda N°3

Punto 2: Con respecto al objeto y/o actividades se confirma que su observación no será tenida en cuenta

Punto 3 y 4: Con respecto a las certificaciones, se confirma que su observación no será tenida en cuenta

Punto 5: Con respecto al plazo de ejecución, se realiza ajuste mediante Adenda N°3

Punto 6: Con respecto al tiempo de experiencia, nos permitimos indicar que su observación no será tenida en cuenta, remitirse al numeral I. OBSERVACIONES GENERALES ítem 2 “Tiempo de experiencia del Proponente” del presente documento.

Observación 2: Numeral 3.3.6 recurso mínimo habilitante, para el gerente de servicio se solicita a La Previsora requerir la disponibilidad en función de la dedicación solicitada del 30% semanal.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE será modificará mediante Adenda N°3

• Numeral 3.3.6 recurso mínimo habilitante, para el gerente de servicio se solicita a La Previsora incluir el postgrado en gerencia de ingeniería o a fines con la gerencia de proyectos.

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta ya que se requiere que el recurso tenga experiencia y conocimiento en servicios de seguridad informática, ciberseguridad o seguridad de la información.

• Solicitamos amablemente a la Previsora aclarar si las hojas de vida del personal del proyecto, gerente, profesionales SOC y ti se deben entregar con la presentación de la oferta.

Respuesta: Nos permitimos aclarar que para un mayor entendimiento se realiza ajuste sobre el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones mediante Adenda N°3

• Numeral 3.3.6 GRUPO DE (4) CUATRO ANALISTAS SOC – REMOTO, para el perfil profesional y experiencia se solicita a La Previsora permitir los perfiles de la siguiente manera:

Profesionales o tecnológicos o técnicos en Ingeniería de sistemas, electrónica, telecomunicaciones o afines con mínimo (2) años de experiencia como Analista SOC o ingenieros junior de seguridad o monitoreo en SOC. Tendrá la responsabilidad del análisis

y la documentación de los eventos presentados, así como las respectivas mediciones y acciones de mejora sobre la plataforma. Certificaciones o cursos, debe acreditar al menos una (1) de las siguientes certificaciones o su equivalente:
- CSA -Certified SOC Analyst - CompTIA ECIH
- EC-Council Certified Incident Handler
- EC-Council CNFE – Network Forensic Investigator
- Mile2 CHFI – Computer Hacking Forensic Investigator
- EC-Council CEH - Certified Ethical Hacker
- EC-Council CRISC - Certified in Risk and Information Security Control
-ISACA CPTE – Certified Pentester Engineer
- Mile2 CPTIA – CREST Practitioner Threat Intelligence Analyst – CompTIA
- Seguridad informática o ciberseguridad

Respuesta: Nos permitimos indicar que se ajustó el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones y este se verá reflejado mediante Adenda N°3

Observación 3: Numeral 3.3.6 UN (1) TÉCNICO DE SEGURIDAD TI, solicitamos a La Previsora permitir la experiencia de la siguiente manera:

- Profesional, técnico o tecnólogo titulado en sistemas, telecomunicaciones o carreras afines con mínimo dos (2) años de experiencia en la administración y gestión de plataformas de seguridad como Firewall Fortinet o dispositivos de seguridad perimetral similares, contar con conocimientos en Consolas de Antivirus para endpoint **o ciberseguridad** entre otros sistemas de seguridad, se requiere mantenimiento y aplicación de reglas a los servicios descritos.

Certificaciones

- De preferencia manejo en (OIM/OIG) o disponibilidad para tomar la gestión de dicha herramienta Gestora de identidades.

Se debe acreditar al menos una (1) de las siguientes certificaciones o su equivalente:
-CCNA Security o similares - Cisco
- NSE4 (preferiblemente) - Fortinet JNCIA-SEC
- Junniper PCNSA
- Palo Alto MTCSE, - Microtik
- **Seguridad informática o ciberseguridad**

Respuesta: Nos permitimos aclarar que:

Punto 1: la palabra ente otros sistemas de seguridad contempla ciberseguridad

Punto 2: con respecto a las certificaciones su observación no será tenida en cuenta

Observación 4: En el ANEXO No. 2 RECURSO HUMANO CALIFICABLE, para el cargo Especialista de Seguridad TI se solicita incluir **el postgrado en seguridad de la información.**

Respuesta: Nos permitimos indicar que el ANEXO No. 2 RECURSO HUMANO CALIFICABLE será modificado mediante la Adenda N°3.

Observación 5: En el ANEXO No. 3 RECURSO HUMANO CALIFICABLE, para el DIRECTOR Y/O COORDINADOR SOC se solicita permitir demostrar **mínimo 5 años de experiencia profesional y 2 años de experiencia específica** en Gerencia de proyectos, coordinación de SOC o consultoría de seguridad de la información, en proyectos de diseño desarrollo e implementación de sistemas de gestión de seguridad de la información bajo el estándar ISO 27001, pruebas de EthicaL Hacking, Gestión de Riesgos, **y/o Arquitectura de Seguridad**.

- **Así mismo solicitamos respetuosamente en las certificaciones incluir la ISO 27001:2013 y COBIT 5.**

Respuesta: Nos permitimos aclarar que:

Punto 1: Con respecto a los años de experiencia se confirma que su observación no será tenida en cuenta.

Punto 2: Con respecto a la experiencia especifica se ajustará el numeral ANEXO No. 2 RECURSO HUMANO CALIFICABLE del pliego de condiciones y este se verá modificado en Adenda N°3

Punto 3: Con respecto a las certificaciones se ajustará numeral ANEXO No. 2 RECURSO HUMANO CALIFICABLE del pliego de condiciones y este se verá modificado en Adenda N°3

Observación 6: En el ANEXO No. 2 RECURSO HUMANO CALIFICABLE para el EXPERTO COORDINADOR DE GRUPO DE RESPUESTAS A INCIDENTES se solicita **incluir la especialización en seguridad informática, así como también incluir certificación en ISO 27032 o CISM**.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y será modificado el ANEXO No. 2 RECURSO HUMANO CALIFICABLE en la Adenda N°3.

Observación 7: Para el numeral 4.1.4. CERTIFICACIONES ADICIONALES (30) PUNTOS, se solicita otorgar el puntaje al proponente con la oferta que en la solución incluyan las certificaciones especificadas.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 4.1.4. CERTIFICACIONES ADICIONALES (30) PUNTOS será modificado en Adenda N°3

Observación 8: En el numeral 4.1.3.1. MEMBRESIA FIRST (20) PUNTOS se incluir que ese asignará el puntaje de veinte (20) puntos, a la propuesta que allegue la membresía de FIRST (Forum of Incident Response and Security Teams) **u otra figura para la respuesta a incidentes** como empresa.

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta.

XVIII. OBSERVACIONES PRESENTADAS POR LA EMPRESA DIGIWARE

Observación 1: GRUPO DE (4) CUATRO ANALISTAS SOC – REMOTO Los recursos solicitados son los mínimos requeridos para la operación del SOC (Para el óptimo cumplimiento del servicio EL PROPONENTE asignara el personal que considere necesario para cumplir con los ANS respectivos, descritos en la presente invitación y cumpliendo con todas las obligaciones mínimas relacionadas al servicio de SOC Nivel 2).

Se solicita especificar si pueden ser recursos globales o debe ser recursos dedicados

Respuesta: Nos permitimos aclarar que los recursos de GRUPO DE (4) CUATRO ANALISTAS SOC - REMOTO no serán dedicados únicamente para La Previsora.

Observación 2: GRUPO DE (4) CUATRO ANALISTAS SOC – REMOTO Los recursos solicitados son los mínimos requeridos para la operación del SOC (Para el óptimo cumplimiento del servicio EL PROPONENTE asignara el personal que considere necesario para cumplir con los ANS respectivos, descritos en la presente invitación y cumpliendo con todas las obligaciones mínimas relacionadas al servicio de SOC Nivel 2).

Se solicita especificar si la totalidad de los recursos deben están en horario 7x24 o uno por turnos o como espera el cliente que sea el esquema operativo

Respuesta: Nos permitimos indicar que el horario, cantidades, turnos del servicio del SOC son responsabilidad del proponente, para la entidad se debe es garantizar el cumplimiento de los ANS descritos en el numeral 3.3.7.4. ACUERDOS DE NIVELES DE SERVICIO.

Observación 3: GRUPO DE (4) CUATRO ANALISTAS SOC – REMOTO Los recursos solicitados son los mínimos requeridos para la operación del SOC (Para el óptimo cumplimiento del servicio EL PROPONENTE asignara el personal que considere necesario para cumplir con los ANS respectivos, descritos en la presente invitación y cumpliendo con todas las obligaciones mínimas relacionadas al servicio de SOC Nivel 2).

Se solicita aclarar cuales son las actividades que el cliente espera que sean desarrolladas por este personal

Respuesta: Nos permitimos informar que las actividades se describen en numeral 3.3.7.1 SERVICIOS DE SOC del pliego de condiciones en donde se especifica las obligaciones generales del servicio.

Observación 4: GRUPO DE (4) CUATRO ANALISTAS SOC – REMOTO Los recursos solicitados son los mínimos requeridos para la operación del SOC (Para el óptimo cumplimiento del servicio EL PROPONENTE asignara el personal que considere necesario para cumplir con los ANS respectivos, descritos en la presente invitación y cumpliendo con todas las obligaciones mínimas relacionadas al servicio de SOC Nivel 2).

Se solicita especificar la cantidad de incidentes mensuales que atienden actualmente por nivel de criticidad

Respuesta: Nos permitimos aclarar la siguiente información es un promedio mes tomada de nuestra matriz de incidentes:

ALTO	MEDIO	BAJO
2	4	16

Observación 5: DOS (2) ANALISTAS DE SEGURIDAD TI: LA PREVISORA S.A (Presencial y/o Remoto) dispondrá en la sede principal un (1) espacio de trabajo físico (puesto de trabajo con extensión telefónica y punto de red), para uno de los analistas, el segundo analista deberá trabajar de manera remota y EL PROPONENTE deberá garantizar los elementos necesarios para la prestación del servicio (Computador y teléfono de contacto).

Se solicita aclarar si las actividades para este personal están enfocadas a ser el nivel 1 de atención, para luego escalarlo al Analistas SOC

Respuesta: Remitirse al numeral 3.3.7.2.1. ANALISTAS DE SEGURIDAD TI del pliego de condiciones, donde se describe las actividades de los DOS (2) ANALISTAS DE SEGURIDAD TI.

Observación 6: DOS (2) ANALISTAS DE SEGURIDAD TI: LA PREVISORA S.A (Presencial y/o Remoto) dispondrá en la sede principal un (1) espacio de trabajo físico (puesto de trabajo con extensión telefónica y punto de red), para uno de los analistas, el segundo analista deberá trabajar de manera remota y EL PROPONENTE deberá garantizar los elementos necesarios para la prestación del servicio (Computador y teléfono de contacto).

Se solicita especificar si la totalidad de los recursos deben están en horario 7x24 o uno por turnos o solo 5x8 o como espera el cliente que sea el esquema operativo. Dado que si es 7x24 se debería incluir más personas

Respuesta: Nos permitimos aclarar que la forma de operación de los recursos Analistas de Seguridad son en horario 8X5. Para mayor claridad se realiza modificación mediante Adenda N°3

Observación 7: UN (1) TECNICO DE SEGURIDAD TI LA PREVISORA S.A en la sede principal brindará el espacio de trabajo físico (puesto de trabajo con extensión telefónica y

punto de red), EL PROPONENTE deberá garantizar los elementos necesarios para la prestación del servicio (Computador y teléfono de contacto). Profesional, técnico o tecnólogo titulado en sistemas, telecomunicaciones o carreras afines con mínimo dos (2) años de experiencia en la administración y gestión de plataformas de seguridad como Firewall Fortinet o dispositivos de seguridad perimetral similares, contar con conocimientos en Consolas de Antivirus para endpoint, entre otros sistemas de seguridad, se requiere mantenimiento y aplicación de reglas a los servicios descritos

Se solicita aclarar si el cliente espera que esta persona trabaje en un horario de 5x8 de lunes a viernes y sea el encargado de gestionar plataformas de Firewall, AV y Office 365

Respuesta: Nos permitimos indicar que su entendimiento es correcto.

Observación 8: UN (1) TECNICO DE SEGURIDAD TI LA PREVISORA S.A en la sede principal brindará el espacio de trabajo físico (puesto de trabajo con extensión telefónica y punto de red), EL PROPONENTE deberá garantizar los elementos necesarios para la prestación del servicio (Computador y teléfono de contacto). Profesional, técnico o tecnólogo titulado en sistemas, telecomunicaciones o carreras afines con mínimo dos (2) años de experiencia en la administración y gestión de plataformas de seguridad como Firewall Fortinet o dispositivos de seguridad perimetral similares, contar con conocimientos en Consolas de Antivirus para endpoint, entre otros sistemas de seguridad, se requiere mantenimiento y aplicación de reglas a los servicios descritos

Se solicita aclarar si en caso de requerir gestión de plataformas, favor indicar la cantidad de plataformas a gestionar, versión y marca

Respuesta: Nos permitimos informar que el estado actual de los equipos es el siguiente:

DISPOSITIVO	**Versión**	**Marca**
Firewall	6.2.6	Fortinet
Antivirus (nube)	2.17	Sophos
OIG	11g	Oracle
Office365 (seguridad en nube)	Licencias E1 y E3	Microsoft

Observación 9: UN (1) TECNICO DE SEGURIDAD TI LA PREVISORA S.A en la sede principal brindará el espacio de trabajo físico (puesto de trabajo con extensión telefónica y punto de red), EL PROPONENTE deberá garantizar los elementos necesarios para la prestación del servicio (Computador y teléfono de contacto). Profesional, técnico o tecnólogo titulado en sistemas, telecomunicaciones o carreras afines con mínimo dos (2) años de experiencia en la administración y gestión de plataformas de seguridad como Firewall Fortinet o dispositivos de seguridad perimetral similares, contar con conocimientos en Consolas de Antivirus para endpoint, entre otros sistemas de seguridad, se requiere mantenimiento y aplicación de reglas a los servicios descritos

Se solicita especificar la cantidad de requerimientos por tecnología a gestionar

Respuesta: Nos permitimos confirmar que al mes se gestionaran un promedio de 20 requerimiento de seguridad sobre las plataformas de seguridad.

Observación 10: EL PROPONENTE deberá ofrecer un servicio integral de SOC, el cual contemple durante la etapa de operación, en los primeros seis (6) meses del servicio, la ejecución del afinamiento y estabilización respectivo de la plataforma de SIEM que ofrezca, para las aplicaciones y demás servicios específicos, alineado a una operación de nivel 1 “Monitorización y análisis”. Finalizada esta etapa la operación del SOC deberá cumplir con un nivel 2 “Análisis exhaustivo y de respuesta” alineado con las mejores prácticas y acorde a las necesidades de LA PREVISORA S.A.

Se solicita aclarar si al mencionar "análisis exhaustivo y repuesta", el cliente quiere indicar que el SOC se encargara de gestionar los incidentes detectados y una vez se identifiquen se analizaran con el fin de encontrar la causa raiz y por último entregar recomendaciones al cliente como parte del proceso de respuesta.

Respuesta: Nos permitimos indicar que para aclarar el entendimiento “análisis exhaustivo y repuesta” se puede remitir al Glosario del pliego de condiciones.

Observación 11: Servicio de monitorización inteligente de eventos de seguridad en modalidad 7x24. La gestión de incidentes se debe realizar a través de la herramienta entregada por LA PREVISORA S.A. El servicio ofrecido deberá alinearse a las políticas, procesos y procedimientos definidos por LA PREVISORA S.A. Anexo No. 4 “Alcance SOC - REQUERIDOS MINIMOS”.

Se solicita aclara a que herramienta de se refiere el cliente, una plataforma SIEM, una herramienta de registros de casos, etc. Dado que no es coherente con el objeto el cual se refiere aun SOC como servicio

Respuesta: Nos permitimos aclarar que la herramienta en referencia es la del registro de los casos de incidentes que se presenten y que deban ser gestionas, esta herramienta que proporcionara la entidad es el acceso a Aranda para el registro y consolidado de los casos.

Observación 12: Servicio de manejo de incidentes realizando el triage de los incidentes de seguridad, correlación de eventos, respuesta ante incidentes, amenazas y ataques contra la plataforma tecnológica y los sistemas de información de la organización. Para estos temas se deberá alinear los procesos con la Taxonomía Única Incidentes Cibernéticos – TUIC establecida por la Superfinanciera de Colombia y el COLCERT.

Se solicita aclarar si al mencionar "respuesta ante incidentes", el cliente quiere indicar que el SOC se encargara de gestionar los incidentes detectados y una vez se identifiquen se analizaran con el fin de encontrar la causa raíz y por último entregar recomendaciones al cliente como parte del proceso de respuesta.

Respuesta: Nos permitimos informarles que de acuerdo al item 3.3.7.1 SERVICIOS DE SOC N° del SOC si se encargara de gestionar los incidentes detectados y una vez se identifiquen se analizaran con el fin de encontrar la causa raíz y por último entregar un informe con recomendación de los incidentes encontrados.

Observación 13: Analizar e implementar mecanismos que permitan a la entidad verificar diferentes fuentes de información tales como sitios web, blogs y redes sociales, esto con el propósito de identificar posibles ataques cibernéticos contra la entidad. Lo anterior alineado a la Circular Externa 008 de la Superfinanciera de Colombia.

Se solicita aclarar si este requerimiento hace referencia a la prestación de un servicio de monitoreo de marca. Si es asi favor aclarar la cantidad de dominios a monitorear, cantidad de usuarios VIP, redes sociales, takedown anuales y si requiere monitoreo en deep y dark web

Respuesta: Nos permitimos indicar que es correcto su entendimiento, la cantidad de marcas (1), dominios web (hasta 5), dominios de correo (1), Aplicaciones (las comunes tipo WEB), Presencia en redes sociales (Las más reconocidas en el mercado Facebook, Instagram, Twitter, etc).

Observación 14: Notificación proactiva de amenazas proporcionando soluciones y estrategias de mitigación, tomar medidas para proteger los sistemas y redes afectados o amenazados por la actividad de intrusos y desarrollar otras estrategias de respuesta o solución alternativa, con escenarios de crisis contra ataques dirigidos como DDoS o amenazas avanzadas.

Se solicita aclarar si este requerimiento hace referencia a que el SOC entregue recomendaciones acerca del fortalecimiento de la postura de seguridad a través de la propuesta de implementar nuevos controles de seguridad

Respuesta: Nos permitimos confirmar que el servicio de SOC si debe entregar recomendaciones acerca del fortalecimiento de la postura de seguridad a través de la propuesta de implementar nuevos controles de seguridad y buenas prácticas vigentes en el mercado.

Observación 15: El servicio ofertado deberá detectar actividades inusuales, recolectar evidencias y correlacionar los eventos para el escalamiento y determinar si corresponde a un evento de seguridad, tendencias, falsos positivos, patrones o firmas de intruso las cuales deberán ser notificadas y documentadas. Sobre este punto de analítica de datos se solicita al proponente contemplar las herramientas que considere necesarias para contar con la inteligencia artificial para la detección de estos eventos.
Se solicita aclarar si el cliente espera contar con un componente de UBA dentro del servicio

Respuesta: Nos permitimos indicar que el componente UBA es requerido en el servicio el cual esta descrito en el numera numeral 3.3.7.1 SERVICIOS DE SOC ítem k del pliego de condiciones.

Observación 16: EL PROPONENTE deberá contar con una herramienta SIEM en modalidad de servicio en nube para el análisis de los registros de eventos de los equipos de seguridad existentes (IPS's, Firewalls, Endpoint, Sandbox, UBA, etc) y respuesta ante eventos inusuales, la integración de la herramienta deberá contemplar múltiples formas de integración, así como envió de logs, agentes u otro para dejar operativo todos los servicios que se requieran monitorear. Por otro lado, se deben contemplar sitios web, bases de datos, servidores, aplicaciones internas y en cómo (office365, saleforce, entre otras) y demás con los que cuente la compañía.

Se solicita especificar si los servicios en nube con los que cuenta el cliente tienen la capacidad de enviar log o si cuentan con API expuesto para su consumo y extracción de logs

Respuesta: Nos permitimos indicar que estas aplicaciones, por ser servicios nuevos se deberá validar entre las partes, por lo que solo se podrá revisar una vez se cuente con el proponente seleccionado. Sin embargo, es de aclarar que al ser aplicación estándar del mercado cualquiera se puede configurar el envió de logs en formato syslog.

Observación 17: EL PROPONENTE deberá contar con una herramienta SIEM en modalidad de servicio en nube para el análisis de los registros de eventos de los equipos de seguridad existentes (IPS's, Firewalls, Endpoint, Sandbox, UBA, etc) y respuesta ante eventos inusuales, la integración de la herramienta deberá contemplar múltiples formas de integración, así como envió de logs, agentes u otro para dejar operativo todos los servicios que se requieran monitorear. Por otro lado, se deben contemplar sitios web, bases de datos, servidores, aplicaciones internas y en nube como (office365, saleforce, entre otras) y demás con los que cuente la compañía.

Se solicita aclarar si al mencionar " demás con los que cuente la compañía" se refiere a la totalidad de componentes listado en la tabla de activos a integrar

Respuesta: Nos permitimos confirmar que la palabra “además con los que cuente la compañía” son equipos de seguridad que se relacionan en el numeral 3.3.7.1 SERVICIOS DE SOC ítem H y también el listado de componente que están en el ANEXO No 1 – DISPOSITIVOS A MONITOREAR.

Observación 18: EL PROPONENTE debe encargarse de realizar todas las tareas necesarias para asegurar la generación, almacenamiento (mínimo 12 meses) y potencial recuperación de respaldos de las configuraciones de todas las plataformas involucradas en el servicio. Estos respaldos podrán ser solicitados por la entidad para ser almacenados en sus instalaciones.

Se solicita aclarar si el almacenamiento de 12 meses se refiere a almacenar los logs en frio por este tiempo para luego ser sobre escritos

Respuesta: Nos permitimos aclarar que la solicitud anterior describe el tiempo de almacenamiento de los logs que se deben salvaguardar, esto con el fin de poder contar con esta información en cualquier momento, una vez cumpla el tiempo límite de retención definido se debe garantizar un esquema de backup y entrega a custodia para posterior reescritura de los logs.

Observación 19: Generar informes diarios de las herramientas de monitoreo indicando eventos, alertas e incidentes presentes y sus respectiva clasificación y acciones.
Se solicita aclarar si esta información puede ser entregada a traves de un portal web donde se indique esta información sin necesidad de generar informes, lo cual mejora la ejecución de actividades operativas relevantes para el servicio

Respuesta: Nos permitimos aclarar que para un mayor entendimiento se realiza modificación mediante Adenda N°3

Observación 20: Contener o neutralizar los ataques detectados en caso de presencia de amenazas, para estos eventos se deberá contar con una matriz de incidencias y deberá estar avalada por LA PREVISORA S.A.

Se solicita aclarar si este requerimiento se refiere a la implementación de un componente tipo SOAR el cual realice acciones de contención automáticas o se refiere a que el SOC notifique a los encargados para que ellos realicen las acciones de forma manual

Respuesta: Nos permitimos aclarar que el servicio solicitado requiere respuesta sobre eventos, por lo cual para temas de ataques se deberán tomar las acciones pertinentes. Así mismo el servicio cuenta con personal que administrara las plataformas respectivas por lo cual se podría manejar un nivel de configuración especifico. Si los dispositivos involucrados hacen parte de la gestión del servicio de seguridad de TI, el recurso Técnico de Seguridad TI deberá estar en capacidad de solventar, contener o neutralizar los eventos en las plataformas definidas en su gestión, si las plataformas involucradas no hacen parte del servicio contratado La Previsora es la responsable de ejecutar las acciones, configuración recomendadas por el Grupo de SOC o Analistas de Seguridad TI.

Observación 21: 3.3.7.2. SERVICIOS DE SEGURIDAD ADMINISTRADA
Asesorar a la entidad en la adopción, implementación e incorporación de nuevos requerimientos normativos relacionados con la gestión tecnológica de Seguridad de la Información y la Ciberseguridad.

Se solicita aclarar si este requerimiento se enfoca en que el analista solamente realizara recomendaciones y acompañamiento y que la implementación estará a cargo del tercero que contrate el cliente, dado que la implementación de controles hace parte de otro alcance diferente al objeto del contrato

Respuesta: Nos permitimos indicar que su entendimiento no es correcto debido a que los servicios administrados implican el soporte y la administración de las plataformas de seguridad en donde son aplicados los controles respectivos, por consiguiente la implementación de controles en las herramientas de seguridad administrada será responsabilidad del servicio de seguridad administrada, si la implementación es sobre otros sistemas de información diferentes a los descritos en este alcance será responsabilidad de La Previsora

Observación 22: Apoyar la implementación segura de los sistemas de información.
Se solicita aclarar si este requerimiento se enfoca en que el analista solamente realizara recomendaciones y acompañamiento y que la implementación estará a cargo del tercero que contrate el cliente, dado que la implementación de controles hace parte de otro alcance diferente al objeto del contrato

Respuesta: Nos permitimos aclarar que los analistas de seguridad crean, actualizan, gestionan y evalúan las líneas base, pero los encargados de su implementación y evidencias son los administradores de cada herramienta o sistema de información de La Previsora, el apoyo en la implementación hace referencia a asesorar o explicar si es el caso algún item de las líneas base.

Observación 23: Realizar análisis del software libre, entregando un informe con la recomendación de uso. Este se manejará a demanda.
Se solicita aclarar si este requerimiento se refiere a un análisis de vulnerabilidades

Respuesta: Nos permitimos aclarar que los análisis de software se solicitan a demanda y estos dependerán de la necesidad de La Previsora, de igual forma el análisis solicitado es para confirmar si el software puede llegar a generar alguna vulnerabilidad a nivel interno, mala reputación, limitaciones o incumplimiento normativo de derechos de autor.

Observación 24: Realizar pruebas que permitan a LA PREVISORA S.A, medir la efectividad de los controles tecnológicos existentes y definir reglas para detectar, reaccionar y contener ataques.

Se solicita aclarar si este requerimiento hace referencia a pruebas de ethical hacking y si es así cuál sería su alcance y periodicidad.

Respuesta: Nos permitimos confirmar que su entendimiento no es correcto, el alcance de las pruebas y demás factores relacionados a este ítem se definirán en común acuerdo entre La Previsora S.A. y el proponente seleccionado ya que dependen de los controles y reglas que defina para la detección de eventos, se aclara adicionalmente que sobre el numeral 3.3.7.2.1. ANALISTAS DE SEGURIDAD TI. Item O se detallan las pruebas de Ethical Hacking

Observación 25: Líneas base de seguridad: Modificar, actualizar e implementar las líneas base de seguridad o buenas prácticas en los sistemas de información de LA PREVISORA S.A e identificadas por la Gerencia de TI. Adicionalmente, se deberá realizar un aseguramiento o medición del cumplimiento de cada una de ellas y entregar informe respectivo de la medición, así como el apoyar a los administradores de TI en la implementación de los parámetros de línea base. Esta ejecución de líneas base se debe realizar de manera anual. Estas deben regirse con los estándares internacionales (eje CIS) y/o de fabricantes según corresponda.

Se solicita incluir este requerimiento como parte de un servicio de consultoría adicional dado que la implementación de una línea base y la medición del cumplimiento se sale del alcance de un servicio de SOC. Por lo que este alcance hace parte más de una consultoría o una persona dedicada para este fin

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta a razón de que La Previsora ya cuenta con líneas base y la medición es efectuada por los Analistas de Seguridad como se describe en el numeral 3.3.7.2.1. ANALISTAS DE SEGURIDAD TI.

Observación 26: Líneas base de seguridad: Modificar, actualizar e implementar las líneas base de seguridad o buenas prácticas en los sistemas de información de LA PREVISORA S.A e identificadas por la Gerencia de TI. Adicionalmente, se deberá realizar un aseguramiento o medición del cumplimiento de cada una de ellas y entregar informe respectivo de la medición, así como el apoyar a los administradores de TI en la implementación de los parámetros de línea base. Esta ejecución de líneas base se debe realizar de manera anual. Estas deben regirse con los estándares internacionales (eje CIS) y/o de fabricantes según corresponda.

Se solicita aclarar como espera el cliente que sea medidos la efectividad de los controles y cuál es la cantidad y tipo de controles que desea medir

Respuesta: Nos permitimos aclarar que se debe validar cada línea base con un muestreo aleatorio por cada línea base, según el número de sistemas de información productivos en el periodo de medición coordinado en el cronograma.

Observación 27: Líneas base de seguridad: Modificar, actualizar e implementar las líneas base de seguridad o buenas prácticas en los sistemas de información de LA PREVISORA S.A e identificadas por la Gerencia de TI. Adicionalmente, se deberá realizar un aseguramiento o medición del cumplimiento de cada una de ellas y entregar informe respectivo de la medición, así como el apoyar a los administradores de TI en la implementación de los parámetros de línea base. Esta ejecución de líneas base se debe realizar de manera anual. Estas deben regirse con los estándares internacionales (eje CIS) y/o de fabricantes según corresponda.

Se solicita aclarar si la línea base es solo para los dispositivos de seguridad

Respuesta: Nos permitimos aclarar que se tienen implementadas veintiocho (28) líneas base las cuales pueden incrementar, la implementación actual es sobre el 100% de los sistemas de información productivos de la entidad (bases de datos, comunicaciones entre otros). Las cantidades y documentos base serán entregados al oferente seleccionado.

Observación 28: Aseguramiento y gestión de vulnerabilidades: Anualmente se deberán generar dos (2) análisis de vulnerabilidad, Ethical Hacking y penetración a la plataforma tecnológica, a los que se deberá elaborar una matriz de seguimiento de los hallazgos encontrados y los planes de remediación y/o mitigación, el cual deberá ser gestionado por EL PROVEEDOR. Para cada uno de los análisis se debe contemplar todos los dispositivos activos de LA PREVISORA S.A los cuales se estiman en un promedio de 600 objetivos. Por otra parte, se debe contemplar análisis de vulnerabilidades a demanda adicionales para nuevas aplicaciones y/o solicitudes internas. Se solicita contemplar por lo menos 2 análisis de código por año y el respectivo Re-test de cada uno de los análisis efectuados, los análisis de penetración a las herramientas se solicita estimación de por lo menos 3 por año.

Se solicita aclarar la cantidad de aplicaciones Web que se encuentran dentro de los 600 dispositivos a evaluar

Respuesta: Nos permitimos aclarar que el promedio de aplicaciones WEB de los 600 dispositivos es de 30 a evaluar

Observación 29: Aseguramiento y gestión de vulnerabilidades: Anualmente se deberán generar dos (2) análisis de vulnerabilidad, Ethical Hacking y penetración a la plataforma tecnológica, a los que se deberá elaborar una matriz de seguimiento de los hallazgos encontrados y los planes de remediación y/o mitigación, el cual deberá ser gestionado por EL PROVEEDOR. Para cada uno de los análisis se debe contemplar todos los dispositivos activos de LA PREVISORA S.A los cuales se estiman en un promedio de 600 objetivos. Por otra parte, se debe contemplar análisis de vulnerabilidades a demanda adicionales para nuevas aplicaciones y/o solicitudes internas. Se solicita contemplar por lo menos 2 análisis de código por año y el respectivo Re-test de cada uno de los análisis efectuados, los análisis de penetración a las herramientas se solicita estimación de por lo menos 3 por año.

Se solicita aclarar si el cliente espera que el ethical hacking sea para todos los 600 dispositivos o solo para una porción.

Respuesta: Nos permitimos aclarar que la definición detallada de los 600 objetivos se realizara en conjunto con el proveedor seleccionado, el escaneo de vulnerabilidades será sobre los 600 objetivos así como su correspondiente re-test, con una periodicidad de 2 veces al año (primer semestre escaneo de vulnerabilidades, segundo semestre el re-test), para el caso del ethical hacking se efectúa sobre los sistemas de información CORE de negocio que promedian en 20 aplicaciones o según defina la prioridad la Gerencia de Riesgos con una periodicidad de 1 vez al años.

Observación 30: Aseguramiento y gestión de vulnerabilidades: Anualmente se deberán generar dos (2) análisis de vulnerabilidad, Ethical Hacking y penetración a la plataforma tecnológica, a los que se deberá elaborar una matriz de seguimiento de los hallazgos encontrados y los planes de remediación y/o mitigación, el cual deberá ser gestionado por EL PROVEEDOR. Para cada uno de los análisis se debe contemplar todos los dispositivos activos de LA PREVISORA S.A los cuales se estiman en un promedio de 600 objetivos. Por otra parte, se debe contemplar análisis de vulnerabilidades a demanda adicionales para nuevas aplicaciones y/o solicitudes internas. Se solicita contemplar por lo menos 2 análisis de código por año y el respectivo Re-test de cada uno de los análisis efectuados, los análisis de penetración a las herramientas se solicita estimación de por lo menos 3 por año.

Se solicita aclarar si al mencionar "planes de remediación y/o mitigación, el cual deberá ser gestionado por EL PROVEEDOR" se refiere a que el proveedor entregara las recomendaciones y el cliente se encargara de aplicar las medidas dado que el proveedor no es el responsable de la administración de las plataformas

Respuesta: Nos permitimos aclarar que es correcto su entendimiento. El proponente seleccionado entregara los planes de acción, y/o recomendaciones, así como asesorar o explicara el hallazgo en caso de ser necesario, La Previsora es el responsable de su implementación en los sistemas de información.

Observación 31: Aseguramiento y gestión de vulnerabilidades: Anualmente se deberán generar dos (2) análisis de vulnerabilidad, Ethical Hacking y penetración a la plataforma tecnológica, a los que se deberá elaborar una matriz de seguimiento de los hallazgos encontrados y los planes de remediación y/o mitigación, el cual deberá ser gestionado por EL PROVEEDOR. Para cada uno de los análisis se debe contemplar todos los dispositivos activos de LA PREVISORA S.A los cuales se estiman en un promedio de 600 objetivos. Por otra parte, se debe contemplar análisis de vulnerabilidades a demanda adicionales para nuevas aplicaciones y/o solicitudes internas. Se solicita contemplar por lo menos 2 análisis de código por año y el respectivo Re-test de cada uno de los análisis efectuados, los análisis de penetración a las herramientas se solicita estimación de por lo menos 3 por año.

Se solicita aclarar si se puede incluir un valor unitario por los análisis por demanda dado que al no saber su alcance no es posible estimarlo dentro del presupuesto

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta, sin embargo, le informamos que el promedio de análisis de vulnerabilidad a demanda por proyectos o pasos a producción son de 3 por mes incluyendo sus respetivos re-test.

Observación 32: Aseguramiento y gestión de vulnerabilidades: Anualmente se deberán generar dos (2) análisis de vulnerabilidad, Ethical Hacking y penetración a la plataforma tecnológica, a los que se deberá elaborar una matriz de seguimiento de los hallazgos encontrados y los planes de remediación y/o mitigación, el cual deberá ser gestionado por EL PROVEEDOR. Para cada uno de los análisis se debe contemplar todos los dispositivos activos de LA PREVISORA S.A los cuales se estiman en un promedio de 600 objetivos. Por

otra parte, se debe contemplar análisis de vulnerabilidades a demanda adicionales para nuevas aplicaciones y/o solicitudes internas. Se solicita contemplar por lo menos 2 análisis de código por año y el respectivo Re-test de cada uno de los análisis efectuados, los análisis de penetración a las herramientas se solicita estimación de por lo menos 3 por año.

Se solicita especificar la cantidad de líneas de código de las aplicaciones, sus lenguajes de programación, si son web, cliente servidor, on premise, nube y si el cliente tiene acceso al código fuente

Respuesta: Nos permitimos aclarar que no contamos con esta información ya que estos análisis se realizan sobre desarrollos nuevos.

Observación 33: Aseguramiento y gestión de vulnerabilidades: Anualmente se deberán generar dos (2) análisis de vulnerabilidad, Ethical Hacking y penetración a la plataforma tecnológica, a los que se deberá elaborar una matriz de seguimiento de los hallazgos encontrados y los planes de remediación y/o mitigación, el cual deberá ser gestionado por EL PROVEEDOR. Para cada uno de los análisis se debe contemplar todos los dispositivos activos de LA PREVISORA S.A los cuales se estiman en un promedio de 600 objetivos. Por otra parte, se debe contemplar análisis de vulnerabilidades a demanda adicionales para nuevas aplicaciones y/o solicitudes internas. Se solicita contemplar por lo menos 2 análisis de código por año y el respectivo Re-test de cada uno de los análisis efectuados, los análisis de penetración a las herramientas se solicita estimación de por lo menos 3 por año.

Se solicita aclarar cuál es el alcance del ethical hacking y su periodicidad

Respuesta: Nos permitimos aclarar que la definición detallada de los 600 objetivos se realizara en conjunto con el proveedor seleccionado, el escaneo de vulnerabilidades será sobre los 600 objetivos así como su correspondiente re-test, con una periodicidad de 2 veces al año (primer semestre escaneo de vulnerabilidades, segundo semestre el re-test), para el caso del ethical hacking se efectúa sobre los sistemas de información CORE de negocio que promedian en 20 aplicaciones o según defina la prioridad la Gerencia de Riesgos con una periodicidad de 1 vez al años.

Observación 34: Se deberá apoyar el proceso de cierre de vulnerabilidades a través de soporte personalizado con cada uno de los administradores de la plataforma tecnológica que fue evaluada en las pruebas de intrusión. Evaluar las vulnerabilidades detectadas en el Ethical Hacking y sus remediaciones, entregando la remediación final previo análisis de impacto de dicha implementación. El aseguramiento de la plataforma deberá considerar la implementación de las recomendaciones resultado de las pruebas de intrusión, Ethicat Hacking y escaneo de vulnerabilidades.

Se solicita modificar este requerimiento por "Se deberá apoyar el proceso de cierre de vulnerabilidades a través de soporte personalizado con cada uno de los administradores de la plataforma tecnológica que fue evaluada en las pruebas de intrusión. Evaluar las vulnerabilidades detectadas en el Ethical Hacking y sus remediaciones, entregando la

remediación final previo análisis de impacto de dicha implementación. Para el aseguramiento de la plataforma deberá considerar el acompañamiento para la implementación de las recomendaciones resultado de las pruebas de intrusión, Ethical Hacking y escaneo de vulnerabilidades." dado que el SOC no es el administrador ni responsable de las plataformas y es el cliente quien conoce su infraestructura y el SOC actúa como consultor de seguridad alienado con las buenas prácticas de seguridad

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta a razón de que estas actividades hacen partes de los roles de los recursos Analistas de Seguridad y no del servicio SOC.

Observación 35: 3.3.7.2.2. TECNICO DE SEGURIDAD TI:

Personal calificado para brindar soporte a las plataformas de seguridad manejadas por la compañía (Firewall, Antivirus, Office365, OIG, entre otras que pertenezcan a la gestión de seguridad de LA PREVISORA S.A), mantener adecuadamente los sistemas y realizar las respectivas mejoras y seguimientos de estas.

Se solicita especificar si este servicio se refiere a prestar el apoyo a los administradores de las plataformas

Respuesta: Nos permitimos aclarar que su entendimiento no es correcto, el servicio solicitado en el numeral 3.3.7.2 SERVICIOS DE SEGURIDAD ADMINISTRADA ahe referencia a Gestión administrada, por lo cual el técnico de seguridad prestara el servicio de soporte de las plataformas de seguridad de la Previsora, sin embargo, se confirma que estas cuentan con soportes especializados y de fabrica respectivamente.

Observación 36: Personal calificado para brindar soporte a las plataformas de seguridad manejadas por la compañía (Firewall, Antivirus, Office365, OIG, entre otras que pertenezcan a la gestión de seguridad de LA PREVISORA S.A), mantener adecuadamente los sistemas y realizar las respectivas mejoras y seguimientos de estas.
Se solicita especificar los productos de Office 365 con los que cuenta el cliente actualmente

Respuesta: Nos permitimos aclarar que los Productos de seguridad de Office son: DLP, AIP y antispam básico, así como el monitoreo de amenazas

Observación 37: Personal calificado para brindar soporte a las plataformas de seguridad manejadas por la compañía (Firewall, Antivirus, Office365, OIG, entre otras que pertenezcan a la gestión de seguridad de LA PREVISORA S.A), mantener adecuadamente los sistemas y realizar las respectivas mejoras y seguimientos de estas.

Se solicita especificar a que plataformas se refiere cuando menciona "entre otras que pertenezcan a la gestión de seguridad de LA PREVISORA S.A", dado que es un alcance muy amplio que difícilmente pueda ser cubierto por una persona

Respuesta: Nos permitimos indicar que otras de las aplicaciones hacen parte del servicio de seguridad son: DLP y Antispam de Office365.

Observación 38: Personal calificado para brindar soporte a las plataformas de seguridad manejadas por la compañía (Firewall, Antivirus, Office365, OIG, entre otras que pertenezcan a la gestión de seguridad de LA PREVISORA S.A), mantener adecuadamente los sistemas y realizar las respectivas mejoras y seguimientos de estas.

Se solicita especificar la cantidad de requerimientos que se reciben mensualmente por plataformas

Respuesta: Nos permitimos indicar que se tiene un promedio de 90 requerimientos mes a nivel general.

Observación 39: Personal calificado para brindar soporte a las plataformas de seguridad manejadas por la compañía (Firewall, Antivirus, Office365, OIG, entre otras que pertenezcan a la gestión de seguridad de LA PREVISORA S.A), mantener adecuadamente los sistemas y realizar las respectivas mejoras y seguimientos de estas.

Se solicita especificar a que se refiere con OIG

Respuesta: Nos permitimos indicar que OIG (Oracle Identity Gobernance) es la aplicación de ciclo de vida de los usuarios de La Previsora.

Observación 40: Personal calificado para brindar soporte a las plataformas de seguridad manejadas por la compañía (Firewall, Antivirus, Office365, OIG, entre otras que pertenezcan a la gestión de seguridad de LA PREVISORA S.A), mantener adecuadamente los sistemas y realizar las respectivas mejoras y seguimientos de estas.

Se solicita especificar el listado de tecnologías, fabricante, ubicación y cantidad

Respuesta: Nos permitimos aclara la siguiente información:

DISPOSITIVO	MARCA	UBICACION	CANTIDAD
Firewall	Fortinet	On-Premise	4
Antivirus (nube)	Sophos	Cloud	1
OIM	Oracle	On-Premise	2

Office365 (seguridad en nube)	Office365	Cloud	1

Observación 41: Personal calificado para brindar soporte a las plataformas de seguridad manejadas por la compañía (Firewall, Antivirus, Office365, OIG, entre otras que pertenezcan a la gestión de seguridad de LA PREVISORA S.A), mantener adecuadamente los sistemas y realizar las respectivas mejoras y seguimientos de estas.

Se solicita especificar si el soporte del antivirus será solamente desde la consola de gestión sin realizar troubleshooting en las estaciones de trabajo de usuario final

Respuesta: Nos permitimos aclarar que su entendimiento no es correcto, el soporte del antivirus implica consola y en algunos casos el ingeniero deberá realizar el respectivo soporte a los usuarios finales, es de aclarar que la herramienta cuenta con soporte de fábrica.

Observación 42: Gestionar el desarrollo e implementación de nuevas políticas, normas, directrices, procedimientos e instructivos de seguridad y ciberseguridad para el óptimo cumplimiento de los controles de seguridad descritos y manejados en cada una de las plataformas.

Se solicita aclarar si espera que este servicio se preste en horario 5x8

Respuesta: Nos permitimos indicar que el servicio brindado es de 5X8, pero que en caso de requerir alguna ventana esta deberá manejarse en horario no hábil, previamente contemplado entre las partes.

Observación 43: Contar con la disponibilidad de recibir capacitación sobre herramientas internas y recibir a satisfacción la administración y soporte base sobre el aplicativo de gestión de identidades OIG. Cabe aclarar que, para cambios de configuración específicos, incidencias y/o modificaciones sobre procesos adicionales LA PREVISORA S.A. cuenta con soporte de aplicativo y de fabricante para subsanar algún inconveniente sobre la herramienta.

Se solicita especificar la cantidad de requerimientos que se reciben mensualmente por plataformas

Respuesta: Nos permitimos indicar que los requerimientos promedio son de 10 casos, muchos de ellos son escalados al proveedor que soporta la herramienta a nivel de configuraciones.

Observación 44: Contar con la disponibilidad de recibir capacitación sobre herramientas internas y recibir a satisfacción la administración y soporte base sobre el aplicativo de

gestión de identidades OIG. Cabe aclarar que, para cambios de configuración específicos, incidencias y/o modificaciones sobre procesos adicionales LA PREVISORA S.A. cuenta con soporte de aplicativo y de fabricante para subsanar algún inconveniente sobre la herramienta.

Se solicita especificar cuál es el alcance esperado, gestión de ciclo de vida, integración de aplicaciones, creación de usuarios, modificación, eliminación, etc

Respuesta: Nos permitimos indicar que el alcance del servicio es nivel 1 a nivel técnico de a herramienta y revisión del adecuado funcionamiento del servicio, el ciclo de vida de los usuarios y demás parámetros no hacen parte de esta gestión.

Observación 45: 3.3.7.4.1. Acuerdos de Niveles de Servicio (ANS) de Gestión de Incidentes

INCIDENTES (7X24X365)					
Nivel de Criticidad	**Descripción**	**Tiempo de Atención**	**Tiempo de Solución**	**% Cumplimiento mensual (promedio TDA y TDS)**	**Entregable**
Alto	Se afecta el servicio contratado de forma total, o se está afectando a la Organización por un evento de seguridad informática	25 minutos	Máximo de 4 horas después de haber realizado el registro del caso.	99,09%	Informe del evento mínimo con la siguiente información: causa, detección, análisis, solución.
		99,83%	98,36%		El informe deberá ser entregado a más tardar 1 día hábil después de solución de este.

Se solicita modificar el requerimiento de Tiempo de Solución, por Tiempo de Respuesta. Dado que en algunos casos las soluciones de fallas no dependen del proveedor si no de un tercero o el fabricante y es imposible cumplir con un tiempo de solución cuando hay factores que afectan los tiempos. Además que existen incidentes que no relacionan servicios provistos por herramientas del SOC, los cuales no podrían ser solucionados por el SOC, dado que la solución la debería aplicar el cliente quien es el dueño de su infraestructura

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta, y el numeral 3.3.7.4. ACUERDOS DE NIVELES DE SERVICIO será modifica en Adenda N°3, así mismo se aclara que los ANS sólo aplica para la infraestructura de seguridad gestionada de forma directa por EL PROPONENTE. También se hace la claridad que todo evento o incidente que dependa de otro sistema de información para ser solucionado deberá ser registrado en la herramienta de casos provista y se escalara al ente resolutor indicado, por ende, la solución no depende del servicio contratado.

Observación 46: 3.3.7.4.2. Acuerdos de Niveles de Servicio (ANS) de Gestión de Requerimientos de Servicio.

8x5				
Nivel de Criticidad	**Descripción**	**Tiempo de Atención**	**Tiempo de Solución**	**% Cumplimiento mensual (promedio TDA y TDS)**
Alto	Requiere adición, modificación y/o cambio de parametros debido a que afecta a la Organización por una nueva funcionalidad y/o modificacion interna	30 minutos	Máximo de 8 horas después de haber realizado el registro del caso.	98,25%
		99,79%	96,71%	
Medio	Requiere adición, modificación y/o cambio de parametros debido a que afecta de forma parcial a la Organizac	2 horas	Máximo de 24 horas, después de haber realizado el registro del caso	96,30%

Se solicita modificar el requerimiento de Tiempo de Solución, por Tiempo de Respuesta. Dado que en algunos casos las soluciones de fallas no dependen del proveedor si no de un tercero o el fabricante y es imposible cumplir con un tiempo de solución cuando hay factores que afectan los tiempos.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta, y el numeral 3.3.7.4. ACUERDOS DE NIVELES DE SERVICIO será modifica en Adenda N°3, así mismo se aclara que los ANS sólo aplica para la infraestructura de seguridad gestionada de forma directa por EL PROPONENTE. También se hace la claridad que todo evento o incidente que dependa de otro sistema de información para ser solucionado deberá ser registrado en la herramienta de casos provista y se escalara al ente resolutor indicado, por ende la solución no depende del servicio contratado.

Observación 47: 3.3.7.5. HERRAMIENTAS DE GESTIÓN DE LA SOLUCIÓN

EL PROPONENTE deberá entregar a LA PREVISORA S.A. por lo menos tres (3) accesos a las herramientas de monitoreo para la validación de los controles y el seguimiento adecuado de todas las políticas, cuadros de inteligencia, dashboard entre otros, en modalidad de consulta.

Se solicita aclarar si el acceso puede ser a través de la consola web en el cual el cliente podrá identificar el estado del servicio, cuadros de mando, SLA, incidentes, etc, sin necesidad de ingresar a la consola de la plataforma SIEM como tal

Respuesta: Nos permitimos informar que si el acceso cumple con las validaciones básicas de monitoreo y gestión se estaría cumpliendo con el ítem descrito.

Observación 48: 3.3.8. ENTREGABLES
Informe general de Seguridad (aplicaciones como firewall, antivirus entre otros), este deberá contemplar temas de disponibilidad y capacidad, así como informes generales por mes sobre cada uno de los aspectos en los que interactúa el dispositivo. Firewall (validación

de firmas e IPS, Análisis de navegación y uso de tráfico de internet, análisis de usuarios y amenazas presentes, principales url visitadas y eventos relevantes realizados sobre el dispositivo), Antivirus (principales ataques y bloqueos, estado de los servidores y funcionalidades adicionales como manejo de USB y app control, así como revisión del tema de DLP), Para las demás aplicaciones se deberá contemplar los aspectos generales de las mismas y las validaciones y acciones realizadas para cada una de ellas.

Se solicita aclara si estos informes solamente aplican para las tecnologías que serán administradas

Respuesta: Nos permitimos aclarar que su entendimiento es correcto.

Observación 49: Informe con acciones, relacionadas a usuarios privilegiados, este deberá contener el resultado del monitoreo de todos los usuarios que realicen acciones de:
a. borrado, inserción y actualización y/o modificación de la información.
b. Modificación de permisos sobre los usuarios.
c. Creación de nuevos usuarios con permisos de administrador o con altos privilegios.
Este monitoreo debe realizarse sobre la infraestructura de LA PREVISORA incluyendo las respectivas bases de datos.

Se solicita especificar si el cliente cuenta con una herramienta de gestion de usuarios privilegiados PAM

Respuesta: Nos permitimos indicar que La Previsora no cuenta con un servicio de PAM, pero se contempla a futuro.

Observación 50: Se deberán contemplar capacitaciones a nivel interno de la compañía para los funcionarios de la previsora, mínimo una vez al año, estas deberán ser coordinadas entre las partes y con la debida autorización del supervisor del contrato. Es de aclarar que estas sesiones se efectúan de manera virtual donde se tratan temas de seguridad y mejores prácticas a nivel de seguridad.

Se solicita aclarar la cantidad de personas a las cuales se les dictará la capacitación y si será una sola sesión o varias sesiones

Respuesta: Nos permitimos aclarar que la periodicidad esta descrita en el numeral 3.3.8. ENTREGABLES y que la cantidad de usuarios de planta es de setecientos cincuenta y cuatro (754), sin embargo, dependerá de la estrategia de capacitación que se defino ejemplo tipo Webinar, Charla, Video, entre otros.

Observación 51: ANEXO No. 1 DISPOSITIVOS MONITOREO
Web Servers (IIS, Apache, Tomcat) *
Se solicita aclarar si las aplicaciones envían logs en formato syslog, cef, API de lo contrario especificar el formato de logs

Respuesta: Nos permitimos indicar que estas aplicaciones, por ser servicios nuevos se deberá validar entre las partes, por lo que solo se podrá revisar una vez se cuente con el proponente seleccionado. Sin embargo es de aclarar que al ser apliación estandar del mercado cualquiera se puede configurar el envió de logs en formato syslog.

Observación 52: AntiVirus / DLP Server *
Se solicita especificar si la consola es cloud o on premise

Respuesta: Nos permitimos indicar que la consola de antivirus/DLP Server es cloud.

Observación 53: Other Applications (ERP, Inhouse, etc) * - ARANDA
Se solicita especificar si este componente permite el envió de logs o la integración mediante API
Respuesta: Nos permitimos indicar que estas aplicaciones, por ser servicios nuevos se deberá validar entre las partes, por lo que solo se podrá revisar una vez se cuente con el proponente seleccionado. Sin embargo, es de aclarar que al ser aplicación estándar del mercado cualquiera se puede configurar él envió de logs en formato syslog.

Observación 54: Salesforce,Litisoft
Se solicita especificar si este componente permite el envio de logs o la integracion mediante API

Respuesta: Nos permitimos indicar que estas aplicaciones, por ser servicios nuevos se deberá validar entre las partes, por lo que solo se podrá revisar una vez se cuente con el proponente seleccionado. Sin embargo, es de aclarar que al ser aplicación estándar del mercado cualquiera se puede configurar él envió de logs en formato syslog.

Observación 55: ARANDA, Salesforce, Litisoft

Se solicita aclarar cuál es el objetivo que espera el cliente en integrar estas aplicaciones

Respuesta: Nos permitimos aclarar que el objetivo de integración es poder monitorear los eventos y controles de seguridad, como creación de cuentas de usuario privilegiado, acceso no autorizados, intentos de intrusos, entre otros.

Observación 56: Debido a que en la actualidad solo se tiene un porcentaje mínimo de monitoreo de algunas herramientas se solicita estimar la capacidad respectiva para cubrir los dispositivos anteriormente manejados

Se solicita aclarar la cantidad de fuentes que se encuentran actualmente integradas

Respuesta: Nos permitimos indicar que en la actualidad se cuentan con los sistemas críticos de la compañía incluido el DA y todos los servicios de seguridad (firewall, antivirus, office365)

Observación 57: Debido a que en la actualidad solo se tiene un porcentaje mínimo de monitoreo de algunas herramientas se solicita estimar la capacidad respectiva para cubrir los dispositivos anteriormente manejados

Se solicita aclarar si durante la etapa de migración se van a integrar solamente las fuentes actuales y durante el afinamiento se integraría el resto, dado que en 1 mes no es posible la integración de 500 fuentes

Respuesta: Nos permitimos aclarar que su entendimiento es correcto, así mismo sobre el numeral 3.3.7.1 SERVICIOS DE SOC de describe que se otorgara una etapa de afinación y estabilización del servicio

Observación 58: Debido a que en la actualidad solo se tiene un porcentaje mínimo de monitoreo de algunas herramientas se solicita estimar la capacidad respectiva para cubrir los dispositivos anteriormente manejados

Se solicita especificar la ubicación de todas las fuentes a integrar, datancenter propio, on premise, cloud, colocation, etc

Respuesta: Nos permitimos aclarar que:

Punto 1: Nos permitimos informar que el promedio de EPS actual es de 1500, pero es de aclarar que esta información solo es una parte de lo que se requiere monitorear. Para mayor claridad por favor remitirse al ANEXO No. 1 DISPOSITIVOS MONITOREO

Punto

2: Se informa que este detalle de información se entregara al oferente seleccionado, junto con el inventario de sistemas de información, para generalidad por favor remitirse al ANEXO No. 1 DISPOSITIVOS MONITOREO

Observación 59: 1.21 CRONOGRAMA DE LA INVITACIÓN ABIERTA
Se solicita prórroga para la presentación de la oferta para el 2 de junio de 2021 de tal forma que permita presentar la oferta de acuerdo a la respuesta de las observaciones.

Respuesta: De manera atenta se informa el numeral 1.21 CRONOGRAMA DE LA INVITACIÓN ABIERTA se ajustó mediante Adenda N°2 publica el 25 de mayo de 2021 en la página web de La Previsora.

Observación 60: solicitamos por favor compartir el documento relacionados en el borrador del contrato de:

1. La política de seguridad de la PREVISORA señalada en el numeral 15 de cláusula novena.

2. “los reglamentos internos” de la PREVISORA a los que hace relación la cláusula vigésima quinta

Respuesta: Agradecemos su observación y dichos documentos serán suministrados al proveedor que quede seleccionado.

XIX. OBSERVACIONES PRESENTADAS POR LA EMPRESA IKUSI

Observación 1: GRUPO DE (4) CUATRO ANALISTAS SOC – REMOTO: Los recursos solicitados son los mínimos requeridos para la operación del SOC (Para el óptimo cumplimiento del servicio EL PROPONENTE asignara el personal que considere necesario para cumplir con los ANS respectivos, descritos en la presente invitación y cumpliendo con todas las obligaciones mínimas relacionadas al servicio de SOC Nivel 2).

Solicitamos amablemente se indique que dedicación mínima se espera para este cargo, o si esta es libre de ajustar por el proponente, siempre y cuando se garanticen los ANS y de acuerdo con sus esquemas de mallas de trabajo definidas para tal fin.

Respuesta: Nos permitimos aclarar que el recurso GRUPO DE (4) CUATRO ANALISTAS SOC – REMOTO es el mínimo requerido, el proponte deberá disponer de la cantidad necesaria para cumplir con los ANS establecidos en el proceso y sus Adendas, así mismo se informa que estos recursos no son dedicados a la entidad ya que lo requerido es el servicio que prestan, el proponente es libre de ajustar cantidad, horario, turnos, forma, conexión, siempre y cuando se garantice los ANS.

Observación 2: DOS (2) ANALISTAS DE SEGURIDAD TI: LA PREVISORA S.A (Presencial y/o Remoto) dispondrá en la sede principal un (1) espacio de trabajo físico (puesto de trabajo con extensión telefónica y punto de red), para uno de los analistas, el segundo analista deberá trabajar de manera remota y EL PROPONENTE deberá garantizar los elementos necesarios para la prestación del servicio (Computador y teléfono de contacto).

Se entiende por la descripción que estos dos perfiles deben tener dedicación 100% para el servicio. Solicitamos respetuosamente confirmar si esto es así, o se tiene proyectada una dedicación mínima para estos cargos.

Respuesta: Nos permitimos aclarar su entendimiento es correcto y el detalle esta descrito en el numeral 3.3.7.2.1. ANALISTAS DE SEGURIDAD TI del pliego de condiciones.

Observación 3: UN (1) TECNICO DE SEGURIDAD TI LA PREVISORA S.A en la sede principal brindará el espacio de trabajo físico (puesto de trabajo con extensión telefónica y punto de red), EL PROPONENTE deberá garantizar los elementos necesarios para la prestación del servicio (Computador y teléfono de contacto).

Se entiende por la descripción que este dos perfil debe tener dedicación 100% para el servicio. Solicitamos respetuosamente confirmar si esto es así, o se tiene proyectada una dedicación mínima para este cargo.

Respuesta: Nos permitimos aclarar que el TECNICO DE SEGURIDAD TI LA PREVISORA S.A contara con una dedicación del 100%, para mayor entendimiento se modificara el numeral 3.3.7.2.2. TECNICO DE SEGURIDAD TI en la Adenda N°3.

Observación 4: EL PROPONENTE seleccionado deberá asignar los recursos y perfiles necesarios para cumplir con el objeto contractual, sin embargo, deberá adjuntar con su propuesta las hojas de vida y las certificaciones de experiencia de los recursos mínimos con los cuales ejecutará el contrato y que a continuación se relacionan:

EL PROPONENTE seleccionado deberá allegar a la PREVISORA S.A cinco (5) días después de la publicación del acta de adjudicación las hojas de vida, las certificaciones de experiencia y certificaciones de estudio de los recursos mínimos con los cuales ejecutará el servicio.

En el primer parrafo (pág-38), se indica que se deben incluir las hojas de vida con la propuesta, sin embargo, en el segundo parrafo (pág-43), se indica que el proponente seleccionado debe adjuntar esta información cinco días hábiles después de la adjudicación. Solicitamos amablemente aclarar si las hojas de vida con sus respectivos soportes deben ser adjuntadas por todos los proponentes en la fase de oferta, o únicamente el proponente adjudicado en los plazos que se indican en la página 43.

Respuesta: Nos permitimos indicar que para una mayor claridad se realizara modificación en el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE, mediante Adenda N°3.

Observación 5: Contener o neutralizar los ataques detectados en caso de presencia de amenazas, para estos eventos se deberá contar con una matriz de incidencias y deberá estar avalada por LA PREVISORA S.A.

Solicitamos amablemente se indique si la contención o neutralización mencionada, implica la gestión de las herramientas de seguridad con las que cuenta la entidad, o por el contrario el alcance del SOC es reportar a los administradores de estas plataformas y apoyar/asesorar a estos en la resolución o contención de dichos ataques.

Respuesta: Nos permitimos aclarar que el servicio solicitado requiere respuesta sobre eventos, por lo cual para temas de ataques se deberán tomar las acciones pertinentes. Así mismo el servicio cuenta con personal que administrara las plataformas respectivas por lo

cual se podría manejar un nivel de configuración especifico. Si los dispositivos involucrados hacen parte de la gestión del servicio de seguridad de TI, el recurso Técnico de Seguridad TI deberá estar en capacidad de solventar, contener o neutralizar los eventos en las plataformas definidas en su gestión, si las plataformas involucradas no hacen parte del servicio contratado La Previsora es la responsable de ejecutar las acciones, configuración recomendadas por el Grupo de SOC o Analistas de Seguridad TI.

Observación 6: Aseguramiento y gestión de vulnerabilidades: Anualmente se deberán generar dos (2) análisis de vulnerabilidad, Ethical Hacking y penetración a la plataforma tecnológica, a los que se deberá elaborar una matriz de seguimiento de los hallazgos encontrados y los planes de remediación y/o mitigación, el cual deberá ser gestionado por EL PROVEEDOR. Para cada uno de los análisis se debe contemplar todos los dispositivos activos de LA PREVISORA S.A los cuales se estiman en un promedio de 600 objetivos. Por otra parte, se debe contemplar análisis de vulnerabilidades a demanda adicionales para nuevas aplicaciones y/o solicitudes internas. Se solicita contemplar por lo menos 2 análisis de código por año y el respectivo Re-test de cada uno de los análisis efectuados, los análisis de penetración a las herramientas se solicita estimación de por lo menos 3 por año

Solicitamos respetuosamente si la entidad cuenta con las herramientas de escaneo, gestión de vulnerabilidades y análisis de código y el Analista se debe encargar únicamente de su gestión, o por el contrario se deben contemplar en el servicio las herramientas y licencias para llevar a cabo los procesos indicados en el numeral.

Respuesta: Nos permitimos aclarar que la entidad no cuenta con ninguna herramienta de las mencionadas y esta deberá ser provista como servicio como se describe en el numeral 3.3.7.5. HERRAMIENTAS DE GESTIÓN DE LA SOLUCIÓN ya que el servicio de análisis de vulnerabilidad, Ethical Hackin hacen parte integral del servicio, así como los Analistas deben encargarse de su gestión y administración, por lo que debe contemplar el servicio de las herramientas y licenciamiento.

Observación 7: Personal calificado para brindar soporte a las plataformas de seguridad manejadas por la compañía (Firewall, Antivirus, Office365, OIG, entre otras que pertenezcan a la gestión de seguridad de LA PREVISORA S.A), mantener adecuadamente los sistemas y realizar las respectivas mejoras y seguimientos de estas.

Solicitamos amablemente aclarar si este cargo será responsable de la administración de las plataformas de seguridad perimetral, o si actuará como un soporte adicional a los administradores de cada plataforma. Si es posible precisar cuáles serían estas plataformas.

Respuesta: Nos permitimos aclarar que su entendimiento no es correcto, el servicio solicitado en el numeral 3.3.7.2 SERVICIOS DE SEGURIDAD ADMINISTRADA hace referencia a Gestión administrada, por lo cual el técnico de seguridad prestara el servicio de soporte de las plataformas de seguridad de la Previsora, sin embargo, se confirma que estas cuentan con soportes especializados y de fabrica respectivamente. Las plataformas en inicio serian Firewall, Antivirus, Office365, OIG.

Observación 8: a. Servicio de monitorización inteligente de eventos de seguridad en modalidad 7x24. La gestión de incidentes se debe realizar a través de la herramienta entregada por LA PREVISORA S.A.

1. Solicitamos a entidad aclarar los niveles de disponibilidad requeridos para la prestación del servicio, y los niveles de disponibilidad de la plataforma SIEM que soportará el servicio.

Respuesta: Nos permitimos indicar que el servicio debe contemplar el cumplimiento de disponibilidad de 99.5%, por lo que el numeral 3.3.7.4. ACUERDOS DE NIVELES DE SERVICIO será modificado mediante Adenda N°3

2. Solicitamos aclarar a la entidad cual es la herramienta de gestión utilizada? La integración se debe realizar por API?

Respuesta: Nos permitimos aclarar que la herramienta de gestión es Aranda la cual es tercerizada, al ser un servicio WEB se considera que se puede integrar mediante API, sin embargo esto deberá revisarse en las primeras reuniones entre el proveedor seleccionado y los administradores de la herramienta.

3. Amablemente solicitamos a la entidad que para el proceso de gestión de incidentes, la herramienta SIEM incorpore nativamente un sistema de ticketing y de esa forma adoptar de forma natural el proceso de gestión de incidentes durante los procesos de análisis y detección de amenazas.

Respuesta: Nos permitimos indicar que, si bien la herramienta de SIEM tiene su sistema de ticketing nativo, esta no será accedida por la entidad ya que contar con doble sistema para la gestión de incidentes no es viable, por lo cual su observación no será tenida en cuenta

Observación 9: b. Detectar y recolectar las evidencias de los eventos (incidencias maliciosas o falsos positivos), que ocurran sobre la infraestructura de LA PREVISORA S.A y dispositivos de red, que puedan poner en peligro la seguridad de la misma.

Solicitamos amablemente a la entidad que contemple incorporar las siguientes variables como críticas dentro del proceso de detección:

• Actualización continua del contexto, de los dispositivos, su software y parches instalados, así como los servicios en ejecución.
• Contexto de usuario, en tiempo real, con seguimiento de direcciones IP, cambios de identidad de usuario, contexto de datos de ubicación física y geo-localización.
• Detectar dispositivos, aplicaciones de red y cambios de configuración no autorizados.
• Monitor de métricas de sistemas integrados en el proceso de monitoreo.

Respuesta: Nos permitimos aclarar que en el anexo N°5 ALCANCE SOC se especifica los requerimientos mínimos del servicio, si la plataforma ofrece adicionales, la previsora acepta las especificaciones y beneficios que esta ofrezca

1. Amablemente solicitamos a la entidad, que como base de servicio se permita el descubrimiento de dispositivos y mantener una base de datos de configuraciones (CMDB), mediante técnicas de auto-descubrimiento y aprendizaje de activos y mapeos inter-relacionales, en entornos tanto físico como virtuales y de cloud, de aplicaciones, usuarios, y dispositivos. En este sentido, el servicio ofertado deberá tener CMDB nativa dentro de la propia herramienta de SIEM.

Respuesta: Nos permitimos aclarar que la entidad no está sesgando las configuraciones de las herramientas de SIEM y que se acepta las especificaciones y beneficios adicionales que esta ofrezca, sin costo alguno para la entidad.

Observación 10: f. Notificación proactiva de amenazas proporcionando soluciones y estrategias de mitigación, tomar medidas para proteger los sistemas y redes afectados o amenazados por la actividad de intrusos y desarrollar otras estrategias de respuesta o solución alternativa, con escenarios de crisis contra ataques dirigidos como DDoS o amenazas avanzadas.

1. Es de nuestro entendimiento que la entidad busca conjunto de respuestas pre-configuradas ante eventos de seguridad, de manera que se permita no sólo la detección sino también la remediación automatizada ante determinadas amenazas.

Respuesta: Nos permitimos aclarar que su entendimiento es adecuado

2. Es de nuestro entendimiento que la entidad busca la posibilidad de activar una secuencia de comandos de corrección cuando se produce un incidente específico?

Respuesta: Nos permitimos aclarar que su entendimiento es adecuado

Observación 11: h. EL PROPONENTE deberá contar con una herramienta SIEM en modalidad de servicio en nube para el análisis de los registros de eventos de los equipos de seguridad existentes (IPS's, Firewalls, Endpoint, Sandbox, UBA, etc) y respuesta ante eventos inusuales, la integración de la herramienta deberá contemplar múltiples formas de integración, así como envió de logs, agentes u otro para dejar operativo todos los servicios que se requieran monitorear.

1. Solicitamos amablemente a la entidad incorporar a la solución de SIEM de nueva generación usada dentro del servicio realizar monitoreo de integridad de archivos en los servidores monitoreados basado en agente, asi como monitorear los cambios

no autorizados de las configuraciones de los dispositivos de redes, esto permitirá establecer un análisis holístico requerido para enfrentar las amenazas actuales y al tiempo garantizar altos estándares de cumplimiento de estándares internacionales.

2. Solicitamos amablemente a la entidad que en aras de mantener altos niveles de rendimientos y para cantidad de plataformas a monitorear, se permita instalación en premisas para responder de forma eficiente y tiempos cercanos al tiempo real en el proceso de detección de amenazas.

Respuesta: Nos permitimos aclarar que:

Punto 1: La Previsora en el numeral 3.3.7.1 SERVICIOS DE SOC detalla a nivel general los elementos de monitoreo entre ellos la analítica de datos, esta observación está incluido en el pliego de condiciones, las demás reglas o políticas específicas de monitoreo se definen con el proveedor seleccionado.

Punto 2: No es clara su observación, pero se indica que, si se requiere la implementación de colectores, los costos e infraestructura deberán correr por parte del proponente, sin ningún costo adicional para la entidad.

Observación 12: k. Proveer en modalidad de servicio, soportada y gestionada una plataforma de análisis de comportamiento de usuarios (UBA) por lo menos 200 usuarios sensibles seleccionados por LA PREVISORA S.A.

1. Solicitamos a la entidad que sea requerido el establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana.

2. Sugerimos amablemente a la entiedad que el servicio de UEBA no conlleve consumo asociado ni de licencia de dispositivos ni de EPS en relación con los disipativos monitoreados, todo con el objeto garantizar un sistema autónomo de UEBA.

Respuesta: Nos permitimos aclarar que:

Punto 1: Las configuraciones y demás políticas para el servicio solicitado serán validadas en conjunto con el proponente seleccionado.

Punto 2: En el numeral 3.3.7.5. HERRAMIENTAS DE GESTIÓN DE LA SOLUCIÓN se describe que el Proponente deberá contar con todas las herramientas necesarias para la prestación del servicio.

Observación 13: EL PROPONENTE deberá ofrecer un servicio integral de SOC, el cual contemple durante la etapa de operación, en los primeros seis (6) meses del servicio, la ejecución del afinamiento y estabilización respectivo de la plataforma de SIEM que ofrezca, para las aplicaciones y demás servicios específicos, alineado a una operación de nivel 1 "Monitorización y análisis"

1. Muy amablemente se solicita a la entidad clarificar si la solución SIEM es requerida en alta disponibilidad.

Respuesta: El proponente deberá adecuar el diseño de la solución SIEM con el fin de cumplir con los ANS estipulados en el servicio.

2. Es de nuestro entendimiento que la entidad solicita una solución de SIEM de nueva generación la cual permita monitorear tanto la seguridad (SIEM), como la disponibilidad y el desempeño de las plataformas (SOC/NOC), de esa forma se puede disponer de un único punto de gestión de datos no sólo de eventos de seguridad, sino también de:
   ◦ Rendimiento y disponibilidad
   ◦ CPU, memoria y almacenamiento.
   ◦ Detección de cambios de configuración.
   ◦ Monitorización de transacciones sintéticas.
   ◦ Cuadros de mando dinámicos

Respuesta: Nos permitimos aclarar que:

Punto 1: El servicio debe contemplar el cumplimiento de disponibilidad de 99.5%, por lo que el numeral 3.3.7.4. ACUERDOS DE NIVELES DE SERVICIO será modificado en Adenda N°3

Punto 2: El servicio solicita sobre un SIEM de nueva generación es para el monitoreo, análisis, gestión y respuesta de incidentes de seguridad y ciberseguridad (SOC Nivel 2). No se contempla servicios de monitoreo de infraestructura tipo NOC. Si la herramienta la proporciona es independiente y no es una exigencia de la entidad.

Observación 14: A continuación, se presenta la tabla para los requerimientos reportados y evidenciadas con horario 8X5 sobre las herramientas y sólo aplica para la infraestructura de seguridad gestionada de forma directa por EL PROPONENTE.

1. Solicitamos a entidad aclarar los niveles de disponibilidad requeridos para la prestación del servicio, y los niveles de disponibilidad de la plataforma SIEM que soportará el servicio.

Respuesta: Nos permitimos aclarar que el detalle se modificara el numeral 3.3.7.4. ACUERDOS DE NIVELES DE SERVICIO en la Adenda N°3, para especificar los ANS de disponibilidad requerida para el servicio.

Observación 15: Debido a que en la actualidad solo se tiene un porcentaje mínimo de monitoreo de algunas herramientas se solicita estimar la capacidad respectiva para cubrir los dispositivos anteriormente manejados

Solicitamos respetuosamente se indique la cantidad de eventos por segundo (EPS) que se reciben en la plataforma actual de monitoreo de seguridad. En caso de no contar con este valor, indicar por cada sistema una descripción y un estimado de los logs generados.

Respuesta: Nos permitimos informar que el promedio de EPS actual es de 1500, pero es de aclarar que esta información solo es una parte de lo que se requiere monitorear. Para mayor claridad por favor remitirse al ANEXO No. 1 DISPOSITIVOS MONITOREO

Observación 16:

La distribución de los costos incluido-impuestos por periodo corresponde a: Servicios de Seguridad - SOC

Año	2021	(Sep-Dic)	=	$	247.954.689
Año	2022	(Ene-Dic)	=	$	743.864.068
Año	2023	(Ene-Dic)	=	$	743.864.068
Año	2024	(Ene-ago)	=	$	495.909.379

Total 36 meses = $ 2.655.594.723

Solicitamos amablemente a la entidad revisar y aclarar el valor de cada año, debido a que al sumar los periodos existe una diferencia frente al valor total del presupuesto.

Respuesta: Nos permitimos aclarar que los valores de las vigencias están sin IVA y el total ya tienen incluido el IVA, de igual forma para mayor claridad se efectuara modificación en el numeral 1.4 FINANCIACIÓN Y PRESUPUESTO OFICIAL en la Adenda N°3.

Observación 17: El objeto, actividades u obligaciones sean iguales o similares al de la presente invitación. Entendiéndose por similar que consista en la prestación de servicios administrados de seguridad y/o servicios de SOC.

Solicitamos amablemente a la entidad aceptar que en el objeto del contrato y/o actividades incluya NOC/SOC, debido a que las compañías, hoy en día, en un solo proceso incluyen ambos servicios (NOC/SOC) y no discriminan el valor de dichos servicios por ser servicios administrados. Esta aceptación por parte de la entidad, permitirá la pluralidad de participación de oferentes.

Respuesta: Nos permitimos informar que su observación es válida a razón de que el objeto y/o actividades son similares a las solicitadas en el pliego de condiciones, toda vez que sea SOC/NOC y no solamente NOC.

Observación 18: Una de las tres certificaciones con las cuales se pretende acreditar la experiencia mínima habilitante debe corresponder a empresas del Sector Gobierno o Sector Financiero.

Teniendo en cuenta que este servicio no es común en el sector financiero o público debido a la información que protege este mercado. Solicitamos amablemente a la entidad aceptar

contratos que se encuentren en ejecución en un porcentraje > o = al 50% para que exista pluralidad de participación de oferentes en beneficio de la entidad. De lo contrario, solicitamos amablemente a la entidad eliminar este requerimiento aclarando que este servicio tecnológico aplica y es calificable para cualquier compañía que se encuentre en cualquier sector.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE será modificará mediante Adenda N°3

Observación 19: EL PROPONENTE deberá allegar con su propuesta las siguientes certificaciones, que se encuentren vigentes:

• Certificación ISO 27001.

Solicitamos amablemente a la entidad aclarar que el SOC que ofrecerá el proponente debe estar certificado en ISO 27001 (Vigente), así mismo debe incluir en el alcance de la certificación la administración y/o implementación y/o administración de vulnerabilidades objeto de este proceso. De tal manera, que el futuro contratista garantizará bajo dicha normatividad la ejecución de los servicios solicitados por la entidad.

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta

Observación 20: EL PROPONENTE seleccionado deberá asignar los recursos y perfiles necesarios para cumplir con el objeto contractual, sin embargo, deberá adjuntar con su propuesta las hojas de vida y las certificaciones de experiencia de los recursos mínimos con los cuales ejecutará el contrato

Solicitamos amablemente a la entidad aceptar que las hojas de vida y certificaciones de experiencia sean entregadas a la firma del acta de inicio, tal como se describe en la página 43, la cual meciona lo siguiente: ...EL PROPONENTE seleccionado deberá allegar a la PREVISORA S.A cinco (5) días después de la publicación del acta de adjudicación las hojas de vida, las certificaciones de experiencia y certificaciones de estudio de los recursos mínimos.

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta, sin embargo, para mayor entendimiento se realizará ajuste del numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE sobre en Adenda N°3

Observación 21: UN (1) GERENTE DE SERVICIO:
* con especialización y/o maestría en Seguridad Informática, Seguridad de la información o seguridad en las TIC.
* Contar con al menos una (1) de las siguientes certificaciones de seguridad o sus equivalentes

Teniendo en cuenta que la entidad claramente da a conocer que la principal función del Gerente de Servicio es: El Gerente de Servicio es la persona encargada de la parte operativa y único canal entre las partes, de manera administrativa durante la vigencia del contrato. Así mismo, como lo define el ente rector PMI (Project Management Institute), quienes forman los Gerentes de Proyectos y/o servicios; este rol tiene por objeto administrar y/o gerenciar el proyecto, quien es el canal principal con las personas que se involucran, procesos, procedimientos, facturación y las demás funciones para que a nivel operativo que cumpla el contrato a cabalidad. Por lo anterior, solicitamos amablemente a la entidad reemplazar o dar la opción en los requerimientos de especialización y/o maestría relacionada con la "seguridad" por "Gerencia de Proyectos" y que la certifcación en "seguridad" sea reemplazada o dar la opción por la certificación "PMP". Lo anterior permite la pluralidad de participación de oferentes.

Respuesta: No es posible adicionar esta certificación, ya que lo que se solicita es que el Gerente de Servicio cuente con conocimientos de seguridad Informática/ Seguridad de la Información o Ciberseguridad y la PMP es una certificación de Gerencia de Proyectos a nivel general.

Observación 22: GRUPO DE (4) CUATRO ANALISTAS SOC – REMOTO
*-Se debe acreditar al menos (1) de las siguientes certificaciones

Solicitamos amablemente a la entidad incluir como opcional la certificación ISO 27001, la cual es válida para acreditar sus conocimientos, ejecutar el rol y las actividades descritas por la entidad.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE será modificará mediante Adenda N°3

Observación 23: DOS (2) ANALISTAS DE SEGURIDAD TI: LA PREVISORA S.A (Presencial y/o Remoto) dispondrá en la sede principal un (1) espacio de trabajo físico (puesto de trabajo con extensión telefónica y punto de red), para uno de los analistas, el segundo analista deberá trabajar de manera remota y EL PROPONENTE deberá garantizar los elementos necesarios para la prestación del servicio (Computador y teléfono de contacto).

Solicitamos a la entidad aclarar si estos dos (2) Analistas de Seguridad TI de forma presencial la entidad suministrará el espacio y/o puesto de trabajo.

Respuesta: Nos permitimos aclarar el detalle de su observación, la pueden encontrar en el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones.

Observación 24: DOS (2) ANALISTAS DE SEGURIDAD TI:
* Se debe acreditar al menos una (1) de las siguientes certificaciones o su equivalente:

Solicitamos amablemente a la entidad incluir como alternativa la certificación ISO 27001, la cual es válida para acreditar sus conocimientos, ejecutar el rol y las actividades desctitas por la entidad.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE será modificará mediante Adenda N°3

Observación 25: LA PREVISORA S.A actualmente cuenta con un SOC tercerizado tradicional nivel 1, que monitoriza y analiza eventos de la infraestructura tecnológica core de negocio y busca fortalecer la seguridad con los nuevos desafíos, por lo que se contempla la evaluación de nivel 1 a nivel 2 “Análisis exhaustivo y de respuesta”. EL PROPONENTE deberá ofrecer un servicio integral de SOC, el cual contemple durante la etapa de operación, en los primeros seis (6) meses del servicio, la ejecución del afinamiento y estabilización respectivo de la plataforma de SIEM que ofrezca, para las aplicaciones y demás servicios específicos, alineado a una operación de nivel 1 “Monitorización y análisis”. Finalizada esta etapa la operación del SOC deberá cumplir con un nivel 2 “Análisis exhaustivo y de respuesta” alineado con las mejores prácticas y acorde a las necesidades de LA PREVISORA S.A.

Solicitamos amablemente a la entidad aclarar, cuál sería el objeto de tener otro SOC de nivel 1 por seis (6) meses, si este ya se encuentra contratado por el operador existente.

Por otro lado, recomendamos a la entidad que el SOC que tiene actualmente continúe con el servicio de nivel 1, y más bien, entre el operador actual que opera el SOC tercerizado de nivel 1 y el nuevo operador del SOC nivel 2 se acuerde los incidentes que se deben priorizar y ser atendidos por el nuevo operador. Esto se debe a que la entidad claramente informa en el segundo párrafo que el nuevo operador en los primeros seis (6) meses estará alineado a la operación de nivel 1.

Respuesta: Nos permitimos aclarar que el SOC es tercerizado y cuando se adjudique el presente proceso, el proponente seleccionado deberá hacer un empalme y/o transición con el proveedor actúa, garantizando el mínimo servicio para iniciar la operación. Para posterior hacer le mejor del servicio al siguiente Nivel.

Observación 26: LA PREVISORA S.A entregará la herramienta para la gestión de alertas, incidentes, problemas, requerimientos, cambios y demás que permita documentar las causas, los tratamientos y la solución de dichos eventos, de igual forma se debe establecer las responsabilidades, roles y los procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes y requerimientos en la seguridad

Solicitamos a la entidad informar cómo se llama la herramienta que actualmente tienen, Quién la ópera. Cuál es el fabricante de la herramienta. La entidad será responsable de la transferencia del conocimiento de la herramienta al nuevo proveedor.

Respuesta: Nos permitimos aclarar que la herramienta para la gestión de los casos actual de La Previsora es Aranda, y es posible realizar la trasferencia de conocimiento para su manejo y uso a los recursos requeridos.

Observación 27: Para lo anterior se deberá adjuntar con su propuesta, la siguiente documentación para cada uno de los profesionales propuestos,
Solicitamos amablemente a la entidad aceptar que las hojas de vida y certificaciones de experiencia sean entregadas a la firma del acta de inicio, tal como se describe en la página 43, la cual menciona lo siguiente: ...EL PROPONENTE seleccionado deberá allegar a la PREVISORA S.A cinco (5) días después de la publicación del acta de adjudicación las hojas de vida, las certificaciones de experiencia y certificaciones de estudio de los recursos mínimos. Así mismo, la entidad informa lo siguiente: Para los siguientes recursos solicitados y garantizar que EL PROPONENTE CUMPLE O NO CUMPLE debe presentar con su propuesta una certificación suscrita por el Representante Legal, en la que se compromete a proveer los recursos mínimos necesarios para la operación del servicio durante la vigencia del contrato.

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta, sin embargo, para un mayor entendimiento se realizará ajuste del numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones mediante Adenda N°3

Observación 28: 1. ISO/IEC 27002:2013.
Solicitamos a la entidad que para esta certificación se permita como alternativa la ISO/IEC 27001:2014 incluyendo en su alcance la certificación del SOC del proveedor. La cual cumple con los objetivos trazados por la entidad al presente proceso.

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta, sin embargo, se aclara que el numeral 4.1.4. CERTIFICACIONES ADICIONALES (30) PUNTOS será modificado mediante Adenda N°3.

Observación 29: 2. ISO27017.
Solicitamos amablemente a la entidad unificar esta certificación con la certificación ISO 27018, la cual cumple con el mismo servicio a nivel cloud y nube, y a su vez, se otorga 20 puntos. Esto se debe a que la certificación ISO 27017 se está remplazando por la ISO 27018 incluyendo en su alcance la certificación del SOC del proveedor.

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta, sin embargo, se aclara que el numeral 4.1.4. CERTIFICACIONES ADICIONALES (30) PUNTOS será modificado mediante Adenda N°3.

Observación 30: Se asignará puntaje de diez (10) puntos por cada una de las siguientes certificaciones adicionales para un máximo de treinta (30) puntos.

Solicitamos a la entidad que se incluya la certificación ISO 22301 con el alcance de servicios administrados en seguridad, la cual le permite a la entidad que el futuro proveedor garantice y disponga de un sistema de gestión de la continuidad del negocio.

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta, a razón de la certificación ISO 22301 hace referencia a continuas de negocio, proceso de la Gestión de Riesgos y no de la Gestión de TI, proceso que no hace parte del objeto de esta licitación, sin embargo, se aclara que el numeral 4.1.4. CERTIFICACIONES ADICIONALES (30) PUNTOS será modificado en Adenda N°3

XX. OBSERVACIONES PRESENTADAS POR LA EMPRESA WEXLER

Observación 1:

Solicitud 1

3. El valor de la sumatoria de las certificaciones deberá acreditar una cuantía igual o superior al 75% del valor del presupuesto.

Solicitamos amablemente a la entidad con el ánimo de permitir la pluralidad de oferentes aceptar que la sumatoria del valor de las certificaciones sea igual o superior 60 % del valor del presupuesto.

Respuesta: Nos permitimos informar que su observación no será tenida en cuenta, a razón que La Previsora considera el porcentaje justo para garantizar la experiencia del proponente en la ejecución del contrato de dicha magnitud.

Observación 2.

Solicitud 2

6. Los contratos certificados deben haber iniciado durante los últimos 5 años a la presentación de la presente invitación.

Solicitamos amablemente a la entidad con el ánimo de permitir la pluralidad de oferentes aceptar certificaciones de contratos terminados durante los últimos 10 años.

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta, remitirse al numeral I. OBSERVACIONES GENERALES ítem 2 “Tiempo de experiencia del Proponente” del presente documento.

Observación 3:

Respetuosamente solicitamos a la entidad no requerir dentro de los requisitos habilitantes que la empresa este certificada en la norma NTC ISO/IEC 27001:2013, ya que según el decreto 734 de 2012 de la Función Pública en el artículo 2.2.9 los requisitos que se piden para habilitar una empresa son los relacionados con:

- Requisitos jurídicos
- Condiciones de experiencia
- Capacidad financiera y de organización.

Y en ninguno de estos requisitos se encuentra que una empresa debe tener una certificación en algún sistema de gestión para poder habilitarse además que este requisito reduce la pluralidad de oferentes.

De manera respetuosa solicitamos a la Entidad se modifique este requisito, toda vez que la Ley 1150 de julio de 2007, por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos, con la cual busca darles una mayor participación a todas las empresas privadas en la contratación con el Estado Colombiano para lo cual de manera perentoria **prohíbe** la exigencia de certificados de sistemas de gestión de calidad, por parte de las entidades estatales, en los procesos de contratación que adelanta.

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta ya que La Previsora S.A. es una empresa vigilada y auditada sobre el cumplimiento de estándares de seguridad de la información del sector financiero, por lo que es importante comprobar que los proveedores, contratistas y aliados estratégicos en servicio de la entidad, cumplan con buenas prácticas de seguridad de la información, estas mismas generan confianza que estamos ante compañías competentes y confiables. Proveedores con conocimiento, experiencia, ejecución en lineamiento y cumplimiento de controles de seguridad de la información y que cumplen todos los requisitos legales derivados de la manipulación de información como ISO 27001, factores claves para garantizar que el oferente cumplirá con la mejor calidad el servicio durante la vigencia del mismo.

Observación 4.

Solicitud 4

Con el fin de cumplir con la experiencia mínima habilitante, EL PROPONENTE deberá adjuntar con su propuesta tres (3) certificaciones de contratos suscritos con empresas públicas o privadas nacionales en las que se acredite experiencia de la siguiente forma:

Solicitamos respetuosamente a la entidad con el ánimo de permitir la pluralidad de oferentes aceptar máximo 5 certificaciones de contratos suscritos con empresas públicas o privadas.

Respuesta: Nos permitimos indicar que el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE del pliego de condiciones se ajustará mediante Adenda N°3, remitirse al numeral OBSERVACIONES GENERALES ítem 3 “Número de certificaciones de experiencia general” del presente documento.

Observación 5:

Solicitud 5

3.3.4. CERTIFICADO POR PARTE DEL FABRICANTE

EL PROPONENTE deberá adjuntar con su propuesta la certificación del producto (SIEM) como canal autorizado o expedida por el fabricante o su representante en Colombia. Esta certificación deberá estar vigente al momento de la presentación de la oferta y firma del contrato.

EL PROPONENTE está obligado a velar por mantener vigente la certificación durante el plazo de ejecución del contrato y tiempo de garantía de los elementos de infraestructura.

De manera atenta solicitamos a la entidad que se modifique la solicitud, con el fin de que la Entidad tenga garantía de la calidad de servicios ofrecidos por el proponente

EL PROPONENTE deberá adjuntar con su propuesta la certificación del producto (SIEM) como Partner en el nivel de membresía más alto con el fabricante; con el fin de garantizar que se preste el mejor servicio para la entidad. Esta certificación deberá estar vigente al momento de la presentación de la oferta y firma del contrato.

Respuesta: Nos permitimos informar que su observación no será tenida en cuenta a razón de que esto limita la pluralidad de oferentes.

Observación 6:

Respecto del perfil profesional del Analista SOC, atentamente solicitamos a la entidad que se consideren como válidas las certificaciones en ISO 27035 – Incident Manager.

Perfil Profesional y Experiencia
Profesionales en Ingeniería de sistemas, electrónica, telecomunicaciones o afines con mínimo (2) años de experiencia como Analista SOC o ingenieros junior de seguridad. Tendrá la responsabilidad del análisis y la documentación de los eventos presentados, así como las respectivas remediaciones y acciones de mejora sobre la plataforma.
Certificaciones
Se debe acreditar al menos (1) de las siguientes certificaciones o su equivalente: CSA -Certified SOC Analyst - CompTIA ECIH – EC-Council Certified Incident Handler - EC-Council CNFE – Network Forensic Investigator - Mile2 CHFI – Computer Hacking Forensic Investigator - EC-Council CEH - Certified Ethical Hacker - EC-Council CRISC - Certified in Risk and Information Security Control -ISACA CPTE – Certified Pentester Engineer - Mile2 CPTIA – CREST Practitioner Threat Intelligence Analyst – CompTIA

Respuesta: Nos permitimos indicar que se ajustara numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones y este se verá reflejado mediante Adenda N°3

Observación 7:

Respecto del perfil profesional del Analista de seguridad de TI, atentamente solicitamos a la entidad que se consideren como válidas las certificaciones en Auditor Líder 27001:2013.

DOS (2) ANALISTAS DE SEGURIDAD TI:

Perfil Profesional y Experiencia	
Profesionales Titulados de Ingeniería de sistemas, telecomunicaciones o carreras afines con mínimo dos (2) años de experiencia como Analista de eventos de seguridad informática, dominio de herramientas de monitoreo y conocimiento de controles de seguridad informática, normas y regulaciones vigentes.	
Certificaciones	
Se debe acreditar al menos una (1) de las siguientes certificaciones o su equivalente: CSA -Certified SOC Analyst - CompTIA ECIH – EC-Council Certified Incident Handler - EC-Council CNFE – Network Forensic Investigator - Mile2 CHFI – Computer Hacking Forensic Investigator - EC-Council CEH - Certified Ethical Hacker - EC-Council CRISC - Certified in Risk and Information Security Control -ISACA CPTE – Certified Pentester Engineer - Mile2 CPTIA – CREST Practitioner Threat Intelligence Analyst - CompTIA	
Cantidad de hojas de vida:	2

Respuesta: Nos permitimos indicar que se ajustara numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE del pliego de condiciones y este se verá modificado en Adenda N°3

Observación 8.

Solicitud 8

De manera atenta solicitamos a la Entidad no sea obligatoria una línea telefónica 01-8000 para la atención de requerimientos, incidentes o solicitudes de servicio; *12. Disponer de los medios de recepción de requerimientos para las solicitudes de servicios o incidentes, de los cuales mínimo uno debe estar disponible 7x24X365: Línea telefónica 01-**8000, Página WEB, Correo Electrónico y Línea Celular.***

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.10. OBLIGACIONES DEL PROVEEDOR será modificará en Adenda N°3

Observación 9:

Se solicita amablemente a la Entidad analizar si es correcta nuestra apreciación ¿Las certificaciones solicitadas son del servicio en nube en la que se va a desplegar el sistema de monitoreo - SIEM?

4.1.4. CERTIFICACIONES ADICIONALES (30) PUNTOS

Se asignará puntaje de diez (10) puntos por cada una de las siguientes certificaciones adicionales para un máximo de treinta (30) puntos.

1. ISO/IEC 27002:2013. Estándar que establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

2. ISO27017. Norma que proporciona controles de seguridad para los servicios cloud

3. ISO27018.Norma que ayuda a los proveedores para proteger la información personal en la nube.

Respuesta: Nos permitimos aclarar que su apreciación no es correcta, las Certificaciones adicionales corresponden a certificaciones del proponente con las cuales le acreditara puntaje, no se está especificando que deben ser sobre el servicio del SIEM, sin embargo, el numeral 4.1.4. CERTIFICACIONES ADICIONALES (30) PUNTOS será modificado en Adenda N°3.

Observación 10:

Se solicita amablemente a la Entidad no requerir esta membresía dado que estarían dándole favorabilidad a un segmento muy pequeño del mercado colombiano que cuentan con esta acreditación, y dejaría en desventaja las empresas tales como la nuestra, que está en proceso de acreditación.

4.1.3.1. MEMBRESIA FIRST (20) PUNTOS

Se asignará el puntaje de veinte (20) puntos, a la propuesta que allegue la membresía de FIRST (Forum of Incident Response and Security Teams) como empresa

Respuesta Nos permitimos indicar que su observación no será tenida en cuenta.

Observación 11:

3.3.7.1 SERVICIOS DE SOC

a. Servicio de monitorización inteligente de eventos de seguridad en modalidad 7x24. La gestión de incidentes se debe realizar a través de la herramienta entregada por LA PREVISORA S.A.

1. Solicitamos a entidad aclarar los niveles de disponibilidad requeridos para la prestación del servicio, y los niveles de disponibilidad de la plataforma SIEM que soportará el servicio.

2. Solicitamos aclarar a la entidad ¿cual es la herramienta de gestión utilizada? ¿La integración se debe realizar por API?

3. Amablemente solicitamos a la entidad que, para el proceso de gestión de incidentes, la herramienta SIEM incorpore nativamente un sistema de ticketing y de esa forma adoptar de forma natural el proceso de gestión de incidentes durante los procesos de análisis y detección de amenazas.

Respuesta: Nos permitimos aclarar que:

Punto 1: Con respecto a los niveles de disponibilidad para la prestación del servicio y para la plataforma de SIEM esta deberá ser de 7X24x365 ya que por ser un servicio de SOC debe contar con disponibilidad de 99,5% y contar con alto contingencia, para más claridad se realiza ajuste en la Adenda N°3.

Punto 2: Actualmente la herramienta de gestión es Aranda la cual es tercerizada, al ser un servicio WEB se considera que se puede integrar mediante API, sin embargo esto deberá revisarse en las primeras reuniones entre el proveedor seleccionado y los administradores de la herramienta.

Punto 3: Nos permitimos indicar que, si bien la herramienta de SIEM tiene su sistema de ticketing nativo, esta no será accedida por la entidad ya que contar con doble sistema para la gestión de incidentes no es viable, por lo cual su observación no será tenida en cuenta.

Observación 12:

3.3.7.1 SERVICIOS DE SOC

b. Detectar y recolectar las evidencias de los eventos (incidencias maliciosas o falsos positivos), que ocurran sobre la infraestructura de LA PREVISORA S.A y dispositivos de red, que puedan poner en peligro la seguridad de la misma.

1. Solicitamos amablemente a la entidad que contemple incorporar las siguientes variables como críticas dentro del proceso de detección:

- Actualización continua del contexto, de los dispositivos, su software y parches instalados, así como los servicios en ejecución.
- Contexto de usuario, en tiempo real, con seguimiento de direcciones IP, cambios de identidad de usuario, contexto de datos de ubicación física y geo-localización.
- Detectar dispositivos, aplicaciones de red y cambios de configuración no autorizados.
- Monitor de métricas de sistemas integrados en el proceso de monitoreo.

2. Amablemente solicitamos a la entidad, que como base de servicio se permita el descubrimiento de dispositivos y mantener una base de datos de configuraciones (CMDB), mediante técnicas de auto-descubrimiento y aprendizaje de activos y mapeos inter-relacionales, en entornos tanto físico como virtuales y de cloud, de aplicaciones, usuarios, y dispositivos. En este sentido, el servicio ofertado deberá tener CMDB nativa dentro de la propia herramienta de SIEM.

Respuesta: Nos permitimos aclarar que:

Punto 1: En el anexo N°5 ALCANCE SOC se especifica los requerimientos mínimos del servicio, si la plataforma ofrece adicionales, la previsora acepta las especificaciones y beneficios que esta ofrezca

Punto 2: Nos permitimos aclarar que la entidad no está sesgando las configuraciones de las herramientas de SIEM y que se acepta las especificaciones y beneficios adicionales que esta ofrezca, sin costo alguno para la entidad.

Observación 13:

3.3.7.1 SERVICIOS DE SOC

f. Notificación proactiva de amenazas proporcionando soluciones y estrategias de mitigación, tomar medidas para proteger los sistemas y redes afectados o amenazados por la actividad de intrusos y desarrollar otras estrategias de respuesta o solución alternativa, con escenarios de crisis contra ataques dirigidos como DDoS o amenazas avanzadas.

1. Es de nuestro entendimiento que la entidad busca conjunto de respuestas pre-configuradas ante eventos de seguridad, de manera que se permita no sólo la detección sino también la remediación automatizada ante determinadas amenazas, ¿nuestro entendimiento es correcto?

2. Es de nuestro entendimiento que la entidad busca la posibilidad de activar una secuencia de comandos de corrección cuando se produce un incidente específico, ¿nuestro entendimiento es correcto?

Respuesta: Nos permitimos aclarar que:

Punto 1: Confirmamos que su entendimiento es correcto

Punto 2: Confirmamos que su entendimiento es correcto

Observación 14:

3.3.7.1 SERVICIOS DE SOC

h. EL PROPONENTE deberá contar con una herramienta SIEM en modalidad de servicio en nube para el análisis de los registros de eventos de los equipos de seguridad existentes (IPS's, Firewalls, Endpoint, Sandbox, UBA, etc) y respuesta ante eventos inusuales, la integración de la herramienta deberá contemplar múltiples formas de integración, así como envió de logs, agentes u otro para dejar operativo todos los servicios que se requieran monitorear.

1. Solicitamos amablemente a la entidad incorporar a la solución de SIEM de nueva generación usada dentro del servicio realizar monitoreo de integridad de archivos en los servidores monitoreados basado en agente, así como monitorear los cambios no autorizados de las configuraciones de los dispositivos de redes, esto permitirá establecer una análisis holístico requerido para enfrentar las amenazas actuales y al tiempo garantizar altos estándares de cumplimiento de estándares internacionales.

2. Solicitamos amablemente a la entidad que en aras de mantener altos niveles de rendimientos y para cantidad de plataformas a monitorear, se permita instalación en premisas para responder de forma eficiente y tiempos cernos al tiempo real en el proceso de detección de amenazas.

Respuesta: Nos permitimos aclarar que:

Punto 1: La Previsora en el numeral 3.3.7.1 SERVICIOS DE SOC detalla a nivel general los elementos de monitoreo entre ellos la analítica de datos, estas observaciones están incluido en el pliego de condiciones., las demás reglas o políticas específicas de monitoreo se definen con el proveedor seleccionado.

Punto 2: No es clara su observación, pero se indica que, si se requiere la implementación de colectores, los costos e infraestructura deberán correr por parte del proponente, para un mayor entendimiento se ajusta numeral 3.3.7.5. HERRAMIENTAS DE GESTIÓN DE LA SOLUCIÓN mediante Adenda N°3

Observación 15:

3.3.7.1 SERVICIOS DE SOC

j. EL PROPONENTE debe encargarse de realizar todas las tareas necesarias para asegurar la generación, almacenamiento (mínimo 12 meses) y potencial recuperación de respaldos de las configuraciones de todas las plataformas involucradas en el servicio. Estos respaldos podrán ser solicitados por la entidad para ser almacenados en sus instalaciones.

1. Solicitamos amablemente a la entidad que la arquitectura de almacenamiento sea escalable, con almacenaje de eventos NoSQL, y correlación distribuida de eventos en tiempo real. De esa forma, se podrá desplegar tantos nodos para procesar la información como nodos recolectores que se quiera sin que esto suponga un coste extra en el licenciamiento durante el servicio.

Respuesta: Nos permitimos aclarar que la solicitud anterior describe el tiempo de almacenamiento de los logs que se deben salvaguardar, esto con el fin de poder contar con esta información en cualquier momento, una vez cumpla el tiempo límite de retención definido se debe garantizar un esquema de backup y entrega a custodia para posterior reescritura de los logs.

Observación 16:

3.3.7.1 SERVICIOS DE SOC

k. Proveer en modalidad de servicio, soportada y gestionada una plataforma de análisis de comportamiento de usuarios (UBA) por lo menos 200 usuarios sensibles seleccionados por LA PREVISORA S.A.

1. Solicitamos a la entidad que sea requerido el establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana.

2. Sugerimos amablemente a la entidad que el servicio de UEBA no conlleve consumo asociado ni de licencia de dispositivos ni de EPS en relación con los dispositivos monitoreados, todo con el objeto garantizar un sistema autónoma de UEBA.

Respuesta: Nos permitimos aclarar que:

Punto 1: Las configuraciones y demás políticas para el servicio solicitado serán validadas en conjunto con el proponente seleccionado.

Punto 2: En el numeral 3.3.7.5. HERRAMIENTAS DE GESTIÓN DE LA SOLUCIÓN se describe que el Proponente deberá contar con todas las herramientas necesarias para la prestación del servicio.

Observación 7:

3.3.7.1 SERVICIOS DE SOC

EL PROPONENTE deberá ofrecer un servicio integral de SOC, el cual contemple durante la etapa de operación, en los primeros seis (6) meses del servicio, la ejecución del afinamiento y estabilización respectivo de la plataforma de SIEM que ofrezca, para las aplicaciones y demás servicios específicos, alineado a una operación de nivel 1 "Monitorización y análisis"

1. Muy amablemente se solicita a la entidad clarificar si la solución SIEM es requerida en alta disponibilidad.

2. Es de nuestro entendimiento que la entidad solicita una solución de SIEM de nueva generación la cual permita monitorear tanto la seguridad (SIEM), como la disponibilidad y el desempeño de las plataformas (SOC/NOC), de esa forma se puede disponer de un único punto de gestión de datos no sólo de eventos de seguridad, sino también de:
   - Rendimiento y disponibilidad
   - CPU, memoria y almacenamiento.
   - Detección de cambios de configuración.
   - Monitorización de transacciones sintéticas.
   - Cuadros de mando dinámicos

¿Nuestro entendimiento es correcto?

Respuesta: Nos permitimos aclarar que:

Punto 1: El servicio debe contemplar el cumplimiento de disponibilidad de 99.5%, por lo que el numeral 3.3.7.4. ACUERDOS DE NIVELES DE SERVICIO será modificado en Adenda N°3

Punto 2: El servicio solicita sobre un SIEM de nueva generación es para el monitoreo, análisis, gestión y respuesta de incidentes de seguridad y ciberseguridad (SOC Nivel 2). No se contempla servicios de monitoreo de infraestructura tipo NOC. Si la herramienta la proporciona es independiente y no es una exigencia de la entidad.

Observación 18:

3.3.7.4.1. Acuerdos de Niveles de Servicio (ANS) de Gestión de Incidentes de Servicio

A continuación, se presenta la tabla para los requerimientos reportados y evidenciadas con horario 8X5 sobre las herramientas y sólo aplica para la infraestructura de seguridad gestionada de forma directa por EL PROPONENTE.

1. Solicitamos a entidad aclarar cuales son los niveles de disponibilidad requeridos para la prestación del servicio, y los niveles de disponibilidad de la plataforma SIEM que soportará el servicio.

Respuesta: Nos permitimos aclarar que el detalle de la disponibilidad del servicio se detalla en el numeral 3.3.7.4. ACUERDOS DE NIVELES DE SERVICIO para incidentes y requerimientos, así mismo se realiza ajusta para aclarar el ANS de disponibilidad en la Adenda N°3.

Observación 19:

Se solicita muy amablemente a la entidad que el proponente tenga por lo menos un (1) ingeniero certificado en la herramienta SIEM ofrecida, con el fin de garantizar la correcta prestación del servicio, estos certificados debe adjuntarse con la propuesta.

Respuesta: Nos permitimos indicar que su observación no será tenida en cuenta a razón de que el servicio solicitado deberá contemplar el soporte de la herramienta SIEM.

XXI. OBSERVACIONES PRESENTADAS POR LA EMPRESA INTERLAN

Observación 1: 3.3.7.1 SERVICIOS DE SOC, d., Servicio de manejo de incidentes realizando el triage de los incidentes de seguridad, correlación de eventos, respuesta ante incidentes, amenazas y ataques contra la plataforma tecnológica y los sistemas de información de la organización. Para estos temas se deberá alinear los procesos con la Taxonomía Única Incidentes Cibernéticos – TUIC establecida por la Superfinanciera de Colombia y el COLCERT.

¿Es posible utilizar MITRE ATT&CK® para dar cobertura a este requerimiento? ¿Es este requerimiento mandatorio?

Respuesta: Nos permitimos aclarar que todas las plataformas que permitan la correcta funcionalidad y validación del servicio corren por cuenta del PROVEEDOR y que estas no generan costo alguno sobre la entidad, se aclara que el requerimiento es necesario para el manejo de incidentes por ende se hace mandatorio. La Previsora no limita el uso de plataformas de bases de conocimiento.

Observación 2: 3.3.7.1 SERVICIOS DE SOC, h., Por otro lado, se deben contemplar sitios web, bases de datos, servidores, aplicaciones internas y en nube como (office365, saleforce, entre otras) y demás con los que cuente la compañía.

¿Cuenta La Previsora con una solución de Firewall de Base de Datos? ¿Si no es así cuál es el mecanismo para monitorizar dichas bases de datos y está este activado?

Respuesta: Nos permitimos aclarar que La Previsora no cuenta con una solución de Firewall exclusiva de Base de Datos.

El esquema de monitoreo de Base de Datos se hace a través de extracción o copia de la tabla de logs de las bases de datos y estas se envía a través de agentes de syslog hacia el colector. Sin embargo, se espera con la nueva solución de servicio mejorar este esquema usando un database monitorin o un databese firewall por instancia o núcleo según la solución ofertada.

Observación 3: 3.3.7.1 SERVICIOS DE SOC, h., Por otro lado, se deben contemplar sitios web, bases de datos, servidores, aplicaciones internas y en nube como (office365, saleforce, entre otras) y demás con los que cuente la compañía.

¿Qué servicios o tecnologías de seguridad en nube específicamente deben monitorizarse como parte del alcance?

Respuesta: Nos permitimos aclarar que se tienen servicios de nube publica con Salesforce, Litisoft, y Office 365 de Microsoft. Por otra parte, próximamente, se tendrán los servicios de IaaS y collocation en nube privada para toda la infraestructura de Datacenter de La Previsora. De igual forma las aplicaciones se describen en el ANEXO No. 1 DISPOSITIVOS MONITOREO

Observación 4: 3.3.7.1 SERVICIOS DE SOC, k. Proveer en modalidad de servicio, soportada y gestionada una plataforma de análisis de comportamiento de usuarios (UBA) por lo menos 200 usuarios sensibles seleccionados por LA PREVISORA S.A.

¿Pueden ser soportado mediante conjunto de reglas o modelos de correlación?

Respuesta: Nos permitimos indicar que siempre y cuando las reglas o modelo de correlación cumpla con la detección del comportamiento de los usuarios, que se basa en la conducta normal de los usuarios, sería posible aceptarlo.

Observación 5: 3.3.7.1 SERVICIOS DE SOC, k., Contener o neutralizar los ataques detectados en caso de presencia de amenazas, para estos eventos se deberá contar con una matriz de incidencias y deberá estar avalada por LA PREVISORA S.A.

¿Podrían detallar la expectativa y alcance de las actividades de contención que deben incluirse como parte del servicio? ¿Es un acompañamiento o recomendación en qué horario?

Respuesta: Nos permitimos aclarar que el servicio solicitado requiere respuesta sobre eventos, por lo cual para temas de ataques se deberán tomar las acciones pertinentes en horario 7X24. Así mismo el servicio cuenta con personal que administrara las plataformas respectivas por lo cual se podría manejar un nivel de configuración especifico. Si los dispositivos involucrados hacen parte de la gestión del servicio de seguridad de TI, el recurso Técnico de Seguridad TI deberá estar en capacidad de solventar, contener o neutralizar los eventos en las plataformas definidas en su gestión, si las plataformas involucradas no hacen parte del servicio contratado La Previsora es la responsable de ejecutar las acciones, configuración recomendadas por el Grupo de SOC o Analistas de Seguridad TI.

Observación 6: 3.3.3 CERTIFICACIONES DEL PROVEEDOR. Certificación ISO 27001. Esta norma permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

Teniendo en cuenta que para la Previsora la protección de sus datos es importante recomendamos considerar certificaciones tanto ISO27001 como SOC2 (Service Organization Control 2). Estos son los marcos de seguridad de la información y gestión de riesgos más populares del mundo, y son afines en los tópicos cubiertos con sus controles de seguridad, incluidos los procesos, las políticas y las tecnologías diseñadas para proteger la información confidencial.

De acuerdo con ITGovernance (2021), "ISO 27001, para lograr el cumplimiento, debe realizar una evaluación de riesgos, identificar e implementar controles de seguridad y revisar su efectividad con regularidad.

El SOC 2, por el contrario, es mucho más flexible. Comprende cinco principios de servicios de confianza: seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad, pero solo el primero de ellos es obligatorio."

Tanto SOC 2 como ISO27001 son certificaciones independientes acreditadas por terceros que dan fe de su nivel de seguridad como organización.

Referencias,
ITGovernance, 2021. https://www.itgovernance.eu/blog/en/iso-27001-vs-soc-2-certification-whats-the-difference

Tubboatlogic.com, 2021. https://www.tugboatlogic.com/blog/iso27001-soc2-certification-similarities/#:~:text=Differences%3A%20The%20main%20difference%20between,place%20to%20manage%20your%20InfoSec

Respuesta: Nos permitimos para un mayor entendimiento se realizará modificación sobre el numeral 4.1.4. CERTIFICACIONES ADICIONALES (30) PUNTOS del pliego de condiciones mediante Adenda N°3.

Observación 7: 3.3.2. EXPERIENCIA DEL PROPONENTE

Se solicita amablemente a la entidad revisar la aceptación de Certificaciones de contratos con más del 50% de ejecución.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE será modificará en Adenda N°3

XXII. OBSERVACIONES PRESENTADAS POR LA EMPRESA 2SECURE

Observación 1: INDICADORES FINANCIEROS: Pag. 30
Para participar en el proceso de selección, EL PROPONENTE deberá cumplir con los siguientes indicadores a 31 de diciembre de 2020. Adicionalmente, para entidades extranjeras se tendrá en cuenta la información disponible al último periodo de 2020, de acuerdo con los cortes de presentación de información del país de origen. Las entidades extranjeras que cuenten con la información actualizada al 2021 deberán presentar esta información:

2. Nivel de Endeudamiento (Pasivo Total/Activo Total): Menor o igual al 70%.

Se solicita a La Previsora disminuir el Nivel de Endeudamiento (Pasivo Total/Activo Total): Menor o igual al 60%. Esto reflejaria menor endeudamiento de la empresa particiante del proceso y garantizaria mejor ejecución de la presente invitación.

Respuesta: Al respecto, nos permitimos informar que la Capacidad Financiera definida por Previsora se basó en el estudio de mercado que se realizó en el cual se contemplaron aspectos como: objeto del contrato, tiempo del contrato, valor del contrato, complejidad y forma de pago del mismo, buscando así que el proveedor tenga la liquidez y solidez necesarias para llevar a cabo el desarrollo del contrato, por lo cual los niveles solicitados para los indicadores establecidos permiten evaluar dicha condición. Adicionalmente, se tuvo en cuenta la información financiera registrada en SuperSociedades de empresas dedicadas a actividades relacionadas con el objeto del contrato.

Así mismo, para la definición de estos indicadores se tuvo en cuenta lo señalado en la forma de pago del contrato y plazo de ejecución del contrato del pliego, ya que los proponentes deberán contar con una capacidad financiera mínima para cumplir con el desarrollo de las actividades que deberán ser asumidas por ellos por el tiempo de ejecución del contrato.

Por lo tanto y con el fin de garantizar los fines de la contratación, se establecieron los indicadores financieros solicitados en la invitación, buscando así una idoneidad financiera de los proponentes, a través de la evaluación de varias dimensiones como lo son capital de trabajo, nivel de endeudamiento y patrimonio, los cuales evalúan aspectos diferentes que en conjunto garanticen liquidez para la ejecución satisfactoria del objeto del contrato.

Teniendo en cuenta lo anterior y considerando que los indicadores solicitados se ajustan a las necesidades de Previsora, se mantiene la capacidad financiera definida inicialmente.

Observación 2: Certificado por parte del Fabricante: Pag. 37
EL PROPONENTE deberá adjuntar con su propuesta la certificación del producto (SIEM) como canal autorizado o expedida por el fabricante o su representante en Colombia. Esta certificación deberá estar vigente al momento de la presentación de la oferta y firma del contrato. EL PROPONENTE está obligado a velar por mantener vigente la certificación durante el plazo de ejecución del contrato y tiempo de garantía de los elementos de infraestructura.

Se solicita a la Previsora incluir a Mayoristas representantes en Colombia para poder brindar certificación de la herramienta.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.4. CERTIFICADO POR PARTE DEL FABRICANTE será modificado en Adenda N°3

Observación 3: Membresía First (20 Puntos): Pag. 71
Se asignará el puntaje de veinte (20) puntos, a la propuesta que allegue la membresía de FIRST (Forum of Incident Response and Security Teams) como empresa.

Se solicita a la Previsora modificar este punto para dar pluralidad a todos los participantes del proceso. De ser posible no exigirlo en el proceso.

Respuesta Nos permitimos aclarar que su observación no será tenida en cuenta.

XXIII. OBSERVACIONES PRESENTADAS POR LA EMPRESA SERVIALCO

Observación 1:

Número	NUMERAL Y TEXTO INVITACIÓN	PÁGINA	OBSERVACIONES Y/O INQUIETUDES
1	***3.3.4. Certificado por parte del Fabricante:*** EL PROPONENTE deberá adjuntar con su propuesta la certificación del producto (SIEM) como canal autorizado o expedida por el fabricante o su representante en Colombia. Esta certificación deberá estar vigente al momento de la presentación de la oferta y firma del contrato. EL PROPONENTE está obligado a velar por mantener vigente la certificación durante el plazo de ejecución del contrato y tiempo de garantía de los elementos de infraestructura.	37	Adicional a canales autorizados o certificación expedida por el fabricante o su representante en Colombia, es posible incluir canal Mayorista para que se pueda certificar la herramienta SIEM?

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.4. CERTIFICADO POR PARTE DEL FABRICANTE será modificado en Adenda N°3

Observación 2:

2	***4.1.3.1. Membresía First (20 Puntos):*** Se asignará el puntaje de veinte (20) puntos, a la propuesta que allegue la membresía de FIRST (Forum of Incident Response and Security Teams) como empresa.	71	Respetuosamente se solicita a la Previsora dejar certificar la Membresia First ó ISO 27001 por los mismo puntos. O se podria retirar esta Membresia de la presente invitación?

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta a razón de:

1. La certificación ISO27001 es un requisito habilítate al presente proceso solicitado en el numeral 3.3.3 CERTIFICACIONES PROVEEDOR
2. La membresía first es un deseable para la entidad generando un nivel de confianza ya que les permite a los proveedores contar con una apoyo adicional para dar respuesta de manera más efectiva ante los riesgos que se puedan presentar, tendrían acceso a un banco de información y buenas prácticas, herramientas, comunicaciones, noticias y tendencias de seguridad y ciberseguridad.

Observación 3:

3	***Indicadores que se deben Acreditar :*** Para participar en el proceso de selección, EL PROPONENTE deberá cumplir con los siguientes indicadores a 31 de diciembre de 2020. Adicionalmente, para entidades extranjeras se tendrá en cuenta la información disponible al último periodo de 2020, de acuerdo con los cortes de presentación de información del país de origen. Las entidades extranjeras que cuenten con la información actualizada al 2021 deberán presentar esta información. 1. Capital de Trabajo (Activo corriente – Pasivo corriente): Mayor o igual al 30% del presupuesto oficial de la contratación. 2. Nivel de Endeudamiento (Pasivo Total/Activo Total): Menor o igual al 70%. 3. Patrimonio Total: Mayor o igual al 30% del presupuesto oficial de la contratación. 4. Índice de Liquidez (Activo corriente/Pasivo corriente): Mayor o igual a 1.	30 y 31	Respetuosamente se solicita a la Previsora tener en cuenta los siguientes indicadores para acreditar en la presente invitación: 1. Capital de Trabajo (Activo corriente – Pasivo corriente): Mayor o igual al 80% del presupuesto oficial de la contratación. 2. Nivel de Endeudamiento (Pasivo Total/Activo Total): Menor o igual al 60%. 3. Patrimonio Total: Mayor o igual al 100% del presupuesto oficial de la contratación. 4. Índice de Liquidez (Activo corriente/Pasivo corriente): Mayor o igual a 1. En resumen, tener un capital de trabajo alto, un patrimonio total del 100% y con nivel de endeudameiento del 60%, indica que es una empresa suficientemente sólida para llevar a cabo el objeto del contrato.

Respuesta: Al respecto, nos permitimos informar que la Capacidad Financiera definida por Previsora se basó en el estudio de mercado que se realizó en el cual se contemplaron aspectos como: objeto del contrato, tiempo del contrato, valor del contrato, complejidad y forma de pago del mismo, buscando así que el proveedor tenga la liquidez y solidez necesarias para llevar a cabo el desarrollo del contrato, por lo cual los niveles solicitados para los indicadores establecidos permiten evaluar dicha condición. Adicionalmente, se tuvo en cuenta la información financiera registrada en SuperSociedades de empresas dedicadas a actividades relacionadas con el objeto del contrato.

Así mismo, para la definición de estos indicadores se tuvo en cuenta lo señalado en la forma de pago del contrato y plazo de ejecución del contrato del pliego, ya que los proponentes deberán contar con una capacidad financiera mínima para cumplir con el desarrollo de las actividades que deberán ser asumidas por ellos por el tiempo de ejecución del contrato.

Por lo tanto y con el fin de garantizar los fines de la contratación, se establecieron los indicadores financieros solicitados en la invitación, buscando así una idoneidad financiera de los proponentes, a través de la evaluación de varias dimensiones como lo son capital de trabajo, nivel de endeudamiento y patrimonio, los cuales evalúan aspectos diferentes que en conjunto garanticen liquidez para la ejecución satisfactoria del objeto del contrato.

Teniendo en cuenta lo anterior y considerando que los indicadores solicitados se ajustan a las necesidades de Previsora, se mantiene la capacidad financiera definida inicialmente.

XXIV. OBSERVACIONES PRESENTADAS POR LA EMPRESA COMWARE

Observación 1: Se asignará el puntaje de veinte (20) puntos, a la propuesta que allegue la membresía de FIRST (Forum of Incident Response and Security Teams) como empresa.

Se solicita amablememte a la entidad y por dar pluralidad entre los proveedores proponentes de retirar este ITEM ó Adicionar la ISO 27001 y que se asignen los mismos puntos por Membresía FIRST ó por ISO 27001, dejando el texto asi:

" Se asignarán el puntaje de 20 puntos, a la propuesta que allegue la membresía de FIRST (Forum of Incident Response and Security Teams) como empresa ó 20 puntos al acreditar mediante certificación ISO 27001 donde se especifique el alcance de esta certificación enfocada a la administración del servicio de correlación de eventos de seguridad, comprendiendo su detección, análisis, clasificación, reporte, y recomendación de acción

inmediata, a través de la solución SIEM gestionada por el centro de operaciones de seguridad SOC.”

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta a razón de:

1. La certificación ISO27001 es un requisito habilítate al presente proceso solicitado en el numeral 3.3.3 CERTIFICACIONES PROVEEDOR
2. La membresía first es un deseable para la entidad generando un nivel de confianza ya que les permite a los proveedores contar con un apoyo adicional para dar respuesta de manera más efectiva ante los riesgos que se puedan presentar, tendrían acceso a un banco de información y buenas prácticas, herramientas, comunicaciones, noticias y tendencias de seguridad y ciberseguridad.

Observación 2: EL PROPONENTE deberá adjuntar con su propuesta la certificación del producto (SIEM) como canal autorizado o expedida por el fabricante o su representante en Colombia. Esta certificación deberá estar vigente al momento de la presentación de la oferta y firma del contrato. EL PROPONENTE está obligado a velar por mantener vigente la certificación durante el plazo de ejecución del contrato y tiempo de garantía de los elementos de infraestructura.

Se solicita a la entidad permitir que a la propuesta se adjunte la Certificación del producto (SIEM) por parte de una Canal MAYORISTA representante de la marca fabricante en Colombia, dejando texto así:

"EL PROPONENTE deberá adjuntar con su propuesta la certificación del producto (SIEM) como canal autorizado o expedida por el fabricante y/o su mayorista o su representante en Colombia. Esta certificación deberá estar vigente al momento de la presentación de la oferta y firma del contrato"

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta y el numeral 3.3.4. CERTIFICADO POR PARTE DEL FABRICANTE será modificado en Adenda N°3

Observación 3:

"3.2. CAPACIDAD FINANCIERA:

1. Capital de Trabajo (Activo corriente – Pasivo corriente): Mayor o igual al 30% del presupuesto oficial de la contratación.

2. Nivel de Endeudamiento (Pasivo Total/Activo Total): Menor o igual al 70%.

3. Patrimonio Total: Mayor o igual al 30% del presupuesto oficial de la contratación.

4. Índice de Liquidez (Activo corriente/Pasivo corriente): Mayor o igual a 1.

Observaciones COMWARE S.A.
Solicitamos amablemente a la Previsora S.A. modificar el margen de los indicadores de la siguiente manera:

"3.2. CAPACIDAD FINANCIERA:

1. Capital de Trabajo (Activo corriente – Pasivo corriente): Mayor o igual al 100% del presupuesto oficial de la contratación.

2. Nivel de Endeudamiento (Pasivo Total/Activo Total): Menor o igual al 60%.

3. Patrimonio Total: Mayor o igual al 100% del presupuesto oficial de la contratación.

4. Índice de Liquidez (Activo corriente/Pasivo corriente): Mayor o igual a 1,4.

Esta modificación se solicita debido a que los índices requeridos por la Entidad pueden poner en riesgo el cumplimiento del contrato a suscribir.

Por ejemplo, el nivel endeudamiento refleja el grado de apalancamiento que corresponde a la participación de los acreedores en los activos de la empresa. Por consiguiente, esto significa que entre más alto sea este indicador la empresa tiene mayores deudas respecto a sus activos. Lo cual puede afectar sin lugar a duda la ejecución del contrato a suscribir.

Ahora bien, con un índice de liquidez mayor o igual 1, la entidad está permitiendo que empresas con baja solidez financiera puedan presentarse al presente proceso. El índice de liquidez nos permite conocer la capacidad de la empresa para cubrir las obligaciones a corto plazo, por cada peso ($) de deuda corriente, cuánto se tiene de respaldo en activo corriente, entre más alto sea, menor riesgo existe que resulten impagadas las deudas a corto plazo. Sugerimos modificar este indicador de mayor o igual a 1 a mayor o igual a 1.4, con este indicador se puede garantizar que el futuro contratista cuente con la solidez y respaldo financiero a corto plazo.

Por otro lado, es indispensable que la entidad amplíe el Capital de trabajo y el Patrimonio Total de Mayor o igual al 30% del presupuesto oficial de la contratación a Mayor o igual al 100% del presupuesto oficial de la contratación, pues una empresa con un capital de trabajo inferior al 100% del presupuesto oficial, demuestra que no es una empresa lo suficientemente sólida para llevar a cabo la perfecta y de forma eficiente la ejecución del contrato.

Con base en lo expuesto, solicitamos a la Previsora aumentar el rango de los indicadores solicitados, lo cual puede beneficiar sin lugar a duda a la entidad.

Respuesta: Al respecto, nos permitimos informar que la Capacidad Financiera definida por Previsora se basó en el estudio de mercado que se realizó en el cual se contemplaron aspectos como: objeto del contrato, tiempo del contrato, valor del contrato, complejidad y

forma de pago del mismo, buscando así que el proveedor tenga la liquidez y solidez necesarias para llevar a cabo el desarrollo del contrato, por lo cual los niveles solicitados para los indicadores establecidos permiten evaluar dicha condición. Adicionalmente, se tuvo en cuenta la información financiera registrada en SuperSociedades de empresas dedicadas a actividades relacionadas con el objeto del contrato.

Así mismo, para la definición de estos indicadores se tuvo en cuenta lo señalado en la forma de pago del contrato y plazo de ejecución del contrato del pliego, ya que los proponentes deberán contar con una capacidad financiera mínima para cumplir con el desarrollo de las actividades que deberán ser asumidas por ellos por el tiempo de ejecución del contrato.

Por lo tanto y con el fin de garantizar los fines de la contratación, se establecieron los indicadores financieros solicitados en la invitación, buscando así una idoneidad financiera de los proponentes, a través de la evaluación de varias dimensiones como lo son capital de trabajo, nivel de endeudamiento y patrimonio, los cuales evalúan aspectos diferentes que en conjunto garanticen liquidez para la ejecución satisfactoria del objeto del contrato.

Teniendo en cuenta lo anterior y considerando que los indicadores solicitados se ajustan a las necesidades de Previsora, se mantiene la capacidad financiera definida inicialmente.

Observación 4:

4.1.2.1. OBSERVACIONES METODO DE EVALUACIÓN Y ASIGNACIÓN DE PUNTAJE POR OFERTA ECONÓMICA:

Las propuestas se ordenarán de menor a mayor valor incluido IVA, y se le asignará el mayor puntaje a la propuesta que ofrezca menor valor en el total de la propuesta, y las demás ofertas serán calificadas por regla de tres (3) inversa.

Para dar pluralidad de los oferentes participantes, se solicita a la entidad atender como Forma de calificación económica la formula de *"Media Geométrica con presupuesto oficial"..*

Consiste en establecer la media geométrica de las ofertas válidas y el presupuesto oficial un número determinado de veces y la asignación de puntos en función de la proximidad de las ofertas a dicha media geométrica, como resultado de aplicar las fórmulas que se indican en seguida.

Para el cálculo de la media geométrica con presupuesto oficial se tendrá en cuenta el número de ofertas válidas y se incluirá el presupuesto oficial del Proceso de Contratación en el cálculo tantas veces como se indica en el siguiente cuadro:

Tabla - Asignación de número de veces del presupuesto oficial

Número de Ofertas (n)	Número de veces que se incluye el presupuesto oficial (nv)
1 - 3	1
4 - 6	2
7 - 9	3
10 – 12	4
13 - 15	5

Y así sucesivamente, por cada tres ofertas válidas se incluirá una vez el presupuesto oficial del presente Proceso de Contratación.

Posteriormente, se determinará la media geométrica con la inclusión del presupuesto oficial de acuerdo a lo establecido en el cuadro anterior, mediante la siguiente fórmula:

$$G_{PO} = \sqrt[nv+n]{PO \times PO \times \ldots \times PO_{nv} \times P_1 \times P_2 \times \ldots \times P_n}$$

Donde,

Gpo= Media geométrica con presupuesto oficial.
nv= Número de veces que se incluye el presupuesto oficial (PO).
n= Número de ofertas válidas.
PO= Presupuesto oficial del Proceso de Contratación.
Pi= Valor de la oferta económica sin decimales del Proponente i.

Establecida la media geométrica se asignará la mayor cantidad de puntos al proponente cuya propuesta esté más cercana a la media por abajo. Para los demás se procederá a determinar el puntaje mediante el siguiente procedimiento:

$$\text{Puntaje i} = \begin{cases} \text{Puntaje} \times \left(1 - \left(\frac{G_{PO} - V_i}{G_{PO}}\right)\right) \text{ para valores menores o iguales a } G_{PO} \\ \text{Puntaje} \times \left(1 - 2\left(\frac{|G_{PO} - V_i|}{G_{PO}}\right)\right) \text{ para valores mayores a } G_{PO} \end{cases}$$

G_{PO} = Media geométrica con presupuesto oficial.

V_i = Valor total corregido de cada una de las Ofertas i

i = Número de propuesta.

Donde,

En el caso de ofertas económicas con valores mayores a la media geométrica con presupuesto oficial se tomará el valor absoluto de la diferencia entre la media geométrica con presupuesto oficial y el valor de la oferta, como se observa en la fórmula de ponderación.

Respuesta: Nos permitimos aclarar que la observación no será tenida en cuenta.

Observación 5: Con el fin de cumplir con la experiencia mínima habilitante, EL PROPONENTE deberá adjuntar con su propuesta tres (3)

es de contratos suscritos con empresas públicas o privadas nacionales en las que se acredite experiencia de la siguiente forma:

1. El objeto, actividades u obligaciones sean iguales o similares al de la presente invitación. Entendiéndose por similar que consista en la prestación de servicios administrados de seguridad y/o servicios de SOC.
2. Una de las tres certificaciones con las cuales se pretende acreditar la experiencia mínima habilitante debe corresponder a empresas del Sector Gobierno o Sector Financiero.
4. El plazo de ejecución de cada contrato certificado incluidas sus prórrogas deberá ser igual o mayor a 12 meses.

6. Los contratos certificados deben haber iniciado durante los últimos 5 años a la presentación de la presente invitación.

1. Con el fin de la pluralidad de oferentes solicitamos amablemente a la entidad que los contratos certificados sean ejecutados en los últimos 5 años.
2. Con el fin de la pluralidad de oferentes solicitamos amablemente a la entidad no limitar en cantidad las certificaciones a Tres (3) sino hasta 3 certificaciones.
3. Con el fin de la pluralidad de oferentes solicitamos amablemente que el plazo de ejecución de los contratos se pueda acreditar en una de las hasta (3) certificaciones aportadas.
4. Es correcto nuestro entendimiento que cuando hace referencia en acreditar una certificación con experiencia mínima habitante debe corresponder a empresas del Sector Gobierno entendiéndose que es igual al sector Público.

Respuesta: Nos permitimos indicar que su observación será tenida en cuenta, el detalle de esta se especifica en el numeral OBSERVACIONES GENERALES ítem 2 “Tiempo de experiencia del Proponente” y 3 “Número de certificaciones de experiencia general” del presente documento. Y el numeral 3.3.2. EXPERIENCIA DEL PROPONENTE será modificará en Adenda N°3 y respecto la cuarta (4) es correcto el entendimiento.

Observación 6: EL PROPONENTE seleccionado deberá asignar los recursos y perfiles necesarios para cumplir con el objeto contractual, sin embargo, deberá adjuntar con su propuesta las hojas de vida y las certificaciones de experiencia de los recursos mínimos con los cuales ejecutará el contrato y que a continuación se relacionan: Gerente de Servicio, Analistas SOC, Analistas de Seguridad TI, Tecnico de Seguridad TI.

Se sugiere a la entidad atender los requisitos mínimos habilitantes para siguiente rol:

1. Gerente de Servicio cuente con Postgrado, Especialización y/o Maestria y/o certificación vigente de PMP y que contemple como certificación minima requerida ITIL V3. En cuanto a la experiencia mínima requerida que cuenta mínimo con 10 años de experiencia profesional

como Gerente de Proyectos en Tecnologías de la Información. Entendiendo que con estos requisitos mínimos la entidad va contar con personal idóneo y calificado para poder gerenciar el proyecto.
2. Analistas SOC: Solicitamos amablemente a la entidad dimisnuir la cantidad de personal requerido en este rol a 2 recursos minimo; teniendo en cuenta que como proveedores del servicio SOC se garantizara personal idoneo y calificado para poder desarrollar el proyecto.

Respuesta: Nos permitimos aclarar que la observación no será tenida en cuenta.

Observación 7: En Pagina 38 dice textual: EL PROPONENTE seleccionado deberá asignar los recursos y perfiles necesarios para cumplir con el objeto contractual, sin embargo, deberá adjuntar con su propuesta las hojas de vida y las certificaciones de experiencia de los recursos mínimos con los cuales ejecutará el contrato y que a continuación se relacionan.

Y en a pagina 43 dice textual : EL PROPONENTE seleccionado deberá allegar a la PREVISORA S.A cinco (5) días después de la publicación del acta de adjudicación las hojas de vida, las certificaciones de experiencia y certificaciones de estudio de los recursos mínimos con los cuales ejecutará el servicio.

Se solicita amablemente a la entidad si nuestra apreciación es correcta: Las hojas de vida se deben presentar cuando ya se seleccione al proponente adjudicado, es correcto nuestro entendimiento? Teniendo en cuenta que en la página 43 indica que la hojas de vida y certificaciones se deberán presentar cinco (5) días después de la publicación del acta de adjudicación.

Respuesta: Nos permitimos indicar que su apreciación no es correcta, sin embargo, se efectúa modificación sobre el numeral 3.3.6. RECURSO HUMANO MINIMO HABILITANTE sobre Adenda N°3

Observación 8: "Cuadro Anexo 2.:

Especialista de Seguridad IT, Director y/o Coordinador SOC, Experto Coordinador de grupo de respuestas a incidentes"

Se sugiere a la entidad dejar disponibilidad o Dedicación **Parcial o Dedicado (no porcentaje)** por los perfiles aquí solicitados, ya que al considerarse un servicio, es el proveedor seleccionado quien se hara responsable de la adecuada prestación del mismo y el cumplimiento de sus ANS.
Asi mismo se sugiere a la entidad que el:
1. Director y/o Coordinador del SOC: Se sugiere a la entidad que para este cargo se debe contar con personal idoneo y calificado tecnicamente;asi mismo requiera minimo 5 certificaciones de las listadas continuación:

ü -CISSP “Certified Information Systems Professional”
ü -CISM “Certified Information Security Management”

ü -CRISC “Certified In Risk and Information Symtems -Control”
ü -Togaf 9
ü -ECIH “Certified Incident Handler”
ü -Auditor Líder ISO 22301 del 2012.
ü -Auditor Líder de Implementación ISO 27001 del 2013
ü -Líder de implementación ISO 270032 del 2017
ü -Auditor Líder ISO 27001 del 2013.
ü -ISO 27032 del 2017
ü -ISO 31000 del 2018
ü -RISK Manager
ü -ITIL Fundation Versión 3 o 4.
ü -ITIL Expert V3
ü -CEH
ü -Certified Data Provacy Solutiones Engineer
ü -NSE4 Fortinet
ü -Certified Archimate 3 Foundation
ü -ABCP (Associate business Continuity Professional)
ü -COBIT Foundation

Respuesta: Nos permitimos indicar que se ajustara ANEXO No. 2 RECURSO HUMANO CALIFICABLE del pliego de condiciones, este se vera modificado en Adenda N°3, de igual forma se especifica el detalle el numeral OBSERVACIONES GENERALES ítem 3 “Certificaciones del Recurso Humano calificable “del presente documento

XXV. OBSERVACIONES PRESENTADAS POR LA EMPRESA GAMA INGENIEROS

Observación 1:

Documento: 005_2021_pliegoCondiciones pagina 33

Alcance

3.3.2. EXPERIENCIA DEL PROPONENTE

3. El valor de la sumatoria de las certificaciones deberá acreditar una cuantía igual o superior al 75% del valor del presupuesto.

4. El plazo de ejecución de cada contrato certificado incluidas sus prórrogas deberá ser igual o mayor a 12 meses.

5. Los contratos certificados deben haberse ejecutado en su totalidad; no se aceptarán certificaciones de contratos en ejecución.

Agradecemos a la entidad validar si es posible adjuntar certificados en ejecución , toda vez que esta experiencia permite verificar el estado actual del servicio en nuestros clientes.

Respuesta: Nos permitimos aclarar que su observación será tenida en cuenta y esta se verá reflejada en Adenda N°3

Observación 2:

Documento: 005_2021_pliegoCondiciones página 46

Alcance

d. Servicio de manejo de incidentes realizando el triage de los incidentes de seguridad, correlación de eventos, respuesta ante incidentes, amenazas y ataques contra la plataforma tecnológica y los sistemas de información de la organización. Para estos temas se deberá alinear los procesos con la Taxonomía Única Incidentes Cibernéticos – TUIC establecida por la Superfinanciera de Colombia y el COLCERT.

Se entiende que la respuesta a incidentes estará determinada únicamente al alcance de los servicios administrados o a recomendaciones y al acompañamiento si este se materializa sobre otros activos de información, agradecemos confirmar si es correcto nuestro entendimiento

Respuesta : Nos permitimos aclarar que su entendimiento es correcto

Observación 3:

Documento: 005_2021_pliegoCondiciones página 46

Alcance

e. Analizar e implementar mecanismos que permitan a la entidad verificar diferentes fuentes de información tales como sitios web, blogs y redes sociales, esto con el propósito de identificar posibles ataques cibernéticos contra la entidad. Lo anterior alineado a la Circular Externa 008 de la Superfinanciera de Colombia.

Se entiende que dentro del alcance solo se deberá monitorear los eventos relacionados con la marca de PREVISORA S.A en la clear web, agradecemos confirmar si es correcto nuestro entendimiento

Respuesta : Nos permitimos aclarar que su entendimiento es correcto

Observación 4:

Documento: 005_2021_pliegoCondiciones página 46

Alcance

f. Notificación proactiva de amenazas proporcionando soluciones y estrategias de mitigación, tomar medidas para proteger los sistemas y redes afectados o amenazados por la actividad de intrusos y desarrollar otras estrategias de respuesta o solución alternativa, con escenarios de crisis contra ataques dirigidos como DDoS o amenazas avanzadas.

Agradecemos confirmar si PREVISORA S.A. ya cuenta con un protocolo de atención a crisis donde se vean alineados los frentes estratégicos, tácticos y operativos o dentro del servicio se espera la construcción de dicho protocolo.

Respuesta Nos permitimos aclarar que La Previsora ya cuenta con el protocolo de gestión de incidentes.

Observación 5:

Documento: 005_2021_pliegoCondiciones página 46

Alcance

g. El servicio ofertado deberá detectar actividades inusuales, recolectar evidencias y correlacionar los eventos para el escalamiento y determinar si corresponde a un evento de seguridad, tendencias, falsos positivos, patrones o firmas de intruso las cuales deberán ser notificadas y documentadas. Sobre este punto de analítica de datos se solicita al proponente contemplar las herramientas que considere necesarias para contar con la inteligencia artificial para la detección de estos eventos.

Por favor indicar si con las características de indicadores de compromiso y análisis de eventos por parte de personal especialista del SOC se daría cumplimiento a este requisito.

Respuesta: Nos permitimos aclarar que su entendimiento no es correcto, se deberá realizar un análisis más detallado sobre el servicio inusual en este caso contemplar analítica de datos para detección de anomalías y/o eventos que no correspondan al funcionamiento adecuado de los sistemas.

Observación 6:

Documento: 005_2021_pliegoCondiciones página 46

Alcance

h. **EL PROPONENTE** deberá contar con una herramienta SIEM en modalidad de servicio en nube para el análisis de los registros de eventos de los equipos de seguridad existentes (IPS's, Firewalls, Endpoint, Sandbox, UBA, etc) y respuesta ante eventos inusuales, la integración de la herramienta deberá contemplar múltiples formas de integración, así como envió de logs, agentes u otro para dejar operativo todos los servicios que se requieran monitorear. Por otro lado, se deben contemplar sitios web, bases de datos, servidores, aplicaciones internas y en nube como (office365, saleforce, entre otras) y demás con los que cuente la compañía.

¿El servicio de SIEM pude ser entregado sobre un Datacenter gestionado por el proveedor?

Respuesta: Nos permitimos aclarar que la solución puede ser on premise, siempre y cuando el oferente asuma todos los costos de collocotión e interconexión al DataCenter de la entidad, sin ningún recargo al servicio o costo adicional a la entidad. La infraestructura no será provista por la entidad.

Observación 7:

Documento: 005_2021_pliegoCondiciones página 47

Alcance

j. **EL PROPONENTE** debe encargarse de realizar todas las tareas necesarias para asegurar la generación, almacenamiento (mínimo 12 meses) y potencial recuperación de respaldos de las configuraciones de todas las plataformas involucradas en el servicio. Estos respaldos podrán ser solicitados por la entidad para ser almacenados en sus instalaciones.

Es de nuestro entendimiento que las copias de respaldo están definidas únicamente al alcance del SIEM y el resto de recursos necesarios para entregar el servicio, en ningún momento se pretende generar las copias de respaldo a servidores, bases de datos de PREVISORA S.A, dispositivos de red y demás, agradecemos confirmar si es correcto nuestro entendimiento

Respuesta: Nos permitimos confirmar que su entendimiento es correcto

Observación 8:

Documento: 005_2021_pliegoCondiciones página 47

Alcance

o. Contener o neutralizar los ataques detectados en caso de presencia de amenazas, para estos eventos se deberá contar con una matriz de incidencias y deberá estar avalada por **LA PREVISORA S.A.**

Es de nuestro entendimiento que solo seria posible contener o neutralizar los ataques o incidentes materializados sobre los activos de información en los cuales se tenga gestión por parte del proveedor, para todos aquellos incidentes que se presenten sobre otros activos de información se darían las recomendaciones pertinentes y acompañamiento para el cierre del caso, agradecemos confirmar si es correcto nuestro entendimiento

Respuesta Nos permitimos confirmar que su entendimiento es correcto

Observación 9:

Documento: 005_2021_pliegoCondiciones página 49

Alcance

j. Realizar pruebas que permitan a **LA PREVISORA S.A**, medir la efectividad de los controles tecnológicos existentes y definir reglas para detectar, reaccionar y contener ataques.

Por favor indicar cuantas pruebas se realizarían al año.

Respuesta: Nos permitimos aclarar que el alcance de las pruebas y demás factores relacionados a este ítem se definirán en común acuerdo entre La Previsora S.A. y el proponente seleccionado ya que dependen de los controles y reglas que defina para la detección de eventos

Observación 10:

Documento: 005_2021_pliegoCondiciones página 49

Alcance

k. Incluir en los procesos de gestión de acuerdo con lo establecido con la entidad la forma de realizar los respectivos reportes a entidades externas y partes interesadas.

Por favor aclarar si dentro de los reportes están incluidos aquellos solicitados por la Super financiera dentro de las diferentes circulares de ciberseguridad.

Respuesta: Nos permitimos indicar que en los reportes se tiene gran parte de la información de la Super financiera de Colombia

Observación 11:

Documento: 005_2021_pliegoCondiciones página 49

Alcance

- **o.** Aseguramiento y gestión de vulnerabilidades: Anualmente se deberán generar dos (2) análisis de vulnerabilidad, Ethical Hacking y penetración a la plataforma tecnológica, a los que se deberá elaborar una matriz de seguimiento de los hallazgos encontrados y los planes de remediación y/o mitigación, el cual deberá ser gestionado por **EL PROVEEDOR**. Para cada uno de los análisis se debe contemplar todos los dispositivos activos de **LA PREVISORA S.A** los cuales se estiman en un promedio de 600 objetivos. Por otra parte, se debe contemplar análisis de vulnerabilidades a demanda adicionales para nuevas aplicaciones y/o solicitudes internas. Se solicita contemplar por lo menos 2 análisis de código por año y el respectivo Re-test de cada uno de los análisis efectuados, los análisis de penetración a las herramientas se solicita estimación de por lo menos 3 por año.

Por favor indicar si el alance de Ethical Hacking y Pentesting también es sobre los 600 objetivos, o es análisis de vulnerabilidades a 600 objetivos y Ethical Hacking y Pentesting a los servicios misionales y sensibles de Previsora, en caso de ser la segunda opción indicar cuantos servicios.

Respuesta : Nos permitimos aclarar que la definición detallada de los 600 objetivos se realizara en conjunto con el proveedor seleccionado, el escaneo de vulnerabilidades será sobre los 600 objetivos así como su correspondiente re-test, con una periodicidad de 2 veces al año (primer semestre escaneo de vulnerabilidades, segundo semestre el re-test), para el caso del ethical hacking se efectúa sobre los sistemas de información CORE de negocio que promedian en 20 aplicaciones o según defina la prioridad la Gerencia de Riesgos con una periodicidad de 1 vez al años.

Observación 12:

Documento: 005_2021_pliegoCondiciones página 50

Alcance

3.3.7.2.2. TECNICO DE SEGURIDAD TI:

Personal calificado para brindar soporte a las plataformas de seguridad manejadas por la compañía (Firewall, Antivirus, Office365, OIG, entre otras que pertenezcan a la gestión de seguridad de **LA PREVISORA S.A**), mantener adecuadamente los sistemas y realizar las respectivas mejoras y seguimientos de estas.

Por favor indicar el fabricante del firewall, antivirus y OIG
Por favor acotar el alcance en lo que se refiere a otras que pertenezcan a la gestión de seguridad de LA PREVISORA S.A, ya que es importante dimensionar el equipo y los esfuerzos puestos a disposición.

Respuesta: Nos permitimos indicar que el Firewall es Fortinet, Antivirus Sophos y el servicio de OIG es con Oracle. Adicionalmente se confirma que “otras” hace referencia a: DLP y Antispam de Office365.

Observación 13:

Documento: 005_2021_pliegoCondiciones página 51

Alcance

g. Identificar los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad, revisión de las configuraciones de hardware y software, enrutadores, cortafuegos, servidores y demás dispositivos para garantizar que coinciden con las políticas de seguridad de las mejores prácticas de la organización o de la industria y las configuraciones estándar.

Por favor aclarar si ya se tienen construidas las líneas bases para los firewalls, componentes de software y hardware, enrutadores entre otros. Por otro lado por favor indicar si los sistemas de información a desarrollar hacen referencia a los dispuestos el por el proveedor para entregar el servicio.

Respuesta: Nos permitimos aclarar que se tienen implementadas veintiocho (28) líneas base las cuales pueden incrementar, la implementación actual es sobre el 100% de los sistemas de información productivos de la entidad (bases de datos, seguridad, comunicaciones, entre otros). Las cantidades y documentos base serán entregados al oferente seleccionado

Observación 14:

Documento: 005_2021_pliegoCondiciones página 53

Alcance

3.3.7.4.1. Acuerdos de Niveles de Servicio (ANS) de Gestión de Incidentes de Servicio

Entendiendo que algunos de los fallos que pueden generar una afectación total son producto de fallos de hardware, bug en las aplicaciones y eventos ajenos a la gestión del SOC es posible generar un documento de exclusiones que no afecten el cumplimiento de los ANS.

Respuesta: Nos permitimos indicar que el numeral 3.3.7.4. ACUERDOS DE NIVELES DE SERVICIO será modifica en Adenda N°3, así mismo se aclara que los ANS sólo aplica para la infraestructura de seguridad gestionada de forma directa por EL PROPONENTE.

Observación 15:

Por favor aclarar si este punto hace referencia al análisis de la marca y su reputación en redes sociales, si es asi por favor indicar que redes sociales desean cubrir.
Por favor acotar el alcance en el cumplimiento de aquellas normas que en el desarrollo del contrato entren en vigencia y le sean aplicables, entendiendo que muchas veces para cubrir un requisito normativo es necesario implementar una solución tecnológica o ampliar el alcance de servicios pactados, lo que tendría sobre costos en la propuesta entregada.

4. Informe con acciones, relacionadas a usuarios privilegiados, este deberá contener el resultado del monitoreo de todos los usuarios que realicen acciones de:
   a. borrado, inserción y actualización y/o modificación de la información.
   b. Modificación de permisos sobre los usuarios.
   c. Creación de nuevos usuarios con permisos de administrador o con altos privilegios.

   Este monitoreo debe realizarse sobre la infraestructura de LA PREVISORA incluyendo las respectivas bases de datos.

Documento: 005_2021_pliegoCondiciones página 54

Alcance

3. Informe de redes sociales por mes, con la finalidad de presentar los informes consolidados de las búsquedas de información en redes sociales, con el objeto de conocer la reputación online de **LA PREVISORA S.A.**, auditar el comportamiento de **LA PREVISORA S.A.**, con el fin de evaluar el nivel de privacidad y seguridad, evaluar tendencias de mercados e identificación y prevención de posibles amenazas en el ámbito de la ciberseguridad, cumpliendo las exigencias de la circular 007 de la Súper Intendencia Financiera y de aquellas normas que en el desarrollo del contrato entren en vigencia y le sean aplicables

Respuesta: Nos permitimos indicar que la cantidad de marcas (1), dominios web (hasta 5), dominios de correo (1), Aplicaciones (las comunes tipo WEB), Presencia en redes sociales (Las más reconocidas en el mercado Facebook, Instagram, Twitter, etc).

Observación 16:

Documento: 005_2021_pliegoCondiciones página 60

Alcance

3. Documentación actualizada de las Circulares de la Superfinanciera de Colombia acordes a la seguridad y ciberseguridad y documentación relacionada para su cumplimiento.

Por favor aclarar a que se hace referencia con este punto, si lo que se requiere es una documentación donde se vea reflejado los requisitos que deben ser cumplidos de la Superfinanciera o a un análisis GAP donde se identifique las brechas existentes en LA PREVISORA con base a los requisitos mandatorios exigidos por la super.

Respuesta: Nos permitimos aclarar que este punto hace referencia a mantener al día documentos de cumplimiento regulatorio como los reporte del MSPI, el SFC CE33, el GAP de Ciberseguridad, para mantenerlos actualizados identificando las brechas, mejoras, niveles de madures para dar respuesta a los requerimientos de ley ante la Superfinanciera de Colombia.

Observación 17:

Documento: 005_2021_pliegoCondiciones página 62

Alcance

13. Informe de los controles existentes para la mitigación de los riesgos y de la medición de nivel de efectividad de los controles identificados.

Por favor indicar si actualmente se tiene un inventario de los controles implementados para la mitigación de riesgos

Respuesta: Nos permitimos aclarar que La Previsora cuenta con un inventario centralizado de los controles de riesgos, pero se indica que este se actualiza anualmente identificando nuevos riesgos o modificando según los cambios de arquitectura.

Observación 18:

Documento: 005_2021_pliegoCondiciones página 62

Alcance

14. Informe de gestión de Activos de Información de la Gerencia de TI y los relacionados con el contexto de ciberseguridad.

Por favor indicar si actualmente se tiene un inventario de activos de TI actualizados.

Respuesta: Nos permitimos aclarar que La Previsora cuenta con un inventario de activos de TI, y se actualiza anualmente.

Observación 19:

Documento: 005_2021_pliegoCondiciones página 62

Alcance

16. Informe del análisis de riesgos informáticos, y de ciberseguridad de los activos de información identificados, incluyendo medición de riesgo inherente y residual y mapas de calor de riesgo de seguridad informática y ciberseguridad.

Por favor aclarar si con este punto se busca que el proveedor realice un análisis de riesgos completo sobre los activos, vulnerabilidades y amenazas de LA PREVISORA.

Respuesta: Nos permitimos aclarar que su entendimiento es correcto, este es uno de los documentos que deben ser entregados por el proveedor según los riesgos informáticos definidos actualmente e identificados en la operación del servicio durante su vigencia.

Observación 20:

Documento: 005_2021_pliegoCondiciones página 62

Alcance

23. Se deberán contemplar capacitaciones a nivel interno de la compañía para los funcionarios de la previsora, mínimo una vez al año, estas deberán ser coordinadas entre las partes y con la debida autorización del supervisor del contrato. Es de aclarar que estas sesiones se efectúan de manera virtual donde se tratan temas de seguridad y mejores prácticas a nivel de seguridad.

Por favor indicar a cuantas personas hay que capacitar

Respuesta: Nos permitimos aclarar que la periodicidad esta descrita en el numeral 3.3.8. ENTREGABLES y que la cantidad de usuarios de planta es de setecientos cincuenta y cuatro (754), sin embargo, dependerá de la estrategia de capacitación que se defino ejemplo tipo Webinar, Charla, Video, entre otros.

Observación 21:

Documento: 005_2021_pliegoCondiciones página 77

Alcance

ANEXO No. 1 DISPOSITIVOS MONITOREO			
Fuente de datos	**Número de dispositivos**	**Ampliación 5%**	**Observaciones**

Por favor indicar los fabricantes de las fuentes de datos, esto con el fin de determinar cuales de estas deben ser normalizadas y dimensionar los esfuerzos.

Respuesta: Nos permitimos aclarar que no es posible especificar el detalle de la informacion, pero se indica que son marcas muy reconocidas en el mercado como HPE, Fortinet, Cisco, Sophos, Microsoft o Red Hat Enterprice, entre otros.

Observación 22:

Documento: 005_2021_pliegoCondiciones, ítem 3.3.7.1 SERVICIOS DE SOC

Alcance

a. Servicio de monitorización inteligente de eventos de seguridad en modalidad 7x24. La gestión de incidentes se debe realizar a través de la herramienta entregada por LA PREVISORA S.A.

1. *Solicitamos a entidad aclarar los niveles de disponibilidad requeridos para la prestación del servicio, y los niveles de dispnibilidad de la plataforma SIEM que soportará el servicio.*

2. Soliticamos aclarar a la entidad cual es la herramienta de gestión utilizada? La integrción se debe realizar por API?

3. Amablemente solictiamos a la entidad que para el proceso de gestión de incidentes, la herramienta SIEM incorpore nativamente un sistema de ticketing y de esa forma adoptar de forma natural el proceso de gestión de incidentes durante los procesos de análisis y detección de amenazas.

Respuesta: Nos permitimos aclarar que:

Punto 1: Con respecto a los niveles de disponibilidad para la prestación del servicio y para la plataforma de SIEM esta deberá ser de 7X24x365 ya que por ser un servicio de SOC debe contar con disponibilidad de 99,5% y contar con alto contingencia, para mas claridad se realiza ajuste en la Adenda N°3.

Punto 2: Actualmente la herramienta de gestión es Aranda la cual es tercerizada, al ser un servicio WEB se considera que se puede integrar mediante API, sin embargo esto deberá revisarse en las primeras reuniones entre el proveedor seleccionado y los administradores de la herramienta.

Punto 3: Nos permitimos indicar que, si bien la herramienta de SIEM tiene su sistema de ticketing nativo, esta no será accedida por la entidad ya que contar con doble sistema para la gestión de incidentes no es viable, por lo cual su observación no será tenida en cuenta.

Observación 23:

Documento: 005_2021_pliegoCondiciones, ítem 3.3.7.1 SERVICIOS DE SOC

Alcance

b. Detectar y recolectar las evidencias de los eventos (incidencias maliciosas o falsos positivos), que ocurran sobre la infraestructura de LA PREVISORA S.A y dispositivos de red, que puedan poner en peligro la seguridad de la misma.

1. Solicitamos amablemente a la entidad que contemple incorporar las siguientes variables como críticas dentro del proceso de detección:

- *Actualización continua del contexto, de los dispositivos, su software y parches instalados, así como los servicios en ejecución.*
- *Contexto de usuario, en tiempo real, con seguimiento de direcciones IP, cambios de identidad de usuario, contexto de datos de ubicación física y geo-localización.*
- *Detectar dispositivos, aplicaciones de red y cambios de configuración no autorizados.*
- *Monitor de métricas de sistemas integrados en el proceso de monitoreo.*

2. Amablemente solicitamos a la entidad, que como base de servicio se permita el descubrimiento de dispositivos y mantener una base de datos de configuraciones (CMDB), mediante técnicas de auto-descubrimiento y aprendizaje de activos y mapeos inter-relacionales, en entornos tanto físico como virtuales y de cloud, de aplicaciones, usuarios, y dispositivos. En este sentido, el servicio ofertado deberá tener CMDB nativa dentro de la propia herramienta de SIEM.

Respuesta: Nos permitimos aclarar que:

Punto1: En el anexo N°5 ALCANCE SOC se especifica los requerimientos mínimos del servicio, si la plataforma ofrece adicionales, la previsora acepta las especificaciones y beneficios que esta ofrezca

Punto 2: Nos permitimos aclarar que la entidad no está sesgando las configuraciones de las herramientas de SIEM y que se acepta las especificaciones y beneficios adicionales que esta ofrezca, sin costo alguno para la entidad.

Observación 24:

Documento: 005_2021_pliegoCondiciones 3.3.7.1 SERVICIOS DE SOC
Alcance

f. Notificación proactiva de amenazas proporcionando soluciones y estrategias de mitigación, tomar medidas para proteger los sistemas y redes afectados o amenazados por la actividad de intrusos y desarrollar otras estrategias de respuesta o solución alternativa, con escenarios de crisis contra ataques dirigidos como DDoS o amenazas avanzadas.

1. Es de nuestro entendimiento que la entidad busca conjunto de respuestas pre-configuradas ante eventos de seguridad, de manera que se permita no sólo la detección sino también la remediación automatizada ante determinadas amenazas.

2. Es de nuestro entendimiento que la entidad busca la posibilidad de activar una secuencia de comandos de corrección cuando se produce un incidente específico?

Respuesta: Nos permitimos aclarar que:

Punto 1: Confirmamos que su entendimiento es correcto

Punto 2: Confirmamos que su entendimiento es correcto

Observación 25:

Documento: 005_2021_pliegoCondiciones 3.3.7.1 SERVICIOS DE SOC

Alcance

h. EL PROPONENTE deberá contar con una herramienta SIEM en modalidad de servicio en nube para el análisis de los registros de eventos de los equipos de seguridad existentes (IPS's, Firewalls, Endpoint, Sandbox, UBA, etc) y respuesta ante eventos inusuales, la integración de la herramienta deberá contemplar múltiples formas de integración, así como envió de logs, agentes u otro para dejar operativo todos los servicios que se requieran monitorear.

1. *Solicitamos amablemente a la entidad incorporar a la solución de SIEM de nueva generación usada dentro del servicio realizar monitoreo de integridad de archivos en los servidores monitoreados basado en agente, asi como monitorear los cambios no autorizados de las configuraciones de los dispositivos de redes, esto permitirá establecer una análisis holistco requerido para enfrentar las amezas actuales y al tiempo garantizar altos estándares de cumplimiento de estándares internacionales.*

2. Solicitamos amablemente a la entidad que en aras de manteneder altos niveles de rendimientos y para cantidad de plataformas a monitorear, se permita instalación en premisas para responder de forma eficiente y tiempos cernos al tiempo real en el proceso de detección de amenazas.

Documento: 005_2021_pliegoCondiciones 3.3.7.1 SERVICIOS DE SOC

Alcance

h. EL PROPONENTE deberá contar con una herramienta SIEM en modalidad de servicio en nube para el análisis de los registros de eventos de los equipos de seguridad existentes (IPS's, Firewalls, Endpoint, Sandbox, UBA, etc) y respuesta ante eventos inusuales, la integración de la herramienta deberá contemplar múltiples formas de integración, así como envió de logs, agentes u otro para dejar operativo todos los servicios que se requieran monitorear.

1. *Solicitamos amablemente a la entidad incorporar a la solución de SIEM de nueva generación usada dentro del servicio realizar monitoreo de integridad de archivos en los servidores monitoreados basado en agente, asi como monitorear los cambios no autorizados de las configuraciones de los dispositivos de redes, esto permitirá establecer una análisis holistco requerido para enfrentar las amezas actuales y al tiempo garantizar altos estándares de cumplimiento de estándares internacionales.*

2. Solicitamos amablemente a la entidad que en aras de manteneder altos niveles de rendimientos y para cantidad de plataformas a monitorear, se permita instalación en premisas para responder de forma eficiente y tiempos cernos al tiempo real en el proceso de detección de amenazas.

Respuesta: Nos permitimos aclarar que:

Punto 1: La previsora en el numeral 3.3.7.1 SERVICIOS DE SOC detalla a nivel general los elementos de monitoreo entre ellos la analítica de datos, por lo cual lo descrito en la observación está incluido en el pliego de condiciones.

Punto 2: No es clara su observación, pero se indica que, si se requiere la implementación de colectores, los costos e infraestructura deberán correr por parte del proponente, para un mayor entendimiento se ajusta numeral 3.3.7.5. HERRAMIENTAS DE GESTIÓN DE LA SOLUCIÓN mediante Adenda N°3

Observación 26:

Documento: 005_2021_pliegoCondiciones 3.3.7.1 SERVICIOS DE SOC

Alcance

j. EL PROPONENTE debe encargarse de realizar todas las tareas necesarias para asegurar la generación, almacenamiento (mínimo 12 meses) y potencial recuperación de respaldos de las configuraciones de todas las plataformas involucradas en el servicio. Estos respaldos podrán ser solicitados por la entidad para ser almacenados en sus instalaciones.

1. *Solicitamos amablemente a la entidad que la arquitectura de almacenamiento sea escalable, con almacenaje de eventos NoSQL, y correlación distribuida de eventos en tiempo real. De esa forma, se podrá desplegar tantos nodos para procesar la información como nodos recolectores que se quiera sin que esto suponga un coste extra en el licenciamiento durante el servicio.*
2. *Agradecemos confirmar a que máquinas se les generará el backup de la totalidad del listado compartido.*

Respuesta: Nos permitimos aclarar que:

Punto 1: La solicitud anterior describe el tiempo de almacenamiento de los logs que se deben salvaguardar, esto con el fin de poder contar con esta información en cualquier momento. El proponente validara la mejor opción que considere en el diseño de su arquitectura para cumplir con la solicitud.

Punto 2: Se deberá salvaguardar el total de logs de eventos del servicio bajo la plataforma SIEM, esto deberá garantizar una retención de mínimo 12 meses, una vez definido su sistema de backup, se puede hacer sobre escritura de los mismos.

Observación 27:

Documento: 005_2021_pliegoCondiciones 3.3.7.1 SERVICIOS DE SOC

Alcance

k. Proveer en modalidad de servicio, soportada y gestionada una plataforma de análisis de comportamiento de usuarios (UBA) por lo menos 200 usuarios sensibles seleccionados por LA PREVISORA S.A.

1. Soliitamos a la entidad que sea requerido el establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana.

2. Sugerimos amablemente a la entiedad que el servicio de UEBA no onlleve consumo asociado ni de licencia de dispositivos ni de EPS en relación con los dispotivos monitoreados, todo con el objeto garantizar un sitema autonoma de UEBA.

Respuesta: Nos permitimos aclarar que:

Punto 1: Las configuraciones y demás políticas para el servicio solicitado serán validadas en conjunto con el proponente seleccionado.

Punto 2: En el numeral 3.3.7.5. HERRAMIENTAS DE GESTIÓN DE LA SOLUCIÓN se describe que el Proponente deberá contar con todas las herramientas necesarias para la prestación del servicio.

Observación 28:

Alcance

EL PROPONENTE deberá ofrecer un servicio integral de SOC, el cual contemple durante la etapa de operación, en los primeros seis (6) meses del servicio, la ejecución del afinamiento y estabilización respectivo de la plataforma de SIEM que ofrezca, para las aplicaciones y demás servicios específicos, alineado a una operación de nivel 1 "Monitorización y análisis"

1. muy amablemente se solicita a la entidad clarificar si la solición SIEM es requerida en alta disponibilidad.

2. Es de nuestro entendimiento que la entidad solicita una solución de SIEM de nueva generación la cual permita monitorear tanto la seguridad (SIEM), como la disponibilidad y el desempeño de las plataformas (SOC/NOC), de esa forma se puede disponer de un único punto de gestión de datos no sólo de eventos de seguridad, sino también de:

- *Rendimiento y disponibilidad*
- *CPU, memoria y almacenamiento.*
- *Detección de cambios de configuración.*
- *Monitorización de transacciones sintéticas.*
- *Cuadros de mando dinámicos*

Respuesta: Nos permitimos aclarar que:

Punto 1: Nos permitimos indicar que el servicio debe contemplar el cumplimiento de disponibilidad de 99.5%, por lo que el numeral 3.3.7.4. ACUERDOS DE NIVELES DE SERVICIO será modificado en Adenda N°3

Punto 2: El servicio solicita sobre un SIEM de nueva generación es para el monitoreo, análisis, gestión y respuesta de incidentes de seguridad y ciberseguridad (SOC Nivel 2). No se contempla servicios de monitoreo de infraestructura tipo NOC. Si la herramienta la proporciona es independiente y no es una exigencia de la entidad.

Observación 29:

Documento: 005_2021_pliegoCondiciones 3.3.7.4.1. Acuerdos de Niveles de Servicio (ANS) de Gestión de Incidentes de Servicio

Alcance

A continuación, se presenta la tabla para los requerimientos reportados y evidenciadas con horario 8X5 sobre las herramientas y sólo aplica para la infraestructura de seguridad gestionada de forma directa por EL PROPONENTE.

1. Solicitamos a entidad aclarar los niveles de disponibilidad requeridos para la prestación del servicio, y los niveles de dispnibilidad de la plataforma SIEM que soportará el servicio.

Respuesta: Nos permitimos aclarar que el detalle de la disponibilidad del servicio se detalla en el numeral 3.3.7.4. ACUERDOS DE NIVELES DE SERVICIO tanto para incidentes como para requerimientos.

Observación 30:

Documento: 005_2021_pliegoCondiciones 3.3.7.2.2. TECNICO DE SEGURIDAD TI

Alcance

Perfil Profesional y Experiencia Profesional, técnico o tecnólogo titulado en sistemas, telecomunicaciones o carreras afines con mínimo dos (2) años de experiencia en la administración y gestión de plataformas de seguridad como Firewall Fortinet o dispositivos de seguridad perimetral similares, contar con conocimientos en Consolas de Antivirus para endpoint, entre otros sistemas de seguridad, se requiere mantenimiento y aplicación de reglas a los servicios descritos. 43 De preferencia manejo en (OIM/OIG) o disponibilidad para tomar la gestión de dicha herramienta Gestora de identidades.

Agradecemos a la entidad confirmar las herramientas que el técnico de seguridad TI debe gestionar. Asi mismo agradecemos confirmar si para la administración y gestión de la herramienta de gestión de Identidades (OIM/OIG) LA PREVISORA ofrece la capacitación al técnico de seguridad TI

Respuesta: Nos permitimos indicar que el Firewall es Fortinet, Antivirus es Sophos y el servicio de gestión de identidades (OIG) es Oracle. Así mismo se contempla la gestión

del módulo de seguridad en Office365, DLP y Antispam. Para las herramientas de OIG se dispondrá por parte de la entidad de capacitación al recurso asignado.

XXVI. OBSERVACIONES PRESENTADAS POR LA EMPRESA O4IT

Observación 1:

DOCUMENTOS	REQUERIMIENTO	OBSERVACIONES
Pliego de condiciones 3.3.6. recurso humano mínimo habilitante	Un (1) gerente de servicio:	Solicitamos con el mayor respeto a la Previsora de Seguros, aceptar ampliar el requerimiento, incluyendo especialización en **gerencia de proyectos en ingeniería y/o Maestría en ingeniería.**
		Solicitamos con el mayor respeto ampliar el requerimiento y aceptar incluir adicionalmente a las requeridas en el pliego de condiciones, las siguientes certificaciones que se encuentran acorde a un Gerente de Servicio: Contar con al menos una: • COBIT 5 • PMP Vigente • Scrum Fundamentals

Respuesta: Nos permitimos aclarar que su observación no será tenida en cuenta.

Observación 2:

Pliego de condiciones Anexo no. 2 recurso humano calificable	Director y/o coordinador soc	Solicitamos con el mayor respeto modificar el requerimiento y solicitar: **Experiencia profesional Demostrar Mínimo 10 años de experiencia profesional y 3 años de experiencia especifica** en Gerencia de proyectos, coordinación de SOC o consultoría de seguridad de la información **o líder en proyectos de seguridad de la información o** en proyectos de diseño desarrollo e implementación de sistemas de gestión de seguridad de la información bajo el estándar ISO 27001, pruebas de EthicaL Hacking, Gestión de Riesgos, y Arquitectura de Seguridad. • Adicionalmente, aceptar e incluir la certificación: CIHE - Certified Incident Handling Engineer – Mile2 que es equivalente a la ya solicitada. ECIH – EC-Council Certified Incident Handler - EC-Council • Asimismo, aceptar incluir la certificación: ISO 27001:2013 Certificación Internacional Auditor Líder.
	Experto coordinador de grupo de respuestas a incidentes	Solicitamos con el mayor respeto aceptar ampliar y modificar el requerimiento así: Demostrar mínimo 5 años de experiencia profesional como coordinador, analista **y/o Consultor de**
		Seguridad de la información y/o supervisor en el área de la ciberseguridad

Respuesta: Nos permitimos indicar que se ajustara ANEXO No. 2 RECURSO HUMANO CALIFICABLE del pliego de condiciones, este se verá modificado en Adenda N°3, de igual forma se especifica el detalle el numeral OBSERVACIONES GENERALES ítem 3 “Certificaciones del Recurso Humano calificable“ del presente documento

Observación 3:

3.3.7.1 SERVICIOS DE SOC. h. EL PROPONENTE	Por otro lado, se deben contemplar sitios web, bases de datos, servidores, aplicaciones internas y en nube como (office365, saleforce, entre otras) y demás con los que cuente la compañía	Por favor suministrar el inventario completo de todos los activos alojados en las distintas nubes a soportar. Con respecto a Offcce 365, cuantos usuarios y que otras aplicaciones adicionales exactamente deben ser tenidas en cuenta.

Respuesta: Nos permitimos aclarar que el inventario completo no será entregado en esta etapa del proceso, si no al oferente seleccionado. Respecto a O365 nos permitimos indicar que la compañía cuenta con 1000 licencias tipo E1 y E3 de uso de la suite completa de las herramientas de O365.