RESPUESTA A OBSERVACIONES

FIDUPREVISORA S.A. en cumplimiento a las actividades del cronograma establecido en la invitación a cotizar No. 001 de 2020, se permite dar respuesta a cada una de las observaciones presentadas, en relación a (…) *"Fiduprevisora S.A. está interesada en cotizar el servicio de Centro de Operaciones de Seguridad – SOC apoyados en la tecnología de correlación de eventos de seguridad, con personal experto de apoyo en horario 7x24 durante la vigencia a cotizar; esto con el fin de monitorear y dar respuesta a los incidentes de seguridad de la infraestructura tecnológica de la entidad.*

Así mismo, se requiere en la cotización incluir el servicio de consultoría en la ejecución de pruebas para el Análisis de Vulnerabilidades sobre la infraestructura tecnológica de Fiduprevisora S.A., sus sistemas de información y sitios web atendiendo las obligaciones relacionadas con las Circulares Externas 029/2014 y 007/2018 de la Superintendencia Financiera de Colombia."

FIDUPREVISORA S.A.
INVITACION A COTIZAR No. 001 - 2020
RESPUESTA A OBSERVACIONES

Fiduprevisora S.A. en respuesta a observaciones a la Invitación a cotizar número 001 - 2020 se procede a responder las observaciones, de la siguiente manera:

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
9	09/01/2020	Correo Electrónico	**CARVAJAL TECNOLOGÍA Y SERVICIOS**

En el ***numeral 3 ALCANCE***, se tienen las siguientes observaciones:

1. En el literal C *"Una (1) prueba de Ethical Hacking tipo caja gris a diez (10) sistemas de información con su respectivo re-test"*, dentro de estos sistemas existen sistemas transaccionales, de ser así por favor indicar cuantos son.

RESPUESTA DE FIDUPREVISORA: Como sistema transaccional se tiene únicamente Peoplesoft.

2. En el literal D *"Una (1) prueba de Ethical Hacking tipo caja negra a diez (10) URL con su respectivo re-test",* dentro de estos sistemas existen sistemas transaccionales, de ser así por favor indicar cuantos son.

RESPUESTA DE FIDUPREVISORA: Son 4, los cuales se indican a continuación: Digitalización FOMAG, Radicación FOMAG, OnBase FOMAG (2 URL).

3. En el literal E *"Cinco (5) pruebas de análisis dinámico de código para cinco (5) sistemas de información (una por cada uno) con su respectivo re-test",* por favor indicar el lenguaje de programación y cuantas líneas de código de cada uno.

RESPUESTA FIDUPREVISORA: Se tienen aplicaciones en JAVA, PeopleSoft (ORACLE). La cantidad de líneas de código no son necesarias dado que el análisis solicitado es dinámico (DAST).

4. En el literal F *"Ofrecer una bolsa de horas para hacking de caja gris y caja negra que pueda ser adquirido en la implementación de nuevos proyectos tecnológicos que impliquen desarrollos, páginas web o URL, entre otros",* en esta bolsa de horas existe un mínimo de horas a ofertar.

RESPUESTA FIDUPREVISORA: No existe mínimo de horas se puede cotizar precio por horas o una cantidad mínima que el oferente proponga y el valor de la hora adicional por si se requiere, o alguna otra alternativa.

5. En el literal G *"Ofrecer una bolsa de horas y plan de trabajo para la remediación de las vulnerabilidades encontradas",* en esta bolsa de horas existe un mínimo de horas a ofertar.

RESPUESTA FIDUPREVISORA: No existe mínimo de horas se puede cotizar precio por horas o una cantidad mínima que el oferente proponga y el valor de la hora adicional por si se requiere, o alguna otra alternativa.

6. Actualmente la entidad cuenta con los siguientes servidores los cuales deben ser monitoreados por el correlacionador de eventos:

- Linux Centos 6.5
- Linux Centos 6.8
- Linux Debian
- Linux Red Hat 5.0
- Linux alcmeon-lmen
- Linux Solaris 11
- Linux Solaris 10
- Vmware ESXI 5.5
- Vmware ESXI 5.0
- OVM Server
- Windows 2016 server
- Windows 2012 server R2
- Windows 2003 server R2
- Windows 2003 server
- Windows 2008 server
- Windows 2008 server R2
- Windows 2008 server R3
- Windows 7 SP1
- Windows XP
- Windows 10
- SaaS en Office365

Por lo anterior se requiere saber que roles cumple cada uno de los servidores Windows, para tener una visibilidad mucho más acotada a los Eventos por Segundo (EPS) que genere esos DatasSurces, adicionalmente se quiere saber cuántos equipos de Windows XP, 10, Linux, etc. hace referencia o es solo uno (1).

RESPUESTA FIDUPREVISORA: Los servidores tienen diversos roles, FileServer, Backup, DataBase, PeopleSoft, WebServer, etc. Estos roles y las cantidades específicas serán detalladas en el momento de la implementación.

En el ***numeral 4 CONDICIONES DEL SERVICIO REQUERIDO***, se tienen las siguientes observaciones:

7. En el sub numeral *4.2.1 Servicio de monitoreo y correlación de eventos de seguridad*, "*el servicio de monitoreo y correlación de eventos debe monitorear todos los eventos recolectados a través del SIEM - Security Information and Event Management y brindar respuesta a incidentes de seguridad de la información en modalidad 7x24 durante la vigencia a cotizar, con una capacidad máxima de mil quinientos (1.500) dispositivos: servidores, dispositivos de red, dispositivos de seguridad y/o equipos de escritorio, etc.*", se requiere comedidamente que sea suministrado el listado de los 1.500 dispositivos a correlacionar con su respectivo rol para acotar la propuesta y sea beneficioso para la compañía.

RESPUESTA FIDUPREVISORA: El listado completo se entregará al momento de implementar la solución a quien se le asigne el contrato, de momento se indica que son 1200 computadores con sistema operativo Windows 10, Windows 7 y XP, los demás son servidores como se mencionan en la parte inferior que cumplen roles diversos como FileServer, Backup, DataBase, Peoplesoft, Webserver, Intranet, etc.

- Linux Centos 6.5
- Linux Centos 6.8
- Linux Debian
- Linux Red Hat 5.0
- Linux alcmeon-lmen
- Linux Solaris 11
- Linux Solaris 10
- Vmware ESXI 5.5
- Vmware ESXI 5.0
- OVM Server
- Windows 2016 server
- Windows 2012 server R2
- Windows 2003 server R2
- Windows 2003 server
- Windows 2008 server
- Windows 2008 server R2
- Windows 2008 server R3
- Windows 7 SP1
- Windows XP
- Windows 10
- SaaS en Office365

8. En el sub numeral *4.5.1 "Obligaciones Específicas – SIEM"*, en su literal A "*Suministrar en modalidad de servicio un SIEM para soportar 1500 dispositivos con un rango de 1000 hasta 1500 eventos por segundo que permita colectar, retener y correlacionar los eventos de seguridad de la infraestructura TI de la entidad. ¿La plataforma deberá colectar los eventos de seguridad de múltiples marcas", dicho esto el manager de Correlacionador puede ser cloud y se podría colocar un receiver en el Datacenter de la Fiduprevisora para recolectar los logs?*

RESPUESTA FIDUPREVISORA: Si es válido hacer esta propuesta, sin embargo, se debe detallar el custodio, responsabilidad y almacenamiento de la información, así como el empalme, la devolución y/o eliminación de la misma cuando el contrato finalice.

9. En el literal K *"El SIEM y el equipo de SOC deberá monitorear interfaces de red de 1GB y 10GB, y ancho de banda de 150MB a 200MB",* para este punto a que hace referencia, a monitoreo de red como análisis de comportamiento y modelaje de red.

RESPUESTA FIDUPREVISORA: Lo que se requiere monitorear es la saturación del ancho de banda de los enlaces y las velocidades de negociación de las interfaces principalmente. Esto para verificar la disponibilidad de la red, así como posibles incidentes de seguridad debidos a saturación de la red, alto consumo de ancho de banda en un equipo, trafico inusual, etc. En el momento de la implementación se informará la cantidad de interfaces de red y las velocidades respectivas.

10. En cuanto a las certificaciones, se acepta que si el personal no tiene la certificación CISSP, pueda presentarse con la certificación CISM vigente.

ROL	OBSERVACIONES
Director de Operaciones	" Numeral 4.6 equipo de trabajo, dentro del perfil *Director de Operaciones* se hace referencia a la certificación CISSP. *Amablemente nos permitimos solicitar se modifique de manera opcional la certificación CISSP O Certificación CISM."*
Coordinador de SOC	" Numeral 4.6 equipo de trabajo, dentro del perfil *Coordinador de SOC* se hace referencia a la certificación CISSP. *Amablemente nos permitimos solicitar se modifique de manera opcional la certificación CISSP O Certificación CISM."*

RESPUESTA DE FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
2	09/01/2020	Correo Electrónico	**EVOLUTION TECHNOLOGIES GROUP S.A.S**

1. De acuerdo con las generalidades y en cuanto a las condiciones del servicio requerido, solicitamos a la entidad y con el fin de la pluralidad de los oferentes, excluir como requisito obligatorio que la organización oferente cuente con la certificación ISO 27001 vigente.

RESPUESTA FIDUPREVISORA: No es posible excluirlo, es parte de la gestión de proveedores y de los lineamientos internos de la dirección de seguridad de la información que todo proveedor de seguridad de la información deba cumplir con esta certificación.

2. Teniendo en cuenta el numeral *4.5.1 Obligaciones Específicas* – SIEM, solicitamos a la entidad aclarar el número de horas requeridas para el entrenamiento de la herramienta SIEM.

RESPUESTA FIDUPREVISORA: El número de horas debe ser sugerido por el proveedor de acuerdo a su experiencia, practicidad del software propuesto y cantidad de equipos a monitorear en la infraestructura, u otro esquema que deseen ofertar según sus posibilidades.

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
19	09/01/2020	Correo Electrónico	**O4IT COLOMBIA S.A.S**

1. ¿La solución se puede ofertar bajo un modelo de servicio en la nube?, es decir; donde las herramientas ofertadas estén en el Datacenter del proveedor.

RESPUESTA FIDUPREVISORA: Si es válido hacer esta propuesta, sin embargo, se debe detallar el custodio, responsabilidad y almacenamiento de la información, así como el empalme, la devolución y/o eliminación de la misma cuando el contrato finalice.

2. En el inventario de versiones de los servidores hay algunos sistemas operativos fuera de soporte del fabricante, por tanto, fuera del inventario oficial de sistemas operativos soportados por las herramientas de correlación y vulnerabilidades, lo cual podría implicar que dichos sistemas operativos no sean viables de monitoreo y/o verificación. ¿Si esto llegará a ocurrir la entidad impondría sanciones al proveedor?

RESPUESTA FIDUPREVISORA: No se impondrán sanciones, pero se solicita al proveedor que proponga controles complementarios o alternativos para mitigar las vulnerabilidades.

3. ¿Con qué tipo de licenciamiento cuenta la entidad en Office 365?

RESPUESTA FIDUPREVISORA: Actualmente se tienen licencias E1, E2 y Quiosco, se están migrando todas a E3 y algunas pocas con Addon para dispositivos móviles.

4. Se le recomienda a la entidad excluir a los equipos de escritorios del monitoreo directo, y hacerlo a través de puntos de concentración como son el Directorio activo y el antivirus.

RESPUESTA FIDUPREVISORA: Como la idea es correlacionar eventos, se requiere tener de primera mano la fuente de la información, en este caso los PCs de los usuarios. Esta información puede ser obtenida del servidor de directorio activo, del servidor de antivirus, o algún agente instalado localmente, pero la cobertura del servicio brindado debe contemplar efectivamente los 1200 equipos de usuarios con algún tipo de solución.

5. ¿Qué espacio físico la entidad entregará al proveedor para poder ubicar los equipos que soportaran las máquinas virtuales?

RESPUESTA FIDUPREVISORA: Actualmente Fiduprevisora cuenta con un Datacenter en IaaS y se puede otorgar un espacio de una unidad de RACK previa validación y aprobación de carga del Data Center.

6. ¿La nube de la entidad, en que ubicaciones se encuentra?

RESPUESTA FIDUPREVISORA: Se encuentra en la Nube privada en el Datacenter de Claro en las ciudades de Bogotá y Medellín.

7. ¿Cuáles son las aplicaciones que la entidad tiene en la nube?

RESPUESTA FIDUPREVISORA: Fiduprevisora tiene toda su plataforma tecnológica en una nube privada de Claro bajo el modelo IaaS, allí se tiene Directorio Activo, FileServer, Intranet, WebServer, aplicaciones inhouse, Backup, entre otras. Así mismo se cuenta con aplicaciones SaaS de office 365.

8. Se le solicita a la entidad dar mayor claridad sobre el ítem n) del aparte obligaciones específicas SIEM: "El SIEM deberá poder monitorear las aplicaciones en la nube de la entidad, utilizando como detección una combinación de DNS, proxy web y registros de firewalls integrándose directamente con los principales servicios en la nube, para proporcionar un solo panel que permita revisar: Cuando sus usuarios inician sesión en los servicios en la nube, dónde se registran sus usuarios (incluso fuera de la red corporativa), qué actividad realizan sus administradores de servicios en la nube, y cuándo los usuarios que ya no estén activos en la empresa continúan autenticándose en los servicios".

   Dado que la solución de monitoreo y correlación depende de la información suministrada a través de los logs de las diferentes herramientas, aplicaciones y los servicios en la nube adquiridos, por tanto, la viabilidad de crear un dashboard con la información solicitada no depende de la solución SIEM, si no de la información remitida a este.

   Por otra parte, detallar el requisito "cuándo los usuarios que ya no estén activos en la empresa continúan autenticándose en los servicios". Las reglas de correlación y/o alertamiento necesitan fuentes de datos que le permitan validar la información, así que la entidad debe indicar como realizar la validación si un usuario está activo o no en la organización.

   Adicionalmente, este último requisito está en mayor medida asociado a un control de seguridad que un usuario retirado y/o inactivo sea retirado y/o inactivado de todos los sistemas de información.

RESPUESTA FIDUPREVISORA: La apreciación es correcta, se hace la aclaración: Cuando un usuario se inactiva en dominio deja de poderse autenticar en las diferentes plataformas a las que esta sincronizada su identidad, sin embargo, se requiere validar los **intentos de autenticación fallidos** de un usuario que este inactivo. Se requieren un(os) dashboard(s) para visualizar el estado de los servicios prestados en tiempo real, y emitir reportes según las necesidades que defina Fiduprevisora S.A., pero no se requiere el desarrollo de una aplicación adicional hecha a la medida que unifique la información requerida.

9. En el literal K del aparte "*obligaciones específicas vulnerabilidades"*, se asume que una única herramienta realiza las validaciones de código, vulnerabilidades, entre otros, si lo que se tiene es un grupo de soluciones no es viable la implementación del requerimiento.

Se le solicita a la entidad acotar el alcance solo a la herramienta de verificación de vulnerabilidades de equipos.

RESPUESTA FIDUPREVISORA: puede ser un mismo software que tenga diversos módulos para las actividades específicas que se requieren, sin embargo, no se exige la implementación de un solo software.

10. Se le solicita a la entidad aclarar, si las Hojas de Vida de equipo de trabajo deben ser aportadas en esta fase del proceso, ósea al momento de la entrega de cotización.

RESPUESTA FIDUPREVISORA: No es necesario que sean aportadas, pero sí que confirmen el cumplimiento con las certificaciones.

11. Se le solicita a la entidad, no solo tener en cuenta para las certificaciones solicitadas de ethical hacking y forense al EC-Council como ente certificador, si no también entes certificadores como Miles2, GIAC, ISACA, CompTIA.

RESPUESTA FIDUPREVISORA: Para los certificados asociados a ethical hacking y forense se solicitan los del EC-Council, para el certificado de CISSP sirve también el CISM de ISACA, sin embargo, se revisarán las condicione de los perfiles.

12. Del personal indicado en el ítem 4.6 como recursos Humanos cuantas personas deberían estar directamente en cliente.

RESPUESTA FIDUPREVISORA: Sería pertinente que estuviera 1 persona por lo menos 2 días a la semana, según la necesidad. Se van a revisar los perfiles requeridos para la licitación.

13. En el numeral 4.5.1 en su literal J, el sistema de tickets tiene que venir integrado, o se puede gestionar a través de una plataforma independiente.

RESPUESTA FIDUPREVISORA: Se considera como plataforma independiente en la que Fiduprevisora pueda tener 4 usuarios y contraseñas para realizar el seguimiento de los eventos e incidentes y tener la trazabilidad de los mismos, pero efectivamente puede ser independiente sin incurrir en gastos de desarrollos hechos a la medida.

14. En el Numeral 4.5. en su literal k). Cuando relacionan el monitoreo de interfaces de red 1GB Y 10 GB, hace referencia a monitorear mediante NIDS (Network Intrusion Detection System).

RESPUESTA FIDUPREVISORA: Lo que se requiere monitorear es la saturación del ancho de banda de los enlaces y las velocidades de negociación de las interfaces principalmente. Esto para verificar la disponibilidad de la red, así como posibles incidentes de seguridad debidos a saturación de la red, alto consumo de ancho de banda en un equipo, trafico inusual, etc.

15. Por favor indicar consola de antivirus.

RESPUESTA FIDUPREVISORA: Actualmente Fiduprevisora cuenta con el Antivirus TrendMicro instalado en los servidores y equipos de usuario.

16. A nivel de red qué dispositivos deben ser monitoreados, referencias de dispositivos.

RESPUESTA FIDUPREVISORA: Los dispositivos de red son switches, routers y Access point marca ARUBA

17. Se tiene previsto ¿bases de datos?, que tipo de base de datos.

RESPUESTA FIDUPREVISORA: Se tienen contemplado en el análisis de vulnerabilidades las Bases de Datos en Oracle.

18. Se tienen sistemas adicionales como proxy, dlp, sandbox, por favor indicarlos.

RESPUESTA FIDUPREVISORA: Se cuenta con Firewall, Antivirus y DLP**.**

19. En el numeral 4.2.3 cuando se indica sobre las tareas de contención y recuperación, estas hacen referencia al acompañamiento del SOC o a ingresar a los servidores y realizar acciones sobre los dispositivos?

RESPUESTA FIDUPREVISORA: Es deber del proveedor identificar las vulnerabilidades, generar el plan de acción para remediarlas y realizar las actividades de remediación en acompañamiento del personal de TI de Fiduprevisora, se debe garantizar la segregación de funciones (para evitar un Conflicto de intereses) entre el análisis de vulnerabilidades y la remediación.

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
3	09/01/2020	Correo Electrónico	**OLIMPIA IT**

1. Actualmente la entidad cuenta con los siguientes servidores los cuales deben ser monitoreados por el correlacionador de eventos:

- Linux Centos 6.5
- Linux Centos 6.8
- Linux Debian
- Linux Red Hat 5.0
- Linux alcmeon-lmen
- Linux Solaris 11
- Linux Solaris 10
- Vmware ESXI 5.5
- Vmware ESXI 5.0
- OVM Server
- Windows 2016 server
- Windows 2012 server R2
- Windows 2003 server R2
- Windows 2003 server
- Windows 2008 server
- Windows 2008 server R2
- Windows 2008 server R3
- Windows 7 SP1
- Windows XP
- Windows 10

- SaaS en Office365

Es preciso indicar que en el numeral 4.2.1 se indica que se tienen 1500 dispositivos entre servidores, dispositivos de red, dispositivos de seguridad y/o equipos de escritorio, etc, se solicita a la entidad aclarar la cantidad de equipos a monitorear y correlacionar.

RESPUESTA FIDUPREVISORA: Es un total de 130 Servidores, 1200 equipos de usuario final, 80 dispositivos de seguridad y un porcentaje para crecimiento de la infraestructura.

2. En el numeral 4.2.3 *"Manejo de incidentes de seguridad",* el cual indica *"Las tareas de prevención, detección, contención y recuperación de ataques, entre otras, deberán estar incluidas dentro del proceso de Manejo de Incidentes de Seguridad de la metodología de atención del SOC - servicio de Centro de Operaciones de Seguridad. Uno de los objetivos clave del servicio de SOC es minimizar el impacto del Incidente de Seguridad, contenerlo, preservar la evidencia para identificar responsables y normalizar la operación lo más pronto posible",* se solicita a la entidad poder indicar la cantidad de incidentes de seguridad que tienen actualmente en un mes.

RESPUESTA FIDUPREVISORA: Actualmente Fiduprevisora tiene entre cinco (5) y diez (10) incidentes de seguridad al mes, sin embargo, se requiere monitorear toda la infraestructura para poder tener la visual completa, por ende, esta cantidad de incidentes puede aumentar.

3. En el numeral 4.5.1 "*Obligaciones Específicas – SIEM"* su literal *A INDICA "Suministrar en modalidad de servicio un SIEM para soportar 1500 dispositivos con un rango de 1000 hasta 1500 eventos por segundo que permita colectar, retener y correlacionar los eventos de seguridad de la infraestructura TI de la entidad. La plataforma deberá colectar los eventos de seguridad de múltiples marcas",* se solicita a la entidad poder indicar la cantidad de incidentes de seguridad que tienen actualmente en un mes.

RESPUESTA FIDUPREVISORA: Actualmente Fiduprevisora tiene entre cinco (5) y diez (10) incidentes de seguridad al mes, sin embargo, se requiere monitorear toda la infraestructura para poder tener la visual completa, por ende, esta cantidad de incidentes puede aumentar.

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
5	09/01/2020	Correo Electrónico	**CBTSEC**

1. Solicitamos respetuosamente nos informen si requieren que el servicio de SIEM este licenciado.

RESPUESTA FIDUPREVISORA: Efectivamente el producto debe estar licenciado.

2. Solicitamos respetuosamente que no se exija tener la calidad de partner de la herramienta de correlación de eventos, acorde con lo solicitado en el numera *4.1. Generalidades*, dado que esto puede limitar la participación de empresas que tienen amplia experiencia en la prestación de servicios que requiere la Fiduprevisora.

RESPUESTA FIDUPREVISORA: Se requiere que el proveedor tenga calidad de partner puesto que esto demuestra respaldo, confianza, experiencia y experticia en el manejo del software propuesto.

3. Solicitamos respetuosamente que en cuanto a la solicitud de que el interesado deba contar con la certificación ISO 27001 vigente, esta incluya también certificado el servicio de SOC, esto con el fin de que se brinde mayor confianza en los procesos para el buen desarrollo del proyecto que adelanta la entidad.

RESPUESTA FIDUPREVISORA: Hace parte de la gestión de proveedores y de los lineamientos internos de la dirección de seguridad de la información que todo proveedor de seguridad de la información deba cumplir con esta certificación. Se tendrá en consideración para etapas de una eventual contratación, en caso de que Fiduprevisora S.A. tome la determinación de hacer un proceso de contratación en un futuro.

4. Acorde con el numeral *4.6. Equipo de trabajo*, solicitamos respetuosamente a la entidad que el cumplimiento de los perfiles deba ser acreditado por la empresa contratista únicamente, dado que es un equipo de trabajo con detalles específicos que podría limitar la participación de empresas en el presente proceso.

RESPUESTA FIDUPREVISORA: Se revisará los requisitos de los perfiles definidos.

5. Adicionalmente, evaluar la disponibilidad 7X24 de todos los roles, dado que, para la operación del servicio, no se requiere que todos los perfiles tengan dicha disponibilidad, a excepción de quienes estarán realizando en monitoreo permanente durante la duración del proyecto.

RESPUESTA FIDUPREVISORA: En cuanto a la disponibilidad 7x24 se exige que esta sea sobre el servicio prestado, sin embargo, se aclara que debe existir una matriz de escalamiento sobre la cual se contactará al nivel más alto solo si los niveles inferiores no pueden brindar solución. ***Se van a revisar los perfiles requeridos para la licitación.***

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
2	09/01/2020	Correo Electrónico	**CADENA S.A**

1. En el numeral 4.6 Equipo de Trabajo se detallan los roles, formación profesional, experiencia y certificaciones de cada uno de los recursos humanos para dar ejecución al contrato. Solicitamos a la entidad aclarar si las certificaciones exigidas para cada uno de los roles son completamente obligatorias o si se puede contar con algunas de estas y garantizar desde el proceso y la estructura del proyecto la idoneidad del personal y la ejecución del mismo.

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación dado el reto informado por los proveedores.***

2. Solicitamos amablemente a la entidad indicar el presupuesto del proceso, lo anterior con el objetivo de presentar una oferta acorde con lo proyectado por la entidad para este servicio y adicionalmente, buscando enmarcar el servicio bajo un presupuesto indicativo.

RESPUESTA FIDUPREVISORA: El presupuesto se informará cuando se emita la licitación para la adjudicación del contrato.

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
18	09/01/2020	Correo Electrónico	**DIGIWARE**

1. En el numeral *3. ALCANCE,* en el literal E *"Cinco (5) pruebas de análisis dinámico de código para cinco (5) sistemas de información (una por cada uno) con su respectivo re-test",* se tienen las siguientes observaciones:

a) Se solicita aclarar la cantidad de líneas de código con que cuenta la aplicación o el peso a nivel de KB del archivo de configuración de la misma, esto con el fin de poder dimensionar el requerimiento

RESPUESTA FIDUPREVISORA: La cantidad de líneas de código no son necesarias dado que el análisis solicitado es dinámico (DAST).

b) Se solicita especificar el lenguaje de programación sobre el cual están desarrolladas las aplicaciones.

RESPUESTA FIDUPREVISORA: Se tienen aplicaciones en JAVA, PeopleSoft (ORACLE).

c) Se solicita aclarar si las aplicaciones son de propiedad de un tercero, si se encuentran en sitio o en nube pública o privada

RESPUESTA FIDUPREVISORA: Se tiene de todo un poco, Peoplesoft (Tercero), Aplicaciones desarrolladas por terceros e InHouse, páginas web de terceros en Datacenter de Fiduprevisora y páginas web en hosting, también se tienen aplicativos en nube.

2. Actualmente la entidad cuenta con los siguientes servidores los cuales deben ser monitoreados por el correlacionador de eventos:

- Linux Centos 6.5
- Linux Centos 6.8
- Linux Debian
- Linux Red Hat 5.0
- Linux alcmeon-lmen
- Linux Solaris 11
- Linux Solaris 10
- Vmware ESXI 5.5
- Vmware ESXI 5.0
- OVM Server
- Windows 2016 server
- Windows 2012 server R2
- Windows 2003 server R2
- Windows 2003 server
- Windows 2008 server
- Windows 2008 server R2

- Windows 2008 server R3
- Windows 7 SP1
- Windows XP
- Windows 10
- SaaS en Office365

a) Se solicita aclarar si el cliente desea realizar solamente la correlación de los eventos provenientes de los sistemas operativos de las plataformas listadas.

RESPUESTA FIDUPREVISORA: Se deben correlacionar eventos de los sistemas operativos, de las aplicaciones que estos soportan y de los equipos de red switches, routers y Access point marca Aruba.

b) Se solicita especificar la cantidad de dispositivos por cada uno de los sistemas operativos a monitorear

RESPUESTA FIDUPREVISORA: Las cantidades específicas serán detalladas en el momento de la implementación.

3. En el sub numeral 4.2.1 "*Servicio de monitoreo y correlación de eventos de seguridad"* el cual indica *"El servicio de monitoreo y correlación de eventos debe monitorear todos los eventos recolectados a través del SIEM - Security Information and Event Management y brindar respuesta a incidentes de seguridad de la información en modalidad 7x24 durante la vigencia a cotizar, con una capacidad máxima de mil quinientos (1.500) dispositivos: servidores, dispositivos de red, dispositivos de seguridad y/o equipos de escritorio, etc.",* Se solicita especificar la cantidad, fabricante y función de: servidores, dispositivos de red, dispositivos de seguridad, equipos de cómputo y de la infraestructura en general que se desea monitorear.

RESPUESTA FIDUPREVISORA: Los servidores tienen diversos roles, FileServer, Backup, DataBase, PeopleSoft, WebServer, etc. Estos roles y las cantidades específicas serán detalladas en el momento de la implementación.

4. En el sub numeral 4.3.4 *"Acompañamiento en la remediación y verificación por el proveedor",* el cual indica *"Se requiere que el proveedor cotice una bolsa de horas para la remediación de las vulnerabilidades encontradas, esto implica que el proveedor debe tener las capacidades técnicas y de personal para poder remediar las vulnerabilidades, si la entidad no autoriza ejecutar el plan de remediación de estas, es deber del proveedor proponer acciones que mitiguen el impacto o probabilidad de ocurrencia de estas",* Se solicita modificar este requerimiento por *"Se requiere que el proveedor cotice una bolsa de horas para el acompañamiento en la remediación de las vulnerabilidades encontradas, esto implica que el proveedor debe tener las capacidades técnicas y de personal para poder sugerir las acciones de remediación de las vulnerabilidades, si la entidad no autoriza ejecutar el plan de remediación de estas, es deber del proveedor proponer acciones que mitiguen el impacto o probabilidad de ocurrencia de estas.". Dado que el cliente al ser el responsable y conocer su infraestructura es el idóneo para ejecutar las acciones de remediación"*

RESPUESTA FIDUPREVISORA: No se modifica debido a que actualmente la Gerencia de TI no dispone de las capacidades suficientes para la atención de las vulnerabilidades, por tal motivo se solicita la bolsa de horas para que un proveedor preste dicho servicio.

5. En el numeral 4.4 *"Entregables"* el cual indica "*El servicio de SOC - servicio de Centro de Operaciones de Seguridad debe contemplar la entrega de reportes mensuales de gestión, los cuales incluyen el detalle de las actividades realizadas en el período, para cada uno de los procesos cubiertos por el servicio de seguridad gestionada, dicho reporte se entregará por medio de un informe ejecutivo y un informe técnico, adicional a esto el proveedor debe generar un informe detallado cuando ocurra alguna alerta urgente o incidencia que pueda o haya afectado a la entidad que incluya como mínimo…"*, se solicita "*incluir la posibilidad de mostrar los resultados del servicio a través de un portal web el cual cuente con dashboard gerenciales y operativos para facilitar el acceso a la información proveniente del resultado de los servicios".*

RESPUESTA FIDUPREVISORA: Se acepta la solicitud.

6. En el numeral 4.4 Entregables su literal J indica *"Cronograma con el plan y alcance de las pruebas de vulnerabilidad, hacking ético, análisis de código e ingeniería social",* se solicita aclarar el alcance que espera el cliente para las pruebas de ingeniería social, si es una vez por año, cantidad de usuarios, tipo de pruebas (correo, física, etc.)

RESPUESTA FIDUPREVISORA: Se solicita mínimo 1 vez por año, puede ser mediante correo.

7. En el numeral 4.5 Obligaciones su literal C *"Garantizar el debido licenciamiento y operatividad de la herramienta para SIEM y análisis de vulnerabilidades"*, se solicita aclara si se desea contar con una herramienta de correlación de eventos, un servicio de SOC el cual cuente con su propio correlacionador y herramientas tecnológicas como servicio o si desea adquirir un SIEM y que este sea gestionado por el oferente. Dado que en el objeto se solicita un servicio y en este ítem solicita garantizar el licenciamiento de la herramienta SIEM.

RESPUESTA FIDUPREVISORA: Se requiere que el proveedor implemente un SIEM el cual debe monitorear la infraestructura tecnológica de la compañía, este SIEM debe notificar a un SOC, también suministrado por el proveedor quien realizará una validación de los eventos recibidos por el SIEM y notificará a Seguridad de la información solo los eventos que considere relevantes o que se puedan catalogar como incidentes de seguridad.

8. En el numeral 4.5 Obligaciones su literal E "*El proveedor deberá suministrar acceso a cuatro (4) usuarios a la plataforma de monitoreo bajo el rol de consulta al dashboard, reglas, gráficas, tablas y reportes"*, se solicita modificar este requerimiento por *"El proveedor deberá suministrar acceso a cuatro (4) usuarios a la plataforma de monitoreo bajo el rol de consulta al dashboard, reglas, gráficas, tablas y reportes o tener la posibilidad de acceder a un portal web donde se visualicen el comportamiento del servicio, realizar consultas mediante dashboard operativos y ejecutivos"*, dado que al contar con un portal centralizado mejora las actividades operativas del cliente.

RESPUESTA FIDUPREVISORA: No se modificará la invitación, pero no se exime si se ofrece este portal web.

9. En el numeral 4.5.1 Obligaciones Específicas – SIEM su literal A *"Suministrar en modalidad de servicio un SIEM para soportar 1500 dispositivos con un rango de 1000 hasta 1500 eventos por segundo que permita colectar, retener y correlacionar los eventos de seguridad de la infraestructura TI de la entidad. La plataforma deberá colectar los eventos de seguridad de múltiples marcas*" se solicita incrementar la cantidad de eventos por segundo a 5.000 o disminuir la cantidad de dispositivos de 100 o 200 y extraer los logs de las estaciones desde el AD o la consola de antivirus, ya que al mencionar que el rango máximo de eps es 1.500 se está asumiendo que cada dispositivo va a generar 1 eps, lo cual por experiencia no acurre en la práctica.

RESPUESTA FIDUPREVISORA: Se acepta la modificación solicitada, no se pedirá un rango definido de EPS siempre y cuando cumpla con la cantidad de equipos solicitados.

10. En el numeral 4.5.1 Obligaciones Específicas – SIEM su literal C *"Los recursos necesarios para la instalación y operación de la herramienta SIEM en relación a la memoria, procesamiento y almacenamiento, deberán ser proporcionados por el contratista"*, se solicita eliminar este requerimiento, ya que el objeto del contrato es un servicio y no una compra de una plataforma.

RESPUESTA FIDUPREVISORA: No se acepta eliminar ya que esto aplica cuando el proveedor ofrece implementar un servidor físico o appliance sobre el cual se prestaría el servicio, si el servidor es una máquina virtual este funcionaría bajo la infraestructura que tiene Fiduprevisora contratada como servicio.

11. En el numeral 4.5.1 Obligaciones Específicas – SIEM su literal D *"La implementación de las reglas del SIEM deberá hacerse al momento de la entrega del funcionamiento correcto y evidenciable de la herramienta y su ajuste deberá realizarse a más tardar en el primer mes de operación de la herramienta*" Se solicita modificar este requerimiento por *" el servicio de SOC deberá contar con reglas de correlación base las cuales deben ser activadas al inicio del servicio" ya que este requerimiento se enfoca en la compra e implementación de un SIEM y no de un servicio de SOC".*

RESPUESTA FIDUPREVISORA: Se modificará el numeral quedando: 4.5.1 Obligaciones Específicas – SIEM y SOC.

12. En el numeral 4.5.1 Obligaciones Específicas – SIEM su literal F *"El SIEM debe permitir asignar un rol de consulta para el equipo de seguridad de la información de la entidad con el fin de obtener información sobre los eventos y las alertas de incidentes, sin interrumpir el flujo de trabajo de otros roles. Los datos deberán poder exportarse para su revisión por miembros del equipo sin la necesidad de acceso a la solución", s*e solicita eliminar este requerimiento, ya que el objeto del contrato es un servicio y no una compra de una plataforma. Se solicita modificar por *"proveer acceso a un portal web desde el cual el grupo de seguridad pueda visualizar las alertas generadas, dar seguimiento a los casos y visualizar todo lo concerniente con el servicio".*

RESPUESTA FIDUPREVISORA: No se modifica el numeral, sin embargo, si el oferente propone un portal web donde se pueda centralizar la información y acceder a esta para el seguimiento es válido, pero debe poderse exportar o generar reportes.

13. En el numeral 4.5.1 Obligaciones Específicas – SIEM su literal J "*El SIEM deberá contar con un sistema propio de tickets*", se solicita modificar este item por "*El servicio SOC deberá contar con una herramienta de tickets*" ya que el objeto del contrato es la adquisición de un servicio y no la compra de una plataforma SOC.

RESPUESTA FIDUPREVISORA: Se hace la aclaración de que el sistema de tickets debe ser del proveedor, no se solicita un módulo en el SIEM, este sistema de tickets es para poder realizar el registro y seguimiento de los incidentes de seguridad que reporta el SOC.

14. En el numeral 4.5.1 Obligaciones Específicas – SIEM su literal K *"El SIEM y el equipo de SOC deberá monitorear interfaces de red de 1GB y 10GB, y ancho de banda de 150MB a 200MB",* Se solicita aclarar cuál es el alcance que espera el cliente, ya que una plataforma SIEM normalmente no monitorea interfaces o anchos de banda. Para esto se utilizan plataformas de monitoreo de red los cuales envían los eventos al SIEM para ser correlacionados.

RESPUESTA FIDUPREVISORA: Lo que se requiere monitorear es la saturación del ancho de banda de los enlaces y las velocidades de negociación de las interfaces principalmente. Esto para verificar la disponibilidad de la red, así como posibles incidentes de seguridad debidos a saturación de la red, alto consumo de ancho de banda en un equipo, trafico inusual, etc.

15. En el numeral 4.5.1 Obligaciones Específicas – SIEM su literal I "*El proveedor deberá brindar capacitación en las funcionalidades de la herramienta SIEM en relación al entendimiento del dashboard, la generación de informes y la visualización y entendimiento de las reglas del SIEM. Este entrenamiento debe ser certificable por el proveedor y será dirigido a cuatro (4) personas que Fiduprevisora S.A. considere deban estar integrados en el proceso"*, se solicita modificar este requerimiento por *"El proveedor deberá brindar capacitación en el acceso al portal web de acceso donde se visualicen las alertas y comportamiento del servicio"* ya que este ítem hace referencia a la compra de una plataforma SIEM y no a un servicio de SOC.

RESPUESTA FIDUPREVISORA: No se modificará, sin embargo, se aclara que se requiere adquirir el servicio de SIEM, SOC y Análisis de vulnerabilidades. Si el oferente propone un portal web donde se pueda centralizar la información y acceder a esta para el seguimiento es válido, pero debe poderse exportar o generar reportes.

16. En el numeral 4.5.1 Obligaciones Específicas – SIEM su literal n *"El SIEM deberá poder monitorear las aplicaciones en la nube de la entidad, utilizando como detección una combinación de DNS, proxy web y registros de firewalls integrándose directamente con los principales servicios en la nube, para proporcionar un solo panel que permita revisar: Cuando sus usuarios inician sesión en los servicios en la nube, dónde se registran sus usuarios (incluso fuera de la red corporativa), qué actividad realizan sus administradores de servicios en la nube, y cuándo los usuarios que ya*

no estén activos en la empresa continúan autenticándose en los servicios", se solicita aclarar si este requerimiento hace referencia a una capacidad de la plataforma.

RESPUESTA FIDUPREVISORA: Este requerimiento hace referencia al uso de la identidad de los usuarios dentro de las aplicaciones SaaS de la nube de Office 365 así como fuera de la red de la compañía, intentos de inicio de sesión fallidos, inicios de sesión inusuales, cambios de contraseña, entre otros eventos que puedan considerarse como incidentes de seguridad.

17. En el numeral 4.5.1 Obligaciones Específicas – SIEM su literal P *"El equipo del SOC deberá generar un informe ejecutivo, así como un informe técnico mensual, y en caso de una alerta urgente o incidencia debe generar un informe detallado",* se solicita incluir la posibilidad de habilitar un acceso a un portal web el cual cuente con dashboard operativos, ejecutivos y tácticos, donde sea posible la visualización de la información de tal forma que se mejoren los procesos operativos del cliente.

RESPUESTA FIDUPREVISORA: Non se modificará la invitación. Sin embargo, adicional al acceso a la plataforma se requiere de los reportes mensuales de gestión identificados en el proceso de gestión.

18. En el numeral 4.5.2 "Obligaciones Específicas – Vulnerabilidades" en su literal K *"Para la remediación de las vulnerabilidades se requiere tener un usuario de Fiduprevisora S.A. que permita analizar en tiempo real si con las modificaciones realizadas (Parcheo, modificación de código, implementación de certificados, entre otros) se remedió la vulnerabilidad detectada, esto con el fin de poder cerrar los controles de cambios oportunamente o realizar rollback si la solución propuesta afecta el desempeño del aplicativo sin remediar la vulnerabilidad"*, se solicita aclarar si el requerimiento de contar con un usuario de acceso, hace referencia al acceso hacia la plataforma de análisis de vulnerabilidades, en la cual pueda ver el comparativo entre cada uno de los análisis ejecutados.

RESPUESTA FIDUPREVISORA: Efectivamente se requiere un usuario de acceso para verificar si al momento de realizar un cambio en un servidor, este permite corregir la vulnerabilidad antes de dejar dicho cambio en producción.

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
8	09/01/2020	Correo Electrónico	**DELOITTE**

1. Con respecto al Numeral *3. ALCANCE*, en el literal a) Una prueba de vulnerabilidades en la infraestructura tecnológica para 130 IP (Servidores virtuales y físicos) con su respectivo re-test, se presentan las siguientes observaciones:

a) ¿Las IPs se encuentran en un mismo segmento de red?

RESPUESTA FIDUPREVISORA: Son diferentes segmentos de red (Ambientes de desarrollo, producción, pruebas, DMZ, negocios, etc)

b) ¿Las IPs son internas o externas?

RESPUESTA FIDUPREVISORA: Las IPs para los 130 servidores son internas.

c) ¿Todas IPs se encuentran ubicadas en la ciudad de Bogotá?, en caso que parte de las IPs estén ubicadas en otras ciudades, ¿Se cuenta con conexión VPN o es necesario desplazarse a las ciudades?

RESPUESTA FIDUPREVISORA: Todas las IPs para los 130 servidores se encuentran en Bogotá y Medellín**,** estos se encuentran interconectados por medio de un canal dedicado del cual se puede hacer uso.

2. Con respecto al Numeral: *3. ALCANCE,* ítem b) Una prueba de vulnerabilidades en la infraestructura tecnológica para 1200 IP (Endpoints) con su respectivo re-test, se presentan las siguientes observaciones:

a) ¿Las IPs se encuentran en un mismo segmento de red?

RESPUESTA FIDUPREVISORA: No, se tienen varios segmentos de red.

b) ¿Las IPs son internas o externas?

RESPUESTA FIDUPREVISORA: Todas las IPs para los 1200 Endpoints son internas.

c) ¿Todas IPs se encuentran ubicadas en la ciudad de Bogotá?, en caso que parte de las IPs estén ubicadas en otras ciudades, ¿Se cuenta con conexión VPN o es necesario desplazarse a las ciudades?

RESPUESTA FIDUPREVISORA: Los 1200 Endpoints se encuentran distribuidos en las diferentes regionales que tiene la compañía a nivel nacional, estas están interconectadas mediante MPLS o SD-WAN de las cuales se puede hacer uso.

3. Con respecto al Numeral: *3. ALCANCE*, ítem e) Cinco (5) pruebas de análisis dinámico de código para cinco (5) sistemas de información (una por cada uno) con su respectivo re-test, se presentan las siguientes observaciones:

a) Por favor, ¿aclarar si se busca un análisis de código estático (SAST) que consiste en la evaluación del código fuente o si se busca un análisis dinámico (DAST) que en ese caso corresponde a realizar un análisis de vulnerabilidades mientras la aplicación está en ejecución?

RESPUESTA FIDUPREVISORA: Se requiere un análisis dinámico (DAST)

b) ¿Cuántas líneas de código se requieren analizar?

RESPUESTA FIDUPREVISORA: La cantidad de líneas de código no son necesarias dado que el análisis solicitado es dinámico (DAST).

c) ¿Cuál es el lenguaje o framework en el cual está desarrollado las aplicaciones?

RESPUESTA FIDUPREVISORA: Se tienen aplicaciones en JAVA, PeopleSoft (ORACLE).

4. Con respecto al Numeral: *3. ALCANCE,* ítem f) Bolsa de horas para hacking de caja gris y caja negra para la implementación de nuevos proyectos. Por favor aclarar si se ha definido un número aproximado de horas de la bolsa.

RESPUESTA FIDUPREVISORA: No existe mínimo de horas se puede cotizar precio por horas o una cantidad mínima que el oferente proponga y el valor de la hora adicional por si se requiere, o cualquier modalidad que considere pertinente para el caso el oferente según sus posibilidades.

5. Con respecto al Numeral: *3. ALCANCE*, ítem g) Bolsa de horas y plan de trabajo para la remediación de las vulnerabilidades encontradas. Por favor aclarar si se ha definido un número aproximado de horas de la bolsa.

RESPUESTA FIDUPREVISORA: No existe mínimo de horas se puede cotizar precio por horas o una cantidad mínima que el oferente proponga y el valor de la hora adicional por si se requiere, o cualquier modalidad que considere pertinente para el caso el oferente según sus posibilidades.

6. Con respecto al Numeral: *3. ALCANCE*, para las pruebas de vulnerabilidades, ethical hacking y análisis dinámico de código; ¿Cuál es el horario de realización de las mismas? Por favor, indicar horarios.

RESPUESTA FIDUPREVISORA: Las pruebas solicitadas se deben hacer en horario no laboral para no afectar la labor de los usuarios y de la gerencia de TI, en ese orden de ideas se recomienda realizarlas de lunes a viernes entre las 10pm y las 6am con previa autorización, siempre y cuando no se cruce con otra actividad programada.

7. Con respecto al Numeral: *4.4. ENTREGABLES*, ítem j) Cronograma con el plan y alcance de las pruebas de vulnerabilidad, hacking ético, análisis de código e ingeniería social, se tienen las siguientes observaciones:

a) Por favor, especificar el alcance de la(s) prueba(s) de ingeniería social

RESPUESTA FIDUPREVISORA: Se requieren pruebas que ayuden a medir el nivel de conciencia en seguridad de la información de los usuarios, estas pueden ser por correo mínimo 1 vez al año.

b) ¿Cuántos son los objetivos?

RESPUESTA FIDUPREVISORA: Todo el personal que trabaja en Fiduprevisora, bien sea de planta, temporal, contratistas y/o practicantes. Aproximadamente 1200 personas.

8. Con respecto al Numeral *4.6. EQUIPO DE TRABAJO*, se tienen las siguientes observaciones:

a) Respecto al rol de Director de Operaciones, ¿está persona tiene que contar con todas las certificaciones mencionadas o con algunas?

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

b) Respecto al rol de Especialista en pruebas de vulnerabilidad, ¿está persona puede contar con un mínimo de tres (3) años de experiencia?

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
20	09/01/2020	Correo Electrónico	**Colombia Telecomunicaciones S. A. ESP**

1. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, ítem 3. ALCANCE. "El servicio de Centro de Operaciones de Seguridad – SOC a cotizar se requiere para realizar monitoreo constante, y de esta manera identificar, detectar, responder y recuperarse ante cualquier incidente de ciberseguridad, con base en una estrategia de ciberseguridad que se articule con recursos humanos y técnicos. Se requiere cotizar por cada año de servicio: a. Una (1) prueba de vulnerabilidades en la infraestructura tecnológica para 130 IP (servidores virtuales y físicos) con su respectivo re-test, considerando que la infraestructura es gestionada como servicio y colocation dentro del datacenter de claro. ", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar y aclarar si los servidores físicos y virtuales deben ser analizados de manera interna (desde la red LAN) o desde internet a través de sus datos públicos.

RESPUESTA FIDUPREVISORA: Para el análisis de vulnerabilidades preferiblemente se requiere hacer desde la red interna (LAN) de Fiduprevisora, y se revisará con el proveedor de data center si se requieren configuraciones adicionales para hacerlos desde la red externa.

2. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, ítem 3. ALCANCE. "El servicio de Centro de Operaciones de Seguridad – SOC a cotizar se requiere para realizar monitoreo constante, y de esta manera identificar, detectar, responder y recuperarse… b. Una (1) prueba de vulnerabilidades para 1200 IP (Endpoints) con su respectivo re-test." Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar y detallar los tipos de sistemas operativos de los equipos endpoints a analizar.

RESPUESTA FIDUPREVISORA: Los endpoints a analizar tienen los siguientes sistemas operativos:

- Windows 7 SP1
- Windows XP
- Windows 10

3. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, ítem 3. ALCANCE. "El servicio de Centro de Operaciones de Seguridad – SOC a cotizar se requiere para

realizar monitoreo constante, y de esta manera identificar, detectar, responder y recuperarse … c. Una (1) prueba de ethical hacking tipo caja gris a diez (10) sistemas de información con su respectivo retest.“, Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar y detallar los tipos de sistemas de información, así como las plataformas (servidores, sistemas operativos, ambientes virtuales o no) sobre las cuales se encuentran operando dichos sistemas de información.

RESPUESTA FIDUPREVISORA: Los servidores a analizar tienen los siguientes sistemas operativos:

- Linux Centos 6.5
- Linux Centos 6.8
- Linux Debian
- Linux Red Hat 5.0
- Linux alcmeon-lmen
- Linux Solaris 11
- Linux Solaris 10
- Vmware ESXI 5.5
- Vmware ESXI 5.0
- OVM Server
- Windows 2016 server
- Windows 2012 server R2
- Windows 2003 server R2
- Windows 2003 server
- Windows 2008 server
- Windows 2008 server R2
- Windows 2008 server R3

4. El documento “Invitación a cotizar Fiduprevisora”, INVITACIÓN A COTIZAR No. 001 DE 2020, ítem 3. ALCANCE. “El servicio de Centro de Operaciones de Seguridad – SOC a cotizar se requiere para realizar monitoreo constante, y de esta manera identificar, detectar, responder y recuperarse … e. Cinco (5) pruebas de análisis dinámico de código para cinco (5) sistemas de información (una por cada uno) con su respectivo re-test.“, Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar y detallar los tipos de sistemas de información, así como las plataformas y ambientes de desarrollo sobre los cuales están desarrollados dichos sistemas de información (java, .net, etc).

RESPUESTA FIDUPREVISORA: Se tienen aplicaciones en JAVA, PeopleSoft (ORACLE). La cantidad de líneas de código no son necesarias dado que el análisis solicitado es dinámico (DAST).

5. El documento “Invitación a cotizar Fiduprevisora”, INVITACIÓN A COTIZAR No. 001 DE 2020, ítem 3. ALCANCE. “El servicio de Centro de Operaciones de Seguridad – SOC a cotizar se requiere para realizar monitoreo constante, y de esta manera identificar, detectar, responder y recuperarse … g. Ofrecer una bolsa de horas y plan de trabajo para la remediación de las vulnerabilidades encontradas.“, Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar y aclarar, cuál debe ser el alcance de la remediación sobre las vulnerabilidades encontradas. ¿Debe ser función del proveedor realizar las actividades de remediación sobre cada activo? ¿O esta labor la realizará el responsable por parte de FIDUPREVISORA?

RESPUESTA FIDUPREVISORA: Es deber del proveedor identificar las vulnerabilidades, generar el plan de acción para remediarlas y realizar las actividades de remediación en acompañamiento del personal de TI de Fiduprevisora, se debe garantizar la segregación de funciones (para evitar un posible Conflicto de intereses) entre el análisis de vulnerabilidades y la remediación.

6. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 4. CONDICIONES DEL SERVICIO REQUERIDO. 4.1 Generalidades. Ítem 8. "Actualmente la entidad cuenta con los siguientes servidores los cuales deben ser monitoreados por el correlacionador de eventos: … ", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar y detallar la ubicación de los servidores a ser monitoreados, si se encuentran en el DataCenter principal, alterno y en qué ciudad".

RESPUESTA FIDUPREVISORA: Los servidores se encuentran en el datacenter de Claro en la ciudad de Bogotá, también se cuenta con un Datacenter alterno en la ciudad de Medellín.

7. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 4. CONDICIONES DEL SERVICIO REQUERIDO. 4.2.1 Servicio de monitoreo y correlación de eventos de seguridad. "El servicio de monitoreo y correlación de eventos debe monitorear todos los eventos recolectados a través del SIEM - Security Information and Event Management y brindar respuesta a incidentes de seguridad de la información en modalidad 7x24 durante la vigencia a cotizar, con una capacidad máxima de mil quinientos (1.500) dispositivos: servidores, dispositivos de red, dispositivos de seguridad y/o equipos de escritorio, etc. ",Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar y aclarar si la cantidad de 1500 dispositivos debe ser monitoreado desde el inicio del proyecto o si se trabajará por fases. Adicionalmente, solicitamos por favor detallar el listado de los 1500 dispositivos, especificando la cantidad y tipo de servidores, equipos de red, dispositivos de seguridad, equipos de escritorio, etc y su ubicación.

RESPUESTA FIDUPREVISORA: Los activos se incluirán al monitoreo por grupos, iniciando con Servidores críticos, equipos de seguridad perimetral, equipos de comunicaciones, demás servidores y equipos de usuarios en grupos por regionales.

8. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 4. CONDICIONES DEL SERVICIO REQUERIDO. 4.2.2 Monitoreo de seguridad. "El sistema de monitoreo y correlación de eventos de seguridad debe contar con módulos que detecten patrones y anomalías en el tráfico de red, recolección de logs de diversas fuentes para su normalización, centralización y análisis. Una vez se recolecten los logs, deberán ser correlacionados y priorizados, con el fin de obtener la valoración del riesgo del evento de seguridad y la información necesaria para dar atención y gestión.", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar y aclarar si FIDUPREVISORA cuenta con un sistema de gestión de riesgos y sobre que activos y procesos se realiza, adicionalmente, si este puede ser socializado durante la ejecución del proyecto.

RESPUESTA FIDUPREVISORA: Fiduprevisora cuenta con una metodología para la gestión de riesgos sobre activos de información, sin embargo, este punto hace referencia a que el proveedor debe realizar un análisis de primer nivel para descartar falsos positivos y reportar los eventos que puedan ser considerados incidentes de seguridad, así mismo, estos deben estar categorizados por nivel de riesgo para dar prioridad a la gestión de estos.

9. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 4. CONDICIONES DEL SERVICIO REQUERIDO. 4.2.3 Manejo de incidentes de seguridad. "Las tareas de prevención, detección, contención y recuperación de ataques, entre otras, deberán estar incluidas dentro del proceso de Manejo de Incidentes de Seguridad de la metodología de atención del SOC - servicio de Centro de Operaciones de Seguridad. Uno de los objetivos clave del servicio de SOC es minimizar el impacto del Incidente de Seguridad, contenerlo, preservar la evidencia para identificar responsables y normalizar la operación lo más pronto posible...", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar y aclarar cuál debe ser el alcance del requerimiento asociado a la recuperación de ataques.

RESPUESTA FIDUPREVISORA: Apoyo y monitoreo de los sistemas afectados después de contener el ataque, así como la verificación de que otros activos pueden haber resultado afectados.

10. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 4. CONDICIONES DEL SERVICIO REQUERIDO. 4.2.4 Monitoreo de disponibilidad. "Se debe vigilar que los elementos bajo contrato estén funcionando todo el tiempo necesario, y en caso de que algún dispositivo se inhabilite o trabaje inadecuadamente sin causa aparente, el SOC tomará las medidas acordadas conjuntamente en los niveles de servicio, para reactivar/restaurar el servicio lo antes posible, de tal forma que se recupere la normalidad de la operación.", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar y aclarar cuál debe ser el alcance del requerimiento asociado a reactivar/restaurar el servicio lo antes posible. Por favor dar claridad si FIDUPREVISORA realizará la administración y operación de los activos que estén bajo el proceso de monitoreo.

RESPUESTA FIDUPREVISORA: Fiduprevisora administrará los activos de información, el alcance se refiere al protocolo de comunicaciones y matriz de escalamiento durante el tiempo que el servicio ser encuentre afectado, esto implica la creación de tickets, notificaciones y seguimiento.

11. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 4. CONDICIONES DEL SERVICIO REQUERIDO. 4.5.1 Obligaciones Específicas – SIEM. "j. El SIEM deberá contar con un sistema propio de tickets.", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar y aclarar si la herramienta de tickets puede ser independiente de la herramienta SIEM.

RESPUESTA FIDUPREVISORA: Se hace la aclaración de que el sistema de tickets debe ser del proveedor, puede ser independiente, no se solicita un módulo en el SIEM, este sistema de tickets es para poder realizar el registro y seguimiento de los incidentes de seguridad que reporta el SOC.

12. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 4. CONDICIONES DEL SERVICIO REQUERIDO. 4.5.1 Obligaciones Específicas – SIEM. "n) El SIEM deberá poder monitorear las aplicaciones en la nube de la entidad, utilizando como detección una combinación de DNS, proxy web y registros de firewalls integrándose directamente con los principales servicios en la nube, para proporcionar un solo panel que permita revisar: Cuando sus usuarios inician sesión en los servicios en la nube, dónde se registran sus usuarios (incluso

fuera de la red corporativa), qué actividad realizan sus administradores de servicios en la nube, y cuándo los usuarios que ya no estén activos en la empresa continúan autenticándose en los servicios.", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar y detallar cuales son y cuál es la cantidad de las aplicaciones en la nube de la entidad. Adicionalmente, si están se encuentran en la capacidad de enviar los registros de acceso, autenticación y autorización.

RESPUESTA FIDUPREVISORA: Fiduprevisora cuenta con la suite de Office365 bajo la modalidad SaaS, se está migrando todo el licenciamiento a E3 y algunos usuarios van a tener Addon de dispositivos móviles.

13. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 4. CONDICIONES DEL SERVICIO REQUERIDO. 4.6 Equipo de Trabajo "El interesado debe contar con el Recurso Humano idóneo para la ejecución del contrato, teniendo como mínimo los siguientes roles en disponibilidad 7x24:", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar si el personal solicitado debe ser de carácter dedicado o si puede ser personal compartido.

RESPUESTA FIDUPREVISORA: Puede ser personal compartido siempre y cuando se cumpla con las competencias necesarias y la disponibilidad 7x24 del recurso cuando se necesite durante el tiempo que dure el contrato.

14. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 4. CONDICIONES DEL SERVICIO REQUERIDO. 4.1 Generalidades "4. El oferente está en la capacidad de disponer de un servidor de propósito específico en sitio, especializado en el Análisis de Vulnerabilidades. Esta herramienta deberá ser instalada, configurada y administrada por el prestador del servicio.", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar y aclarar si se habla de un servidor propiedad del cliente que puede ser utilizado por el proponente o se habla de un servidor físico que debe proporcionar el proponente.

RESPUESTA FIDUPREVISORA: Si el proponente ofrece implementar un servidor físico o appliance sobre el cual se prestaría el servicio debe suministrar y gestionar los recursos tecnológicos que este necesita para su funcionamiento, si el servidor es una máquina virtual este funcionaría bajo la infraestructura que tiene Fiduprevisora contratada como servicio.

15. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 3. ALCANCE. "e. Cinco (5) pruebas de análisis dinámico de código para cinco (5) sistemas de información (una por cada uno) con su respectivo re-test.", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, especificar un aproximado de la cantidad de líneas de código que se deben analizar.

RESPUESTA FIDUPREVISORA: La cantidad de líneas de código no son necesarias dado que el análisis solicitado es dinámico (DAST).

16. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 3. ALCANCE. "g. Ofrecer una bolsa de horas y plan de trabajo para la remediación de las

vulnerabilidades encontradas.", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, aclarar si la bolsa de horas será dedicada a generar los planes de trabajo o se espera una bolsa de horas de nivel técnico para ejecutar sobre las plataformas las acciones de remediación.

RESPUESTA FIDUPREVISORA: La bolsa de horas es tanto para el plan de trabajo que se va a desarrollar como la ejecución del mismo en acompañamiento de personal de TI y bajo previa aprobación.

17. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 4. CONDICIONES DEL SERVICIO REQUERIDO. 4.2 Actividades SOC "4.2.2. El servicio de monitoreo y correlación de eventos debe monitorear todos los eventos recolectados a través del SIEM - Security Information and Event Management y brindar respuesta a incidentes de seguridad de la información en modalidad 7x24 durante la vigencia a cotizar, con una capacidad máxima de mil quinientos (1.500) dispositivos: servidores, dispositivos de red, dispositivos de seguridad y/o equipos de escritorio, etc.", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, aclarar si los logs deben encontrarse en sitio y si se necesita alta disponibilidad de la captura de logs.

RESPUESTA FIDUPREVISORA: Sí, los logs se deben encontrar en sitio, siendo éste el data center de Fiduprevisora S.A., pero el proveedor puede utilizar herramientas en nube si así lo considera. En cuanto a la alta disponibilidad no se tiene contemplado a nivel de servidor dado que no es un servicio crítico y con la disponibilidad brindada por el datacenter es suficiente. Sin embargo, el servicio que preste el proveedor sí debe cumplir con unos ANS para la prestación de todos los servicios ofrecidos y sí está entre sus posibilidades con una alta disponibilidad para el SOC.

18. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 4. CONDICIONES DEL SERVICIO REQUERIDO. 4.2 Actividades SOC "4.2.4. Se debe vigilar que los elementos bajo contrato estén funcionando todo el tiempo necesario, y en caso de que algún dispositivo se inhabilite o trabaje inadecuadamente sin causa aparente, el SOC tomará las medidas acordadas conjuntamente en los niveles de servicio, para reactivar/restaurar el servicio lo antes posible, de tal forma que se recupere la normalidad de la operación..", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, aclarar si todos los equipos incluyendo los equipos de escritorio o de usuario final deben ser monitoreados en salud.

RESPUESTA FIDUPREVISORA: En cuanto a salud y disponibilidad solo se deben monitorear los equipos de la infraestructura tecnológica de Fiduprevisora.

19. El documento "Invitación a cotizar Fiduprevisora", INVITACIÓN A COTIZAR No. 001 DE 2020, 4. CONDICIONES DEL SERVICIO REQUERIDO. 4.5 Obligaciones "4.5.1.k El SIEM y el equipo de SOC deberá monitorear interfaces de red de 1GB y 10GB, y ancho de banda de 150MB a 200MB.", Colombia Telecomunicaciones S. A. ESP solicita muy respetuosamente, aclarar si el monitoreo de salud puede realizarse con una herramienta diferente al SIEM.

RESPUESTA FIDUPREVISORA: Se puede realizar con una herramienta diferente siempre y cuando no requiera instalar otro servidor físico, puede ser virtualizado, así mismo, se deben

correlacionar los eventos de ambos softwares para que a Fiduprevisora se le entregue la información como si fuera una sola fuente o remitente.

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
9	09/01/2020	Correo Electrónico	**COMWARE**

1. Se solicita amablemente a la entidad modificar el perfil del Coordinador de SOC de la siguiente manera:

"Director de Operaciones Profesional universitario en ingeniería electrónica o ingeniería de | sistemas o ingeniería de telecomunicaciones o afines con maestría o especialización en seguridad de la información o informática o carreras afines. Experiencia mínima específica de cinco (5) años certificada en proyectos relacionados con seguridad de la información o informática. Certificación como auditor líder ISO 27001 y diplomado o certificación en Ethical Hacker o certificado como CHFI o certificado como CISSP o certificado como CISM o certificado de seminario de investigación aplicada en gestión de la seguridad y el riesgo informático o certificado de Rapid 7 Insight Vulnerability Management Certified Administrator""

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

2. Se solicita amablemente a la entidad adicionar un "y/o" en las certificaciones que le solicitan a este rol. Para tener mayor claridad de nuestra solicitud, a continuación, encontrarán el párrafo con nuestra solicitud:

- "Dos (2) Analistas Junior de Seguridad SOC
- Profesionales universitarios en ingeniería electrónica o ingeniería de sistemas o ingeniería de telecomunicaciones.
- Experiencia mínima de tres (3) años de experiencia certificada en proyectos relacionados con seguridad de la información o informática
- Certificado como Ethical Hacker del EC-Council y/o certificado como CISM"

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

3. Se solicita amablemente a la entidad ampliar el nivel académico para este rol, adicionando "Técnico, tecnólogo o". Para tener mayor claridad de nuestra solicitud, a continuación, encontrarán el párrafo con nuestra solicitud:

- "Cuatro (4) Ingenieros de Operación
- Técnico, tecnólogo o profesional universitario en ingeniería electrónica, de sistemas, telecomunicaciones o carreras afines.
- Experiencia de dos (2) años en proyectos relacionados con Centros de Operaciones de Seguridad - SOC. Dedicación Tiempo completo Soporte 7x24, con operación remota; homologable un año, cuenta con alguna certificación relacionada con seguridad de la información y/o ciberseguridad".

RESPUESTA FIDUPREVISORA: No se acepta la solicitud, el nivel mínimo será de ingenieros - ***Se van a revisar los perfiles requeridos para la licitación.***

4. Se solicita amablemente a la entidad ampliar las certificaciones técnicas para este rol, adicionando "o certificaciones de SIEM y/o certificaciones de fabricantes de tecnologías ATP" en la solicitud ya que estás complementan los conocimientos requeridos en las condiciones del servicio requerido. Para tener mayor claridad de nuestra solicitud, a continuación, encontrarán el párrafo con nuestra solicitud:

- "Analista de Seguridad"
- Profesionales universitarios en ingeniería electrónica o ingeniería de sistemas o ingeniería de telecomunicaciones.
- Experiencia mínima de dos (2) años de experiencia certificada en proyectos relacionados con seguridad de la información o informática
- Certificado como Ethical Hacker (vigente) o Licensed Penetration Tester de EC-Council o certificaciones de SIEM y/o certificaciones de fabricantes de tecnologías ATP"

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

5. Se solicita amablemente a la entidad aclarar si es responsabilidad del proponente aplicar/ejecutar las remediaciones sobre la infraestructura del cliente, o si esto se refiere solo al acompañamiento.

RESPUESTA FIDUPREVISORA: Es deber del proveedor generar el plan de acción para remediar las vulnerabilidades y realizar las actividades de remediación en acompañamiento del personal de TI de Fiduprevisora S.A. tal como se especifica en la Invitación a Cotizar 001 de 2020.

6. Se solicita amablemente a la entidad que dentro de las características y funcionalidades del SOC se solicite características de User and entity behavior analytics (UEBA) y Security orchestration, automation and response (SOAR).

RESPUESTA FIDUPREVISORA: No se procede con la solicitud, esto puede considerarse en una próxima invitación cuando la madurez del área y del proceso sea mayor.

7. Se solicita amablemente a la entidad aclarar el alcance para la ejecución del monitoreo de disponibilidad. Si es para la infraestructura de la Fiduprevisora o si se requiere tener indicadores de disponibilidad del servicio.

RESPUESTA FIDUPREVISORA: Se requiere tener conocimiento de disponibilidad de infraestructura siendo este uno de los tres pilares de la seguridad de la información, lo cual puede convertirse en un evento o incidente de seguridad. En cuanto a la disponibilidad del servicio se debe cumplir con unos ANS pactados en caso de contratarse el servicio.

8. Se solicita amablemente a la entidad aclarar si la entidad está interesada en incluir un servicio de monitoreo de red NTA. En caso afirmativo, solicitamos indicar la cantidad de interfaces a monitorear y tipo (fibra o cobre, velocidad)

RESPUESTA FIDUPREVISORA: No se está interesado.

9. Se solicita amablemente a la entidad indicar qué o cuáles son los servicios de nube que se desea integrar al monitoreo.

RESPUESTA FIDUPREVISORA: Fiduprevisora cuenta con la suite de Office365 bajo la modalidad SaaS, se está migrando todo el licenciamiento a E3 y algunos usuarios van a tener Addon de dispositivos móviles.

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
27	09/01/2020	Correo Electrónico	**IT SECUTRITY SERVICES**

1. Entendiendo que "la presente invitación a cotizar en ningún caso podrá considerarse oferta para celebrar contrato" y que "el fin de esta solicitud es el de analizar las condiciones del mercado respectivo y la viabilidad de la contratación mediante la medición de variables como oportunidad, calidad, costo, etc" (según indica el numeral 1), amablemente solicitamos confirmar que la presente solicitud únicamente se entiende como un RFI (Request for Information) y bajo ningún concepto se podrá considerar como una oferta para celebrar contrato. Adicionalmente, solicitamos confirmar cuáles serán las etapas del presente proceso.

RESPUESTA FIDUPREVISORA: Como se señala en la invitación a cotizar, la misma no se considera una oferta y corresponde única y exclusivamente al insumo necesario para adelantar un estudio de mercado por parte de Fiduprevisora. En consecuencia, tanto la presente invitación a cotizar como la cotización que lleguen a remitir los oferentes interesados no constituyen una oferta comercial.

Por su parte debido a que el presente procedimiento corresponde a un estudio de mercado, las siguientes etapas se surten al interior de la Fiduciaria con la finalidad de obtener un conocimiento del mercado, el cual será analizado por la Entidad para considerar la posibilidad de adelantar un eventual proceso de contratación.

2. Amablemente solicitamos aclarar cuál va a ser la metodología de calificación de las propuestas y de selección de proveedor.

RESPUESTA FIDUPREVISORA: En el presente ejercicio de cotización no se calificarán las propuestas, sin embargo, las cotizaciones recibidas se utilizarán para realizar un reporte o documento de estudio de mercado que permita definir las condiciones con las que se armarían los términos de la siguiente etapa, en caso de que Fiduprevisora S.A. considere la posibilidad de adelantar un eventual proceso de contratación.

3. En el apartado *"Una (1) prueba de vulnerabilidades en la infraestructura tecnológica para 130 IP (servidores virtuales y físicos) con su respectivo re-test, considerando que la infraestructura es gestionada como servicio y colocation dentro del datacenter de claro"* Amablemente solicitamos confirmar cuántas direcciones IP son externas y cuántas son internas. Adicionalmente, confirmar si la prueba se debe hacer con o sin credenciales.

RESPUESTA FIDUPREVISORA: Para el análisis de vulnerabilidades se consideran solo las IPs internas (LAN) y se revisará con el proveedor de data center si se requieren configuraciones adicionales para hacerlos desde la red externa.

4. En el apartado *"Una (1) prueba de ethical hacking tipo caja gris a diez (10) sistemas de información con su respectivo re-test."*, amablemente solicitamos confirmar si los sistemas de información son de acceso externo o interno.

RESPUESTA FIDUPREVISORA: Solo se tiene uno de acceso externo, los demás son internos.

5. En el apartado *"Una (1) prueba de ethical hacking tipo caja gris a diez (10) sistemas de información con su respectivo re-test.",* amablemente solicitamos confirmar si cada sistema de información se compone de 1 sola IP, o si se compone de varias IPs. En caso de que sea la segunda opción, por favor confirmar la cantidad de IPs por cada sistema de información.

RESPUESTA FIDUPREVISORA: El sistema de información FRL tiene 2 IPs, Peoplesoft tiene 4 IPs, y el resto de sistemas todos cuentan con 1 sola IP.

6. En el apartado *"Una (1) prueba de ethical hacking tipo caja gris a diez (10) sistemas de información con su respectivo re-test"*, amablemente solicitamos confirmar, a nivel de la capa de aplicación de los sistemas de información, cuántos sistemas de información corresponden a aplicaciones Web y cuántos a aplicaciones cliente-servidor. Adicionalmente, solicitamos confirmar la cantidad de aplicaciones (sean URLs o cliente-servidor) en cada sistema de información.

RESPUESTA FIDUPREVISORA: Cliente-Servidor solo 1 Aplicación y las demás son WEB.

7. En el apartado *"Una (1) prueba de ethical hacking tipo caja gris a diez (10) sistemas de información con su respectivo re-test"*, amablemente solicitamos confirmar si el Ethical Hacking debe realizarse sobre la(s) aplicación(es) del sistema de información, la infraestructura (servidores) sobre la cual se encuentra la aplicación, o los dos.

RESPUESTA FIDUPREVISORA: Solo la aplicación del sistema de información.

8. En el apartado *"Una (1) prueba de ethical hacking tipo caja negra a diez (10) URL con su respectivo re-test"*, amablemente solicitamos confirmar cuántas URLs son internas y cuántas son externas.

RESPUESTA FIDUPREVISORA: 2 Internas y 8 externas.

9. En el apartado *"Cinco (5) pruebas de análisis dinámico de código para cinco (5) sistemas de información (una por cada uno) con su respectivo re-test",* amablemente solicitamos confirmar si lo que realmente se requiere es un análisis DAST (Dynamic Application Security Testing) para cada uno de los 5 sistemas de información, o un análisis estático de código fuente. En caso de que sea la segunda opción, por favor confirmar la cantidad aproximada de líneas de código y el lenguaje de programación del código correspondiente a cada sistema de información.

RESPUESTA FIDUPREVISORA: Se requiere un análisis Dinámico (DAST)

10. En el apartado *"Cinco (5) pruebas de análisis dinámico de código para cinco (5) sistemas de información (una por cada uno) con su respectivo re-test.", a*mablemente solicitamos confirmar si cada sistema de información se compone de 1 sola IP, o si se compone de varias IPs. En caso de que sea la segunda opción, por favor confirmar la cantidad de IPs por cada sistema de información.

RESPUESTA FIDUPREVISORA: El sistema de información FRL tiene 2 IPs, Peoplesoft tiene 4 IPs, y el resto de sistemas todos cuentan con 1 sola IP.

11. En el apartado *"Cinco (5) pruebas de análisis dinámico de código para cinco (5) sistemas de información (una por cada uno) con su respectivo re-test.",* amablemente solicitamos confirmar, a nivel de la capa de aplicación de los sistemas de información, cuántos sistemas de información corresponden a aplicaciones Web y cuántos a aplicaciones cliente-servidor. Adicionalmente, solicitamos confirmar la cantidad de aplicaciones (sean URLs o cliente-servidor) en cada sistema de información.

RESPUESTA FIDUPREVISORA: Cliente-Servidor solo 1 Aplicación y las demás son WEB.

12. En el numeral 4.4 su literal j ") Cronograma con el plan y alcance de las pruebas de vulnerabilidad, hacking ético, análisis de código e ingeniería social", amablemente solicitamos confirmar cuál es el alcance de las pruebas de ingeniería social solicitadas en el presente punto.

RESPUESTA FIDUPREVISORA: Se requieren pruebas que ayuden a medir el nivel de conciencia en seguridad de la información de los usuarios, estas pueden ser por correo mínimo 1 vez al año.

13. En el apartado *"Suministrar el servidor virtual de propósito específico, instalado en el lugar que Fiduprevisora S.A. disponga, atendiendo a las condiciones previstas en el anexo técnico de la Convocatoria Privada",* amablemente solicitamos confirmar que Fiduprevisora va a proveer la infraestructura de hardware de virtualización para la instalación y configuración (por parte del oferente) del servidor virtual.

RESPUESTA FIDUPREVISORA: Si el proponente ofrece implementar un servidor físico o appliance sobre el cual se prestaría el servicio debe suministrar y gestionar los recursos

tecnológicos que este necesita para su funcionamiento, si el servidor es una máquina virtual este funcionaría bajo la infraestructura que tiene Fiduprevisora contratada como servicio.

14. En los apartados *"e) El proveedor deberá suministrar acceso a cuatro (4) usuarios a la plataforma de monitoreo bajo el rol de consulta al dashboard, reglas, gráficas, tablas y reportes y f) El SIEM debe permitir asignar un rol de consulta para el equipo de seguridad de la información de la entidad con el fin de obtener información sobre los eventos y las alertas de incidentes, sin interrumpir el flujo de trabajo de otros roles. Los datos deberán poder exportarse para su revisión por miembros del equipo sin la necesidad de acceso a la solución",* amablemente solicitamos confirmar el número de usuarios de consulta que debe tener la consola de visualización de eventos del SIEM, debido a que los numerales citados mencionan cantidades diferentes de usuarios

RESPUESTA FIDUPREVISORA: El número de usuarios que requiere tener acceso es de 4.

15. En el apartado *"El SIEM deberá contar con un sistema propio de tickets"*, Amablemente solicitamos que se admita la integración de una herramienta de gestión de incidentes (tickets) de seguridad con el SIEM, con el fin de que permita aprovechar al máximo la utilización de herramientas especializadas como parte del servicio.

RESPUESTA FIDUPREVISORA: Se hace la aclaración de que el sistema de tickets debe ser del proveedor, no se solicita un módulo en el SIEM, este sistema de tickets es para poder realizar el registro y seguimiento de los incidentes de seguridad que reporta el SOC.

16. En el apartado *"Para la remediación de las vulnerabilidades se requiere tener un usuario de Fiduprevisora S.A. que permita analizar en tiempo real si con las modificaciones realizadas (Parcheo, modificación de código, implementación de certificados, entre otros) se remedió la vulnerabilidad detectada, esto con el fin de poder cerrar los controles de cambios oportunamente o realizar rollback si la solución propuesta afecta el desempeño del aplicativo sin remediar la vulnerabilidad.",* Amablemente solicitamos confirmar si este numeral se refiere a la ejecución de un scan de vulnerabilidades posterior a la remediación de una vulnerabilidad en un activo específico, donde el objetivo del scan es validar si la vulnerabilidad en cuestión fue exitosamente remediada o no.

RESPUESTA FIDUPREVISORA: Efectivamente se refiere al scan de vulnerabilidades posterior a la actividad de remediación propuesta y ejecutada.

17. En el apartado *"El interesado debe contar con el Recurso Humano idóneo para la ejecución del contrato, teniendo como mínimo los siguientes roles en disponibilidad 7x24:",* amablemente solicitamos que la disponibilidad 7x24 solo aplique para el perfil de Ingenieros de Operación, debido a que tener un equipo de trabajo en modalidad 5x8 (con excepción de los Ingenieros de Operación) garantiza de todas formas la prestación robusta y adecuada del servicio, sin tener que aumentar los costos del servicio para obtener una disponibilidad de 7x24 para todo el equipo de trabajo.

RESPUESTA FIDUPREVISORA: La disponibilidad del servicio prestado debe brindarse en una modalidad 7x24, sin embargo, se aclara que debe existir una matriz de escalamiento sobre la cual se contactará al nivel más alto solo si los niveles inferiores no pueden brindar solución. ***Se van a revisar los perfiles requeridos para la licitación.***

18. En el apartado 4.6 – Director de Operaciones *"Certificado como Ethical Hacker del EC-Council.",* amablemente solicitamos que se admita, como alternativa a CEH, la certificación CPTE (Mile2), debido a que esta última tiene un contenido curricular y práctico equivalente a CEH, y adicionalmente es también una certificación reconocida en la industria de ciberseguridad.

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

19. En el apartado 4.6 – Director de Operaciones *"Certificado como CHFI",* Entendiendo que el alcance del servicio no contempla actividades relacionadas con ingeniería forense, amablemente solicitamos eliminar el presente requisito o considerar (como alternativa) la certificación CDFE (Mile2), debido a que esta última tiene un contenido curricular y práctico equivalente a CHFI, y adicionalmente es también una certificación reconocida en la industria de ciberseguridad.

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

20. En el apartado 4.6 – Director de Operaciones "*Certificado como CISSP",* amablemente solicitamos que, para el presente perfil, se considere CISSP como opcional y CISM como obligatoria, debido a que el perfil está enfocado en la gestión y gobierno de las operaciones asociadas al servicio, haciendo que CISM sea la certificación idónea para el perfil.

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

21. En el apartado 4.6 – Coordinador SOC *"Certificado como auditor líder ISO 27001:2013 "*, amablemente solicitamos que se admita, como alternativa a Auditor Líder ISO 27001:2015, la certificación Implementador Líder 27001:2015, debido a que esta última contiene un componente técnico y práctico que es más relevante para el servicio a contratar. Adicionalmente, el servicio no contempla labores de auditoría del sistema de gestión de seguridad de la información. Todo lo anterior garantiza la pluralidad de proponentes y no afecta la prestación del servicio.

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

22. En el apartado 4.6 – Coordinador SOC *"Certificado como Ethical Hacker del EC-Council*", amablemente solicitamos que se admita, como alternativa a CEH, la certificación CIHE (Mile2), debido a que esta última está enfocada en la gestión de incidentes de seguridad y por lo tanto brinda conocimientos y habilidades que son más relevantes para el perfil en cuestión. Lo anterior garantiza la pluralidad de proponentes y no afecta la prestación del servicio.

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

23. En el apartado 4.6 – Director de Operaciones "*Certificado como CISSP",* amablemente solicitamos que se admita, como alternativa a CISSP, una Maestría en Seguridad de la Información, Seguridad Informática, Arquitectura de Tecnología o carreras afines, debido a que uno de los Posgrados brinda conocimientos y habilidades equivalentes a los de la certificación CISSP. Lo anterior garantiza la pluralidad de proponentes y no afecta la prestación del servicio.

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
15	09/01/2020	Correo Electrónico	**A3SEC**

1. Sería posible suministrar un estimado de la cantidad de líneas de código que puede tener cada aplicación, esta información es necesaria para el dimensionamiento de este servicio.

RESPUESTA FIDUPREVISORA: La cantidad de líneas de código no son necesarias dado que el análisis solicitado es dinámico (DAST).

2. ¿Sería posible suministrar un estimado del número de proyectos que pueden salir durante un año y que requieran de estos servicios?

RESPUESTA FIDUPREVISORA: En promedio son 2 proyectos por año.

3. ¿Es válido para el cliente que se suministre una OVA, creada directamente por el fabricante para que sea instalada en el sistema de virtualización que el cliente maneja?

RESPUESTA FIDUPREVISORA: Si es válido.

4. Los sistemas operativos Saloris 10, Windows Xp, Windows 2008, Win 7, Win 2003, no cuentan con soporte por parte del fabricante por lo que es común que los agentes de integración a las soluciones SIEM no cuenten con soporte a estos sistemas operativos. ¿Es válido para el cliente si se utilizan herramientas externas a la solución para la colección de eventos?

RESPUESTA FIDUPREVISORA: Si es válido, siempre que se cubran todos los elementos solicitados y que los informes, notificaciones y seguimiento se puedan realizar como uno solo.

5. En el requerimiento se especifica que debe ser un servidor de propósito específico y luego se solicita una máquina virtual. ¿El cliente espera que se entregue un servidor con el escáner de vulnerabilidades o es válido para el cliente que se suministre solo la máquina virtual para que sea instalada en su sistema de virtualización?

RESPUESTA FIDUPREVISORA: Si el proponente ofrece implementar un servidor físico o appliance sobre el cual se prestaría el servicio debe suministrar y gestionar los recursos

tecnológicos que este necesita para su funcionamiento, si el servidor es una máquina virtual este funcionaría bajo la infraestructura que tiene Fiduprevisora contratada como servicio.

6. ¿Dentro del alcance de las acciones de remediación, el cliente espera que el proveedor ejecute las configuraciones directamente sobre los sistemas o espera el acompañamiento con el administrador de la infraestructura para que sean ejecutadas en conjunto?

RESPUESTA FIDUPREVISORA: Es deber del proveedor identificar las vulnerabilidades, generar el plan de acción para remediarlas y realizar las actividades de remediación en acompañamiento del personal de TI de Fiduprevisora, se debe garantizar la segregación de funciones (evitando un Conflicto de intereses) entre el análisis de vulnerabilidades y la remediación.

7. Dentro del alcance de las acciones de remediación, ¿el cliente espera que el proveedor ejecute las configuraciones directamente sobre los sistemas o espera el acompañamiento con el administrador de la infraestructura para que sean ejecutadas en conjunto?

RESPUESTA FIDUPREVISORA: Es deber del proveedor identificar las vulnerabilidades, generar el plan de acción para remediarlas y realizar las actividades de remediación en acompañamiento del personal de TI de Fiduprevisora, se debe garantizar la segregación de funciones (evitando un Conflicto de intereses) entre el análisis de vulnerabilidades y la remediación.

8. ¿Cuantos usuarios necesitan tener acceso a la información de vulnerabilidades directamente sobre la plataforma?

RESPUESTA FIDUPREVISORA: Se requiere tener acceso para 4 usuarios.

9. ¿Es válido para el cliente que la arquitectura de la solución SIEM esté basada en infraestructura en la nube?

RESPUESTA FIDUPREVISORA: Si es válido hacer esta propuesta, sin embargo, se debe detallar el custodio, responsabilidad y almacenamiento de la información, así como el empalme, la devolución y/o eliminación de la misma cuando el contrato finalice.

10. Este usuario está incluido en los solicitados en el numeral 4.5-e o es un usuario adicional?

RESPUESTA FIDUPREVISORA: No se entiende la pregunta.

11. ¿Cuenta el cliente actualmente con una solución que pueda monitorear el tráfico de red tipo (IDS, IPS) o espera que se incluya dentro de la propuesta de servicio?

RESPUESTA FIDUPREVISORA: El Firewall tiene módulo de IPS, sin embargo, **no se requiere de este servicio adicional.**

12. ¿Es válido para el cliente si se realiza una transferencia de conocimiento sobre la implementación realizada o es indispensable contar con el certificado por parte del fabricante?

RESPUESTA FIDUPREVISORA: Si el punto se refiere a la capacitación sobre el personal de seguridad de la información de Fiduprevisora, se requiere una transferencia de conocimiento de lo implementado más una capacitación de las bondades y funcionamiento de la herramienta, no se requiere certificado de fábrica, el certificado que se solicita debe ser emitido por el proveedor indicando que se brindó la capacitación.

13. Las tareas de contención en un incidente de seguridad suelen ser ejecutadas por el administrador de la infraestructura, estas tareas suelen generar una carga operativa importante dentro del proceso de atención de incidentes, actualmente los SOCs inteligentes cuentan con soluciones tipo SOAR (Security Orchestration, Automation and Response) que permiten automatizar este tipo de tareas de contención integrándose con los controles de seguridad del cliente. ¿Cuenta actualmente el cliente con este tipo de solución o desea que se incluya dentro de la propuesta de servicios?

RESPUESTA FIDUPREVISORA: Aunque no se está solicitando, se puede cotizar como valor agregado o punto aparte de manera que se pueda segregar para una evaluación o comparación más equitativa.

14. ¿El cliente está solicitando que el director de operaciones cuente con todas las certificaciones mencionadas o con una de ellas?

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

15. ¿El cliente está solicitando que el Coordinador SOC cuente con todas las certificaciones mencionadas o con una de ellas?

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
6	09/01/2020	Correo Electrónico	**BSECURE**

1. En el numeral ***3. ALCANCE*** en el literal E. *"Cinco (5) pruebas de análisis dinámico de código para cinco (5) sistemas de información (una por cada uno) con su respectivo re-test",* agradecemos nos indiquen con cuantas líneas de código cuenta cada una de las aplicaciones.

RESPUESTA FIDUPREVISORA: La cantidad de líneas de código no son necesarias dado que el análisis solicitado es dinámico (DAST).

2. En el numeral ***4. CONDICIONES DEL SERVICIO REQUERIDO*** *"actualmente la entidad cuenta con los siguientes servidores los cuales deben ser monitoreados por el correlacionador de eventos",* agradecemos nos proporcionen la cantidad total de activos que monitorean en la actualidad y que incluyen servidores, dispositivos de red, dispositivos de seguridad y/o equipos de escritorio, etc.

RESPUESTA FIDUPREVISORA: Es un total de 130 Servidores, 1200 equipos de usuario final, 80 equipos de comunicaciones y un porcentaje para crecimiento de la infraestructura.

3. En el numeral ***4.2.1 Servicio de monitoreo*** y correlación de eventos de seguridad *"El servicio de monitoreo y correlación de eventos debe monitorear todos los eventos recolectados a través del SIEM - Security Information and Event Management y brindar respuesta a incidentes de seguridad de la información en modalidad 7x24 durante la vigencia a cotizar, con una capacidad máxima de mil quinientos (1.500) dispositivos: servidores, dispositivos de red, dispositivos de seguridad y/o equipos de escritorio, etc."* , agradecemos nos puedan informar la cantidad de Mensajes por Segundo (MPS) que actualmente está monitoreando la organización.

   RESPUESTA FIDUPREVISORA: Se estaban monitoreando capacidad de hasta 1500 MPS, se reciben ofertas de valores superiores de MPS que considere el proveedor de acuerdo a la infraestructura relacionada en la invitación.

4. En el numeral 4.3.1 **Herramienta de Apoyo** *"A lo largo de la duración definida del servicio, la empresa oferente deberá contar con un servidor de propósito específico instalado en el sitio, que permita correlacionar eventos y que sea especializado en la realización de Análisis de Vulnerabilidades y que cumpla con las siguientes características",* Las tecnologías de análisis de vulnerabilidades no permiten correlacionar eventos. Solicitamos eliminar este requerimiento.

   RESPUESTA FIDUPREVISORA: Se requiere el servicio de SIEM, SOC y análisis de vulnerabilidades, debe ser con 1 solo appliance físico, pero virtualizado los diferentes softwares dentro de este, o pueden ser varias máquinas virtuales para implementar en la IaaS que tiene contratada Fiduprevisora.

5. En el numeral 4.5 Obligaciones:

   a) "Suministrar el servidor virtual de propósito específico, instalado en el lugar que Fiduprevisora S.A. disponga, atendiendo a las condiciones previstas en el anexo técnico de la Convocatoria Privada.
   b) Llevar a cabo lo correspondiente a la instalación configuración, parametrización y administración del servidor dispuesto para la ejecución del servicio.
   c) Garantizar el debido licenciamiento y operatividad de la herramienta para SIEM y análisis de vulnerabilidades."

   Agradecemos indicar si es posible ofrecer servicios 100% de nube.

   RESPUESTA FIDUPREVISORA: Si es válido hacer esta propuesta, sin embargo, se debe detallar el custodio, responsabilidad y almacenamiento de la información, así como el empalme, la devolución y/o eliminación de la misma cuando el contrato finalice.

6. En el numeral ***4.6.Equipo de trabajo*** "El interesado debe contar con el Recurso Humano idóneo para la ejecución, teniendo como mínimo los siguientes roles en disponibilidad 7x24:".

En función de garantizar la pluralidad de los oferentes, se solicita amablemente modificar el requerimiento de la siguiente manera:

GERENTE DE PROYECTOS - CERTIFICACIONES:
Certificado en PMP vigente o certificado como auditor líder ISO:
27001:2013 o Services supplement for CMMI o Estudios comprobables en gerencia de proyectos.

DIRECTOR DE OPERACIONES - CERTIFICACIONES:
Certificado como auditor líder ISO 27001:2013 o Certificado como Ethical Hacker del EC-Council o Certificado como CHFI o Certificado como CISSP o Certificado como CISM.

COORDINADOR DE SOC - CERTIFICACIONES:
Certificado como auditor líder ISO 27001:2013 o Certificado como Ethical Hacker del EC-Council o Certificado como CISSP o Certificado como CISM.

ANALISTAS JUNIOR DE SEGURIDAD - CERTIFICACIONES:
Certificado como Ethical Hacker del EC-Council o Certificado como CISM o CDFE Certified Digital Forensics Examiner.

INGENIEROS DE OPERACIONES - EXPERIENCIA:
Experiencia de un (1) año en proyectos relacionados con Centros de Operaciones de Seguridad - SOC. Dedicación Tiempo completo Soporte 7x24, con operación remota.

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

N° DE OBSERVACIONES	FECHA DE RECIBO	MEDIO DE RECIBO	OBSERVANTE
10	09/01/2020	Correo Electrónico	**PWC**

1. La presente invitación a cotizar se entenderá como estudio de mercado o como una propuesta vinculante.

   RESPUESTA FIDUPREVISORA: La presente invitación a cotizar es el documento con el cual se invita a cotizar para la elaboración del estudio de mercado. En consecuencia, tanto la presente invitación a cotizar como la cotización que lleguen a remitir los oferentes interesados no constituyen una oferta comercial.

2. Para el ítem 1.8. Experiencia Específica, es necesario que el servicio ya haya finalizado o podrán relacionarse contratos en ejecución.

   RESPUESTA FIDUPREVISORA: Todas las experiencias son, bienvenidas, sin embargo, entre más reciente la experiencia mejor, por ello también se pueden incluir experiencias de contratos en

ejecución. Deben revisar que el objeto de las experiencias que remitan contemplen el objeto de la presente invitación a cotizar, según lo indicado en el ítem 1.7 Experiencia Específica.

3. Dentro del ítem 3 e) relacionado con el alcance del servicio a contratar, están requiriendo Cinco (5) pruebas de análisis dinámico de código para cinco (5) sistemas de información (una por cada uno) con su respectivo re-test, para ello es pertinente conocer cuántas líneas de código tiene cada sistema de información y el lenguaje sobre el cual está desarrollado cada uno de éstos (por ejemplo: Java, Javascript, Python, etc.)

RESPUESTA FIDUPREVISORA: Se tienen aplicaciones en JAVA, PeopleSoft (ORACLE). La cantidad de líneas de código no son necesarias dado que el análisis solicitado es dinámico (DAST).

4. La entidad cuenta con un modelo o procedimiento implementado para la gestión de incidentes de seguridad.

RESPUESTA FIDUPREVISORA: Sí, la entidad cuenta con un procedimiento para la gestión de incidentes.

5. En el ítem 4.4 j) Entregables se menciona como entregable: Cronograma con el plan y alcance de las pruebas de vulnerabilidad, hacking ético, análisis de código e ingeniería social, sin embargo, en el Alcance no se hace mención de pruebas de ingeniería social.

RESPUESTA FIDUPREVISORA: Se requieren pruebas que ayuden a medir el nivel de conciencia en seguridad de la información de los usuarios, estas pueden ser por correo mínimo 1 vez al año.

6. En el ítem 4.5 a) se menciona un anexo técnico, sin embargo, dicho anexo no está relacionado dentro del documento.

RESPUESTA FIDUPREVISORA: No se tiene para el presente ejercicio un anexo con condiciones técnicas, dado que la mayoría de servicios suelen brindar servidores virtuales o en nube, sin embargo, se aceptarán propuestas con servidores físicos.

7. En el ítem 4.5.1 l) Obligaciones Específicas - SIEM se solicita un entrenamiento certificable para cuatro (4) personas, ¿dicho entrenamiento debe ser certificado directamente por el fabricante?

RESPUESTA FIDUPREVISORA: No necesariamente, se requiere certificado del proveedor de la capacitación impartida.

8. Respecto al equipo de trabajo, no todos los roles del equipo de trabajo requieren tener disponibilidad de 7x24 dada las funciones inherentes al rol, por ejemplo: Gerente de proyecto, Director de Operaciones.

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

9. ¿Las certificaciones solicitadas para los roles Director de Operaciones y Coordinador de SOC se requieren todas las certificaciones relacionadas o al menos una (1) de estas?

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

10. Para el rol de analista junior de seguridad SOC podría considerarse Técnicos o Tecnólogos en electrónica, sistemas o afines y certificación en herramientas o soluciones SIEM como obligatoria y el CEH opcional, toda vez que para este rol tienen mayor relevancia conocimientos en este tipo de soluciones.

RESPUESTA FIDUPREVISORA: ***Se van a revisar los perfiles requeridos para la licitación.***

Atentamente,

Fiduprevisora S.A

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