INVITACIÓN A COTIZAR No. 001 DE 2020

Objeto:
Fiduprevisora S.A. a través de la Gerencia de Riesgos está interesada en contratar 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.

Apertura de la Invitación: enero 3 de 2020

Fecha límite para presentar observaciones: enero 9 de 2020

Audiencia de exposición del proyecto y respuesta a observaciones: enero 13 de 2020 a las 10:00 horas Calle 72 No. 10-03 Piso 5 Salas Auxiliares

Recepción de Cotizaciones: enero 17 de 2020 hasta las 17:00 horas a través del correo electrónico intdemercados@fiduprevisora.com.co

Área Responsable: Gerencia de Riesgos

Contacto: intdemercados@fiduprevisora.com.co

1. INFORMACIÓN GENERAL

Fiduprevisora S.A. aclara que la presente invitación a cotizar en ningún caso podrá considerarse oferta para celebrar contrato; por lo tanto, no podrá deducirse relación contractual alguna. Así las cosas, se precisa 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. También, se realizarán las gestiones pertinentes si alguna de las cotizaciones allegadas cumple con las expectativas de la entidad, la cual debe satisfacer las necesidades conforme a los requerimientos descritos en el documento respectivo o si se requiere, se reestructura la solicitud de acuerdo con el presupuesto definido o en el evento en el cual las entidades consultadas no cumplieren con los requisitos para la prestación integral de los servicios solicitados.

1.1. Régimen Jurídico

La presente invitación a cotizar, se encuentra sujeta a las normas del derecho privado y al Manual de Contratación de Bienes y Servicios de Fiduprevisora S.A., de acuerdo con lo establecido en el Artículo 15 de Ley 1150 de 2007. Así mismo, se aplicarán los principios de la función administrativa y de la gestión fiscal de que tratan los artículos 209 y 267 de la Constitución Política.

1.2. Confidencialidad de la Información

Los interesados se obligan con Fiduprevisora S.A., a manejar y utilizar de manera confidencial cualquier información que le sea entregada o a la que tenga acceso con ocasión del presente proceso, garantizando por todos los medios a su alcance que los empleados a su servicio y demás personas autorizadas respetarán la obligación de guardar secreto y confidencialidad sobre cualquier información recibida u obtenida.

1.3. Protección de datos personales

Los interesados en desarrollo de las actividades previas, de ejecución, terminación y conexas a esta invitación a cotizar; reconocen y autorizan que podrán realizarse tratamiento de datos personales en los términos de la ley 1581 de 2012, su Decreto reglamentario 1377 de 2013 y demás normas que las adicionen, aclaren o modifiquen, y además bajo la completa observancia de lo preceptuado en la Política de Protección de Datos Personales, manuales y procedimientos internos establecidos por FIDUPREVISORA S.A.

Así mismo, los proveedores interesados declaran que para efectos de trámites relativos a consultas o reclamos relacionados con datos personales, tienen habilitado el correo electrónico: protecciondedatos@fiduprevisora.com.co

1.4. Criterios Ambientales

El proveedor deberá cumplir con la normatividad ambiental vigente que le aplique y aportar la documentación pertinente que solicite la entidad; además, deberá ceñirse a las políticas y lineamientos del Sistema de Gestión Ambiental de la entidad, cuando sea aplicable al servicio a contratar, el cual podrá ser consultado a través de la página web www.fiduprevisora.com.co, en el link que se relaciona a continuación:

http://www.fiduprevisora.com.co/documents/Contratacion%20en%20linea/Protocolo%20de%20buenas%20practicas%20(1).pdf

1.5. Forma de presentación de la Cotización

Los interesados deben presentar sus ofertas por medio de correo electrónico, en idioma español, dentro de las fechas establecidas para cada etapa del proceso relacionadas en el cronograma y acompañadas de los documentos solicitados.

1.6. Documentos de carácter jurídico y financiero

Las respectivas cotizaciones deberán estar acompañadas de los documentos que se relacionan a continuación, con el fin de realizar un análisis de tipo jurídico y financiero de cada interesado; veamos:

- **I.** Certificado de Existencia y Representación Legal con fecha de expedición no mayor a 30 días
- **II.** Registro Único Tributario - RUT
- **III.** Estados Financieros con corte a diciembre de 2018

1.7. Condiciones de la Invitación

Las cotizaciones se recibirán a más tardar el día viernes 17 de enero de 2020 hasta las 17:00 horas, a través del correo electrónico intdemercados@fiduprevisora.com.co .

1.8. Experiencia Específica

El interesado debe relacionar experiencia de ejecución de contratos cuyo objeto contemple las actividades citadas en el objeto de esta invitación.

No	EMPRESA O ENTIDAD CONTRATANTE	OBJETO	FECHA INICIO	FECHA FIN	VALOR TOTAL EJECUTADO EN SMMLV INCLUIDO IVA
1					
2					
3					

2. OBJETO

Fiduprevisora S.A. a través de la Gerencia de Riesgos está interesada en contratar 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.

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.

b. Una (1) prueba de vulnerabilidades para 1200 IP (Endpoints) con su respectivo re-test.
c. Una (1) prueba de ethical hacking tipo caja gris a diez (10) sistemas de información con su respectivo re-test.
d. Una (1) prueba de ethical hacking tipo caja negra a diez (10) URL con su respectivo re-test
e. Cinco (5) pruebas de análisis dinámico de código para cinco (5) sistemas de información (una por cada uno) con su respectivo re-test.
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.
g. Ofrecer una bolsa de horas y plan de trabajo para la remediación de las vulnerabilidades encontradas.

4. CONDICIONES DEL SERVICIO REQUERIDO

4.1 Generalidades

1. El interesado debe contar con domicilio o sucursal en Colombia.
2. El interesado debe contar con la Certificación ISO 27001 vigente.
3. El interesado debe tener la calidad de partner de la herramienta de correlación de eventos, para ello, deberá suministrar la certificación donde conste su calidad de partner de la herramienta de correlación que implemente para la prestación de servicio.
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.
5. El servicio de SOC debe ser ofrecido en modalidad 7x24 durante toda la vigencia a cotizar.
6. El oferente deberá suministrar los tiempos de respuesta empleados para dar el reporte y respuesta a los incidentes de seguridad detectados.
7. Deberá contar con el Recurso Humano idóneo para la ejecución del servicio.
8. 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

4.2 Actividades SOC

El servicio de monitoreo de los eventos de seguridad, se requiere para acompañar a la organización en cada una de las fases del proceso de la siguiente manera:

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.

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.

Como parte de la operación se realizarán afinamientos periódicos a las reglas de correlación con base en el análisis de la información, los falsos positivos identificados y sobre la evolución de la organización, la infraestructura y las amenazas tecnológicas.

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.

Cuando se produce un incidente de seguridad se debe generar una alerta informando al equipo de Seguridad de la Información el incidente detectado y el método de respuesta para atenderlo.

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.

4.3 Actividades Vulnerabilidades

El servicio de apoyo en la gestión de vulnerabilidades ofrecido y diseñado se requiere para acompañar a la organización en cada una de las fases del proceso de la siguiente manera:

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:

a) Instalación y configuración de un servidor virtual con la solución, en las instalaciones definidas por Fiduprevisora S.A., administrado y soportado por el proveedor.
b) Estar homologado por el CVE - Common Vulnerabilities and Exposures.
c) Hacer uso del CVSS - Common Vulnerability Scoring System para clasificar las vulnerabilidades.
d) Permitir generar reportes diferenciales de vulnerabilidades, acumulativos, por fecha de escaneos, assets, exclusiones, etc.
e) Identificar vulnerabilidades de acuerdo a los códigos CVE.
f) Actualización periódica de la definición de nuevas vulnerabilidades.

4.3.2 Escaneo de Vulnerabilidades

El proveedor será el responsable de parametrizar la herramienta para ejecutar los escaneos de vulnerabilidades necesarios. Dentro de esta parametrización se tendrán en cuenta aspectos como:

a) Periodicidad de los escaneos.
b) Uso de ancho de banda adecuado dependiendo de la ubicación y criticidad de los activos.
c) Horarios y duración de los escaneos, teniendo en cuenta las necesidades de la operación de la entidad.
d) Personalización de plantillas de informes de acuerdo a las necesidades del negocio.
e) Permitir generar reportes diferenciales de vulnerabilidades, acumulativos por fecha de escaneos, activos, exclusiones, entre otros.

De acuerdo a la programación de escaneos, el proveedor se encargará de verificar la correcta ejecución de los mismos, los tiempos empleados en cada escaneo y que se hayan analizado efectivamente los activos configurados. Esto permitirá la re-parametrización o la realización de cambios en los escaneos programados, en busca del afinamiento más acorde para el servicio.

4.3.3 Generación de reportes por parte del proveedor.

Se generará informes técnicos y ejecutivos por cada test y re-test ejecutado de acuerdo a la periodicidad establecida, con el fin de detectar de manera oportuna:

a) Nuevas vulnerabilidades informáticas presentes en la infraestructura de la organización.
b) Informe del plan sugerido de remediación de las vulnerabilidades reportadas.
c) Aparición de nuevos activos informáticos sobre las redes de datos de la organización.

Se deberá enviar reporte de alertas tempranas respecto a nuevas vulnerabilidades que puedan llegar a afectar la infraestructura de Fiduprevisora S.A.

4.3.4 Acompañamiento en la remediación y verificación por el proveedor

De acuerdo a las vulnerabilidades encontradas y a la criticidad de las mismas, el proveedor generará dentro de los reportes técnicos y ejecutivos un plan de remediación sugerido para que la organización revise y apruebe conforme a sus políticas y procesos con el fin de remediar de manera efectiva y eficiente las vulnerabilidades encontradas.

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.

Adicionalmente, se realizará seguimiento a los niveles de remediación logrados y se reportará en el informe trimestral de estado de la remediación de las vulnerabilidades.

4.4 Entregables

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:

a) Fecha y hora en la que se descubrió el incidente
b) Tipo de incidente
c) Prioridad de tratamiento
d) IP origen
e) IP afectada
f) Detalle del incidente
g) Acciones ejecutadas de detección y contención de ataques
h) Recomendaciones de remediación

En cuanto al servicio de análisis de vulnerabilidades, el proveedor debe entregar:

i) Informe de la instalación, configuración y prueba de operación de la plataforma
j) Cronograma con el plan y alcance de las pruebas de vulnerabilidad, hacking ético, análisis de código e ingeniería social.
k) Por cada prueba y re-test que se realice se deberá entregar: informe anexo técnico, informe ejecutivo y plan de remediación sugerido.

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.
d) La plataforma deberá tener una consola del tipo dashboard en la cual se pueda personalizar varios tipos de gráficas, tablas y reportes, para permitir tener una visión global de los eventos, incidentes de seguridad y reglas implementadas en la herramienta.
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.
f) Cumplir con las condiciones adicionales con las cuales se haya comprometido.
g) Realizar el pago oportuno de salarios y prestaciones sociales al personal designado para la ejecución del contrato.
h) Atender oportunamente los requerimientos de Fiduprevisora S.A., en lo que tiene que ver con las actividades que emanan de la ejecución del contrato. Conforme a lo anterior el contratista designará un interlocutor el cual servirá como canal de comunicación con la entidad.

4.5.1 Obligaciones Específicas - SIEM

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.
b) El SIEM debe proporcionar una arquitectura escalable donde la capacidad de procesamiento, memoria y almacenamiento se puede aumentar o disminuir de acuerdo con la carga real en la producción.
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.
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.
e) El SIEM debe almacenar datos relacionados con los incidentes y eventos, incluido el comportamiento de los usuarios y activos asociados durante el período de vigencia del contrato en forma de búsqueda para un estándar de 90 día y custodia durante 12 meses.
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.
g) El SIEM deberá proporcionar información en tiempo real de los eventos generados por los dispositivos de seguridad administrada, así como de las alarmas que permitan identificar los eventos relevantes y que puedan afectar la integridad, confidencialidad o disponibilidad de los servicios protegidos de Fiduprevisora S.A.
h) El SIEM debe proteger la integridad y confidencialidad de la información almacenada con algoritmos de hashing fuertes mínimo SHA 256.
i) El SIEM deberá permitir el afinamiento periódico a las reglas de correlación con base en el análisis de información, los falsos positivos identificados y sobre la evolución de la

organización, la infraestructura y las amenazas tecnológicas, sin generar sobrecostos en el contrato.

j) El SIEM deberá contar con un sistema propio de tickets.
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.
l) 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.
m) El SIEM deberá tomar los datos del evento incluyendo las marcas de tiempo y poder correlacionar esto a través de todo el análisis.
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.
o) El equipo del SOC - servicio de Centro de Operaciones de Seguridad o el especialista encargado deberá realizar las labores correspondientes a la instalación, configuración, parametrización y administración del SIEM dispuesto para la ejecución del servicio que debe incluir la creación de los conectores necesarios para un correcto monitoreo/correlación de las plataformas que se requieran.
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.
q) El equipo del SOC deberá brindar respuesta a incidentes de seguridad de la información 7x24 durante la vigencia del contrato incluyendo como mínimo las tareas de prevención, detección y contención de ataques, y los tiempos de nivel de servicio para la atención de estos de acuerdo al nivel de criticidad.
r) Dentro del servicio provisto por el SOC se deberán detectar acciones tales como:
    - **i.** Credenciales comprometidas.
    - **ii.** Movimiento lateral.
    - **iii.** Ataques tipo “Pass the Hash”.
    - **iv.** Escalamiento de privilegios.
    - **v.** Anomalías en el ingreso a los sistemas.
    - **vi.** Visibilidad de la red interna, nube y direcciones IP asociadas a un incidente.
    - **vii.** Eliminación anómala de logs.
    - **viii.** Malware.

4.5.2 Obligaciones Específicas – Vulnerabilidades

Por cada año de servicio a cotizar, el proveedor deberá:

a) Verificar la correcta ejecución de los escaneos y llevar a cabo los ajustes necesarios, con el fin de contar con información confiable y actualizada.

b) Ejecutar una (1) prueba de vulnerabilidades para 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.
c) Ejecutar una (1) prueba de vulnerabilidades para 1200 IP (Endpoints) con su respectivo retest.
d) Ejecutar una (1) prueba de ethical hacking tipo caja gris a diez (10) sistemas de información con su respectivo re-test.
e) Ejecutar una (1) prueba de ethical hacking tipo caja negra a diez (10) URL con su respectivo re-test.
f) Ejecutar cinco (5) pruebas de análisis dinámico de código para cinco (5) sistemas de información (una por cada uno) con su respectivo re-test.
g) 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.
h) Ofrecer una bolsa de horas y plan de trabajo para la remediación de las vulnerabilidades encontradas.
i) Generar informes técnicos y ejecutivos conforme las especificaciones requeridas por Fiduprevisora S.A.
j) Generar el plan de remediación sugerido, en lo que corresponde a las vulnerabilidades reportadas y hacer seguimiento a los niveles de remediación logrados.
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.
l) En el momento de realizar el re-test sobre los servidores, URLs, páginas WEB y demás, se debe resaltar qué vulnerabilidades del análisis anterior fueron solucionadas y cuales quedan pendientes, así mismo como identificar y reportar las nuevas vulnerabilidades a las que se esté expuesto que hayan sido identificadas en el lapso de tiempo entre el test y el re-test.
m) Garantizar la operatividad del software dispuesto para la ejecución de las pruebas contempladas en el contrato.

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:

RECURSO HUMANO MINIMO REQUERIDO			
Rol	**Formación profesional**	**Experiencia**	**Certificaciones**
Gerente de Proyecto	Profesional universitario en ingeniería electrónica o ingeniería de sistemas o telecomunicaciones, con maestría o especialización en seguridad de la información o informática o carreras afines.	Experiencia mínima específica de tres (3) años certificada en gerencia de proyectos de tecnología y/o Seguridad Informática.	• Certificado en PMP vigente. • Certificado como auditor líder ISO: 27001:2013 (opcional)
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.	• Certificado como auditor líder ISO 27001:2013. • Certificado como Ethical Hacker del EC-Council. • Certificado como CHFI. • Certificado como CISSP. • Certificado como CISM (opcional)
Coordinador de SOC	Profesional universitario en ingeniería electrónica o ingeniería de sistemas o ingeniería de telecomunicaciones	Experiencia mínima de cinco (5) años experiencia certificada en proyectos relacionados con seguridad de la información	• Certificado como auditor líder ISO 27001:2013. • Certificado como Ethical Hacker del EC-Council • Certificado como CISSP
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. • Certificado como CISM (opcional)

RECURSO HUMANO MINIMO REQUERIDO			
Rol	**Formación profesional**	**Experiencia**	**Certificaciones**
Cuatro (4) Ingenieros de Operación	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.	N/A.
Especialista en pruebas de vulnerabilidad	Profesional universitario en ingeniería electrónica o ingeniería de sistemas o ingeniería de telecomunicaciones	Experiencia mínima de cinco (5) años experiencia certificada en proyectos relacionados con seguridad de la información	Certificado como Ethical Hacker del EC-Council (Vigente) o Licensed Penetration Tester de EC-Council
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) Licensed Penetration Tester de EC-Council

5. Duración

La duración establecida para la prestación del servicio es de veinticuatro (24) meses.

El licenciamiento de la herramienta SIEM debe iniciar desde la implementación y funcionamiento correcto y evidenciable a satisfacción del cliente

6. Forma de pago

Fiduprevisora S.A. bajo ninguna circunstancia realizará anticipos o pagos anticipados, el pago del valor estimado del servicio se hará en veinticuatro (24) cuotas iguales mensuales vencidas, por cada año de servicio o en forma proporcional al servicio prestado, bajo la modalidad de mes vencido.

> ***Nota:*** *FIDUPREVISORA S.A., conforme a su portafolio de servicios financieros, lo invita a invertir en un Fondo de Inversión Colectiva administrado por ésta, con el fin de que los pagos derivados del eventual contrato, sean generados a través de dicho medio. Para lo anterior, podrá solicitar información al correo electrónico mcotes@FIDUPREVISORA.com.co.*

7. OFERTA ECONÓMICA

El valor total de la propuesta debe estar en pesos colombianos, debe incluir forma de pago, IVA y demás impuestos a los que haya lugar.

	24 meses
Oferta Económica	**Pesos $ M/cte.**
Total IVA	
Total	

Para Fiduprevisora S.A., es importante contar con su oferta teniendo en cuenta su experiencia y reconocimiento en el mercado; con el fin de conocer las mejores prácticas que se están llevando a cabo, para así establecer condiciones equitativas y factores objetivos de selección.

Agradecemos su participación.

Elaboró: Daniel León Lovera – Profesional Seguridad de la información
Aprobó: David Jaimes Builes – Gerente de Riesgos