INVITACIÓN A COTIZAR No. 002 DE 2020

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

Prestar los servicios especializados de análisis de vulnerabilidades y pruebas de hacking ético sobre la infraestructura tecnológica de Fiduprevisora, atendiendo las obligaciones relacionadas con la Circular Externa 042 de 2012 de la Superintendencia Financiera de Colombia.

Apertura de la Invitación: 7 de enero de 2021

Fecha límite para presentar observaciones: 14 de enero de 2021

Respuesta a Observaciones: 27 de enero de 2021

Recepción de Cotizaciones: 1 de febrero de 2021 hasta las 17:00 horas a través del correo electrónico intdemercados@fiduprevisora.com.co

Área Responsable: Vicepresidencia de Tecnología de la Información, Vicepresidencia de Transformación y Arquitectura Organizacional y la Gerencia de Riesgos

Contacto: intdemercados@fiduprevisora.com.co

1. INFORMACIÓN GENERAL

FIDUPREVISORA S.A., informa que la presente solicitud de cotización no se puede considerar como una oferta para celebrar contrato; por lo tanto, no podrá deducirse relación contractual alguna.

En consecuencia, la finalidad de la presente solicitud es analizar las condiciones del mercado correspondiente, la viabilidad de la contratación mediante la medición de variables como la oportunidad, la calidad, el costo, etc. De acuerdo con lo anterior, el presente documento no corresponde al inicio de un proceso de contratación de invitación pública o cerrada en los términos del Manual de Contratación de la Fiduciaria.

1.1. Régimen Jurídico

La presente solicitud de cotización, se realiza conforme con lo establecido en el Artículo 15 de Ley 1150 de 2007. Por otro lado, está sujeta a las normas del derecho privado, y al Manual de Contratación de Bienes y Servicios de Fiduprevisora S.A. Sin perjuicio de lo anterior, y en cumplimiento de lo señalado en la Ley, Fiduprevisora S.A., aplicará para los temas contractuales 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 solicitud de cotización; 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 Fiduciaria; además, deberá ceñirse a las políticas y lineamientos del Sistema de Gestión Ambiental de la Entidad, cuando sea aplicable al servicio a cotizar, el cual podrá ser consultado a través de la página web www.fiduprevisora.com.co, en el link que se relaciona a continuación:

https://www.fiduprevisora.com.co/wp-content/uploads/2019/12/Protocolo-de-buenas-practicas-1.pdf

1.5. Forma de presentación de la Cotización

Los interesados deben presentar sus cotizaciones 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 2019

1.7. Condiciones de la Cotización

Las cotizaciones se recibirán a más tardar el día lunes 1 de febrero de 2021 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. En caso, de que el (los) interesado(s) tenga(n) experiencia con entidades del sector financiero, favor relacionarlas de forma adicional.

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

2. OBJETO

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

Prestar los servicios especializados de análisis de vulnerabilidades y pruebas de hacking ético sobre la infraestructura tecnológica de Fiduprevisora, atendiendo las obligaciones relacionadas con la Circular Externa 042 de 2012 de la Superintendencia Financiera de Colombia.

3. ALCANCE

El servicio de monitoreo y correlación de eventos de la infraestructura tecnológica de la Entidad incluye el monitoreo de la plataforma de servidores alojados en los diferentes Datacenter de la entidad como también las nubes públicas y privadas, aplicaciones, bases de datos, plataforma de correo electrónico, seguridad informática y de la información, Redes LAN, WLAN y WAN y servicios conexos.

El servicio de Gestión apoyo y colaboración en la infraestructura tecnológica de la Entidad comprende las acciones de soporte en sus diferentes niveles del servicio requeridos por la Vicepresidencia de Tecnología de la Información.

4. CONDICIONES DEL SERVICIO REQUERIDO

4.1 Generalidades

- El interesado debe contar con domicilio o sucursal en Colombia.
- El interesado debe contar con la certificación ISO 27001 vigente o certificar la implementación de buenas prácticas de reconocimiento mundial a nivel de seguridad y ciberseguridad de la información, para esto el proponente deberá presentar el certificado emitido por una entidad certificadora, y cuyo alcance deberá estar relacionado con las actividades operacionales propias y exclusivas de un centro de operaciones de seguridad, deseable el proceso de gestión de incidentes.
- El servicio debe ser ofrecido en modalidad 7*24 durante la vigencia del contrato.
- El contratista deberá suministrar los tiempos de respuesta empleados para dar el reporte y repuesta de las vulnerabilidades e incidentes de seguridad detectados.
- Actualmente la entidad cuenta con los siguientes dispositivos, que se deben incluir en la solución:

- AIX 5.3 (1)
- AIX 6.1 (1)
- FreeBSD Pre-11 versions (64-bit) (2)
- Linux Centos 4/5 (2)
- Linux Centos 6 (5)
- Linux Centos 7 (1)
- Linux Redhat 6/7 (32)
- Linux Solaris 10/11 (34)
- Vmware ESXI 5.5 (1)
- Windows 2003 Server (20)
- Windows 2008 Server (3)
- Windows 2008 Server R2 (28)
- Windows 2012 Server (22)
- Windows 2012 Server R2 (2)
- Windows Server Estándar 2016 (4)
  Windows 2019 Server (3)
- Firewall fortinent
- Suite Trend Micro (antinirus, antimalware, DLP, device control)
- Office 365

- Switches Aruba (60)
- NAC
- Directorio Activo

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

- Página WEB
- Hasta 10 aplicaciones
- Hasta 10 portales WEB

4.1 Especificaciones Solución SOC

Especificación	Cumple / No cumple	Justificación
1) El sistema de monitoreo y correlación de eventos de seguridad debe contar con módulos que detecten patrones y anomalías 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 o incidente de seguridad y la información necesaria para dar atención y gestión.		
2) Se deben afinar 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.		
3) Las tareas de prevención, detección, contención y recuperación de ataques, entre otras, deberán estar incluidas dentro del proceso de manejo de incidentes de seguridad de la metodología de atención del SOC.		
4) Se debe vigilar que los elementos bajo contrato estén funcionando durante todo el tiempo necesario y, en caso de que algún equipo se inhabilite o trabaje inadecuadamente sin causa aparente, el SOC tomará las medidas acordadas en los niveles de servicio, en conjunto con el cliente, para reactivar/restaurar el servicio lo antes posible.		
5) El servicio debe contemplar la entrega de informes (ejecutivo y técnico) mensuales de gestión, los cuáles deben incluir el detalle de las actividades realizadas		

en el período, para cada uno de los procesos cubiertos por el servicio. Adicional el proveedor debe entregar un informe detallado cuando ocurra alguna alerta urgente o incidencia que pueda o haya afectado a la entidad que incluya como mínimo: - Fecha y hora en la que se descubrió el incidente - Tipo de incidente - Prioridad en el tratamiento - IP origen - IP afectada - Detalle del incidente - Acciones ejecutadas de detección y contención de ataques - Recomendaciones de remediación		
6) El servicio de monitoreo y correlación de eventos debe monitorear todos los eventos recolectados a través del SIEM y brindar respuesta a incidentes de seguridad de la información 7*24 durante la vigencia del contrato, con una capacidad máxima de mil (1.000) dispositivos (servidores, dispositivos de red, dispositivos de seguridad y/0 equipos de escritorio, etc.)		
7) Suministrar en modalidad de servicio un correlacionador para soportar 1000 dispositivos con un rango de 700 hasta 1000 eventos por segundo que permita colectar, retener y correlacionar los eventos de seguridad de la Infraestructura TI.		
8) La plataforma deberá colectar los eventos de seguridad de múltiples marcas.		
9) El correlacionador debe proporcionar una arquitectura escalable donde la capacidad de procesamiento, memoria y almacenamiento se puede aumentar o disminuir de acuerdo con la carga real en producción.		
10) Los recursos necesarios para la instalación y operación de la solución en relación a la memoria, procesamiento y almacenamiento, deberán ser proporcionados por el contratista.		
11) La implementación de las reglas del SIEM deberán hacerse al momento de la entrega del		

funcionamiento correcto y evidenciable de la herramienta y su ajuste deberá realizarse a más tardar en el primer mes de la operación de la herramienta.		
12) El correlacionador debe almacenar datos relacionados con los incidentes y eventos, incluidos el comportamiento de los usuarios y activo asociados durante el período de vigencia del contrato, en forma de búsqueda para un estándar de 90 días y custodia durante 12 meses.		
13) La plataforma deberá tener una consola tipo dashboard en la cual se pueda personalizar varios tipos de gráficas, tablas y reportes, para permitir tener una visión global de los eventos, incidentes de seguridad y reglas implementadas en la herramienta.		
14) El correlacionador deberá proporcionar información en tiempo real de los eventos generados por los dispositivos de seguridad administrada, así como las alarmas que permitan identificar los eventos relevantes y que puedan afectar la integridad, confidencialidad o disponibilidad de los servicios protegidos de FIDUPREVISORA S.A.		
15) El correlacionador debe proteger la integridad y confidencialidad de la información almacenada con algoritmos de hashing fuertes mínimo SHA256		
16) El correlacionador y el equipo de SOC deberá monitorear interfaces de red de 1GB y 10 GB y ancho de banda de 150 MB a 200MB.		
17) EL proveedor deberá brindar capacitación en las funcionalidades de la solución, en relación al entendimiento del dashboard, la generación de informes, y la visualización y entendimiento de las reglas del correlacionador de eventos. Este entrenamiento debe ser certificable por parte del proveedor.		
18) El correlacionador deberá poder monitorear las aplicaciones en la nube de la entidad, utilizando como detección de una combinación de DNS, proxy web y registros de firewalls integrándose directamente con los principales servicios en la nube, para proporcionar un solo panel, que permita revisar: inicios de sesión en los servicios en la nube, donde se		

registran los usuarios (incluso fuera de la red corporativa), qué actividad realizan los administradores de servicios en la nube, usuarios retirados que continúen autenticándose en los servicios.		
19) Garantizar el debido licenciamiento y operatividad de la herramienta.		
20) El equipo del SOC o especialista encargado deberá realizar las labores correspondientes a la instalación, configuración, parametrización y administración del correlacionador dispuesto para la ejecución del servicio, que debe incluir la creación de los conectores necesarios para un correcto monitoreo/correlación de las plataformas que se requieran		
21) Dentro del servicio provisto por el SOC se deberán detectar acciones tales como: - Credenciales comprometidas - Movimiento lateral - Ataques tipo “Pass the Hash” - Escalamiento de privilegios - Suplantación de identidad (correos electrónicos sospechosos, phishing) - Anomalías en el ingreso a los sistemas - Visibilidad de la red interna, nube y direcciones IP asociadas a incidente. - Eliminación anómalas de logs - Cambios directos sobre las bases de datos - Malware		
22) El servicio del SOC deberá contar con alta disponibilidad.		
23) Debe contar con alianzas directas y activas para combatir el cibercrimen a nivel nacional o mundial como ICSPA o equivalente. Especificar cuáles y contactos para revalidar alianzas.		
24) Debe tener una vinculación directa y activa con grupos de respuesta a incidentes de seguridad informática como FIRST por ejemplo. Especificar con cuáles.		
25) El proveedor está en capacidad de prestar el servicio en el idioma español, para la interacción de las áreas de operación.		

26) Los centros de cómputo que alojan la infraestructura de TIC del servicio de SOC se encuentren acreditados en su mayoría como TIER 3 o su respectivo equivalente. (Deseable). Especificar		
27) El proponente deberá tener un SOC propio.		
28) Debe contar con protecciones físicas contra daño por: Incendio, inundación, terremoto, explosión, manifestaciones sociales, otras formas de desastre natural o artificial.		
29) Debe contar con perímetros de seguridad tales como: Paredes, puertas de acceso controladas para personal autorizado con sistema biométrico.		
30) El proponente deberá contar con procesos de eliminación segura de la información que ya no se requiera		
31) El proponente deberá indicar el cumplimiento e incumplimiento de SLA pactados a nivel mensual, para hacerle seguimiento.		
32) Las instalaciones del SOC deberán tener periódicamente información de indicadores sobre plataforma monitoreada.		
33) El proponente deberá contar con un informe detallado sobre alertas mundiales que puedan afectar la seguridad sobre la infraestructura de la Entidad.		
34) El proponente deberá desarrollar estrategias que permitan hacer inteligencia de ataques y detección de nuevo malware y APTs y establecer procedimientos de contención y erradicación de los mismos.		
35) El SOC debe tener discriminado claramente los procesos, personas y roles que intervienen en las tareas de operación de seguridad, con las funciones de inteligencia de amenazas, monitoreo, correlación, análisis de tendencias en seguridad, atención, manejo y contención de incidentes de seguridad.		
36) El proponente deberá contar con personal especializado para el seguimiento al cumplimiento del servicio contratado, una gerencia de servicio.		
37) El proponente deberá certificar la revisión para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes		

que interactúen con el SOC, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y son proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y a los riesgos percibidos.		
38) El proponente debe tener operación y personal dedicado para la gestión y atención de incidentes.		
39) El modelo de operación del SOC, debe basarse en estándares y metodologías reconocidos a nivel mundial en la implementación de CSIRT, CERT o sus equivalentes. Especificar cuáles.		
40) Especificar la marca de la solución de correlacionador de eventos con la que trabaja el SOC.		
41) El servicio debe tener la capacidad de proporcionar una herramienta de tickets dentro de la operación del SOC con el fin de poder generar y notificar requerimientos puntuales tanto de parte de la Fiduprevisora como de parte del SOC hacia la entidad. (Indicar si es posible integración con Aranda, en la entidad se cuenta con bus de integración)		
42) El servicio debe contar con un mecanismo que permita obtener inteligencia de amenazas tanto en el contexto externo como interno de la organización.		
43) El servicio debe contar con procesos de analítica para detección de anomalías y comportamientos sospechosos sobre la información recolectada.		
44) El oferente debe tener mecanismos de monitoreo de la actividad de las fuentes de log recolectadas para notificar cuando estas dejen de enviar eventos a los equipos de correlación.		
45) La solución deberá tener mecanismos de centralización de logs de aplicación propietarias con formatos *.txt y/o tablas y que los mismas sean procesados a fin de definir alertas/reportes sobre dicha información.		
46) Los conectores de eventos deberán enviar en todo momento y en tiempo real los eventos recolectados hacia la solución de correlación de eventos, salvo que se requiera habilitar bajo demanda el envío asíncrono de eventos.		
47) El servicio debe permitir correlacionar la información de accesos a nivel perimetral (Firewalls), junto con las		

vulnerabilidades detectadas a nivel de equipos, esto con el fin de simular propagaciones de malware y explotaciones de vulnerabilidades.		
48) La solución debe permitir definir correlaciones estáticas y dinámicas.		
49) La solución debe permitir detectar fluctuaciones en la recepción de logs por fuente de información.		
50) La solución de permitir mecanismos de búsquedas rápidas, eficientes y que permitan ser exportadas a formatos tales como *.csv.		
51) El Servicio de vulnerabilidades debe estar integrado con el monitoreo y correlación y se deben declarar incidentes ante vulnerabilidades detectadas.		
52) La solución de correlación de eventos debe soportar mecanismos nativos para tomar acciones sobre endpoint (Ej., bloqueo de IP, bloqueo de usuarios) en casos de incidentes críticos.		
53) La solución de correlación de eventos debe ser también alimentada por fuentes de inteligencia externas de amenazas que contengan listas de reputación (IP) y/o dominios catalogados como sospechosos para la generación de indicadores de compromiso.		
54) El motor analítico de la solución de correlación debe permitir identificar patrones anómalos de comportamiento por usuario y/o IP.		
55) Monitoreo permanente de los motores de bases de datos (SQL, Oracle), garantizando y asegurando disponibilidad, integridad, consistencia, seguridad, control de las bases de datos dando continuidad a la operación en los ambientes productivos.		
56) El servicio requerido deberá estar alineado con las mejores prácticas definidas por ITIL V3, por lo que deberá contar con: diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio.		

4.2 Análisis de Vulnerabilidades

Especificación	Cumple / No cumple	Justificación
1) Proveer un sistema de análisis de vulnerabilidades de propósito específico –*appliance*- instalado y configurado en las instalaciones de Fiduprevisora, soportado por el proveedor y licenciado por un año a nombre del cliente.		
2) Generar de manera automática dos (2) informes consolidados de carácter técnico, de las vulnerabilidades encontradas y su respectiva categorización. Uno por semestre.		
3) Generar de manera automática dos (2) informes ejecutivos, de las vulnerabilidades encontradas y su respectiva categorización. Uno por semestre		
4) Generar un informe técnico y uno gerencial mensual, de seguimiento sobre el estado de la remediación de las vulnerabilidades encontradas.		
5) Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual del inmediatamente anterior.		
6) Homologación con el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización. Mitre (www.mitre.org).		
7) Usa el CVS (Common Vulnerability Scoring System) para clasificar las vulnerabilidades.		

4.3 Ethical Hacking

Especificación	Cumple / No cumple	Justificación
1) Realizar dos pruebas de Ethical Hacking externas (caja negra), donde se valide como mínimo: - SQL Injection - Cross Site Scripting - CSRF - Blind SQL - Ataques de directorio transversal - Ataques por referencia directa a objetos		

Especificación	Cumple / No cumple	Justificación
2) Realizar test de penetración interno tipo caja blanca, una vez al año		
3) Prueba de ingeniería social. Dependiendo del tipo de prueba debe realizarse como mínimo a 20 funcionarios (objetivos específicos) o masivas a la totalidad de usuarios de correo electrónico.		
4) Generar un informe técnico y uno gerencial por cada prueba realizada.		

5. Duración

El proveedor debe cotizar el servicio a 12, 24 y 36 meses.

Forma de pago

Fiduprevisora S.A. bajo ninguna circunstancia realizará anticipos o pagos anticipados, el pago del valor estimado del servicio se hará conforme a los servicios prestados.

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 operacionesfic@fiduprevisora.com.co .*

6. VALOR DE LA COTIZACIÓN

El valor de la cotización debe estar en pesos colombianos, debe incluir vigencia, IVA y demás impuestos a los que haya lugar y se debe discriminar el valor de cada uno de los servicios por separado:

	Valor Total con IVA		
Cotización	**12 meses**	**24 meses**	**36 meses**
Servicio SOC – Correlacionador de eventos			
Análisis de Vulnerabilidades			
Ethical Hacking			
Sub- Total			
IVA			

	Valor Total con IVA		
Cotización	**12 meses**	**24 meses**	**36 meses**
Total con IVA*			

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

Agradecemos su participación.

Elaboró: Sergio Jaimes – Líder de Inteligencia de Mercados
Revisó: Carolina Giraldo Duque – Gerente de Adquisiciones & Contratos (e)
Aprobó: Sergio Plazas - Director de Infraestructura
Aprobó: Angelica Martin – Oficial de Seguridad de la Información
Aprobó: Alexander Vasquez – Director de Innovación
Aprobó: Juan Gabriel Barrera – Director de Proyectos Especiales