INVITACIÓN A COTIZAR No. 027 DE 2022

Objeto: Fiduprevisora S.A. a través de la Gerencia de Riesgos está interesada en recibir cotizaciones para contratar una solución para prestar el servicio de SOC (Security Operation Center) con correlacionador de eventos de seguridad, realizar análisis de vulnerabilidades y pruebas de Ethical Hacking con personal experto, en horario 7*24, 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 y la Circular Externa 042 de 2012 de la Superintendencia Financiera de Colombia.

Apertura de la Invitación: 14 de junio de 2022

Fecha límite para presentar observaciones: 17 de junio de 2022 hasta las 17:00 horas

Respuesta a Observaciones: 23 de junio de 2022

Recepción de Cotizaciones: 30 de junio de 2022 hasta las 17:00 horas a través del correo electrónico intdemercados@fiduprevisora.com.co y/o plataforma SECOP II.

Área Responsable: Gerencia de Riesgos.

Contacto: intdemercados@fiduprevisora.com.co y/o plataforma SECOP II.

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 correspondiente, la viabilidad de la contratación mediante la medición de variables como la oportunidad, la calidad, el costo, etc. Adicionalmente, se realizarán las gestiones pertinentes si alguna de las cotizaciones allegadas cumple con las expectativas de la Fiduciaria, la cual debe satisfacer las necesidades de acuerdo con 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 solicitud de cotización se realiza conforme con lo establecido en el Artículo 15 de Ley 1150 de 2007 la cual establece lo siguiente: “DEL RÉGIMEN CONTRACTUAL DE LAS ENTIDADES FINANCIERAS ESTATALES. El parágrafo 1o del artículo 32 de la Ley 80 de 1993, quedará así: “Artículo 32. (...) Parágrafo 1°. Los contratos que celebren los Establecimientos de Crédito, las compañías de seguros y las demás entidades financieras de carácter estatal, no estarán sujetos a las disposiciones del Estatuto General de Contratación de la Administración Pública y se regirán por las disposiciones legales y reglamentarias aplicables a dichas actividades.

En todo caso, su actividad contractual se someterá a lo dispuesto en el artículo 13 de la presente ley", especialmente a los principios de la función administrativa y de la gestión fiscal de que tratan los artículos 209 y 267 de la Constitución Política.

Sin perjuicio de lo anterior, la presente invitación está sujeta a las normas del derecho privado y al Manual de Contratación de Bienes y Servicios de Fiduciaria La Previsora S.A.

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 de la presente invitación, 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 Ley 1581 de 2012, sus decretos reglamentarios, y demás normas concordantes que la adicionen, aclaren o modifiquen, por las cuales se establecen disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos; 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 deberán manifestar en su cotización, que, para efectos de trámites relativos a consultas o reclamos relacionados con datos personales, tienen habilitados los siguientes medios de contacto: _____

Fiduprevisora S.A., informa que para el mismo efecto tiene habilitados los siguientes canales de atención: página WEB https://www.fiduprevisora.com.co/solicitudes-quejas-y-reclamos/; Teléfono: (1) 756 6633 y dirección física: calle 72 # 10-03, Bogotá, Colombia.

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. Matriz Riesgos

N°	FUENTE	ETAPA	TIPO	DESCRIPCION	CONSECUENCIA DE LA OCURRENCIA DEL EVENTO	PROBABILIDAD	IMPACTO	VALORACION DEL RIESGO	CATEGORIA	A QUIEN SE LE ASIGNA
1	Interna	Planeación	Operacional	No contar con el presupuesto para la adquisición del bien y/o servicio	-No adquisición del bien y/o servicio -Demoras en el inició de la etapa de selección	3	3	6	Alto	Entidad
2	Interna	Planeación	Operacional	Errores en los pliegos de condiciones y/o en la invitación a cotizar	-Demoras en la adjudicación del contrato -Adquirir productos o servicios que no satisfacen las necesidades del área usuaria -Reprocesos	3	2	5	Medio	Entidad
3	Externo	Ejecución	Operacional	Incumplimiento en las especificaciones técnicas contratadas	Afectación en la calidad del producto y/o servicio	4	4	8	Extremo	Contratista
4	Externo	Ejecución	Operacional	No cumplimiento en la entrega de los bienes y/o servicios contratados	Incumplimiento del contrato	3	3	6	Alto	Contratista

2. INFORMACIÓN PARA LA COTIZACIÓN.

2.1. ALCANCE

Fiduprevisora S.A. requiere recibir cotizaciones para obtener la prestación de servicios de una solución SOC (Security Operation Center) debido a que la supervisión y análisis permanente (7/24) de las actividades de los datos permite la detección de incidentes de seguridad (ransomware, phishing, ataque DDOS, entre otros) sin tener en cuenta la fuente, la hora del día o el tipo de ataque, así como la protección de la confidencialidad, integridad y disponibilidad de la información en los diferentes componentes de la infraestructura de la entidad en sus diferentes entornos (On-Premise y Cloud). Generando una reducción de tiempo de identificación y reacción, reduciendo el impacto en la prestación de servicios y continuidad de negocio.

2.2. ESPECIFICACIONES TECNICAS DEL SERVICIO

Para la prestación de los servicios se debe contar con el cumplimiento en su totalidad de los requisitos presentados a continuación.

1. El servicio del SOC deberá contar con alta disponibilidad.
2. La solución SIEM deberá soportar un mecanismo de autenticación nativo además de soportar mecanismos alternativos como: Microsoft Active Directory, Autenticación de doble factor, LDAP y Radius.
3. El servicio de monitoreo y correlación de eventos debe monitorear todos los eventos recolectados a través del SIEM y brindar alertamientos de eventos o incidentes de seguridad de la información 7*24, con una capacidad mínima de cuatrocientos (400) dispositivos (servidores, dispositivos de red, dispositivos de seguridad, equipos de cómputo de usuarios con privilegios de administración o cargos críticos).
4. La implementación de las reglas del SIEM deberán hacerse al momento de la entrega del funcionamiento correcto y evidenciable de la herramienta; debe incluir todas las actividades para la implementación de SIEM (reglas, correlación, recepción de logs, etc.) y su ajuste deberá realizarse a más tardar en el segundo mes de operación (deseable).
5. La plataforma deberá colectar los eventos de seguridad de múltiples marcas.
6. La solución de SIEM debe contar de forma integrada y sin necesidad de licenciamiento aparte, un módulo para la creación de nuevos recolectores para tecnología no soportada por el fabricante de forma nativa.
7. La solución SIEM deberá permitir la integración de dispositivos y aplicaciones de diferentes fabricantes con el objetivo de evitar el desarrollo de los conectores.
8. La solución SIEM deberá permitir la correlación de eventos entre distintos dispositivos (Cross Device Correlation) almacenar todos los eventos recolectados en una única tabla dentro de su base de datos, independiente del tipo de dispositivo o aplicativos que la genere, permitiendo así la definición de contenido de correlación entre distintos de dispositivos (firewalls, IDPs, Sistemas Operativos, etc.) sin la necesidad de utilizar estructuras complejas o lenguajes de acceso a datos para la consulta y unión de datos.
9. Suministrar en modalidad de servicio un SIEM para soportar de 150 a 400 dispositivos, con capacidad de colectar, retener y correlacionar los eventos de seguridad de la Infraestructura TI; de hasta 500 eventos por segundo EPS (Eventos por Segundo).
10. Debe incluir diseño de la arquitectura de la solución.
11. 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 producción.
12. El SIEM deberá proporcionar información en tiempo real o con diferencias de máximo 3 minutos 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.
13. La solución SIEM deberá permitir entre otros usos monitorear, detectar y tomar medidas correctivas a través de la integración nativa con elementos de seguridad en el endpoint y en el perímetro, al momento de detectar comportamientos asociados a amenazas avanzadas. La solución debe permitir agregar indicadores de compromiso (IOC) de manera

automática, los cuáles permitan incrementar la capacidad de análisis que posee la herramienta.

La solución SIEM debe monitorear y detectar amenazas entre las que se encuentran:

- Contenedores
- Redes
- Shadow IT
- Entornos de nube.

La solución SIEM debe realizar la investigación y correlación de eventos utilizando inteligencia artificial (IA) y priorizar los incidentes.

La solución SIEM debe adoptar la estructura MITRE ATT&CK para el desarrollo de modelos de amenazas y metodologías específicos en el sector gobierno.

14. La solución debe prevenir los problemas detectando anomalías en su fase inicial.
15. Las tareas de prevención y detección deberán estar incluidas dentro del proceso de manejo de incidentes de seguridad de la metodología de atención del SOC.
16. 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.
17. Implementación de nuevos casos de uso en la detección de incidentes de seguridad y ciberseguridad de la información.
18. La solución debe contar con la capacidad de importar e instalar paquetes de contenidos que incluyan reglas de correlación, alarmas, vistas, variables y listas de monitoreo orientadas a casos de uso específicos que ayuden a responder a las amenazas existentes de manera más eficiente.
19. 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.
20. La solución SIEM deberá proveer mecanismos para asegurar la integridad de los logs almacenados.
21. 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: 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.
22. La solución SIEM deberá soportar la integración de eventos provenientes de Active Directory, DHCP y concentradores VPN para monitorear la asignación de direcciones IP y asociar eventualmente los usuarios.
23. La solución SIEM debe permitir la creación de paneles y el monitoreo de actividad de usuarios privilegiados en el dominio tales como: Monitoreo del manejo de cuentas (altas, bajas, reset password, etc.); elevación de privilegios, monitoreo de cuentas de usuario VIP, monitoreo de cuentas de usuario privilegiados entre otros.
24. Dentro del servicio provisto por el SOC se deberán detectar acciones tales como:

- Ataques tipo “Pass the Hash”
- Visibilidad de la red interna, nube y direcciones IP asociadas a incidente
- Eliminaciones anómalas de logs
- Cambios directos sobre las bases de datos

USO INDEBIDO DE LA MARCA

- Suplantación de sitio web
- Registro de DNS
- Suplantación de cuentas
- Phising

MODIFICACION Y/O ALTERACION NO AUTORIZADA

- Modificación no autorizada de la infraestructura
- Agregar, alterar, o eliminar información clave

CIBERSABOTAJE

- Hacktivismo
- Noticias Falsas

EXPLOTACION DE VULNERABILIDADES

- Mala configuración
- Sistema no actualizado

ATAQUES CIBERNETICOS DIRIGIDOS

- Whaling,
- Ingeniera Social
- Spear Phishing
- AVT: Amenaza volátil avanzada,
- Espionaje industrial y Robo de propiedad intelectual.

CODIGO MALICIOSO (MALWARE)

- Infección Extendida
- Infección Única

DISRUPCION DE SISTEMAS

- Denegación de servicio (DoS, DDoS)
- Indisponibilidad de servicios de proveedores críticos

ACCESO NO AUTORIZADO

- Inyección SQL
- Intentos de login
- Cuentas de usuario comprometidas
- Elevación de privilegios
- Movimientos laterales

PRUEBAS Y RECONOCIMIENTO

- Scanning
- Sniffing

USO NO AUTORIZADO DEL SISTEMA

- Cryptojacking
- Botnet

OTRAS

- Gestión de Inteligencia de Amenazas.
- Activar mecanismos de intercambio de información de amenazas con diferentes fuentes de la misma, ya sean públicas o privadas, para mejorar la proactividad en la detección y la protección.
- Mejorar los procesos de búsqueda de indicadores de compromiso.
- Automatizar acciones sobre diferentes mecanismos de seguridad para enriquecerlos con los indicadores de compromiso recibidos de las diferentes fuentes.
- Contar con espacios de discusión sobre nuevas técnicas de ataques, herramientas de seguridad, mejores prácticas, etc.

25. 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.
26. La solución SIEM debe estar en la capacidad de hacer push de scripts, como parte de las opciones de respuesta accionables.
27. La solución SIEM deberá contar con un módulo que permita recolectar a manera de sniffer información de sentencias transaccionales a bases de datos con el objetivo de monitorear, analizar, correlacionar y alertar estos eventos. La solución no deberá requerir modificaciones en las bases de datos a monitorear.
28. El servicio de vulnerabilidades debe estar integrado con el monitoreo y correlación y se deben declarar incidentes ante vulnerabilidades detectadas.
29. El componente de recolección debe permitir restringir el ancho de banda utilizado en la red, el cual podrá ser definido en Kilobits por segundo (Kbps), Megabits por segundo (Mbps) o Gigabits por segundo (Gbps).
30. La solución SIEM deberá ser capaz de recibir eventos multilínea y manejarlo como un solo registro. Se entiende por multilínea aquellos eventos que se extienden a más de una línea, por ejemplo, registros de excepciones o errores.
31. Los conectores de eventos deberán enviar en todo momento y en tiempo real los eventos recolectados hacia la solución SIEM, salvo que se requiera habilitar bajo demanda el envío asíncrono de eventos.
32. El componente de recolección debe proveer mecanismos que garanticen la entrega de eventos y que los eventos no se pierdan si el sistema no está disponible. Debe poder almacenar eventos en un caché local durante una situación de falla en la red y entregar los eventos cuando el sistema vuelva a estar en línea.
33. El servicio debe contar con procesos de analítica para detección de anomalías y comportamientos sospechosos sobre la información recolectada.
34. La solución debe permitir definir correlaciones estáticas y dinámicas.
35. El motor analítico de la solución de correlación debe permitir identificar patrones anómalos de comportamiento por usuario y/o IP.

36. El motor de correlación de la solución SIEM, deberá estar basado en métodos de lógica booleana, reglas personalizables, así como la detección de comportamiento anómalo mediante correlación estadística a través de cálculos de promedio. Adicionalmente debe incluir reglas de correlación a nivel de seguridad preconfiguradas (Ej.: Ataques de fuerza bruta).
37. El SIEM debe ser también alimentado 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.
38. La comunicación entre todos los componentes de la solución SIEM debe ser cifrada sin impactar en la performance.
39. El SIEM debe proteger la integridad y confidencialidad de la información almacenada con algoritmos de hashing fuertes mínimo SHA256.
40. Para el análisis del tráfico cifrado que viaja vía HTTPS o por aplicaciones que utilizan protocolos de encriptación punto a punto, se debe utilizar un sistema de Descifrado SSL que funciona como túnel, el cual desencripta los datos, hace la lectura del payload y en la salida de la función vuelve a cifrarlos, para que viajen totalmente seguros permitiendo analizar ese 80% del actual tráfico Web que viaja de forma cifrada.
41. 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.
42. La solución debe permitir detectar fluctuaciones en la recepción de logs por fuente de información
43. El SIEM debe almacenar datos relacionados con los incidentes y eventos, incluidos el comportamiento de los usuarios y activos asociados durante el período de vigencia del contrato, en forma de búsqueda para un estándar de 90 días y custodia durante 12 meses. Al finalizar el contrato se deben entregar los logs.
44. 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 S.A. como de parte del SOC hacia la entidad. (Indicar si es posible integración con Aranda, en la entidad se cuenta con bus de integración).
45. La solución SIEM deberá ser capaz de enviar alertas vía email, así como notificaciones directas a usuarios de la misma consola de administración.
46. La solución SIEM deberá proporcionar una interface de administración gráfica (GUI) propia. Esta interfaz debe ser WEB y segura (HTTPS).
47. 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.
48. La solución SIEM debe incluir contenido en modo de filtros, reglas predefinidas de correlación, monitores gráficos (Dashboard) y reportes pre-configurados de monitoreo de dispositivos de red perimetral, enfocado a las mejores prácticas de seguridad y ataques más comunes.
49. Como requisito "mínimo", la solución debe contar con los siguientes componentes:
    *Componente de gestión, administración y operación de la solución.

*Componente de recolección de eventos y/o logs de seguridad.
*Componente de almacenamiento de eventos y/o logs, agentes y conectores para recolectar eventos de seguridad de terceros.
*Componente de reportes.
*Componente de edición de parsers custom.
*Componente de auditoría (Registro de las actividades de los administradores y operadores de la solución)

50. El sistema de monitoreo y correlación de eventos (SIEM) de seguridad debe contar con módulos que detecten patrones y anomalías de diversas fuentes para su normalización, centralización y análisis (inteligencia de amenazas cibernéticas). 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.
51. La solución SIEM deberá contar con una fórmula parametrizable que evalúe el nivel de riesgo de todos los eventos que son recibidos por el motor de correlación considerando los siguientes factores; importancia del evento, criticidad del evento y vulnerabilidades.
52. La solución SIEM debe realizar automáticamente la generación de un mapa de calor, asociándole valores de riesgo cualitativo (Alto, Medio y Bajo) a los incidentes que se están presentando en un período de tiempo determinado La solución de permitir mecanismos de búsquedas rápidas, eficientes y que permitan ser exportadas a formatos tales como *.csv.
53. El servicio debe contar con un mecanismo que permita obtener inteligencia de amenazas tanto en el contexto externo como interno de la organización.
54. El proponente deberá desarrollar estrategias que permitan hacer inteligencia de amenazas cibernéticas y detección de nuevos malware y APTs y establecer procedimientos de contención y erradicación de los mismos.
55. La solución debe contar con funcionalidades de analítica avanzada que permitan la cacería de amenazas, y capacidades de big data lo que mejora sustantivamente la velocidad de acceso a los datos, el análisis de información y la capacidad de respuesta ante incidentes, esas son características importantes mencionadas por analistas independientes como Gartner.
56. Dentro de la metodología para la prestación del servicio SOC se deben contemplar pruebas de red team.
57. Proveer un sistema de análisis de vulnerabilidades de propósito específico –appliance— instalado y configurado en las instalaciones de Fiduprevisora S.A., soportado por el proveedor y licenciado por un año a nombre del cliente.
58. Generar de manera automática dos (2) informes consolidados de carácter técnico, de las vulnerabilidades encontradas y su respectiva categorización. Uno por semestre.
59. Generar de manera automática dos (2) informes ejecutivos, de las vulnerabilidades encontradas y su respectiva categorización. Uno por semestre.
60. Generar un informe técnico y uno gerencial mensual, de seguimiento sobre el estado de la remediación de las vulnerabilidades encontradas. Para aclarar se espera realizar únicamente dos análisis de vulnerabilidades en el año (uno por semestre) o cada vez que se

realice un cambio en la infraestructura TI, con su respectivo retest a los tres meses de realizado el análisis, de los cuales se generará un informe técnico y otro gerencial y posteriormente, mes a mes se generará un informe de seguimiento de remediación de las vulnerabilidades identificadas en cada semestre (también técnico y gerencial).

61. Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual del inmediatamente anterior.
62. Homologación con el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización. Mitre (www.mitre.org).
63. Usa el CVS (Common Vulnerability Scoring System) para clasificar las vulnerabilidades.
64. 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
    - Man in the middle

    Se debe realizar una prueba por semestre, con su respectivo retest a los tres meses de realizada la prueba.

65. Realizar test de penetración interno tipo caja blanca, una vez al año.
66. Realizar análisis estático y dinámico.
67. 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.
68. Generar un informe técnico y uno gerencial por cada prueba realizada.

2.3. CONDICIONES DEL SERVICIO REQUERIDO

1. El Contratista deberá tener un SOC propio.
2. Para los centros de cómputo que alojan la infraestructura de TIC del servicio de SOC se debe garantizar que la acreditación del centro de cómputo TIER3 o equivalente no solamente sea en diseño, también debe cumplir con acreditación en construcción.
3. Contar con protecciones físicas contra daño por: Incendio, inundación, terremoto, explosión, manifestaciones sociales, otras formas de desastre natural o artificial.
4. Contar con perímetros de seguridad tales como: Paredes, puertas de acceso controladas para personal autorizado con sistema biométrico.
5. 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.
6. Garantizar la operación y personal dedicado para la gestión y atención de incidentes.

7. Brindar capacitación en las funcionalidades de la solución, con relación al entendimiento del dashboard, la generación de informes, y la visualización y entendimiento de las reglas y notificaciones del SIEM. Este entrenamiento debe ser certificable por parte del proveedor. Máximo para 5 funcionarios.
8. La solución debe ser reconocida dentro del cuadrante mágico de Gartner u otro analista independiente.
9. Especificar la marca de la solución de SIEM con la que trabaja el SOC.
10. Prestar el servicio en el idioma español, para la interacción de las áreas de operación
11. Contar con alianzas directas y activas para combatir el cibercrimen a nivel nacional o mundial como ICSPA, OTX de Alien Vault o vinculación directa y activa con grupos de respuestas a incidentes como FIRST o similares (cualquiera de estas es válida, así como los grupos similares presentados). Especificar cuáles y contactos para revalidar alianzas.
12. 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.
13. 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.
14. Los recursos necesarios para la instalación y operación de la solución con relación a la memoria, procesamiento y almacenamiento deberán ser proporcionados por el contratista.
15. Licenciamiento por un año del servicio contratado, luego de la implementación y pruebas realizadas.
16. La garantía que se requiere es con vigencia de un (1) año de la prestación del servicio, al ser solicitado de forma administrada, velando por el buen funcionamiento de la herramienta y las notificaciones en los tiempos establecidos.
17. Deberá contar con un soporte y mantenimiento mínimo de un (1) año.
18. 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. Esto de cara al servicio prestado.
19. Responder ante cualquier falla que se llegue a materializar en la prestación del servicio y resolver en los tiempos de respuesta estipulado en los acuerdos de niveles de servicio (ANS), los cuáles serán parte integral del Contrato.
20. El equipo del SOC o 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.
21. Indicar el cumplimiento e incumplimiento de SLA pactados a nivel mensual, para hacerle seguimiento.
22. Las instalaciones del SOC deberán tener periódicamente información de indicadores sobre plataforma monitoreada.
23. 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.

Adicionalmente 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 (si se toma el servicio con esta última opción).
- Recomendaciones de remediación.
- Posibilidad de manejar gráficos tipo pie, barras y otras características de personalización tales como incluir los logos de la compañía.

24. Permitir la generación de informes de eventos de seguridad que permita realizar validaciones históricas de eventos y notificaciones de las ofensas de seguridad.
25. Los componentes de la solución SIEM que realizan la recolección de eventos deberán ofrecer la capacidad de ajuste en la hora de los eventos, en el caso de que el dispositivo que genere el evento no cuente con la hora correcta o no tenga configurado un servidor NTP.
26. Deberá contar con un informe detallado sobre alertas mundiales que puedan afectar la seguridad sobre la infraestructura de la Entidad.
27. Deberá contar con procesos de eliminación segura de la información que ya no se requiera.
28. Los equipos a monitorear en el SOC y realizar el análisis de vulnerabilidades son:

- 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)
- Bases de Datos: Oracle 11G y 12C
- Firewall fortinent
- Suite Trend Micro (antivirus, antimalware, DLP, device control) (monitoreo SOC)
- Servidor de correo

- Switches Aruba (60)
- NAC
- Directorio Activo
- Para el servicio de Ethical Hacking se tiene:
- Página WEB
- Hasta 10 aplicaciones
- Hasta 10 portales WEB

2.4. DURACIÓN.

La empresa interesada debe cotizar el servicio para 12 y 24 meses.

2.5. FORMA DE PAGO

Fiduprevisora S.A. bajo ninguna circunstancia realizará anticipos o pagos anticipados, el pago se realizará una vez se preste efectivamente el servicio en mensualidades vencidas.

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 operacionesfic@fiduprevisora.com.co.*

3. INFORMACIÓN ESPECÍFICA DE LA COTIZACIÓN.

3.1. Forma de presentación de la Cotización

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

3.2. 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 Representación Legal con fecha de expedición no mayor a 30 días calendario.
II. Registro Único Tributario – RUT.
III. Estados Financieros con corte a diciembre de 2021 o corte más reciente.

3.3. Experiencia Específica

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

N°	EMPRESA O ENTIDAD CONTRATANTE	OBJETO	FECHA INICIO	FECHA FIN	VALOR TOTAL EJECUTADO INCLUIDO IVA
1					
2					
3					

Nota* se recomienda que preferiblemente la experiencia relacionada no sea superior a 5 años respecto de la actual vigencia.

4. VALOR DE LA COTIZACIÓN

El valor de la propuesta debe presentarse en pesos colombianos, debe incluir impuestos, tasas y/o contribuciones a los que haya lugar, así como costos directos e indirectos.

En caso en que el servicio se encuentre exento o excluido del IVA, es pertinente informar las razones financieras, tributarias y/o jurídicas que así lo contemplen.

Descripción	Tiempo de Servicio	Valor (Antes de IVA)	IVA (En caso de aplicar)	Valor Total
Servicio de SOC con correlacionador de eventos, realizar análisis de vulnerabilidades y pruebas de Ethical Hacking.	12 meses			
	24 meses			

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

Agradecemos su participación.

Elaboró: R. Álvarez - Profesional Inteligencia de Mercados.
Revisó: María José Barguil Borja - Directora de Contratos Empresa.
Revisó: Carolina Giraldo Duque – Gerente de Adquisiciones & Contratos.
Aprobó: Sergio Andrés Pérez Mesa - Gerente de Riesgos.