INVITACIÓN 1045

OBJETO DE LA INVITACIÓN

La Fiduciaria Colombiana de Comercio Exterior S.A. FIDUCOLDEX, está interesada en recibir propuestas para contratar los servicios de monitoreo SOC (Security Operation Center) en la modalidad 7dias 24hs 365días al año, para el fortalecimiento de la ciberseguridad de la Fiduciaria, con las siguientes especificaciones:

a) Monitoreo permanente de la plataforma computacional (7x24x365)
b) Monitoreo de marca (Fiducoldex y PA)-Proceso continuo de identificación, priorización, mitigación y comprobación de existencia de una o varias vulnerabilidades en el entorno tecnológico de cada una de las marcas mencionadas.
c) Pruebas de seguridad: análisis de vulnerabilidades (Trimestral) y Pruebas de Ethical Hacking (1 al año) y retest
d) Soporte a la gestión de incidentes
e) Soporte a las pruebas de "ataque cibernético"
f) Apoyo para el fortalecimiento de la ciberseguridad
g) Apoyo a los incidentes de seguridad de la información y ciberseguridad presentados en la entidad y sus patrimonios autónomos
h) Servicio de Red Team: explotación avanzada y controlada de vulnerabilidades en ventanas de mantenimiento coordinadas.
i) Pruebas de Phishing (Ingeniería Social)

RESPUESTA OBSERVACIONES

De acuerdo con lo establecido en los Términos de Referencia de la Invitación 1045, **FIDUCOLDEX** procede a dar respuesta a las observaciones conforme al cronograma establecido, en los siguientes términos:

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
FIVE STRATEGY	**1**	Se indica que obtendrá 5 puntos la propuesta que ofrezca como valor agregado la herramienta de monitoreo SIEM que tenga cada proveedor, se requiere en prueba de concepto por 6 meses (25 puntos), 4 meses (15 puntos) y 2 meses (10 puntos). ¿Cuántos son los activos que deben ser monitoreados por esta herramienta?	Los activos son los que se indican en el Anexo No. 3
FIVE STRATEGY	**2**	Entendemos que cualquier requerimiento de licenciamiento relacionado con Splunk es responsabilidad de la Fiduciaria, y no entra dentro de las obligaciones del oferente. ¿Es nuestro entender acertado?	El licenciamiento es contratado por la Fiduciaria, pero, la administración, configuración y mantenimiento es responsabilidad del especialista asignado por el proveedor.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
FIVE STRATEGY	**3**	Se solicita que el proponente cuente con personal capacitado para operar en caso de contingencia, en horario 7x24x365 dando cumplimiento a los SLA's solicitados. ¿Podrían informarnos los perfiles mínimos requeridos para este personal?	La Fiduciaria le informa que la información requerida se encuentra contenida en la Adenda No. 1
FIVE STRATEGY	**4**	Se solicita brindar soporte a la gestión de incidentes a través de un equipo de respuesta a incidentes. ¿Podrían informarnos los perfiles mínimos requeridos para este personal?	La Fiduciaria le informa que la información requerida se encuentra contenida en la Adenda No. 1
FIVE STRATEGY	**5**	El Proponente debe presentar las licencias o certificados de propiedad de los derechos de autor, sobre las herramientas que sean utilizadas en el servicio SOC. ¿Este requerimiento aplica también para los otros servicios solicitados dentro del proceso?	La Fiduciaria exige que la infraestructura, el software y el hardware utilizados dentro del servicio deben estar debidamente licenciados por el futuro contratista que preste el servicio.
LUMACLOUD	**6**	En el Anexo 3 se indica que el servicio SOC será por medio del SIEM propio SPLUNK, se solicita amablemente permitir que el servicio de SOC se entregue a partir de otra plataforma.	No es posible atender favorablemente esta solicitud , dado que hace parte del alcance definido para el servicio.
LUMACLOUD	**7**	Favor indicar sistema Operativo de los 100 Servidores a Monitorear	Los sistemas operativos dentro la infraestructura de la Fiduciaria corresponden a productos estándar de la industria.
LUMACLOUD	**8**	Se indica que se realizara pruebas Análisis de vulnerabilidades a 400 direcciones IP, favor indicar a que corresponden las IPs (Activos, aplicaciones Web, aplicaciones Mobiles) y cuantos y cuáles de cada uno.	En el Anexo No. 3 se indica hasta 400 direcciones IP, así mismo, en el anexo se menciona para que proyectos de la Fiduciaria se tomará el servicio, el cual, es por demanda, lo que lo convierte en un dato variable.
LUMACLOUD	**9**	¿Pruebas de Ethical Hacking a cuantos y cuáles activos?	En el Anexo No. 3 se indica hasta 400 direcciones IP, así mismo, en el anexo se menciona que para proyectos de la fiduciaria es por demanda, lo que lo convierte es variable.
LUMACLOUD	**10**	¿Análisis de código a demanda, sobre qué base se tendrá estimado, teniendo en cuenta que la valoración va a partir de líneas de código, aplicaciones y lenguaje de desarrollo?	No se tiene una base estimada ya que no se encuentra definido bajo estos criterios, dado que este tipo de pruebas surgen en la medida que se genere un nuevo desarrollo o implementación de una solución, por lo tanto, se dependería de una definición de alcance lo que lo convierte en un dato variable.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
LUMACLOUD	**11**	El Anexo 3 se encuentra con las celdas Bloqueadas, lo cual impide la visualización total de cada uno de los puntos, favor entregar los documentos desbloqueados.	Efectivamente el documento se encuentra bloqueado, sin embargo, los Ítem los pueden copiar si requiere hacer algún resumen de ellos.
OLIMPIAIT	**12**	"SOLICITUD DE ACLARACIÓN: Se solicita aclarar si el valor de $600.000.000 por certificación corresponde al valor total del contrato o al valor anual, considerando que el presupuesto del presente proceso es de $660.326.612,47 IVA incluido. Esta exigencia podría limitar la participación de proponentes con experiencia adecuada, pero en contratos de menor cuantía individual. También se solicita considerar mínimo 1 y máximo 4 certificaciones. /Términos de Referencia-3.3.1.1-->15-16/"	No es posible acceder favorablemente a esta solicitud; dado que los criterios aplican para todos los proponentes en igualdad de condiciones.
OLIMPIAIT	**13**	"SOLICITUD DE ACLARACIÓN: Se solicita aclarar si los '5 años mínimos' se refieren a la antigüedad del cliente o a la duración de la experiencia en SIEM. Adicionalmente, se solicita confirmar si la certificación del fabricante de SIEM es alternativa válida a las certificaciones de clientes. /Términos de Referencia-3.3.1.2-->16/"	Los 5 años se refieren a la certificación de la prestación del servicio SIEM que puede ser con uno o varios clientes. Frente a la segunda pregunta, no es posible acceder a su petición, ya que las certificaciones a acreditar son las mencionadas en Anexo No. 3.
OLIMPIAIT	**14**	"OBSERVACIÓN: Esta restricción podría limitar la libre competencia al impedir que empresas complementarias se asocien para ofrecer una propuesta más robusta. Se sugiere permitir al menos uniones temporales con responsabilidad solidaria. /Términos de Referencia-3.1 NOTA DOS-->12/"	No es posible acceder favorablemente a esta solicitud; dado que los criterios aplican para todos los proponentes en igualdad de condiciones.
OLIMPIAIT	**15**	"SOLICITUD DE ACLARACIÓN: Se solicita proporcionar el listado o características de las 190 aplicaciones web a monitorear para dimensionar correctamente el servicio y la propuesta económica. /Anexo 3 - Servicio_SOC-Ítem 1-->N/A/"	Esta información sería suministrada al adjudicatario en etapa posterior a la suscripción del contrato.
OLIMPIAIT	**16**	"SOLICITUD DE ACLARACIÓN: Se solicita aclarar si todas estas funcionalidades deben ser provistas por el proponente o si FIDUCOLDEX cuenta con algunas de ellas actualmente. Adicionalmente, definir qué se entiende por 'Casos de uso Ilimitados' ya que esto impacta significativamente el alcance y costo. /Anexo 3 - Servicio_SOC-Ítem 50-->N/A/"	Como se indicó en Anexo No. 3, el proveedor debe suministrar una solución que contemple estas herramientas y que, a su vez, se integre al SIEM de la Fiduciaria.
OLIMPIAIT	**17**	"SOLICITUD DE MODIFICACIÓN: Se solicita establecer un período de estabilización inicial (30-60 días) durante el cual las penalidades por disponibilidad no apliquen, permitiendo la correcta configuración e integración con el SIEM Splunk existente.	No se puede acceder a esta solicitud, debido a que, por temas de cumplimiento a entes de control como la Superintendencia Financiera de Colombia, debemos dar continuidad a los servicios y debemos tener en cuenta

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
		/Anexo 3 - Servicio_SOC-Ítem 63-->N/A/"	los SLA establecidos, por tal razón los ajustes se deben hacer dentro del periodo mismo de estabilización.
OLIMPIAIT	**18**	"OBSERVACIÓN: Existe inconsistencia entre el texto (5 puntos) y la tabla (25 puntos para 6 meses). Se solicita aclarar el puntaje correcto para este criterio. /Términos de Referencia-4.1.4-->19-20/"	Es una tabla de puntaje que se da según el ofrecimiento de los valores agregados, los puntos asignados corresponden acorde a la oferta en meses dando como máximo para ese ítem 25 puntos y mínimo 10 puntos, así: 6 meses 25 puntos 4 meses 15 puntos 2 meses 10 puntos Aclaramos que al ser un valor agregado si no se ofertan meses para este servicio la calificación será 0.
OLIMPIAIT	**19**	"SOLICITUD DE ACLARACIÓN: Se solicita confirmar si se requieren las tres certificaciones (SOC1, SOC2 y SOC3) simultáneamente o si basta con una de ellas. Las certificaciones SOC son costosas y no todas las empresas tienen las tres. /Anexo 3 - Certificaciones-Ítem 8-->N/A/"	Se debe suministrar la certificación SOC 2, cuyo enfoque es la gestión de la Seguridad de la Información.
OLIMPIAIT	**20**	"SOLICITUD DE ACLARACIÓN: Considerando el volumen de documentación requerida (evidencias de cumplimiento de más de 100 requisitos), se solicita confirmar el límite de tamaño de archivos adjuntos aceptado o establecer mecanismo alternativo para documentos de gran tamaño. /Términos de Referencia-2.1-->9/"	Se debe cumplir con la evidencia solicitada, según el Anexo No. 3, el tamaño de archivos adjuntos es el que deben cumplir con la evidencia misma de RFP, se aceptan archivos comprimidos.
OLIMPIAIT	**21**	"SOLICITUD DE ACLARACIÓN: Se solicita aclarar la frecuencia de las pruebas de phishing y qué se entiende por 'licencias reutilizables'. ¿Son 200 usuarios únicos o 200 intentos de phishing durante todo el contrato? /Anexo 3 - Servicio_EthicalHacking-Ítem 6-->N/A/"	Las licencias no estarán asociadas a usuarios nombrados, sino que se pueda ejecutar campañas con distinto grupos de personas y áreas de la entidad así las cosas que la licencia sea reutilizable nos dan para que en el año se hagan pruebas de 2400 usuarios.
OLIMPIAIT	**22**	"SOLICITUD DE ACLARACIÓN: Se solicita el listado completo y definitivo de todas las marcas/patrimonios autónomos a monitorear, incluyendo dominios, redes sociales y palabras clave específicas para cada uno. /Anexo 3 - Servicio_Marca-Ítem 1-->N/A/"	Como se indica en Anexo No. 3, el número exacto de dominios son 7. Equivalentes a: Dominio Fiducoldex y 6 negocios fiduciarios administrados.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
OLIMPIAIT	**23**	"OBSERVACIÓN: La exigencia de póliza con 4 meses adicionales para cumplimiento es estándar. Sin embargo, se solicita confirmar si el valor base para el cálculo del 20% incluye o excluye el IVA. /Términos de Referencia-5.5-->23/"	El valor de los amparos de las pólizas se calcula sobre el valor total del Contrato, es decir, base + IVA.
OLIMPIAIT	**24**	"SOLICITUD DE ACLARACIÓN: Este requisito parece más exigente que el Anexo 3 para servicios en nube. Se solicita confirmar cuáles certificaciones son obligatorias vs. deseables para servicios SOC que operan remotamente. /Anexo 4 - FT-GRI-023-Sección 4-->N/A/"	Esta información se espera conocer de parte del proveedor, teniendo en cuenta que se debe garantizar el cumplimiento normativo exigido por la Superintendencia Financiera de Colombia
OLIMPIAIT	**25**	"SOLICITUD DE MODIFICACIÓN: Se sugiere ampliar el período de experiencia válida a partir del 1 de enero de 2020, considerando que muchos contratos SOC de largo plazo iniciados antes de 2022 siguen siendo experiencia relevante y vigente. /Términos de Referencia-3.3.1.1-->15/"	No es posible atender favorablemente este requisito, dado que hace parte del alcance definido.
OLIMPIAIT	**26**	"SOLICITUD DE ACLARACIÓN: Se requiere conocer la arquitectura de red actual de FIDUCOLDEX (número de segmentos, VLANs, ubicaciones) para dimensionar correctamente la cantidad de sensores necesarios y su ubicación. /Anexo 3 - Servicio_Vulnerabilidades-Ítem 5-->N/A/"	En Anexo No. 3 se indica hasta 400 direcciones IP, así mismo, en el anexo se menciona que para proyectos de la fiduciaria es por demanda, lo que lo convierte es variable.
OLIMPIAIT	**27**	"SOLICITUD DE ACLARACIÓN: Se solicita a la entidad aclarar el alcance del requisito de borrado seguro de los datos en medios de almacenamiento, considerando que el objeto del proceso corresponde a un servicio de monitoreo SOC sobre plataformas existentes de la entidad, lo cual no necesariamente implica la provisión de infraestructura o medios de almacenamiento por parte del proponente; en este sentido, se entiende que dicha obligación debería aplicar únicamente cuando el contratista suministre o administre infraestructura, herramientas o almacenamiento propios donde se alojen datos de la entidad. /Anexo 3 - Certificaciones-Políticas-->34-->N/A/"	Esto aplica si durante la ejecución del servicio, el proponente debe almacenar o procesar información relacionada con la Fiduciaria.
OLIMPIAIT	**28**	"SOLICITUD DE ACLARACIÓN: Se solicita a la entidad aclarar el alcance de este requisito, considerando que en el marco del presente proceso el servicio corresponde a la operación y monitoreo sobre plataformas de seguridad existentes propiedad de la Fiduciaria, en las cuales los mecanismos de autenticación, incluyendo MFA, se encuentran embebidos y son gestionados directamente por la entidad; en este sentido, se entiende que dicha obligación debería aplicar únicamente en escenarios donde el proponente	El MFA, aplica para por ejemplo VPN acceso a Fiducoldex, acceso a las plataformas que se van a integrar con el SIEM de Fiducoldex.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
		suministre herramientas, consolas o plataformas propias para la prestación del servicio, por lo que se solicita precisar si este requisito es exigible en servicios de administración sobre herramientas existentes de la Fiduciaria o únicamente cuando el acceso se realice sobre plataformas provistas por el contratista. /Anexo 3 - Certificaciones-Políticas-->35-->N/A/"	
OLIMPIAIT	**29**	"SOLICITUD DE ACLARACIÓN: Se requiere a la entidad aclaración respecto a la infraestructura necesaria para la implementación y configuración de los conectores adicionales (nuevos logs) en Splunk. Específicamente, se solicita confirmar si los servidores o máquinas virtuales requeridos para el despliegue de los forwarders, heavy forwarders o cualquier componente de recolección de logs deben ser suministrados por el proponente como parte del servicio, o si FIDUCOLDEX proveerá dicha infraestructura. Esta definición es fundamental para dimensionar adecuadamente la propuesta técnica y económica del servicio SOC. /Anexo 3 - Servicio_SOC-->Ítem 1-->N/A/"	Como parte de la integración del servicio al SIEM actual, esta debe ser suministrada por el proveedor.
OLIMPIAIT	**30**	"SOLICITUD DE ACLARACIÓN: Se solicita aclaración respecto al alcance del servicio de análisis forense. Dado que este tipo de servicios especializados se cotiza habitualmente por horas de consultoría debido a su naturaleza variable y la imposibilidad de predecir su requerimiento, se requiere confirmar si FIDUCOLDEX tiene contemplada una bolsa de horas anuales para este servicio o si se manejará bajo demanda con facturación adicional. Esta definición es necesaria para estructurar adecuadamente la propuesta técnica y económica. /Anexo 3 - Servicio_SOC-->Ítem 53-->N/A/"	Como se indica en el Anexo No. 3, los análisis forenses hacen parte del alcance del servicio solicitado, Fiducoldex no cuenta con herramientas para este tipo de análisis, dado que no son actividades recurrentes, el número de estos ejercicios es variable.
OLIMPIAIT	**31**	"SOLICITUD DE ACLARACIÓN: Se solicita a la entidad aclarar el alcance del requisito relacionado con el servicio de análisis de sitios web (vulnerabilidades, brechas de seguridad, entre otros), considerando que este tipo de evaluación normalmente requiere el uso de herramientas especializadas diferentes a las empleadas en un servicio SOC tradicional; en este sentido, se solicita precisar si dicho servicio debe ejecutarse con herramientas definidas por la entidad o si el proponente puede hacer uso de herramientas propias debidamente licenciadas para la prestación del servicio; adicionalmente, se solicita confirmar si el alcance del análisis aplica sobre la totalidad de los activos web asociados al SOC o	La herramienta utilizada para el escaneo de vulnerabilidades debe ser aquella que el contratista utilice para prestación del servicio, tener en cuenta, que esta deber ser una licencia a nombre del contratista y no debe ser de tipo "Software Libre (Open Source)".

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
		sobre un conjunto específico de sitios, dominios o aplicaciones previamente definidos por la Fiduciaria. /Anexo 3 - Servicio_Vulnerabilidades-->17-->N/A/"	
OLIMPIAIT	**32**	"SOLICITUD DE ACLARACIÓN: Considerando el volumen de documentación requerida (evidencias de cumplimiento de más de 100 requisitos), se solicita confirmar el límite de tamaño de archivos adjuntos aceptado o establecer mecanismo alternativo para documentos de gran tamaño. /Términos de Referencia-->2,1-->9/"	Se debe cumplir con la evidencia solicitada, según el RFP, el tamaño de archivos adjuntos es el que deben cumplir con la evidencia misma de RFP, se aceptan archivos comprimidos.
OLIMPIAIT	**33**	"SOLICITUD DE ACLARACIÓN: Se solicita a la entidad precisar la cantidad estimada de eventos de take down que deben contemplarse dentro del alcance del servicio o si se espera que este sea bajo demanda, así como definir si existe un volumen mínimo o máximo esperado, con el fin de que los proponentes puedan dimensionar adecuadamente la solución y estructurar de forma correcta la propuesta técnica y económica. /Anexo 3 - Servicio_Marca-->17-->N/A/"	Actualmente Fiducoldex no ha tenido este tipo de eventos, sin embargo, esto no implica que no sucedan. Adicionalmente, actualmente este tipo de eventos se consideran "variables" y no se tiene el número de eventos.
OLIMPIAIT	**34**	"SOLICITUD DE ACLARACIÓN: Se solicita a la entidad el inventario estimado de activos a monitorear, incluyendo el número de dominios, subdominios, direcciones IP públicas y palabras clave asociadas a la entidad y sus marcas, considerando que estos elementos son fundamentales para dimensionar adecuadamente la solución, determinar el esfuerzo operativo requerido y estructurar de manera correcta la propuesta técnica y económica del servicio. /Anexo 3 - Servicio_Marca-->N/A-->N/A/"	Como se indica en Anexo No. 3, el número exacto de dominios son 7. Equivalentes a: Dominio Fiducóldex y 6 negocios fiduciarios administrados. El detalle de estos activos, solo se informarán al proveedor que sea adjudicado posterior a la firma de los debidos acuerdos de confidencialidad.
OLIMPIAIT	**35**	"Solicitamos respetuosamente a la entidad evaluar la posibilidad de ajustar el número mínimo exigido de certificaciones de cuatro (4) a tres (3), manteniendo las demás condiciones. Esta solicitud se fundamenta en que la exigencia simultánea de múltiples servicios altamente especializados dentro de cada certificación, sumado al requisito de cuantía individual significativa, limita considerablemente la pluralidad de oferentes, especialmente considerando que este tipo de servicios suelen ser contratados de manera independiente o por fases dentro de las organizaciones, y no necesariamente bajo un único contrato integral. Permitir la acreditación mediante tres (3) certificaciones no disminuye la capacidad técnica ni la experiencia requerida para la adecuada	No es posible atender favorablemente este requisito, dado que hace parte del alcance definido para el servicio.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
		ejecución del contrato, sino que favorece una mayor participación de proponentes idóneos, fortalece los principios de pluralidad, selección objetiva y libre concurrencia, y permite a la entidad contar con un escenario más amplio y competitivo para la evaluación de ofertas. /260422 Términos de Referencia SOC-->3.3.1.1 -->Certificaciones experiencia/"	
OLIMPIAIT	**36**	"Solicitamos aclarar si dicha Certificacion de experiencia se puede acreditarse mediante proyectos ejecutados en sectores con exigencias equivalentes de seguridad, cumplimiento y operaciones críticas, tales como salud, gobierno, telecomunicaciones o infraestructura crítica. /260422 Términos de Referencia SOC-->3.3.1.2 -->Certificación SIEM/"	Al ser Fiducoldex una sociedad de servicios financieros, se espera que las certificaciones estén relacionadas con el sector financiero.
OLIMPIAIT	**37**	"Solicitamos precisar los alcances del Servicio de Monitoreo de marca que identifica el pliego /260422 Términos de Referencia SOC-->5.2.1.-->Monitoreo de Marca/"	Como se indica en Anexo No. 3, el número exacto de dominios son 7. Equivalentes a: Dominio Fiducóldex y 6 negocios fiduciarios administrados, el detalle está estipulado en los 13 Ítem de alcance del servicio.
OLIMPIAIT	**38**	"Se menciona los servicios de Red Team, pero no se define cantidad de ejercicios, profundidad técnica ni alcance de activos /260422 Términos de Referencia SOC-->5.2.1.-->Servicios RED TEAM/"	Como se indica en Anexo No. 3, el alcance del ejercicio de Red Team se basa en la explotación avanzada de vulnerabilidades dentro de un ambiente contralado, a partir de ventanas de servicio coordinadas por la entidad.
OLIMPIAIT	**39**	"Solicitamos evaluar la inclusión de un mecanismo de compensación razonable cuando existan inversiones iniciales relevantes en herramientas, personal o licenciamiento dedicados al servicio. /260422 Términos de Referencia SOC-->5.3.-->Terminación anticipada/"	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas de contratación de la sociedad fiduciaria y lo establecido en su Manual de Contratación.
OLIMPIAIT	**40**	"La entidad cuenta con herramienta de gestión de vulnerabilidades, o esta debe ser proporcionada por el oferente y entregada a la entidad para la gestión del servicio/260422 Términos de Referencia SOC-->2.1.-->/"	Como se indica en el Anexo No. 3, los análisis de vulnerabilidades y ethical hacking hacen parte del alcance del servicio solicitado, Fiducoldex no cuenta con herramientas de análisis de vulnerabilidades.
OLIMPIAIT	**41**	"Nos gustaría la aclaratoria sobre si proponente debe monitorear la plataforma computacional - infraestructura tecnológica y los servicios informáticos críticos, utilizando la herramienta SPLUNK o queda a criterio del proponente usar otra herramienta que tenga certificada/Anexo 3 Requisitos_RFP_Marzo_2026 - V1.1 (1)-->3-->Herramienta SPLUNK/"	Lo que Fiducoldex busca es que el proponente cubra con los requerimientos del presente proceso y el uso del SIEM de la entidad, posterior a ello, los requerimientos técnicos para la implementación serán parte los criterios establecidos en la contratación, así como la integración de

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
			servicios especiales, que son responsabilidad por parte del proveedor.
OLIMPIAIT	**42**	"¿Por favor confirmar si para la configuración de nuevos conectores, la entidad suministraría el licenciamiento adicional de Splunk o este deberá ser asumido por el Contratista? /Anexo 3 Requisitos-->1-->El proponente debe gestionar, operar, configurar y mantenber el servicio del SOC por medio del SIEM propio de la Fiduciaria (Splunk), lo siguiente:No. de servidores a Monitorear 100No. de Firewalls a Monitorear 4No. de Usuarios Privilegados a Monitorear 40No. de cuentas en redes sociales 10No. de aplicaciones web expuestas en internet 190Nota: Así mismo, incluir y configurar los conectores adicionales (Nuevos logs) en la herramienta Splunk, que se requieran para la gestión del servicio. /"	Todas las configuraciones, mantenimiento y soporte de la licencia actual, están a cargo del proveedor adjudicado, es decir que en caso de requerirse algún tema adicional el proveedor debe asumirlo
OLIMPIAIT	**43**	"Agradecemos informar a la entidad como está conformado su equipo de respuesta de incidentes y su nivel de especialización. /Anexo 3 Requisitos-->44-->El proponente debe brindar soporte a la gestión de incidentes a través de un equipo de respuesta a incidentes que soportará las actividades a desarrollar en caso de presentarse un incidente, el cual debe integrarse al equipo de respuesta de incidentes de la fiduciaria, soportando el análisis forense respectivo. /"	Esta información se compartiría al adjudicatario una vez exista un contrato suscrito.
OLIMPIAIT	**44**	"Estas funcionalidades que el proponente debe incluir e integrar con el SIEM de la entidad, se permiten que sean de tipo Software libre siempre y cuando se cumplan con las características técnicas y de niveles de servicio solicitados?/Anexo 3 Requisitos-->50-->El proponente debe implementar en su servicio propuesto e integrarlo al SIEM de la fiduciaria, características y/o funcionalidades SOAR, características y/o funcionalidades para analizar el comportamiento de usuarios UEBA, características y/o funcionalidades XDR, respuesta anti malware, respuesta anti ransomware, Machine Learning, Inteligencia Artificial (IA), EDR, Casos de uso Ilimitados./"	Por política de la Fiduciaria, no se permite el uso de software sin licencia, así que se debe tener en cuenta que el proveedor puede implementar alguna de ellas dentro del servicio, pero esta debe ser licenciada.
OLIMPIAIT	**45**	"Por favor aclarar la frecuencia esperada de estas copias de respaldo/Anexo 3 Requisitos-->51-->El proponente debe realizar copias de respaldo configuración herramientas de monitoreo/"	Las copias de seguridad deben hacerse semanal

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
OLIMPIAIT	**46**	"Por favor aclarar si el servicio de análisis forense se cotizaría por separado o hasta qué punto de análisis forense espera la entidad que sea ofrecido dentro de la propuesta/Anexo 3 Requisitos-->53-->El proponente debe contar con la posibilidad de ofrecer el servicio de análisis forense/"	Lo que la Fiduciaria espera contratar es el soporte a demanda del servicio forense, dado que actualmente no se cuenta con un número promedio de este tipo de requerimientos dada su no ocurrencia, sin embargo, esto no garantiza que no suceda. Por lo anterior esto debe estar incluido dentro del valor total del Contrato.
OLIMPIAIT	**47**	a) "¿El appliance debe ser físico y quedar instalado en el centro de datos de la entidad, o se permiten soluciones virtuales/cloud?/ b) Anexo 3 Requisitos-->1-->El proponente debe realizar análisis de vulnerabilidades de hasta 400 direcciones IP basado en un hardware de propósito específico (Appliance), en cumplimiento de la Circular Externa 008 de junio 2018 de la SFC, sobre la infraestructura de Fiducoldex y los negocios administrados tanto a nivel interno como externo, con una periodicidad mínima trimestral (4)./"	a) Para el appliance o servidor que será utilizado por el contratista para el escaneo de vulnerabilidades, el contratista podrá implementar el esquema que considere pertinente para la prestación del servicio, lo importante es que las soluciones utilizadas estén debidamente licenciadas a nombre del contratista. b) Como se informó en Anexo No. 3, hasta 400 ips; para escaneo vulnerabilidades.
OLIMPIAIT	**48**	"Por favor indicarnos si dentro de las 400 Ips indicadas en el numeral 1, están incluidos todos los activos tecnológicos de Fiduciaria/Anexo 3 Requisitos-->1-->El proponente con su solución debe poder detectar todos los activos instalados en la infraestructura tecnológica de la red de la Fiduciaria. /"	Se encuentran incluidos todos los activos.
OLIMPIAIT	**49**	"Agradecemos a la entidad anclarnos ¿A cuántos directivos específicos se debe monitorear y cuantos Patrimonios autónomos? /Anexo 3 Requisitos-->12-->El proponente deberá realizar monitoreo de marca de directivos de la Fiduciaria y sus Patrimonios Autónomos. /"	Como se indicó en Anexo No. 3, se deberán monitorear como mínimo 15 objetivos (marcas / dominios)
OLIMPIAIT	**50**	"¿Cuál es el alcance específico en términos de objetivos (IPs, aplicaciones o procesos de negocio) para este ejercicio de Red Team? /Anexo 3 Requisitos-->5-->El proponente debe realizar un ejercicio de Pruebas de seguridad Red Team (Pruebas de explotación avanzada y controlada de vulnerabilidades en ventanas de mantenimiento coordinadas con la Dirección de Seguridad de la Información de la Fiduciaria) /"	Como se informó en Anexo No. 3, para el Ethical Hacking, hasta 400 ips; para Red Team, explotación avanzada de vulnerabilidades en entornos controlados y en ventanas coordinadas por la entidad.
OLIMPIAIT	**51**	"En el marco del proceso de selección y con el fin de estructurar una propuesta técnica y económica eficiente, sostenible y alineada con las necesidades de la Entidad, solicitamos respetuosamente se aclare la posibilidad de que el proponente pueda integrar dentro de su oferta	Por política de la Fiduciaria, no se permite el uso de software sin licencia, así que se debe tener en cuenta que el proveedor puede implementar alguna de las soluciones propuestas.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
		una solución SIEM/SOAR de tecnología Open Source de reconocimiento y adopción global, siempre que esta cumpla con los requerimientos funcionales, operativos y de seguridad exigidos en el pliego./CONDICIONES GENERALES-->-->SIEM OPENSOURCE/"	
OLIMPIAIT	**52**	"Se solicita a la entidad indicar si certificaciones como ISO 27001, ISO 20000-1, así como la certificación de que el SOC del proveedor este inscrito en el FIRST (Forum of Incident Response and Security Teams) pueden ser consideradas como parte de los criterios de evaluación con % de ponderación./260422 Términos de Referencia SOC-->4.1.-->EVALUACIÓN Y PONDERACIÓN DE PROPUESTAS/"	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas del proceso de contratación y su anexo técnico.
OLIMPIAIT	**53**	"Se solicita a la entidad ampliar el tiempo del cronograma./Proceso-->260422 Términos de Referencia Servicios de Monitoreo SOC (Security Operation Center)--> PÁG 7CRONOGRAMA DE LA INVITACIÓN"	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas del proceso de contratación y su anexo técnico.
TIGO	**54**	"Atentamente solicitamos a la entidad aclarar y reconsiderar el numeral que indica que no se aceptan proponentes en consorcio o unión temporal, dado que estas figuras se encuentran legalmente habilitadas y su exclusión podría restringir la participación de potenciales oferentes./Proceso-->260422 Términos de Referencia Servicios de Monitoreo SOC (Security Operation Center)--> PÁG 123.1. QUIENES PUEDEN SER PROPONENTES:NOTA DOS: No se aceptan proponentes en formas asociativas tipo consorcios o uniones temporales."	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas de contratación de la sociedad fiduciaria y lo establecido en su Manual de Contratación
TIGO	**55**	"""¿La posibilidad de subcontratar personal para la ejecución de los servicios implica también la formación de una unión temporal, o son conceptos y figuras separadas según los términos de la invitación?""/Proceso-->260422 Términos de Referencia Servicios de Monitoreo SOC (Security Operation Center)--> PÁG 123.1. QUIENES PUEDEN SER PROPONENTES:NOTA DOS: No se aceptan proponentes en formas asociativas tipo consorcios o uniones temporales."	El futuro contratista debe contar con el equipo descrito en la Adenda No. 1 que modifica el Anexo No. 3. El futuro Contratista es responsable por el cumplimiento del Contrato, por lo que la figura de subcontratación es diferente a la de Unión temporal ya que el único responsable ante la Fiduciaria será el futuro contratista.
TIGO	**56**	"Solicitamos a la entidad validar las penalidades dobles, si existe un descuento por ANS para el servicio de esta naturaleza no deberían incluirse multas ni cláusula penal ya que se afecta el equilibrio financiero del contrato. Se solicita su eliminación. /Proceso-->260422 Términos de Referencia Servicios de Monitoreo SOC (Security	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas de contratación de la sociedad fiduciaria y lo establecido en su Manual de Contratación

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
		Operation Center)--> PÁG 24CLÁUSULA PENALMULTASPÓLIZAS."	
TIGO	**57**	"Se solicita limitar la cuantía de los perjuicios y que estos sean debidamente probados/Jurídica-->Términos de Referencia Servicios de Monitoreo SOC--> PÁG 31.7. CONFIDENCIALIDAD DE LA INFORMACIÓN, Quien incumpla sus obligaciones de reserva y las de garantizar la reserva de sus potenciales subcontratistas o empleados, pagará a FIDUCOLDEX una suma equivalente al cinco por ciento (5%) del presupuesto asignado a esta invitación. La anterior suma se deberá como multa. Su pago no indemniza los perjuicios sufridos por FIDUCOLDEX ni limita en nada las posibilidades de reclamación de esta última por los daños sufridos."	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas de contratación de la sociedad fiduciaria y lo establecido en su Manual de Contratación. La cuantía está establecida por el 5% del presupuesto asignado a la invitación en el numeral 1.7 de los Términos de referencia.
TIGO	**58**	"Se solicita la disminución de los porcentajes de los amparos de las Pólizas, pues los amparos deben ser proporcionales a la naturaleza del servicio a prestar, al valor del contrato y su plazo. Por ello se solicita disminuir al 10% la póliza de cumplimiento y 2 meses más; 10% póliza calidad del servicio y 2 meses más; y por último la vigencia de la póliza de salarios 2 meses más. /Jurídica-->Términos de Referencia Servicios de Monitoreo SOC--> PÁG 62.3. DURACIÓN DEL CONTRATO... No obstante lo anterior, el contrato que se suscriba como resultado del presente proceso de selección, podrá ser terminado de manera anticipada por FIDUCOLDEX, en cualquier tiempo, dando aviso por escrito de tal hecho al Contratista con una antelación mínima de quince (15) días calendario a la fecha de terminación, previo reconocimiento y pago de los servicios prestados y recibidos a entera satisfacción por parte de FIDUCOLDEX, sin que este hecho genere obligación alguna de indemnizar o bonificar al Contratista."	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas de contratación de la sociedad fiduciaria y lo establecido en su Manual de Contratación
TIGO	**59**	"Se solicita la disminución de los porcentajes de los amparos de las Pólizas, pues los amparos deben ser proporcionales a la naturaleza del servicio a prestar, al valor del contrato y su plazo. Por ello se solicita disminuir al 10% la póliza de cumplimiento y 2 meses más; 10% póliza calidad del servicio y 2 meses más; y por último la vigencia de la póliza de salarios 2 meses más/Jurídica--	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas de contratación de la sociedad fiduciaria y lo establecido en su Manual de Contratación

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
		>Términos de Referencia Servicios de Monitoreo SOC--> PÁG 235.5. POLIZAS"	
TIGO	**60**	"Se propone la cláusula penal bilateral en los siguientes términos: El incumplimiento por cualquiera de LAS PARTES de la totalidad de las obligaciones derivadas de este contrato dará derecho a aquella que hubiere cumplido o se hubiere allanado a cumplir, para exigir inmediatamente a título de pena aplicable, a quien no cumplió o no se allanó a cumplir, el pago de una suma equivalente al diez por ciento (10%) del valor total de este contrato, la cual será exigible por la vía ejecutiva sin necesidad de requerimiento o constitución en mora, derechos estos a los cuales renuncian LAS PARTES en su recíproco beneficio. Cuando se trate de un incumplimiento parcial, LAS PARTES de común acuerdo tasarán el porcentaje correspondiente a título de sanción. Igualmente, LAS PARTES tasarán independientemente al porcentaje de la sanción, los perjuicios ocasionados por el incumplimiento parcial. /Jurídica-->Términos de Referencia Servicios de Monitoreo SOC--> PÁG 245.7. CLÁUSULA PENAL"	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas de contratación de la sociedad fiduciaria y lo establecido en su Manual de Contratación.
TIGO	**61**	"Se solicita, que esta facultad proceda siempre y cuando la responsabilidad del contratista se encuentre debidamente probada en vía judicial y haya condena en firme. De igual forma se solicita que, se limite la indemnidad al valor del contrato y al plazo del mismo./Jurídica-->Términos de Referencia Servicios de Monitoreo SOC--> PÁG 255.11 INDEMNIDAD"	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas de contratación de la sociedad fiduciaria y lo establecido en su Manual de Contratación
TIGO	**62**	"Al respecto, consideramos que la exigencia simultánea de un alto número de certificaciones y una cuantía elevada individual por cada contrato puede resultar restrictiva de la participación, toda vez que este tipo de servicios especializados en ciberseguridad suelen contratarse de manera modular o por componentes, aun cuando el proveedor cuente con experiencia técnica sólida y debidamente comprobable.En este sentido, solicitamos respetuosamente a la Entidad evaluar la posibilidad de disminuir la cantidad de certificaciones exigidas, a un minimo dos (2) certificaciones; o, en caso de no considerarse viable dicha modificación, que se permita que la cuantía exigida de SEISCIENTOS MILLONES DE	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas del proceso de contratación y su anexo técnico.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
		PESOS ($600.000.000) sea acreditada mediante la sumatoria del valor de todas las certificaciones aportadas, siempre que estas correspondan a contratos ejecutados o en ejecución dentro del período señalado y cuyo objeto esté alineado con los servicios requeridos.La adopción de alguna de estas alternativas permitiría verificar adecuadamente la experiencia del proponente, sin afectar la idoneidad técnica del contratista ni los intereses de la Entidad, y contribuiría a garantizar los principios de libre concurrencia, pluralidad de oferentes y selección objetiva./General-->Términos de Referencia Servicios de Monitoreo SOC--> PÁG 153.3.1.1 Certificación de experiencia:El proponente deberá presentar como mínimo cuatro (4) certificaciones sobre contratos ejecutados o en ejecución, que se hayan suscrito a partir del 1 de enero de 2022 y hasta la fecha de presentación de la propuesta, cuyo objeto sea o haya incluido Servicios de Monitoreo de SOC, análisis de vulnerabilidades, pruebas de ethical, monitoreo de marca, pruebas de red team y pruebas de phishing, cuya cuantía por cada Certificación de contrato sea o haya sido, igual o superior a SEISCIENTOS MILLONES DE PESOS ($600.000.000) o su equivalente en dólares americanos, en caso de que el contrato se haya pactado en una moneda diferente al peso colombiano."	
TIGO	**63**	"Se solicita revisar el numeral 3.3.1.2, toda vez que la exigencia de certificaciones adicionales específicas en implementación, gestión y configuración de plataformas SIEM para el sector financiero resulta excesiva y restrictiva de la competencia, al duplicar requisitos ya evaluados mediante las certificaciones de experiencia del numeral 3.3.1.1. En dicho numeral se acredita de manera suficiente la ejecución de servicios SOC y operación de SIEM, incluyendo actividades de implementación, gestión y configuración. En consecuencia, se solicita que el cumplimiento del numeral 3.3.1.1 se entienda como suficiente para acreditar el requisito establecido en el numeral 3.3.1.2, evitando redundancias que limiten la pluralidad de oferentes sin aportar mayor valor a la verificación de la capacidad técnica./General-->Términos de Referencia Servicios de Monitoreo SOC--> PÁG 163.3.1.2 Certificaciones en Implementación, Gestión y Configuración de SIEM.El Proponente deberá presentar Certificación	No es posible atender favorablemente este requisito, dado que hace parte del alcance definido para el servicio.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
		por escrito emitida por Clientes del Proponente (mínimo 5 años) y/o fabricantes, que demuestren que cuenta con la experiencia y/o certificación en implementación, gestión y configuración de diferentes marcas de Plataformas SIEM, y que estos proyectos y/o servicios (SOC SIEM) fueron implementados para el sector financiero."	
TIGO	**64**	"Se solicita a la Entidad amablemente indicar si actualmente cuenta con el Servicio de Monitoreo SOC y de ser así cuál es su proveedor actual. /General-->Términos de Referencia Servicios de Monitoreo SOC--> PÁG 1NA"	Sí, actualmente se cuenta con el servicio de SOC, sin embargo, esta información no se suministrará en esta etapa del proceso, solamente al proveedor adjudicatario.
TIGO	**65**	"Se solicita a la entidad amablemente se aclare la inconsistencia en la cantidad de campañas de Ethical Hacking: el TDR principal menciona 1 al año, mientras el Anexo 3 exige 2 ejercicios al año con retest./Técnica-->TDR 1.1.c / 2.1.c / 5.2.1 vs Anexo 3 Servicio_EthicalHacking ítem 1--> PÁG 1ITEM 1"	La campaña de Ethical Hacking será 1 al año, favor ver Adenda No. 1 que modifica el Anexo No. 3
TIGO	**66**	"Confirmar si el servicio de Red Team corresponde a un solo ejercicio anual o a más de una campaña, y delimitar si incluye persistencia, movimiento lateral y exfiltración controlada. /Técnica-->TDR 1.1.h / Anexo 3 Servicio_EthicalHacking ítem 5--> PÁG 1ITEM 5"	Este es un ejercicio anual y se enfoca en lo siguiente: "Servicio de Red Team: explotación avanzada y controlada de vulnerabilidades en ventanas de mantenimiento coordinadas".
TIGO	**67**	"Definir el alcance exacto de 'soporte a las pruebas de ataque cibernético' y de los dos simulacros de incidente: tabletop, purple team, técnico en productivo o laboratorio./Técnica-->TDR 1.1.e / Anexo 3 Servicio_EthicalHacking ítem 8--> PÁG ITEM 8"	El soporte solicitado para este tipo de ejercicios es de tipo "consultivo", en caso de que la entidad lo decida realizar.
TIGO	**68**	"Confirmar si 'remediar las deficiencias de seguridad' del Ethical Hacking implica ejecución hands-on del proveedor o si el alcance es estrictamente consultivo con acompañamiento./Tecnica-->Anexo 3 Servicio_EthicalHacking ítem 3--> PÁG ITEM 3"	Las remediaciones estarán a cargo de la Fiduciaria, se acudirá al proveedor en modo "consultivo".
TIGO	**69**	"Confirmar la arquitectura y licenciamiento vigente de Splunk en Fiducoldex (ES, SOAR, UBA, ingestion, almacenamiento, conectores disponibles, soporte vigente)./Tecnica-->Anexo 3 Servicio_SOC ítems 1, 3, 50, 54--> PÁG ITEM 1, 3, 50, 54"	La Fiduciaria solo tiene licenciamiento para "SPLUNK", las demás aplicaciones las deberá suministrar e implementar el proveedor
TIGO	**70**	"Precisar si el proveedor debe asumir costos/licencias adicionales de Splunk por nuevos conectores, casos de uso o incremento de ingestión./Tecnica-->Anexo 3 Servicio_SOC ítem 1--> PÁG ITEM 1"	En caso de requerirse un nuevo conector debe ser asumido por el proveedor.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
TIGO	**71**	"Solicitar volumetría de eventos/EPS, retención actual en Splunk, número de fuentes y log sources críticos para modelar operación 7x24 y tuning./Tecnica-->Anexo 3 Servicio_SOC / uso de Splunk--> PÁG uso de Splunk"	La tasa es la siguiente: Eventos por segundo (EPS): EPS promedio: 624 eventos por segundo EPS máximo: 6,765 eventos por segundo
TIGO	**72**	"Aclarar qué patrimonios autónomos y negocios administrados hacen parte exacta del alcance del monitoreo de marca y del SOC durante la vigencia contractual./Tecnica-->TDR 1.1 / Anexo 3 Servicio_Marca ítem 1--> PÁG ITEM 1"	Esta información se suministrará por medio de acuerdo de confidencialidad al proveedor adjudicado.
TIGO	**73**	"Confirmar el número exacto de cuentas de redes sociales por cada patrimonio autónomo y directivo, y las plataformas objetivo para monitoreo/takedown./Tecnica-->Anexo 3 Servicio_SOC ítem 1 / Servicio_Marca ítems 6, 12, 13--> PÁG ITEM 6, 12, 13"	Máximo 15 cuentas
TIGO	**74**	"Definir si el monitoreo de directivos contempla solo detección o también acompañamiento de takedown y gestión de BEC/suplantación. /Técnica-->Anexo 3 Servicio_Marca ítems 12 y 13--> PÁG ITEM 12, 13"	El monitoreo de marca debe contemplar todas las fases, desde la detección hasta su inhabilitación.
TIGO	**75**	"Aclarar si las 400 direcciones IP del servicio de vulnerabilidades son internas + externas en total o por campaña, y si incluyen activos cloud / web apps / appliances./Técnica-->Anexo 3 Servicio_Vulnerabilidades ítem 1--> PÁG ITEM 1"	Este análisis contempla Ips internas y externas (pueden incluir nube).
TIGO	**76**	"Confirmar si el análisis de sitios web del servicio de vulnerabilidades es adicional a las 190 aplicaciones expuestas informadas para SOC o si forman parte del mismo universo. /Técnica-->Anexo 3 Servicio_SOC ítem 1 / Servicio_Vulnerabilidades ítems 11 y 14--> PÁG ITEM 11 , 14"	Hacen parte del "universo" de activos analizados.
TIGO	**77**	"Precisar si el appliance de vulnerabilidades debe quedar on-premise, en comodato o como servicio temporal administrado por el proveedor. /Técnica-->Anexo 3 Servicio_Vulnerabilidades ítems 1 y 4--> PÁG ITEM 1, 4"	Esta herramienta queda a discreción por parte del proveedor en cuanto a su implementación.
TIGO	**78**	"Definir si el phishing de 200 usuarios corresponde a una sola población fija o a campañas reutilizables con rotación de usuarios durante el año. /Técnica-->Anexo 3 Servicio_EthicalHacking ítem 6--> PÁG ITEM 6"	Corresponde a campañas reutilizables y con rotación de usuarios.
TIGO	**79**	"Precisar si el análisis de código SAST/DAST a demanda debe incluirse en el precio base o si se evaluará solo como valor agregado opcional. /Técnica-->TDR 4.1.3--> PÁG TDR 4.1.3"	El análisis de código se reitera que se realizaría por demanda, dado que este tipo de pruebas puede ser variable en cuanto a su cantidad.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
TIGO	**80**	"Aclarar la inconsistencia del criterio 'Valores Agregados': el texto menciona 5 puntos, pero la tabla y el total del cuadro de evaluación asignan hasta 25 puntos. /Técnica-->TDR 4.1 / 4.1.4 / tabla de puntajes--> PÁG tabla de puntajes"	Es una tabla de puntaje que se da según el ofrecimiento de los valores agregados, los puntos asignados corresponden acorde a la oferta en meses dando como máximo para ese ítem 25 puntos y mínimo 10 puntos, así: 6 meses 25 puntos 4 meses 15 puntos 2 meses 10 puntos Aclaramos que al ser un valor agregado si no se ofertan meses para este servicio la calificación será 0.
TIGO	**81**	"Confirmar si la PoC del SIEM del proveedor debe ser obligatoriamente sin costo para la entidad o si puede presentarse como bonificación condicionada. /Técnica-->TDR 4.1.4--> PÁG TDR 4.1.4"	Debe ser sin costo para la Fiduciaria, pues es un valor agregado.
TIGO	**82**	"Validar si la entidad aceptará propuesta con desglose por servicio y adicionalmente una propuesta consolidada, dada la exigencia de valores desagregados por componente. /Técnica-->TDR 2.10 Nota 4--> PÁG TDR 2.10 Nota 4"	La propuesta debe estar discriminada por los conceptos exigidos en la TDR, así como se indica en los mismos.
TIGO	**83**	"Solicitar precisión sobre el plazo de pago en días calendario/hábiles, ya que el TDR habla de mensualidades vencidas, pero no fija número de días para desembolso. /Técnica-->TDR 2.5 / 5.4--> PÁG TDR 2.5 / 5.4"	Los pagos son mensuales (vencidos), el proveedor debe radicar su factura hasta el día 24 de cada mes.
TIGO	**84**	"Aclarar la diferencia entre el preaviso de terminación anticipada: 15 días en el numeral 2.3 y 10 días en la cláusula 5.3./Técnica-->TDR 2.3 vs 5.3--> PÁG TDR 2.3 vs 5.3"	Por favor consultar la Adenda No. 1
TIGO	**85**	"Confirmar si la póliza de 'calidad de los bienes' aplica cuando la solución se presta mayoritariamente como servicio gestionado sin transferencia de hardware a la entidad. /Técnica-->TDR 5.5--> PÁG TDR 5.5"	Es correcta la interpretación, no hay transferencia de Hardware a la Fiduciaria.
TIGO	**86**	"Confirmar si la prohibición de consorcios/UT impide un esquema donde TIGO sea aliado comercial y SONDA subcontratista/ejecutor especializado. /Técnica-->TDR 3.1 Nota 2--> PÁG TDR 3.1 Nota 2"	El Contrato únicamente se suscribirá acorde a lo manifestado en el capítulo III de los términos de Referencia, será el futuro contratista, quien responde en su totalidad por el cumplimiento del contrato ante Fiducoldex. Por lo que es responsabilidad exclusiva del futuro contratista la subcontratación para cumplir con los

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
			perfiles solicitados vía Adenda No. 1 que modifica el Anexo No. 3.
TIGO	**87**	"Precisar si la experiencia requerida puede acreditarse por el proponente principal más el subcontratista especializado o solo por el oferente que firma la propuesta. /Técnica-->TDR 3.3.1.1 y 3.3.1.2--> PÁG TDR 3.3.1.1 y 3.3.1.2"	Solamente se acredita por el proponente que firma la propuesta.
TIGO	**88**	"Confirmar si el presupuesto máximo sin IVA (COP 554,9M) es tope rígido inmodificable aun cuando se incorporen valores agregados puntuables. /Técnica-->TDR 2.4 / 4.1.3 / 4.1.4--> PÁG TDR 2.4 / 4.1.3 / 4.1.4"	Este presupuesto es el tope máximo aprobado por la entidad y es inmodificable.
TIGO	**89**	"Consultar si aceptan precios en pesos con fórmulas de reajuste cero durante 1 año o si requieren absorción total de variaciones de TRM y OEM durante toda la vigencia. /Técnica-->TDR 3.3.1.5 / Anexo 1 numeral 24--> PÁG TDR 3.3.1.5 / Anexo 1 numeral 24"	La propuesta debe ser entregada en valores en pesos colombianos.
TIGO	**90**	"Solicitar el tiempo objetivo de empalme/implementación esperada por Fiducoldex para definir una oferta competitiva en el criterio de 5 puntos. /Técnica-->TDR 4.1.2--> PÁG TDR 4.1.2"	El tiempo de Implementación será de 15 días.
TIGO	**91**	"Solicitar que las certificaciones exigidas para los perfiles del proyecto se acepten como opcionales y homologables por equivalencia según el rol o perfil requerido, permitiendo acreditar una o más certificaciones equivalentes del fabricante, de la industria o de ciberseguridad general. /Técnica-->Anexo 3 – Sección de perfiles / certificaciones del equipo de trabajo--> PÁG Anexo 3 – Sección de perfiles / certificaciones del equipo de trabajo"	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas del proceso de contratación y su anexo técnico.
TIGO	**92**	"Aclarar la cantidad exacta de objetivos a evaluar dentro del alcance de Ethical Hacking: número de aplicaciones, IPs, portales, servicios internos/externos y si el retest aplica sobre todos o solo sobre hallazgos críticos/altos. /Técnica-->TDR 1.1.c / 2.1.c / Anexo 3 Servicio_EthicalHacking--> PÁG TDR 1.1.c / 2.1.c / Anexo 3 Servicio_EthicalHacking"	Como se informó en Anexo No. 3, para el Ethical Hacking, hasta 400 ips; para Red Team, explotación avanzada de vulnerabilidades en entornos controlados y en ventanas coordinadas por la entidad.
TIGO	**93**	"Solicitamos respetuosamente a la entidad evaluar la posibilidad de flexibilizar el requisito relacionado con las certificaciones exigidas para los perfiles de soporte, permitiendo que estas sean consideradas como referentes y no como obligatorias, o bien aceptando certificaciones equivalentes y/o experiencia demostrable en	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas del proceso de contratación y su anexo técnico.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
		funciones similares. Lo anterior, teniendo en cuenta que una exigencia estricta de certificaciones específicas podría limitar la pluralidad de oferentes, cuando la combinación de experiencia relevante en entornos financieros y en la gestión de incidentes sobre plataformas SIEM puede garantizar de manera adecuada y efectiva el soporte requerido./Técnica-->TDR Capítulo III / requisitos de experiencia / Anexo 3 Servicio_SOC (uso de Splunk)--> PÁG TDR Capítulo III / requisitos de experiencia / Anexo 3 Servicio_SOC (uso de Splunk)"	
TIGO	**94**	"Aclarar si la herramienta para análisis de vulnerabilidades, las campañas de phishing y el servicio/herramienta de protección o monitoreo de marca será provista por la entidad o si debe ser suministrada integralmente por el proveedor dentro del alcance económico. /Técnica-->TDR 2.2 / Anexo 3 Servicio_Vulnerabilidades / Servicio_EthicalHacking / Servicio_Marca--> PÁG TDR 2.2 / Anexo 3 Servicio_Vulnerabilidades / Servicio_EthicalHacking / Servicio_Marca"	Las herramientas para la prestación de todo el servicio (a excepción del SIEM SPlunk, Licencia de Fiducoldex), deben ser implementados, gestionados, configurados y con soporte por parte del Proveedor Adjudicado.
TIGO	**95**	"Aclarar a qué se refiere la entidad cuando indica que el licenciamiento de phishing es 'reutilizable', especificando si corresponde a licencias reutilizables por campaña, por usuario rotativo o por vigencia anual, así como la frecuencia esperada de uso durante el contrato. /Técnica-->Anexo 3 Servicio_EthicalHacking – componente de campañas de phishing--> PÁG Anexo 3 Servicio_EthicalHacking – componente de campañas de phishing"	Es correcto, deben ser reutilizables y por campañas rotativas en el año.
GMS	**96**	Observación al requerimiento 3.3.1.2 - Certificaciones en Implementación, Gestión y Configuración de SIEM: Respecto a la acreditación de experiencia en plataformas SIEM/SOC, solicitamos amablemente a la Entidad permitir que las certificaciones presentadas no se limiten exclusivamente al sector financiero. Sugerimos que se acepte experiencia técnica comprobada en otros sectores de la economía colombiana durante los últimos tres (3) años, considerando que las capacidades de implementación y gestión de estas tecnologías son transversales y demuestran la idoneidad del oferente para proteger infraestructuras críticas de diversa índole.	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas del proceso de contratación y su anexo técnico.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
GMS	**97**	Observación al requerimiento 3.3.1.1 - Certificación de experiencia: Para promover una mayor pluralidad de oferentes, solicitamos amablemente a la Entidad considerar la modificación de este requisito permitiendo acreditar la experiencia con un mínimo de tres (3) certificaciones. En su defecto, sugerimos flexibilizar la cuantía mínima exigida por cada contrato reduciéndola a $500.000.000 COP, garantizando así una amplia participación sin comprometer la idoneidad técnica requerida.	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas del proceso de contratación y su anexo técnico.
GMS	**98**	Observación sobre la herramienta SIEM a utilizar: En relación con la indicación de operar el servicio a través del SIEM propio de la Fiduciaria (Splunk), solicitamos amablemente confirmar si el uso de esta herramienta específica es de carácter obligatorio. Agradecemos aclarar si la Entidad estuviese abierta a considerar el cambio y adopción de una plataforma SIEM alternativa propuesta por el oferente, en caso de que esta demuestre brindar mejores capacidades técnicas y operativas para el SOC.	Sí, es de carácter obligatorio ya que esta herramienta está licenciada por la entidad, a futuro se podría contemplar el cambio de esta herramienta, siempre y cuando se pueda hacer la PoC de los valores agregados.
GMS	**99**	Observación sobre los elementos a monitorear y aplicaciones web: Para garantizar un dimensionamiento técnico preciso en el SIEM, solicitamos amablemente indicar la marca y modelo de los cuatro (4) firewalls descritos. Adicionalmente, sobre las 190 aplicaciones web expuestas a internet, agradecemos confirmar si estas corresponden a servicios alojados en los servidores internos a integrar, o si el alcance esperado es su monitoreo externo continuo como parte del servicio de Protección de Marca Digital.	Esta información se entregará al proveedor adjudicado, previa firma de acuerdos de confidencialidad.
GMS	**100**	Observación sobre la herramienta para análisis de vulnerabilidades: Respecto al análisis de las 400 direcciones IP, solicitamos amablemente a la Entidad confirmar si es posible homologar el requerimiento de usar exclusivamente un hardware de propósito específico (Appliance).Proponemos que se permita el uso de herramientas tecnológicas alternativas (software, nube o agentes) que faciliten la gestión de vulnerabilidades sobre los activos, garantizando igualmente el cumplimiento de la Circular Externa 008 de la SFC.	Estará a cargo del proveedor el uso de herramientas, debidamente licenciadas, para la ejecución de análisis de vulnerabilidades.
GMS	**101**	Observación sobre servicio ethical hacking: Con el propósito de estandarizar las propuestas, asegurar condiciones de igualdad entre los oferentes y evitar desviaciones en la estimación del proyecto, solicitamos muy amablemente a la Fiduciaria	Como se informó en Anexo No. 3, para el Ethical Hacking, hasta 400 ips; para Red Team, explotación avanzada de vulnerabilidades en entornos

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
		aclarar el siguiente punto: ¿Cuál es la cantidad máxima y el tipo de activos de información (por ejemplo: número de direcciones IP públicas/privadas, cantidad de aplicaciones web, aplicaciones móviles, infraestructura de red, etc.) que conformarán el alcance para cada uno de los dos (2) ejercicios de Ethical Hacking solicitados? De no tenerse un alcance definido en este momento, ¿es posible establecer un límite máximo (ej. hasta "X" direcciones IP y "Y" aplicaciones web por ejercicio) o cotizar estos servicios bajo un esquema de bolsa de horas?	controlados y en ventanas coordinadas por la entidad. Frente al ejercicio de Ethical Hacking favor revisar Adenda No. 1. Frente a contemplar límites no es posible en atención a que se trata de valores variables.
GMS	**102**	Observación sobre servicio protección de marca: Con el fin de garantizar la correcta estimación técnica y financiera de la solución de monitoreo, y asegurar que todos los proponentes coticen bajo las mismas reglas de negocio, solicitamos amablemente a la Fiduciaria aclarar el alcance de este numeral: En el texto del requerimiento se listan explícitamente siete (7) entidades o marcas principales: - FIDUCOLDEX - Patrimonio Autónomo Procolombia - Patrimonio Autónomo Innpulsa Colombia - Patrimonio Autónomo Fontur - Patrimonio Autónomo Fondo Mujer Libre y Productiva - Patrimonio Autónomo Fondo Francisco José de Caldas - Patrimonio Autónomo Fondo para la Vida y la Biodiversidad ¿Es posible confirmar si el alcance del servicio de monitoreo de marca se limitará estrictamente a los siete (7) nombres/marcas mencionados explícitamente en el pliego (y sus dominios principales asociados)?	Como lo indican en la pregunta, claramente, el alcance sí corresponde al entendimiento sobre este ítem.
GMS	**103**	Observación sobre simulación de crisis: Con el propósito de asegurar que todos los oferentes coticen bajo las mismas condiciones y dimensionen adecuadamente el esfuerzo, solicitamos amablemente a la Fiduciaria aclarar la expectativa de este requerimiento: ¿Es posible confirmar si los dos (2) simulacros de incidente cibernético solicitados corresponden a un "¿Ejercicio de Escritorio" (Tabletop Exercise) enfocado en la validación académica y procedimental de los planes de respuesta, o si la expectativa de la Fiduciaria es realizar una emulación técnica activa de un ataque real (ej. ransomware) ejecutada sobre un ambiente controlado para evaluar los controles tecnológicos?	Estos ejercicios pueden combinar escenarios "de escritorio" o "replicación en ambientes tecnológicos" controlados.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co

PROPONENTE	No OBS.	PREGUNTA	RESPUESTA
GMS	**104**	Observación sobre certificaciones equipo: Con el fin de garantizar la pluralidad de oferentes y permitir que la Fiduciaria cuente con el respaldo de equipos de consultoría altamente maduros y experimentados, solicitamos amablemente evaluar la siguiente modificación: ¿Es posible que la Fiduciaria amplíe este requerimiento para aceptar certificaciones internacionales equivalentes o similares orientadas a la respuesta y gestión de incidentes (ej. GCIH, ECIH, CISM, CISSP, etc.) o, alternativamente, permita homologar este requisito mediante la acreditación de experiencia específica y certificada del equipo de consultores en la atención, gobierno y resolución de incidentes de ciberseguridad?	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas del proceso de contratación y su anexo técnico.

El presente documento se publica a los cinco (5) días del mes de mayo del año 2026, en la página web https:// www.fiducoldex.com, y en el Sistema Electrónico para la Contratación Pública – SECOP II – Modulo Publicitario, https://www.colombiacompra.gov.co/secop-ii

FIDUCOLDEX

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C.
PBX: (601) 7470909 o Línea Gratuita Nacional 01 8000 124211
fiducoldex@fiducoldex.com.co
www.fiducoldex.com.co