INVITACIÓN 1042

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 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 1042, **FIDUCOLDEX** procede a dar respuesta a las observaciones conforme al cronograma establecido, en los siguientes términos:

PROPONENTE	No OBSERVACIÓN	PREGUNTA	RESPUESTA
CROSSBORDER	**1**	Solicitamos amablemente a la Fiduciaria permitir la acreditación de experiencia mediante certificaciones de contratos suscritos a partir del 1 de enero de 2022. Lo anterior garantiza la pluralidad de oferentes y no afecta la prestación del servicio.	La entidad accede a modificar la fecha de las certificaciones por favor ver la Adenda No. 2

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
CROSSBORDER	**2**	Solicitamos respetuosamente a la Fiduciaria modificar el requisito de la siguiente manera: "El proponente deberá acreditar mínimo 6 años de experiencia continua en la prestación de servicios de SOC para entidades vigiladas por la Superintendencia Financiera de Colombia. Dicha experiencia se acreditará mediante certificaciones de contratos ejecutados expedidas por el representante legal o funcionario competente de la entidad contratante, que contengan como mínimo: objeto del contrato, fecha de inicio y terminación, valor y datos de contacto del contratante." Lo anterior se fundamenta en que el objeto del presente proceso está relacionado con servicios de SOC en un entorno regulado y de alto riesgo. Por esta razón, la experiencia en el sector financiero resulta ser un indicador de idoneidad técnica relevante, objetiva y verificable, que incluye la gestión de plataformas SIEM, aunque no sea específicamente con el SIEM que la entidad usa actualmente, especialmente cuando los requisitos solicitados por la Fiduciaria sobrepasan la capacidad de la herramienta actual, es decir, que se requiere integrar otras soluciones para dar cumplimiento a dichos requisitos. Es importante resaltar que las entidades del sector financiero exigen a los proveedores el cumplimiento de altos estándares de disponibilidad, confidencialidad e integridad de la información, lo cual garantiza que el proponente con experiencia en dicho sector cuenta con las capacidades técnicas y de gestión para prestar el servicio. Lo anterior garantiza la pluralidad de oferentes y no afecta la prestación del servicio.	La entidad modifica el requisito, por favor ver Adenda No. 2
CROSSBORDER	**3**	Solicitamos respetuosamente a la Fiduciaria evaluar este requisito, teniendo en cuenta que no estaba en el estudio de mercado y la integración de soluciones como SOAR, UEBA y XDR generarían un	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 OBSERVACIÓN	PREGUNTA	RESPUESTA
		costo importante que superaría el presupuesto oficial asignado.	
CROSSBORDER	**4**	Dado que se utilizará el SIEM actual licenciado por la Fiduciaria, se entiende que la infraestructura tecnológica de la Fiduciaria soporta la capacidad de almacenamiento para cumplir con el tiempo establecido para la retención de logs.	La capacidad de Retención de datos que cuenta la Fiduciaria es la siguiente: Configuraciones de retención 30 días 60 días 180 días
CROSSBORDER	**5**	Solicitamos respetuosamente a la Fiduciaria evaluar este requisito, teniendo en cuenta que no estaba en el estudio de mercado. Solicitamos indicar el número de análisis anual o una métrica que permita dimensionar el alcance y costo para cumplir dicho requisito.	No es posible atender favorablemente este requisito, dado que hace parte del alcance definido para el servicio y tampoco se cuenta con una métrica ya que es una actividad por demanda y es variable.
CROSSBORDER	**6**	Solicitamos respetuosamente a la Fiduciaria evaluar este requisito, teniendo en cuenta que no estaba en el estudio de mercado. Solicitamos indicar el número de plataformas y/o sistemas por año o una métrica que permita dimensionar el alcance y costo para cumplir dicho requisito.	No es posible atender favorablemente este requisito, dado que hace parte del alcance definido para el servicio y tampoco se cuenta con una métrica ya que es una actividad por demanda y es variable.
ETB	**7**	¿La forma de pago permite facturar pagos únicos al inicio del proyecto (ej. por costos de setup, implementación, hardware y licenciamiento de herramientas entregadas en el mes 1) o el 100% de la inversión inicial debe ser diferida y amortizada obligatoriamente dentro de las 12 mensualidades iguales?	No es viable acceder a este requerimiento en atención a que la forma de pago son mensualidades sucesivas a mes vencido, dividiendo el valor total del Contrato durante los 12 meses del servicio.
ETB	**8**	Considerando que se exigen plataformas EDR, SOAR, ML, XDR (Ítem 50 Anexo 4), ejercicios de Red Team, EH y licenciamiento de SOC, ¿este presupuesto contempla la adquisición de licenciamiento nuevo o asume que Fiducoldex ya cuenta con estas herramientas base operativas?	Fiducoldex no cuenta con estas herramientas y no va a adquirir licencias, el proponente debe contar con las licencias e implementarlas en su servicio. Así como integrarlas a nuestro SIEM. El presupuesto definido en los términos de referencia es el previsto para prestación del servicio y en cumplimiento a las aprobación otorgadas al interior de la sociedad fiduciaria.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
ETB	**9**	Con el propósito de presentar una oferta integral, competitiva y estrictamente alineada con los requerimientos técnicos y de ciberseguridad exigidos por la entidad, solicitamos de manera respetuosa la ampliación del plazo para el Cierre de la Invitación y entrega de propuestas por un término mínimo de 8 días hábiles, modificando la fecha actual del 8 de abril de 2026 para el 20 de abril de 2026. Esta solicitud se fundamenta en las siguientes consideraciones: Complejidad de la Arquitectura: El dimensionamiento de un modelo de SOC 7x24x365 que exige la integración de soluciones avanzadas como Splunk, SOAR, UEBA, EDR y XDR requiere un diseño arquitectónico minucioso con múltiples fabricantes Alineación Financiera y de Licenciamiento: Determinar el alcance exacto de los costos de ingesta de logs, almacenamiento en línea por seis meses y las plataformas para pruebas de Ethical Hacking y Red Team demanda cotizaciones formales con mayoristas y partners internacionales, cuyos tiempos de respuesta (SLA) superan los 5 días hábiles El cronograma actual establece que Fiducoldex publicará las respuestas a las observaciones el 6 de abril de 2026 y el cierre de la invitación es el 8 de abril de 2026. Contar con menos de 48 horas hábiles para incorporar las aclaraciones de la entidad en los modelos financieros, matrices de riesgo y arquitecturas técnicas resulta materialmente insuficiente y eleva el riesgo de presentar propuestas económicamente inviables o con vacíos técnicos	No es posible acceder favorablemente a este requerimiento dado que el plazo establecido está asignado por las políticas internas y las instancias de aprobación de la Fiduciaria en cumplimiento a requerimientos regulatorios y de control, siendo así la fechas establecidas no permiten la ampliación.
ETB	**10**	¿Existe un tiempo de gracia o ventana de implementación "Setup" (ej. 30 a 60 días) que no esté sujeto a penalidades de SLA (Ítem 63) mientras se afina el SIEM Splunk y se generan las líneas base?	El servicio deberá tener un tiempo de implementación (empalme) de 15 días hábiles y deberá iniciar operación a partir del 01 de junio de 2026. Aclaramos que el tiempo de implementación (empalme) no es facturable.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
ETB	**11**	Para un correcto dimensionamiento, solicitamos especificar el alcance volumétrico exacto: ¿Cuántas direcciones IP públicas/privadas, aplicaciones web, móviles o APIs se deben incluir en el escaneo trimestral y en el Ethical Hacking anual?	En el Anexo Técnico 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.
ETB	**12**	¿Cuál es el alcance del ejercicio de Red Team (¿incluye compromiso físico, Wireless, ingeniería social avanzada, evasión de EDR)? ¿Se requiere modelo Black-box, Gray-box o White-box?	Como se indica en el Anexo Técnico, 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.
ETB	**13**	¿A cuántos buzones/colaboradores se deben dirigir las campañas de Phishing y cuál es la frecuencia esperada (mensual, trimestral, anual)?	Como se indica en el Anexo Técnico, corresponde a 1000 buzones
ETB	**14**	¿Cuál es el número exacto de dominios, submarcas y Patrimonios Autónomos (PA) que deben ser incluidos en la plataforma de monitoreo de Threat Intelligence y protección de marca digital?	Como se indica en el Anexo Técnico, el número exacto de dominios son 7. Equivalentes a: Dominio Fiducóldex y 6 negocios fiduciarios administrados.
ETB	**15**	Si Fiducoldex ya cuenta con Splunk (Ítem 1), ¿cuál es el objetivo arquitectónico de este SIEM en prueba de concepto? ¿Debe ingestar los mismos datos que Splunk en paralelo (requiriendo doble ancho de banda/almacenamiento) o es para un entorno aislado?	En cuanto la ingesta de información será la misma que reciba el Splunk, el objetivo de esta PoC es evaluar otras herramientas.
ETB	**16**	Al ser pruebas "a demanda", ¿existe un límite máximo anual de líneas de código (SAST), repositorios o aplicaciones (DAST) a analizar para acotar el esfuerzo del servicio?	Este número 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.
ETB	**17**	Tratándose de un servicio de Ciberseguridad que gestiona incidentes críticos, ¿requiere la entidad una póliza de Responsabilidad Civil Extracontractual o Riesgos Cibernéticos (Cyber Insurance) por parte del proveedor?	Sí, la Fiduciaria solicitará al adjudicatario una vez suscrito el Contrato que en calidad de contratista constituya a favor de la Fiduciaria la garantía de Responsabilidad Civil Extracontractual en una compañía de seguros legalmente establecida y autorizada para funcionar en Colombia.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
ETB	**18**	¿Las multas establecidas en el numeral 5.6 son independientes y acumulables con los descuentos por incumplimiento de disponibilidad (SLA) definidos en el Ítem 63 del Anexo Técnico?	Sí, son independientes, de conformidad con lo establecido en los términos de referencia publicados y su anexo técnico.
ETB	**19**	Se observa que el requisito limita la concurrencia a proponentes que operen exclusivamente sobre una tecnología específica. Considerando que el objeto es la prestación de un servicio de monitoreo SOC y fortalecimiento de ciberseguridad, solicitamos a la entidad permitir la acreditación de este requisito mediante certificaciones en plataformas XDR (Extended Detection and Response) o SIEM de otros fabricantes tales como Stellar Cyber, Qradar, FortiSiem, etc.	La entidad modifica el requisito, por favor ver Adenda No. 2
ETB	**20**	Respecto al puntaje por 'Valores Agregados' (numeral 4.1.4), la entidad menciona la herramienta 'SIEM'. Teniendo en cuenta las tendencias tecnológicas actuales hacia la visibilidad unificada, ¿la entidad otorgará el mismo puntaje si el proponente pone a disposición una plataforma Open XDR que integre las funciones de SIEM, NDR y EDR, ofreciendo una capacidad de detección superior?"	Se dará el mismo puntaje, lo que requiere es la evaluación de otra herramienta que cumpla con los requerimientos exigidos, no obstante, esto no implica la asignación de un mayor puntaje.
ETB	**21**	Sugerimos muy respetuosamente, que el valor asegurado debe ser equivalente al diez por ciento (10%) del valor total del contrato, con una vigencia igual al plazo de ejecución de este y cuatro (4) Meses más. Lo anterior teniendo en cuenta la amplia trayectoria y reconocimiento de la ETB S.A. ESP. en el cumplimiento de este tipo de contratos.	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.
ETB	**22**	Se solicita muy respetuosamente, que el valor asegurado de este amparo se establezca por el diez por ciento (10%) del valor del contrato y una vigencia por la duración del contrato y cuatro meses más. Este es el porcentaje y vigencia usual en el mercado asegurador para este tipo de riesgo.	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 OBSERVACIÓN	PREGUNTA	RESPUESTA
ETB	**23**	Se solicita muy respetuosamente, que el porcentaje del amparo de Salarios sea el 5% con fundamento en: a) Este es el porcentaje usual en el mercado asegurador para este tipo de riesgo; b) el bajo riesgo teniendo en cuenta que ETB es una empresa con participación estatal en su patrimonio que está sujeta a la vigilancia y control de todos los entes de control; y c) La seriedad, responsabilidad, solidez financiera, antigüedad, reconocimiento social y la existencia de un sindicato de trabajadores que defiende los intereses de su gremio.	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.
ETB	**24**	Respetuosamente solicitamos a la entidad considerar que la experiencia requerida pueda ser acreditada no únicamente con contratos ejecutados directamente por el proponente, sino también a través de la experiencia de fabricantes y/o aliados estratégicos que respalden la propuesta. Lo anterior, siempre que se demuestre una relación formal (acuerdos, certificaciones o cartas de respaldo) que garantice la disponibilidad de dichas capacidades durante la ejecución del contrato. Esta precisión permitiría ampliar la pluralidad de oferentes y alinear el proceso con las prácticas actuales del mercado de ciberseguridad, sin afectar el nivel técnico exigido.	No es posible atender favorablemente esta solicitud, de acuerdo con los lineamientos y políticas del proceso de contratación y su anexo técnico.
ETB	**25**	¿El licenciamiento actual de Splunk de Fiducoldex cuenta con la cuota de ingesta (GB/día) suficiente para agregar los "conectores adicionales" requeridos, o el proponente debe proveer licencias de expansión de ingesta para Splunk?	Sí cuenta con la cuota de ingesta, en el caso de requerirse, Fiducoldex solicita al proveedor del Splunk la ampliación de esta.
ETB	**26**	¿Cuál es la distribución de Sistemas Operativos de estos 100 servidores (Windows, Linux distribuciones, AIX, etc.) para definir los agentes de recolección compatibles (ej. Splunk Universal Forwarder)?	Se identifican múltiples fuentes de ingesta a través de forwarders (Universal Forwarders)
ETB	**27**	¿Cuál es la marca, modelo y versión de firmware de estos 4 firewalls (ej. Fortinet, Palo Alto, ¿CheckPoint) para garantizar la	La marca es Fortinet

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
		disponibilidad de parsers nativos en Splunk?	
ETB	**28**	¿Fiducoldex cuenta con una bóveda de contraseñas (PAM - Privileged Access Management) centralizada de donde extraer los logs de estos 40 usuarios, o el monitoreo dependerá exclusivamente de logs de Directorio Activo?	La Fiduciaria no cuenta con la bóveda en cuestión.
ETB	**29**	¿Estas 190 aplicaciones están centralizadas detrás de un WAF (Web Application Firewall) o Balanceador de carga desde donde se puedan extraer los logs, o se debe extraer la bitácora desde 190 servidores web (IIS/Apache/Nginx) individuales?	No son individuales ya que los logs se extraen desde los equipos de seguridad perimetral (firewall) y desde los servidores más críticos que soportan los servicios esenciales de la entidad, no son 190 fuentes de orígenes distintas.
ETB	**30**	¿A qué plataformas específicas (Twitter, LinkedIn, Facebook, Instagram, etc.) pertenecen estas 10 cuentas para validar la disponibilidad de APIs de monitoreo e integración?	Con base a los objetivos suministrados, la idea es monitorear dichos perfiles en ambientes de DeepWeb, DarkWeb o campañas de desprestigio o suplantación. Las plataformas no serían específicas, dado que un usuario podría contar con distintos perfiles.
ETB	**31**	¿Cuál es la periodicidad exigida para esta sesión de entendimiento con la Dirección de Seguridad de la Información (semanal, quincenal, mensual)?	Mensual (Para presentación de informes, ejecutivo) y quincenal para entendimiento del informe técnico.
ETB	**32**	Para habilitar la modalidad remota, ¿Fiducoldex proveerá una conexión VPN Site-to-Site, ZTNA, o VDI (escritorios virtuales) para el acceso seguro de los analistas del proveedor al Splunk On-Premise/Cloud de la Fiduciaria?	Sí, Fiducoldex suministra la conexión segura al Splunk
ETB	**33**	¿Fiducoldex exige que el registro de incidentes se realice en su propia herramienta de ITSM (Mesa de Ayuda interna), o el proponente debe proveer e integrar una herramienta de Ticketing externa bidireccional?	Deseable que el proveedor pueda integrar su herramienta de tickets con la herramienta centralizada de la entidad (Binaps)
ETB	**34**	¿Fiducoldex permite la ejecución de Threat Hunting activo en los endpoints de los 100 servidores (Assumed Breach), o la caza se realizará exclusivamente basada en la telemetría pasiva almacenada en Splunk?	Si permite la ejecución, debe ser Threat Hunting activo.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
ETB	**35**	¿Cuáles son los tiempos objetivo de RTO (Recovery Time Objective) y RPO (Recovery Point Objective) exigidos para la operación del SOC en un escenario de desastre de las instalaciones principales del proveedor?	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 y que menciona la disponibilidad de los servicios contratados sobre el 99.95%,
ETB	**36**	Además de correo electrónico, ¿se requiere proveer una línea telefónica dedicada (Toll-free/SIP) o la integración con una planta telefónica específica de Fiducoldex para los reportes de incidentes?	Sí se requiere, los medios de reporte serán el correo electrónico y las líneas telefónicas corporativas que hagan parte del árbol de comunicaciones, el proveedor deberá tener una línea móvil activa sobre la cual responder en caso de un incidente.
ETB	**37**	¿Este informe debe incluir métricas de cumplimiento específicas para entidades vigiladas por la Superintendencia Financiera de Colombia (Circulares 007, 008, 029)?	Sí debe incluir métricas, en especial lo exigido en la circular externa 033 del 2020 emitida por la Superintendencia Financiera de Colombia y lo relacionada al Formato 408 sobre indicadores de gestión de ciberseguridad.
ETB	**38**	¿Fiducoldex cuenta ya con un marco de KPIs/KRIs de seguridad de la información maduro que el proponente deba adoptar, o se espera que el proveedor desarrolle la totalidad del dashboard directivo desde cero?	La entidad no cuenta con un marco de KPIs/KRIs, estas métricas deberán ser diseñadas y construidas en conjunto con el proveedor de cómo puede medir su eficiencia en el servicio, posteriormente, la entidad haría sus observaciones o solicitaría las modificaciones pertinentes.
ETB	**39**	¿Fiducoldex cuenta actualmente con suscripciones a plataformas de Threat Intelligence Comerciales (ej. Recorded Future, VirusTotal Enterprise) o recaerá 100% en las fuentes propietarias y de código abierto del proveedor?	Fiducoldex no cuenta con estas suscripciones, estas fuentes harían parte del servicio SOC, es decir, el proveedor hará uso de sus herramientas o fuentes para dar cumplimiento a este ítem.
ETB	**40**	¿El ecosistema de identidades es 100% On-Premise (Active Directory) o existe un entorno híbrido/cloud (Microsoft Entra ID, AWS IAM) cuyos logs deban ser ingeridos y correlacionados?	El ecosistema de identidad se encuentra bajo Microsoft 365
ETB	**41**	¿Fiducoldex posee una herramienta DAM (Database Activity Monitoring) de donde el SIEM pueda consumir las alertas de consultas SQL anómalas, o se requiere auditar transacciones nativas activando logs que pueden afectar el rendimiento de las BD?	La Fiduciaria no podde con una herramienta DAM.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
ETB	**42**	Para discernir entre cambios legítimos y no autorizados, ¿el SIEM Splunk podrá ser integrado (vía API) con la herramienta de control de cambios (RFC) corporativa de Fiducoldex?	Todos los cambios deberán ser consensuados con la entidad y presentados en el comité de esta, con el fin de obtener la autorización respectiva en pro de no afectar el servicio.
ETB	**43**	¿Existe un servidor NTP central (interno) que obligue a los 100 servidores y 4 firewalls a estar sincronizados, y el SOC debe alertar cualquier desincronización respecto a este servidor primario?	No existe un servidos NTP Central, se exige que haya sincronización con la hora oficial del país.
ETB	**44**	¿Existe una base de datos de gestión de la configuración (CMDB) madura y actualizada que clasifique qué recursos son considerados "críticos" para la correlación de eventos?	No existe una base de datos de gestión de la configuración (CMDB).
ETB	**45**	¿Cuál es la tasa promedio de eventos por segundo (EPS) actual que procesa Splunk para poder estimar el volumen de "Heartbeats" requeridos para monitorear la caída de los loggers?	La tasa es la siguiente: . Eventos por segundo (EPS): EPS promedio: 624 eventos por segundo EPS máximo: 6,765 eventos por segundo
ETB	**46**	¿Qué tecnología(s) de acceso remoto utilizan los usuarios (VPN Cisco, Fortinet, GlobalProtect, ZTNA)? Necesitamos esto para asegurar los parsers en Splunk.	La fiduciaria otorgaría los accesos respectivos con base a la herramienta habilitada para este fin.
ETB	**47**	¿La resolución de DNS de cara a internet está alojada en proveedores externos (Cloudflare, AWS Route 53) o en servidores físicos propios que requieran monitoreo interno?	Sí, está alojada en proveedores externos.
ETB	**48**	De las 190 aplicaciones web, ¿cuántas cuentan con un esquema centralizado de Single Sign-On (SSO) versus autenticación nativa independiente, para mapear las fuentes de recolección de eventos de autenticación?	Menos de 10 aplicaciones
ETB	**49**	¿El monitoreo de disponibilidad debe ser sintético/transaccional (simular un login y navegación) o es suficiente con monitoreo técnico básico tipo HTTP Estatus 200 OK / ICMP Ping?	La fiduciaria solo exige que exista un monitoreo en la disponibilidad de sus servicios, con lo cual, la técnica utilizada queda a discreción del proponente.
ETB	**50**	¿Posee Fiducoldex telemetría de red a nivel de flujos (NetFlow, sFlow, IPFIX) exportada a Splunk para poder identificar patrones de tráfico multicasting anómalo en la capa de red interna?	Fiducoldex no tiene telemetría de red a nivel de flujos.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
ETB	**51**	¿Esta visibilidad a capa 7 se obtendrá de un WAF perimetral existente o se debe extraer mediante la ingesta y parseo profundo de logs raw de IIS/Apache?	La entidad actualmente cuenta con un WAF para la publicación de sus sitios web más críticos de negocio.
ETB	**52**	¿Qué motores de Bases de Datos manejan (SQL Server, Oracle, PostgreSQL) y qué versión, para asegurar la viabilidad técnica de monitorear concurrencia sin afectar los recursos transaccionales?	La Fiduciaria cuenta con: SQL Server en varias versiones y Oracle en varias versiones
ETB	**53**	¿Se cuenta con políticas de Active Directory de "Account Lockout" vigentes? De ser así, el SOC debe correlacionar no solo el login fallido, sino el evento de bloqueo del sistema operativo.	Si se cuenta, las GPO solo bloquean las cuentas de usuario, más no el sistema operativo.
ETB	**54**	Para la detección de propagación lateral, ¿se cuenta con plataformas IDS/IPS internas en segmentos clave de la LAN, o la detección dependerá de alertas nativas de Endpoint Protection (EDR/Antivirus)?	Actualmente la Fiduciaria cuenta con una solución de Antivirus / EDR en los servidores y estaciones de trabajo.
ETB	**55**	¿Están configuradas las políticas de auditoría avanzada de Windows ("Audit Account Management") en todos los Controladores de Dominio para permitir esta correlación de tiempo?	Fiducoldex no cuenta con esta configuración.
ETB	**56**	¿Cuál es la consola de seguridad de Endpoints (EPP/EDR/Antivirus) centralizada actual de Fiducoldex que enviará las alertas de malware detectado/bloqueado al SIEM?	La Consola configurada en Fiducoldex es Symantec
ETB	**57**	¿Fiducoldex cuenta con servicios de mitigación Anti-DDoS en la capa de su proveedor de internet (ISP) o Cloud (ej. AWS Shield, Cloudflare) desde los cuales Splunk pueda extraer la telemetría volumétrica?	Fiducoldex no cuenta con esto.
ETB	**58**	Siendo ataques sin firma conocida, ¿cuenta la infraestructura con herramientas de Sandbox de red/correo, o la detección dependerá de la integración obligatoria de herramientas EDR/XDR/UEBA exigidas en el Ítem 50?	Fiducoldex no cuenta con esta infraestructura, se dependerá de la integración de estas herramientas por parte del Proveedor.
ETB	**59**	¿Este requerimiento hace referencia al monitoreo de credenciales en repositorios públicos/Dark Web (Threat Intelligence) o a cuentas de directorio activo que muestren comportamiento atípico de inicio de sesión (Identity Threat Detection)?	Es correcto.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
ETB	**60**	¿Se cuenta con una herramienta DLP (Data Loss Prevention) instalada en red, endpoints y correo que sirva como fuente primaria de alertas de exfiltración hacia Splunk?	Fiducoldex no cuenta con esta herramienta.
ETB	**61**	La "contención en tiempo real" requiere automatización y ejecución de scripts/agentes en los 100 servidores (Ej. aislar red). ¿Cuenta Splunk con licencias de Splunk SOAR, o el proponente debe proveer la plataforma SOAR completa e instalar los conectores de respuesta activa?	Esta validación hace parte de las condiciones tecnológicas que el proponente dispone para la prestación del servicio, actualmente Fiducoldex no cuenta con licencias Splunk SOAR.
ETB	**62**	Dado el nivel de complejidad e incertidumbre de un ataque real, ¿el soporte forense está incluido dentro del costo fijo con horas ilimitadas, o se permite proponer una bolsa de horas específica para la respuesta a incidentes Nivel 3 / Forense Digital?	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.
ETB	**63**	¿El proponente debe aportar e incluir el licenciamiento de las plataformas especializadas de adquisición y análisis forense (ej. EnCase, FTK, Axiom) que se usarán en caso de incidente?	Es correcto. Debe aportarlo el Proponente
ETB	**64**	PREGUNTA CRÍTICA: ¿El proponente debe COTIZAR, ADQUIRIR y LICENCIAR todas estas soluciones (EDR para los servidores/equipos, XDR, plataformas UEBA y SOAR) y cederlas durante el contrato, o se trata únicamente de "integrar lógicamente" herramientas ya existentes en Fiducoldex al servicio SOC?	Claramente, el servicio SOC se debe integrar a la herramienta SPLUNK de la fiduciaria, la integración con las demás herramientas mencionadas en el ítem debe ser ofrecida por el proponente.
ETB	**65**	Considerando el Ítem 1 (que el SIEM es Splunk propio de Fiducoldex), ¿este ítem exige que toda infraestructura secundaria (ej. colectores de logs, plataformas de Threat Intel, Ticketing, motores SOAR, EDR) sea hosteada y licenciada al 100% como servicio en la nube por el proponente?	Lo que la Fiduciaria exige es que la información esté disponible en línea por 6 meses y luego almacenarla en medios externos (cintas, archivo, entre otros).
ETB	**66**	¿Fiducoldex aceptará una arquitectura 100% Cloud-Native (SaaS/PaaS) provista por el proponente para el SOC, o se requiere instalar componentes físicos (Appliances) dentro del Datacenter de la Fiduciaria?	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

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
			criterios establecidos en la contratación.
ETB	**67**	¿El almacenamiento (Storage SAN/NAS) requerido para retener 6 meses continuos de los logs de los 100 servidores, 4 firewalls y 190 apps web será suministrado y costeado por la infraestructura actual de Fiducoldex o el proveedor debe incluir ese almacenamiento (Cloud u On-Premise) en su costo?	Fiducoldex busca que sea suministrado por el proveedor
ETB	**68**	¿Existen restricciones físicas respecto a este "medio digital" (ej. entrega en discos duros encriptados físicos en Bogotá) o es aceptable proporcionar un bucket de Cold Storage en la nube (ej. AWS S3 Glacier) accesible por el cliente?	Es viable la alternativa, lo importante es garantizar la transferencia segura de la información.
ETB	**69**	¿El SLA del 99,95% (aprox. 21 minutos de indisponibilidad mensual) se refiere a la plataforma SIEM/herramientas o al Tiempo Medio de Respuesta (MTTR) a un incidente por parte de los analistas humanos?	Se refiere a la disponibilidad del servicio SOC (SIEM y herramientas)
ETB	**70**	Si existen pestañas ocultas o no divulgadas en los archivos XLSX originales (que cubran Ciberseguridad Cloud o Redes), solicitamos la publicación oficial de todas las "páginas" de los Anexos 3 y 4 en formato nativo para garantizar el cumplimiento irrestricto exigido.	La información oficial y exigida es la que se ha dispuesto en los canales de publicación, por lo tanto, no existe diferencia en los requerimientos para la prestación del servicio SOC.
ETB	**71**	¿Esta base de conocimiento (KB) debe entregarse en idioma español, e integrarse en una wiki/plataforma interna como Confluence/SharePoint propia de Fiducoldex?	Se esperaría que fuera en español, en la medida de lo posible, se podría validar la integración con la herramienta sharepoint de la entidad.
ETB	**72**	¿Cuántos Casos de Uso (Use Cases) o SOPs operativos exige la Fiduciaria documentar e implementar como métrica mínima de aceptación para el inicio de la operación o fase de afinamiento (baseline)?	Se validaría en consenso entre l Fiduciaria y el adjudicatario.
ETB	**73**	¿La arquitectura de red de Fiducoldex cuenta con microsegmentación (Zero Trust Network Access - ZTNA) en su Data Center o la red interna es plana, lo cual dificultaría drásticamente la detección de movimientos laterales sin herramientas adicionales de red?	Fiducoldex no cuenta con ello.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
ETB	**74**	En caso de que se exija el desarrollo de scripts de integraciones personalizadas (Playbooks de SOAR, parseo a la medida en Splunk), ¿la propiedad intelectual de estos scripts desarrollados a medida será del contratista o se transferirá a Fiducoldex al finalizar el servicio?	Sí, requeriríamos la transferencia de la propiedad intelectual de los scripts desarrollados para Fiducoldex
ETB	**75**	¿Fiducoldex ha desarrollado previamente un Análisis de Riesgos Cuantitativo o un ejercicio de "Crown Jewels" (Identificación de Activos Críticos) que sirva como punto de partida, o el proponente debe ejecutar una consultoría de modelado de amenazas corporativo desde cero?	Sí Fiducoldex, cuenta con un inventario de activos críticos
ETB	**76**	Existe una contradicción sobre la propiedad del licenciamiento. ¿El proponente debe cotizar licencias de ingesta/EPS para el Splunk existente de Fiducoldex, o Fiducoldex ya cuenta con el licenciamiento base y el proponente solo debe aportar licencias de herramientas complementarias?	La fiduciaria cuenta con el licenciamiento del SPLUNK, lo demás que se utilice en el servicio e SOC, estaría a cargo del proveedor.
ETB	**77**	Para dimensionar correctamente la arquitectura de almacenamiento y garantizar la retención en línea de 6 meses, ¿cuál es el volumen actual o estimado de ingesta diaria de logs (en GB/día o EPS) generado por la infraestructura descrita?	La Fiduciaria cuenta con Implementación actual tipo standalone (un solo nodo) No se cuenta con separación de roles (Search Head / Indexer) Se dispone de forwarders gestionados mediante Deployment Server
ETB	**78**	¿Fiducoldex cuenta actualmente con licenciamiento de módulos nativos de Splunk (como Splunk Enterprise Security o Splunk SOAR) o plataformas EDR/XDR desplegadas, o el proponente debe incluir desde cero el licenciamiento, despliegue e infraestructura de todas estas tecnologías (SOAR, EDR, XDR, UEBA)?	Sí, la Fiduciaria cuenta con la Versión instalada: Splunk Enterprise 9.4.9 Conectores existentes: Se identifican múltiples fuentes de ingesta a través de forwarders (Universal Forwarders) Integraciones activas mediante diferentes sourcetypes e índices configurados
ETB	**79**	La contención en "tiempo real" requiere típicamente capacidades de respuesta automatizada en el endpoint (EDR). ¿Permitirá Fiducoldex la integración del SOAR del SOC con sus herramientas de seguridad de endpoint actuales para ejecutar playbooks de aislamiento y contención activa sobre sus 100 servidores?	Sí, claramente este tipo de integraciones o cambios se deberán presentar previamente al comité respectivo para su aprobación, de allí dependerá que se implemente o no.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
ETB	**80**	Para dimensionar el esfuerzo de las pruebas ofensivas, ¿cuál es el alcance específico (cantidad de direcciones IP, aplicaciones móviles/web, e instalaciones físicas si aplica) que se debe contemplar tanto para el ejercicio anual de Ethical Hacking como para las operaciones de Red Team?	Como se informó en el Anexo Técnico, para el Ethical Hacking, hasta 400 ips; para Red Team, explotación avanzada de vulnerabilidades en entornos controlados y en ventanas coordinadas por la entidad.
ETB	**81**	Teniendo en cuenta que el monitoreo de marca abarca tanto a Fiducoldex como a sus Patrimonios Autónomos (PA), ¿cuántos Patrimonios Autónomos y/o marcas secundarias específicas deben ser incluidos en el alcance del monitoreo continuo?	Como se informó en el Anexo Técnico se tratará de 7 inclusiones correspondientes a: Dominio Fiducóldex y 6 negocios administrados.
CLARO	**82**	Agradecemos a la entidad confirmar si las cantidades de activos a monitorear (servidores, firewalls, usuarios privilegiados y aplicaciones) son fijas durante toda la vigencia del contrato o si pudieran incrementarse, y en tal caso, en qué proporción aproximada.	Con relación a la cantidad de activos, podría presentarse un aumento de máximo un 20%, puesto que la entidad tiene previsto ir actualizando su infraestructura para luego evaluar su incremento.
CLARO	**83**	Agradecemos a la entidad suministrar el dimensionamiento actual del SIEM Splunk (EPS promedio y máximo, retención, capacidad de almacenamiento, arquitectura, versión instalada y conectores existentes).	El dimensionamiento actual del SIEM Splunk es: EPS promedio: 624 eventos por segundo EPS máximo: 6,765 eventos por segundo Se identificaron configuraciones de retención variables por índice, con valores que oscilan entre: 30 días 60 días 180 días Capacidad de almacenamiento: Capacidad total configurada: ~2.5 TB Uso actual: ~943 GB Porcentaje de utilización aproximado: 37% Versión: Splunk Enterprise 9.4.9 Conectores: Se identifican múltiples fuentes de ingesta a través de forwarders (Universal Forwarders) Integraciones activas mediante diferentes sourcetypes e índices configurados

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
CLARO	**84**	Solicitamos muy amablemente a la entidad indicar cuántas horas/año o cuántas intervenciones deben considerarse para la prestación del soporte forense dentro del contrato.	No es posible indicar un dato preciso en atención a que la prestación del soporte forense no se establece en una cantidad específica de horas, sino la ejecución de este cuando la entidad lo requiera como fruto de una investigación o gestión de un incidente materializado. Lo que lo convierte en un dato variable.
CLARO	**85**	Agradecemos a la entidad confirmar la frecuencia exacta y el alcance esperado de las actividades de Threat Hunting durante la operación del servicio.	Para el servicio de Threat Hunting (permanente), la entidad espera ser informada inmediatamente en la medida en que se presente una alerta de ciberseguridad, a través de los canales oficiales que se establezcan en la contratación del servicio.
CLARO	**86**	Agradecemos confirmar el tipo de prueba requerido para el ejercicio de Ethical Hacking (caja negra, gris o blanca), así como el inventario de activos y/o aplicaciones que deben incluirse.	Como se indicó en el Anexo Técnico, el ejercicio de Ethical Hacking se deberá realizar sobre activos que hagan parte de la infraestructura interna y externa, las pruebas tendrían un alcance de caja negra, gris o blanca según lo indique la entidad.
CLARO	**87**	Solicitamos a la entidad confirmar si el ejercicio de Red Team debe alinearse explícitamente con técnicas MITRE ATT&CK y cuál es el alcance táctico y técnico esperado.	Como se indicó en el Anexo Técnico, el ejercicio de Red Team lo concibe la entidad como la explotación avanzada de vulnerabilidades y en ventanas de mantenimiento coordinadas con la entidad, con lo cual no se obliga a la aplicación de un marco de referencia como el mencionado.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
CLARO	**88**	Agradecemos a la entidad confirmar si el ejercicio de phishing debe realizarse con un único escenario o múltiples escenarios, y qué tipo de reporte final se requiere (individual, consolidado o ambos).	Para la prueba de Phishing se espera que se realice mediante mecanismos que inviten al usuario a ingresar a sitios falsos o descarga de sw malicioso, por lo tanto, los escenarios se podrían coordinar con la entidad por medio de campañas y con base a las herramientas que suministre el proveedor. En cuanto el reporte, claramente se requiere ambos tipos (Individual y consolidado) teniendo en cuenta que se pueda identificar personas que caigan en el engaño, que interactúen con el contenido, entre otros aspectos. Adicionalmente, implementar una alternativa de capacitación para los usuarios que caigan en la prueba.
CLARO	**89**	Agradecemos confirmar el número de marcas, dominios, directivos y fuentes (OSINT, Deep Web, Dark Web, redes sociales, etc.) que deben ser monitoreados dentro del servicio de protección de marca.	Como se indicó en el Anexo Técnico, se deberán monitorear como mínimo 15 objetivos (marcas / dominios)
CLARO	**90**	Solicitamos a la entidad aclarar si el proveedor debe ejecutar directamente las gestiones de Takedown o si únicamente debe acompañar el proceso mediante asesoría y evidencias técnicas.	Como se indicó en el Anexo Técnico, el proponente deberá realizar la gestión del respectivo "TakeDown" del sitio web o perfil de red social fraudulento.
CLARO	**91**	Agradecemos a la entidad compartir el listado de directivos que deben incluirse en el monitoreo y la periodicidad esperada del análisis (diario, semanal, mensual).	El listado de directivos se compartiría al adjudicatario una vez exista un contrato suscrito. En cuanto a la periodicidad, se deberá hacer un monitoreo constante y que sea reportado a la entidad de forma inmediata con el fin de tomar acciones al respecto.
CLARO	**92**	Agradecemos confirmar si la entidad acepta la inclusión de justificaciones técnicas en aquellos ítems marcados como "No aplica" dentro de los anexos técnicos.	Si se acepta, la idea es tener respuesta de los ítems enviados para la contratación del servicio, con lo cual, se espera tener una justificación cumplimiento o no aplicación del ítem para poder validar si este llegara o no a tener afectación en la calificación.
CLARO	**93**	Solicitamos cordialmente confirmar si, antes de aplicar las multas establecidas en el numeral correspondiente, existe una etapa de aclaración o intercambio	Sí, esa etapa es de 3 días una vez notificado la causa originadora. Por favor ver el numeral 5.6 de los Términos de Referencia.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
		técnico para validar las posibles causas del incumplimiento.	
CLARO	**94**	Agradecemos a la entidad precisar si la cláusula penal del 20% aplica únicamente en casos de incumplimiento total o si también aplica para incumplimientos parciales.	Aplica para el incumplimiento total de las obligaciones a cargo del Contratista, por favor ver numeral 5.7 de los Términos de Referencia.
CLARO	**95**	Agradecemos a la entidad indicar si existen herramientas o soluciones adicionales del ecosistema de seguridad (por ejemplo: EDR, WAF, IAM, PAM, CASB, DNS Security, NAC, entre otras) que deban integrarse al SOC.	Como se indicó en el Anexo Técnico, el proveedor debe suministrar una solución que contemple estas herramientas y que, a su vez, se integre al SIEM.
CLARO	**96**	Agradecemos confirmar si la entidad cuenta con infraestructura interna para sincronización NTP o si el proveedor debe suministrar y/o asegurar la conectividad hacia la hora legal del INM (Colombia).	La Fiduciaria no cuenta con este servidor. El proveedor debe suministrar y/o asegurar la conectividad hacia la hora legal del INM (Colombia).
CLARO	**97**	Agradecemos a la entidad confirmar si, adicionalmente al uso del SIEM Splunk de la Fiduciaria, el proveedor puede proponer el servicio de SOC–SIEM como servicio, incluyendo una modalidad SIEM-less o SIEM propio, como alternativa técnica dentro de la oferta.	Como se indicó en el Anexo Técnico, el alcance del contrato es el servicio del SOC gestionando el SIEM (Splunk) de la entidad. Lo referente al servicio SOC del proveedor, esto ítems se mencionan en los valores agregados por parte del oferente y los cuales tienen su respectiva evaluación.
CLARO	**98**	Agradecemos a la entidad confirmar si la prueba de concepto del SIEM, contemplada como valor agregado, puede considerarse por un periodo menor al indicado (6 meses), teniendo en cuenta que dicho plazo resulta extenso desde el punto de vista operativo y de costos. En caso afirmativo, indicar el tiempo mínimo aceptable.	Como se indicó en el Anexo Técnico, estos valores agregados tienen un nivel de calificación según el tiempo que se tenga esta PoC, acorde a los lineamientos establecidos por la Fiduciaria. Dentro de la oferta el proponente determina si lo ofrece o no y la cantidad de tiempo acorde a lo referido dentro de los Términos de Referencia. La calificación varía según lo mencionado en los Términos de Referencia publicados.
CLARO	**99**	Agradecemos a la entidad confirmar si dentro del alcance del servicio se requiere incluir pruebas de análisis de código (estático y/o dinámico). En caso afirmativo, solicitamos indicar.	Como se indicó en el Anexo Técnico, si se requiere incluir análisis de código estático y dinámico para desarrollos o proyectos que la fiduciaria implemente en su operación, estas pruebas son a demanda.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
CLARO	**100**	Aplicaciones para evaluar.	Esta solicitud es por demanda.
CLARO	**101**	Lenguajes de programación.	Lenguajes de fabricantes conocidos en el medio corporativo a nivel de base de datos y aplicaciones.
CLARO	**102**	Cantidad aproximada de aplicaciones.	Esta solicitud es por demanda.
CLARO	**103**	Volumen estimado de líneas de código (LOC).	Esta solicitud es por demanda.
CLARO	**104**	Agradecemos muy respetuosamente confirmar si es posible considerar un ajuste a la cláusula de terminación anticipada del contrato, de manera que dicha terminación se encuentre soportada en lineamientos, criterios objetivos o evidencias formales que indiquen que el servicio no ha cumplido con los niveles, alcances o condiciones acordadas, y no de forma discrecional.	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.
CLARO	**105**	Solicitamos la modificación del cronograma del proceso, ampliando la fecha de Cierre y entrega de propuestas en 9 días calendario hasta el 17 de abril de 2026 hasta las 4:00 p.m. con el fin de garantizar el diseño correcto de las soluciones y servicios solicitados.	No es posible acceder favorablemente a esta solicitud, este parámetro ha sido establecido por la entidad en cumplimiento a requerimientos normativos, cuyas actividades, incluyendo la presente, cuenta con tiempos definidos para su ejecución.
CLARO	**106**	Teniendo en cuenta que Fiducoldex nos entregaría respuestas de las preguntas el 6 de abril, es posible nos amplie el tiempo de entrega de la Oferta, ¿ya que solo tendríamos 2 días para ajustarnos a las respuestas que nos brinde del RFP?	No es posible acceder favorablemente a esta solicitud, este parámetro ha sido establecido por la entidad en cumplimiento a requerimientos normativos, cuyas actividades, incluyendo la presente, cuenta con tiempos definidos para su ejecución.
CLARO	**107**	Dentro del documento TÉRMINOS DE INVITACIÓN - 3.3.1.1 Certificación de experiencia indica: "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 2023 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 tema y pruebas de phishing". Teniendo esto en cuenta, entonces para el Anexo 4, solo indicamos si cumplimos y justificamos, pero no es necesario	No es correcta su interpretación. Como se indicó en el Anexo Técnico, el Proponente debe tener en cuenta que en los ítems en donde se responda que se cumple y que implique prueba de ello deberá suministrar los documentos como evidencia para la realización del proceso 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 OBSERVACIÓN	PREGUNTA	RESPUESTA
		incluir un documento de certificación, ya que estos van dirigidos a lo que se menciona en el ítem 3.3.1.1 Certificación de experiencia. ¿Nos podrían confirmar si es correcta nuestra interpretación?	
CLARO	**108**	En este caso, ¿qué tipo de evidencia espera recibir Fiducoldex? Ya que los acuerdos como tal son información catalogada como confidencial.	El proveedor nos deberá certificar que cuenta con este tipo de acuerdos (suministrar una proforma tipo plantilla), sin que esto implique conocer la información confidencial de este (política de acuerdo de confidencialidad por parte del oferente).
CLARO	**109**	¿Solicitamos a la entidad aclarar el applienace puede ser físico o un VM? ¿Si es una VM la entidad la puede proporcionar o el proponente? ¿Adicionalmente indica que son eventos trimestrales, pero en el número se observa (4), cual es el correcto?	Las herramientas pueden ser físicas o virtuales en atención a que deben ser suministradas por el proveedor y queda bajo su discrecionalidad. Se confirma que son eventos trimestrales, es decir, en total se trataría de cuatro eventos al año.
CLARO	**110**	Solicitamos a la entidad aclarar la cantidad precisa de IPs o activos para realizar ETH Pentesting.	Como se indicó en el Anexo Técnico, hasta 400 direcciones IP.
CLARO	**111**	Solicitamos a la entidad sugerir un cambio en este requerimiento, porque la responsabilidad de realizar remediaciones de los hallazgos encontrados es por parte de la Fiduciaria.	Como se indicó en el Anexo Técnico, claramente la remediación está a cargo de la fiduciaria, el proponente solo interactúa en modo "consultivo".
CLARO	**112**	Solicitamos cordialmente a la entidad que indique bien sea la cantidad total de EPP o Gigas consumidas al mes o al año, o en su defecto el consumo de cada uno de los equipos o aplicaciones descritos en este alcance, para realizar un dimensionamiento real del consumo actual.	La cantidad total de Gigas son: Volumen promedio diario: 30 – 35 GB/día Consumo mensual estimado: ~1 TB Consumo anual estimado: ~11 – 12 TB

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
CLARO	**113**	¿Solicitamos cordialmente a la entidad si es correcto que la plataforma para redes sociales solo necesitas tener acceso el proveedor?	No es correcto, para este tipo de monitoreo no implica el acceso a ninguna plataforma de redes sociales, todo se basa en la revisión que se haga como parte de esta actividad.
CLARO	**114**	¿Solicitamos cordialmente a la entidad confirmar cuantos takedowns necesita o ha requerido en el pasado?	Esta solicitud es por demanda, actualmente la entidad no ha tenido un evento de este tipo, pero ello no indica que no esté expuesto a esta situación.
CLARO	**115**	Solicitamos cordialmente a la entidad confirmar los dominios (URLs) en concreto que se deberían monitorear, detallar cada URLs por separado.	Esta información sería suministrada al adjudicatario en etapa posterior a la suscripción del contrato.
ALLIANCE	**116**	1. ¿Es obligatorio que el proponente ofrezca la totalidad de los servicios (incluyendo SOC 7x24x365), o es posible presentar propuestas parciales enfocadas en componentes específicos como pruebas de seguridad (Ethical Hacking, Red Team, ¿análisis de vulnerabilidades y phishing)?	Sí, se considera obligatoria la totalidad de los servicios del SOC, tanto en la disponibilidad como en los ítems mencionados en el documento de "Términos y condiciones". Por lo anterior, no se ejecutarán servicios de forma parcial o independiente.
ALLIANCE	**117**	¿El servicio de Red Team está concebido como ejercicios puntuales o como un programa continuo durante la vigencia del contrato?	El ejercicio Red Team está concebido como la explotación avanzada de amenazas, así mismo, en validación con el proveedor y la entidad, se estudiaría la posibilidad de algún escenario puntual. Este ejercicio se debe realizar mientras dure la vigencia del contrato, esto no implica de modo continuo sino programado por la entidad y coordinado con el proveedor.
ALLIANCE	**118**	¿Las pruebas de phishing (ingeniería social) tienen una frecuencia definida o se ejecutan bajo demanda?	Las pruebas de Phishing se conciben para que sean realizadas bajo una programación coordinada entre la entidad y el proveedor, buscando la posibilidad de generar una periodicidad trimestral.
ALLIANCE	**119**	¿Cuál es el alcance esperado del análisis de vulnerabilidades trimestral (interno, externo, autenticado/no autenticado)?	El análisis de vulnerabilidades trimestral se debe hacer sobre la infraestructura tecnológica interna y externa (sitios expuestos en el ciberespacio); en cuanto a lo relacionado con la autenticación de dicho ejercicio, se evaluaría en el momento de definir el alcance de los activos a ser analizados y si estos se

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
			permite una evaluación autenticada o no.
GMS	**120**	¿Es posible que el Cliente modifique este requerimiento para aceptar certificaciones de experiencia y alianzas (partnership) con otros fabricantes de soluciones SIEM líderes en la industria, en lugar de limitarlo exclusivamente a la herramienta Splunk?, teniendo en cuenta que la adopción del SIEM diferente a SPLUNK no genere costo adicional para FIDUCOLDEX.	La Fiduciaria acepta la modificación, por favor ver la Adenda No. 2
GMS	**121**	¿Es posible modificar el numeral 3?3.1.1 para reducir la cantidad exigida y aceptar como mínimo dos (2) certificaciones de experiencia, manteniendo la condición de que cada una sea por una cuantía igual o inferior a SEISCIENTOS MILLONES DE PESOS ($600.000.000 COP) y que en su conjunto acrediten los alcances solicitados?	No es posible acceder favorablemente a esta solicitud; dado que los criterios aplican para todos los proponentes en igualdad de condiciones.
GMS	**122**	¿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?	Como se indicó en el Anexo Técnico, para el ejercicio de Ethical Hacking se podrá tomar la cantidad de IPs como infraestructura interna y externa, hasta 400 direcciones, pero esta cantidad podría ser menor dependiendo de la definición de alcance que se haga al momento de ejecutar la prueba.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
GMS	**123**	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)?	Sí en total son 7 marcas principales, aplica para Fiducoldex y sus 6 negocios administrados, los cuales se encuentran relacionados en el Anexo Técnico.
GMS	**124**	¿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?	La ejecución de estos simulacros se esperaría que fueran en ambientes controlados para lograr niveles cercanos a la realidad, no obstante, según la definición del alcance entre la entidad y el oferente, se determinaría el tipo exclusivo o combinado.
GMS	**125**	¿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, las certificaciones a acreditar son las mencionadas en el 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 OBSERVACIÓN	PREGUNTA	RESPUESTA
PASSWORD	**126**	¿Este requisito es de carácter habilitante o excluyente dentro del proceso, o puede ser considerado como un criterio evaluable? Teniendo en cuenta que, en el mercado, la operación de SOC suele operar en marcos especializados de ciberseguridad (como ISO 27001, NIST, CIS), que cubren de manera directa la gestión de seguridad de la información.	Se considera de carácter "Habilitante y obligatorio", porque esta certificación demostraría que el oferente cuenta con procedimientos adecuados, consistentes y robustos en la administración de servicios tecnológicos; evitando la aplicación de acciones que pongan riesgo el servicio y la seguridad de la entidad contratante. Adicionalmente, con esta certificación el oferente estaría en la capacidad de demostrar como el servicio SOC puede contribuir en los procesos de continuidad del negocio, gestión y priorización de incidentes, entrega de resultados consistentes y métricas sobre el estado del servicio y el nivel de seguridad de la entidad contratante.
PASSWORD	**127**	¿Este requisito es de carácter habilitante o excluyente dentro del proceso, o puede ser considerado como un criterio evaluable? Teniendo en cuenta que, en el mercado, la operación de SOC suele operar en marcos especializados de ciberseguridad (como ISO 27001, NIST, CIS), que cubren de manera directa la gestión de seguridad de la información.	Se considera de carácter "Habilitante y obligatorio", porque esta certificación demuestra que el oferente implementa adecuados controles de seguridad que garanticen la confidencialidad, integridad, disponibilidad y privacidad de los datos. Adicionalmente, evidencia que el oferente está en la capacidad de apoyar la continuidad del servicio, apoyar en la gestión de incidentes y riesgos de ciberseguridad que afecten a la entidad contratante.
PASSWORD	**128**	Se solicita a la entidad aclarar si el requerimiento implica que el proponente debe suministrar y licenciar herramientas adicionales (SOAR, UEBA, ML, IA, XDR, EDR) como parte del servicio SOC, o si se espera que dichas capacidades, en caso de ya existir en la entidad, sean únicamente integradas, configuradas y operadas sobre el SIEM actual (Splunk Enterprise Security). Así mismo, se agradece precisar el alcance esperado en términos de implementación vs. operación de estas funcionalidades.	Como se indicó en el Anexo Técnico, el proponente debe implementar herramientas SOAR, UEBA, ML, IA, XDR, EDR, entre otras, integradas al SIEM Splunk

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
PASSWORD	**129**	Se solicita a la entidad aclarar el alcance del requisito relacionado con la presentación de licencias o certificados de derechos de autor de las herramientas del servicio SOC, específicamente si se espera que el proponente suministre y adquiera el licenciamiento de la herramienta Splunk Enterprise Security o si este ya es provisto por la entidad. Así mismo, se agradece precisar si este requerimiento hace referencia a las herramientas adicionales mencionadas (SOAR, UEBA, XDR, EDR, entre otras) y, en tal caso, especificar cuáles soluciones deben ser incluidas dentro del alcance del servicio.	Como se indicó en el Anexo Técnico, el proponente debe garantizar y demostrar que todos los elementos tecnológicos empleados para la prestación del servicio SOC, estén debidamente licenciados y autorizados para su uso. Adicionalmente, la licencia de la herramienta SPLUNK está a cargo de Fiducoldex siendo esta la encargada de su gestión en términos de renovación y/o vigencia.
PASSWORD	**130**	Se solicita a la entidad aclarar el alcance del requerimiento de almacenamiento y backup de la información, específicamente si los backups hacen referencia a los datos y logs gestionados en la plataforma Splunk Enterprise Security o a la información generada por la operación del SOC (como casos de seguridad, incidentes, reportes y tickets). Así mismo, se agradece precisar el tipo de información, formato y volumen esperado para la entrega de dichos backups en medio digital.	Como se indicó en el Anexo Técnico, este ítem hace referencia a que el proponente debe garantizar el almacenamiento de la información relacionada con el servicio prestado a la Fiduciaria, la cual sirva de insumo para la atención de posibles requerimientos por entes de control internos o externos, o la gestión de incidentes de seguridad e investigaciones resultantes de esta actividad.
PASSWORD	**131**	Se solicita a la entidad aclarar el alcance del requerimiento de planes de continuidad, específicamente si este hace referencia a la continuidad del servicio SOC prestado por el proponente o a la continuidad de la plataforma Splunk Enterprise Security. Así mismo, se agradece precisar si se espera la entrega de un plan propio del proponente o la construcción conjunta de planes de continuidad y recuperación ante desastres (DRP/BCP) con la entidad.	Como se indicó en el Anexo Técnico, el proponente debe demostrar que cuenta con la implementación y ejecución de planes de continuidad en caso de desastres o interrupción del Servicio SOC, presentando a la Fiduciaria un plan de acción que sería empleado al momento de la ocurrencia de algún evento negativo que comprometa la prestación del servicio. Por otro lado, podría ser posible la interacción a modo "Consultor" para la Fiduciaria, cuando esta se encuentre en el diseño de sus estrategias de continuidad y desee contar con la opinión de actor ajeno a sus procesos internos

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
SISAP	**132**	1- ¿Se necesita contar con un SIEM para cumplimiento con un estándar o regulación local?	Si se necesita, como se indicó en el Anexo Técnico, el alcance del SIEM es gestionar la solución de la entidad (Splunk)
SISAP	**133**	1.1-Especificar el estándar o regulación local	Fiducoldex cuenta con regulación local, en Cumplimiento a las disposiciones normativas aplicables a Fiducoldex, en materia de seguridad de la información y ciberseguridad, particularmente las Circulares Externas expedidas por la Superintendencia Financiera de Colombia CE007/18 Numeral 4.1.8, 4.2.3, CE008/18 Numeral 2.3.7 y CE029/14 Numeral 2.3.4.9.2
SISAP	**134**	2- ¿Cuál de las siguientes funcionalidades desea que tenga la solución SIEM?	Tener presente que debe administrar el SIEM de la entidad, cuya marca es SPLUNK
SISAP	**135**	2.1-Correlación de eventos	Si se correlacionan
SISAP	**136**	2.2-UEBA – Análisis de comportamiento de usuarios y entidades	Si, este deber suministrado por el oferente e integrado con el SPLUNK
SISAP	**137**	2.3-Monitoreo de red	Si se debe monitorear la red
SISAP	**138**	2.4-Machine Learning	No aplica
SISAP	**139**	2.5-Otro (especificar cuál)	Tener en cuenta que se debe proponer por parte del oferente, servicios como: UEBA, SOAR, XDR, entre otros; los cuales deben ser integrados al SPLUNK.
SISAP	**140**	3- ¿Cuánto tiempo de retención de eventos debe tener la solución?	El tiempo de retención de eventos que debe tener la solución se responde en la pregunta 141 y 142 del presente documento.
SISAP	**141**	3.1-En línea	El tiempo de retención de eventos que debe tener la solución son 6 meses
SISAP	**142**	3.2-Fuera de línea	El tiempo de retención de eventos que debe tener la solución se debe almacenar en dispositivos externos de respaldo. No tiene tiempo por ser archivo.
SISAP	**143**	4- ¿Cómo se desea que se entregue la solución?	La solución de prueba de concepto está definida en los términos de referencia, acorde a lo que determine autónomamente el Proponente.

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
SISAP	**144**	4.1-Si se desea virtual, ¿cuentan con recursos para la virtualización de la solución?	La solución de prueba de concepto está definida en los términos de referencia, acorde a lo que determine autónomamente el Proponente.
SISAP	**145**	5- ¿Desean que el licenciamiento del SIEM esté a nombre de la organización?	Como se indicó en el Anexo Técnico, la entidad cuenta con el licenciamiento de SPLUNK a nombre propio
SISAP	**146**	6- ¿Requieren entrenamiento sobre cómo administrar la solución SIEM? ¿Para cuántas personas?	Como se indicó en el Anexo Técnico, el oferente debe gestionar al 100% el SIEM de la entidad. No es necesario realizar un entrenamiento al personal de Fiducoldex ya que es el Adjudicatario quien ejecutará y gestionará el 100% de la herramienta.
SISAP	**147**	7- ¿Cuántos usuarios se conectan a la red de la organización?	Aproximadamente 1000 usuarios
SISAP	**148**	8- ¿Se puede configurar puerto espejo dentro de la red?	No es posible configurar puerto espejo.
SISAP	**149**	9- ¿La red a monitorear es una red plana o está segmentada?	Es una red Segmentada
SISAP	**150**	9.1- ¿En cuántas VLAN está segmentada la red?	En 10 Vlans
SISAP	**151**	9.2- ¿Cómo se encuentran distribuidas (localidades) las VLAN?	Se encuentran distribuidas: 6 Vlans en la sede principal, 3 vlans en las sedes de los PA y 1 vlan en el datacenter de contingencia
SISAP	**152**	9.3- ¿Quién es el orquestador de las VLAN?	El Equipo de red Core Alcatel
SISAP	**153**	9.4-Aproximadamente, ¿cuántos dispositivos se pueden identificar en cada VLAN?	Las vlans más ocupadas son las 1 y la 2, las cuales contienen los equipos de los usuarios y los servidores, el resto de vlans no superan los 30 dispositivos
SISAP	**154**	10- ¿Cuentan con una solución IPS o IDS?	No se tiene en la Fiduciaria esta solución.
SISAP	**155**	11- ¿Cuántos centros de datos tienen y dónde se encuentran ubicados?	Se cuenta con un CAO y CAPD
SISAP	**156**	12- ¿Cuál es el throughput de la red a monitorear?	No se tiene esa información
SISAP	**157**	13- ¿Cuentan con servicios en nube? ¿En qué nube?	Sí, Azure y proyectos con terceros que usan AWS y Oracle
SISAP	**158**	13.1- ¿Cuántos equipos/activos se encuentran en cada nube?	No se tiene esa información
SISAP	**159**	13.2- ¿Cuál es el throughput de la red en nube a monitorear?	No se tiene esa información

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 OBSERVACIÓN	PREGUNTA	RESPUESTA
SISAP	**160**	13.2- ¿Cuál es el throughput de la red en nube a monitorear?	No se tiene esa información
SISAP	**161**	1-Windows Servers – HIGH EPS	0
SISAP	**162**	2-Windows Servers – MED EPS	0
SISAP	**163**	3-Windows Servers – LOW EPS	0
SISAP	**164**	4-Windows Domain Controller Servers	2
SISAP	**165**	5-User Endpoints (Laptops / Tablets / POS / Mobile)	790 activos
SISAP	**166**	6-Application Servers	20
SISAP	**167**	7-Linux / Unix Servers	20
SISAP	**168**	8-Hypervisores (ESXi, Hyper-V, etc.)	7
SISAP	**169**	9-Email Servers	2
SISAP	**170**	10-DNS Servers	2
SISAP	**171**	11-Conmutadores	2
SISAP	**172**	12-Backup Servers	2
SISAP	**173**	13-Other Servers	40
SISAP	**174**	14-Network Routers	6
SISAP	**175**	15-Network Switches	17
SISAP	**176**	16-Network Flows (NetFlow / S-Flow)	N/A
SISAP	**177**	17-Network Wireless LAN Controllers	1
SISAP	**178**	18-Network Load-Balancers	N/A
SISAP	**179**	19-Access Points	17
SISAP	**180**	20-Storage Devices (NAS / SAN)	2
SISAP	**181**	21-Other Network Devices	N/A
SISAP	**182**	22-Network Firewalls (Internal)	5
SISAP	**183**	23-Network Firewalls (DMZ)	N/A
SISAP	**184**	24-Network IPS / IDS	N/A
SISAP	**185**	25-Network VPN / SSL VPN Concentrators	1
SISAP	**186**	26-Network Web Proxy	N/A
SISAP	**187**	27-Other Security Devices	N/A

El presente documento se publica a los ocho (8) días del mes de abril 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