Count	Sección	Tipo de Observación (Sustancial/Formal)	Texto de la sección comentada	Observación / Comentario	Sugerencia de Ajuste	Respuesta
1	1.2	Sustancial	La entidad informa El servicio del SOC deberá contar con mínimos dos (2) centros de datos geográficamente ubicados en diferentes lugares dentro de Bogotá D.C o uno de estos puede estar fuera de Bogotá, siendo este para contingencia o alta disponibilidad, aclarando que el datacenter principal de donde se prestará el servicio de SOC y las capacidades contratadas, debe encontrarse en la ciudad de Bogotá. El proponente debe especificar la cantidad de Centro de Datos de los que dispone para el SOC, su ubicación y el rol de cada uno de ellos.	Con el fin de garantizar los principios de pluralidad de oferentes, transparencia y participación internacional en el proceso, solicitamos a la entidad precisar y permitir que, en los casos en que el proponente ofrezca dos (2) Centros de Operaciones de Seguridad (SOC), al menos uno de estos pueda estar ubicado fuera de la ciudad de Bogotá, siempre que se garantice la disponibilidad, continuidad y niveles de servicio exigidos.	No se exija para pluralidad, transparencia y participación internacional	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, tal como se indica en el requerimiento, el futuro proveedor de SOC puede entregar dos Centros de Operaciones en la ciudad de Bogotá u optar por tener uno en la Ciudad de Bogotá y otro en otra locación diferente a esta ciudad, aclarando que lo que se requiere es que el SOC (Personal, Infraestructura Física y Técnica, entre otros) esté en la Ciudad de Bogotá, más no el centro de datos que soporta dicha operación, en el entendido de que muchos SOC´s tienen su operación en la nube o en un centro de datos de terceros, sin embargo, para una mejor comprensión de lo solicitado y así evitar equivocos, se informa que se hará la respectiva modificación que se publicará en adenda en los próximos días, para los ítems 1.2 y 12.80 quedando de la siguiente manera: 1.2 Se debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá que cuente con las condiciones adecuadas para garantizar la continuidad operativa, la seguridad física y lógica, y el cumplimiento de las mejores prácticas del sector. Desde donde se administrarán todos los productos, capacidades, plataformas, soluciones y servicios, que sean requeridos para dar cumplimiento a lo solicitado en el anexo técnico y que le permitan realizar todas las actividades encomendadas en este documento por la DIAN. Aclarando que lo que se requiere es que el SOC (Personal, Infraestructura Física y Técnica, entre otros) esté en la Ciudad de Bogotá, más no el centro de datos que soporta dicha operación, en el entendido de que muchos SOC´s tienen su operación en la nube o en un centro de datos de terceros. Entendiéndose que el CONTRATISTA realizará toda la gestión, monitoreo, administración, optimización, actualización, acompañamiento, soporte y garantía de los mismos, cobijando toda la infraestructura tecnológica de la Entidad. Para el efecto debe tener la capacidad de detectar, escalar, informar, acompañar apoyar y soportar a la DIAN en la resolución de cada uno de los incidentes encontrados por el SOC durante el tiempo que dure el proyecto en mención. Los activos y demás características de estos se encuentran detallados en el apartado de inventarios y las especificaciones de cada una de las soluciones, plataformas, capacidades, servicios, soporte y garantía se encuentran en este anexo técnico de obligatorio cumplimiento. 12.80 El servicio del SOC deberá contar como mínimo con dos (2) centros de operaciones de seguridad geográficamente ubicados en diferentes lugares dentro de Bogotá D.C o uno de estos puede estar fuera de Bogotá, siendo este para contingencia o alta disponibilidad, así mismo se indica que lo que se requiere es que el SOC (Personal, Infraestructura Física y Técnica, entre otros) esté en la Ciudad de Bogotá, más no el centro de datos que soporta dicha operación, en el entendido de que muchos SOC´s tienen su operación en la nube o en un centro de datos de terceros
3	2.5	Sustancial	Dimensionamiento EPS	Amablemente se solicita aclarar si los 25.000 EPS corresponden al total esperado o si se debe considerar crecimiento asociado a más de 24.000 activos.	Aclarar dimensionamiento real y crecimiento proyectado	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el total esperado para los Eventos por Segundo (EPS) del SIEM son 25000.
4	2.7	Formal	Retención de logs	Amablemente se solicita precisar si la retención offline requiere disponibilidad inmediata o puede manejarse en almacenamiento secundario.	Permitir esquema de archivado	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la retención offline debe tener una disponibilidad inmediata.
5	3.59	Sustancial	Automatización	Amablemente se solicita confirmar el nivel esperado de automatización de playbooks.	Definir porcentaje esperado	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se tiene un porcentaje en especifico para la automatización de los respectivos playbooks, ya que ello dependerá del grado de complejidad de lo solicitado, así como de la misma automatización perse.
6	1.3	Sustancial	Guardium	Amablemente se solicita aclarar coexistencia con Guardium hasta 2027.	Definir integración/migración	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el futuro proveedor de SOC deberá administrar la plataforma GUARDIUM - IBM de la Entidad desde el inicio del contrato y hasta 31 de diciembre de 2027, realizando labores y actividades propias de operación, administración y gestión de la respectiva plataforma. Una vez esto ocurra el futuro proveedor de SOC con antelación y planeación deberá realizar la implementación del nuevo servicio de firewall de bases de datos, teniendo en cuenta las fechas de terminación de los servicios del anterior firewall, para así no impactar en la operación del servicio en mención y dar continuidad ininterrumpida a la operación .
7	5.7.8	Formal	Frecuencia escaneo	Amablemente se solicita confirmar periodicidad de escaneos.	Definir frecuencia	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los escaneos solicitados son ilimitados, es decir se deben realizar programados, por demanda en cualquier momento requerido por la entidad. Para el caso de la capacidad de aseguramiento de directorio activo este debe ser en tiempo real para la totalidad del directorio activo sin ningún límite durante la duración del licenciamiento ofertado. Para el caso de la capacidad de seguridad en nube publica esta debe ser en todas sus funcionalidades en tiempo real y conectada con las nubes publicas de la DIAN para lograr un aseguramiento continuo e integral sin ningún límite durante la duración del licenciamiento ofertado. Para el caso de las capacidades de escaneo de aplicaciones web se requieren escaneo ilimitado sin ningún límite durante la duración del licenciamiento ofertado.
8	6.3.1	Sustancial	Capacidad	Amablemente se solicita confirmar que puede implementarse mediante múltiples herramientas.	Aceptar arquitectura integrada	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se puede realizar mediante varias herramientas, siempre y cuando se cumplan con las características técnicas solicitadas para este servicio.
9	8.24	Formal	Lenguajes	Amablemente se solicita confirmar lenguajes y frameworks.	Listar tecnologías	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, dentro de los términos se especifica lo siguiente: "Debe soportar lenguajes como: Java, JavaScript, Python, Php, Ruby, C++, C, C#, otros".
10	General	Sustancial	Integraciones	Amablemente se solicita listado completo de integraciones.	Detallar integraciones	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no es posible dar respuesta a su observación por cuanto no se entiende la pregunta y no hace referencia a algún ítem en especial.
11	General	Sustancial	Activos	Amablemente se solicita confirmar si los 24.000 activos son alcance total.	Confirmar alcance	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el alcance en cuanto a dispositivos es por la cantidad de 25000.
12	1.3	Formal	Licenciamiento IBM QRADAR e IBM GUARDIUM	Amablemente se solicita aclarar la fecha de inicio y fin que se espera tener el servicio de gestión/administración y monitoreo de cada uno de los servicios. Entendemos que el licenciamiento y soporte de las soluciones y plataformas es por tres (3) años a partir de su puesta en funcionamiento, sin embargo, para los servicios de gestión/administración y monitoreo no es claro su fecha de inicio y fin.	Aclarar	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, la operación, seguimiento, gestión, monitoreo y administración por parte del futuro proveedor de todos los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho a uso, licenciamiento, suscripciones, actualizaciones, soporte y garantía irá por tres (3) años y sus periodos se contabilizarán a partir de la puesta en operación de cada uno de los servicios requeridos, incluyendo lo siguiente: Tener en cuenta que desde el inicio del contrato se deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 nuevo SIEM (solicitado en el ítem 2) que hace parte integral de este proyecto por el tiempo solicitado (Tres años) con licenciamiento soporte, garantía y derecho a uso hasta agosto 31 de 2030. La protección de bases de datos (Firewall de bases de datos) irá a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031. El futuro contratista deberá, recibir, gestionar, administrar y operar desde el inicio del contrato el actual firewall de bases de datos propiedad de la DIAN del fabricante IBM Referencia GUARDIUM hasta diciembre 31 de 2027 tiempo en el que termina el soporte de este dispositivo por parte del fabricante, una vez esto ocurra deberá implementar el nuevo firewall de bases de datos solicitado en las capacidades requeridas por la DIAN. Para la capacidad de NDR se deberá tener en cuenta que este comenzará a operar a partir de enero de 2028 previamente autorización de la DIAN, para lo cual deberá implementar, administrar, operar, soportar y garantizar el servicio mencionado, con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031.

13	1.3	Forma	La administración, operación, gestión de los servicios y demás actividades de las plataformas, soluciones, software, hardware, entre otros...	Amablemente se solicita aclarar la fecha de inicio y fin de la administración, operación, gestión y demás servicios teniendo en cuenta que no todos empiezan al tiempo dado que algunos con los que cuenta la entidad siguen vigentes durante la ejecución.	Aclarar	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, la operación, seguimiento, gestión, monitoreo y administración por parte del futuro proveedor de todos los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho a uso, licenciamiento, suscripciones, actualizaciones, soporte y garantía irá por tres (3) años y sus periodos se contabilizarán a partir de la puesta en operación de cada uno de los servicios requeridos, incluyendo lo siguiente: Tener en cuenta que desde el inicio del contrato se deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 nuevo SIEM (solicitado en el ítem 2) que hace parte integral de este proyecto por el tiempo solicitado (Tres años) con licenciamiento soporte, garantía y derecho a uso hasta agosto 31 de 2030. La protección de bases de datos (Firewall de bases de datos) irá a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031. El futuro contratista deberá, recibir, gestionar, administrar y operar desde el inicio del contrato el actual firewall de bases de datos propiedad de la DIAN del fabricante IBM Referencia GUARDIUM hasta diciembre 31 de 2027 tiempo en el que termina el soporte de este dispositivo por parte del fabricante, una vez esto ocurra deberá implementar el nuevo firewall de bases de datos solicitado en las capacidades requeridas por la DIAN. Para la capacidad de NDR se deberá tener en cuenta que este comenzará a operar a partir de enero de 2028 previamente autorización de la DIAN, para lo cual deberá implementar, administrar, operar, soportar y garantizar el servicio mencionado, con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031.
14	Mínimo de Trabajo	Forma	Deberá contar con personal en sitio (mínimo un Ingeniero) en el horario laboral entre semana (8x5) y si por alguna circunstancia fortuita o de acuerdo a la necesidad de la DIAN..	Amablemente solicitamos aclarar si este rol esta considerado dentro del "Equipo Mínimo de Trabajo" definido en el anexo técnico o se debe considerar un rol adicional y dedicado a este propósito.	Aclarar	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, el perfil solicitado para este ítem está incluido en el equipo mínimo de trabajo.
15	12.81	Sustancial	Para la plataforma de gestión de vulnerabilidades, se debe tener el servicio de gestión y remediación según lo reportado en la herramienta , de modo que sirva de apoyo al área de DIGIT, para resolver todos los casos a remediar según los informes.....	Amablemente se solicita a la entidad tener en cuenta que la remediación de los componentes que hacen parte del presente proceso estarán a cargo del proveedor, sin embargo, las remediaciones de la infraestructura propia de la entidad deberá realizarla la entidad misma teniendo en cuenta que es quien la administra, opera y soporta.	Aclarar	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, las remediaciones y la intervenciones a las que haya lugar en la infraestructura propia de la Entidad, las realizará el personal de la DIAN, el futuro proveedor del SOC deberá realizar el acompañamiento desde el inicio y hasta la solución de las mismas, tal como se indica en el anexo técnico: 8.17 Apoyar con los recursos necesarios (personal idóneo) constantemente a la Dian realizando el respectivo acompañamiento, apoyo, experticia, experiencia, conocimiento en la resolución y remediación de todas y cada una de las vulnerabilidades encontradas durante la ejecución del contrato, se aclara que el personal de la Dian estará al frente de dichas actividades.
16	Mínimo de Trabajo	Sustancial	La certificación LPT	Amablemente se solicita a la entidad permitir certificaciones homologables como cehpt; ecppt,eJPT dado que la certificación LPT es poco común en el mercado y limita la participación	Se acepte para pluralidad, transparencia y participación internacional	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los perfiles solicitados obedecen a necesidades especificas de la Entidad, acorde a su misionalidad, por lo tanto, su cambio no es posible.
17	2.12	Sustancial	El ítem 2.12 exige "monitoreo de transacciones sintéticas o tecnologías similares o equiparables" dentro del SIEM. Las transacciones sintéticas son una funcionalidad típica de herramientas de monitoreo de disponibilidad (como SolarWinds, Datadog, Dynatrace), no de SIEM	. ¿Se acepta que esta capacidad se cumpla mediante la integración del SIEM con la herramienta de monitoreo existente (Orion) o con una herramienta de synthetic monitoring externa, cuyos resultados alimenten al SIEM?	Se acepte	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem permite equivalencia al mencionar que las características solicitadas se pueden cumplir con herramientas similares o equiparables, sin embargo, para evitar equivocos en el requerimiento de la Entidad, el ítem en mención 2.12 será eliminado del respectivo anexo técnico, cambio que se verá reflejado en la adenda a publicar en los próximos días.
18	2.20	Sustancial	El ítem 2.20 lista contextos de dispositivos incluyendo "Dispositivos ambientales como UPS, HVAC, hardware del dispositivo".	¿La Entidad confirma que estos dispositivos ambientales deben ser monitoreados directamente por el SIEM, o se acepta que sean monitoreados por la plataforma NOC (Orion) y sus alertas se integren al SIEM? Esta diferenciación es importante porque no todos los SIEM tienen parsers nativos para dispositivos HVAC/UPS.	Se acepte para pluralidad, transparencia y participación internacional	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la plataforma SIEM debe estar en capacidad de realizar la correlación de todas las fuentes mencionadas en el anexo de características técnicas y que sean susceptibles a ello, en este caso particular aplica para las UPS.
19	2.23	Sustancial	El ítem 2.23 exige "Supervisión del cambio de configuraciones en tiempo real" con funciones como "Recopilar archivos de configuración de red almacenados en repositorio versionado" y "Detección automatizada de cambios en el registro de Windows". Estas son capacidades de FIM (File Integrity Monitoring) y NCM (Network Configuration Management), funcionalidades que en la mayoría de SIEM se logran mediante agentes o integraciones.	¿Se confirma que se acepta cumplir esta capacidad mediante agentes del SIEM o mediante integración con herramientas especializadas?	Se confirme	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la plataforma SIEM debe estar en capacidad de realizar la correlación de todas las fuentes enunciadas en los diferentes ítems del anexo técnico para esta plataforma, en este caso se puede hacer con agentes del SIEM, siempre y cuando se cumpla con lo requerido para este ítem.
20	2.33	Sustancial	El ítem 2.33 exige "Supervisión de disponibilidad" con capacidades como "Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP" y "Cálculo de SLA". Estas son funcionalidades de plataformas de monitoreo de disponibilidad, no de SIEM	¿Se acepta que la Entidad utilice su plataforma Orion existente para estas funciones y que el SIEM las complemente mediante correlación de datos recibidos?	se acepte	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem refiere a la integración que debe tener este servicio con la plataforma de disponibilidad de la Entidad, sin embargo, para evitar equivocos en el requerimiento de la Entidad, el ítem en mención 2.33 será eliminado del respectivo anexo técnico, cambio que se verá reflejado en la adenda a publicar en los próximos días.
21	5.4.11	Sustancial	El ítem 5.4.11 exige que la solución "deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management)".	¿Se aceptaría también la categoría Gartner "Exposure Assessment Platforms" (publicada en noviembre 2025) como equivalente, dado que Gartner ha evolucionado la categoría de Vulnerability Risk Management hacia Exposure Assessment? Si solo se acepta el MQ de VRM antiguo, se está usando una referencia que Gartner ya discontinuó.	Se aclara la observación, se aceptaran fabricantes lideres de Gartner o Forrester en los cuadrantes Vulnerability Risk Management o Unified Vulnerability Management siempre y cuando se cumplan con los requerimientos	La Dirección de Impuestos y Aduanas Nacionales - DIAN, aclara al observante que, para el ítem en cuestión se aceptaran fabricantes lideres de Gartner o Forrester en los cuadrantes Vulnerability Risk Management o Unified Vulnerability Management siempre y cuando se cumplan con los requerimientos técnicos soportados con documentación publica del fabricante.
22	7.23 - 7.24	Sustancial	Los ítems 7.23 y 7.24 exigen capacidades de "investigación autónoma basada en inteligencia artificial" que genere reportes con "resumen ejecutivo del incidente" y "narrativa basada en procesamiento de lenguaje natural".	¿Se acepta que esta capacidad se logre mediante la integración del NDR con el SIEM/SOAR y herramientas de IA complementarias, o debe ser una funcionalidad nativa del NDR? La investigación autónoma con NLP embebido en el NDR es una característica de Darktrace Cyber AI Analyst, pero no es estándar en la industria NDR.	se acepte	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta su observación por cuanto la característica solicitada obedece a necesidades puntuales de la Entidad y se requiere que la Inteligencia de Amenazas la pueda realizar.
23	8.20	Sustancial	El ítem 8.20 exige que "las herramientas del CONTRATISTA deben utilizar SASE (Secure Access Services Edge), buscando seguridad en dispositivos móviles, Internet de las cosas y migración de aplicaciones on-premise hacia Cloud"	SASE es una arquitectura de red/seguridad (Zscaler, Palo Alto Prisma, Netskope) y no una funcionalidad de herramientas de análisis de código. ¿Podría la Entidad aclarar la relación entre SASE y el análisis de código del ítem 8? Tal como está redactado, introduce un requisito que no guarda relación funcional con SAST/DAST/SCA y podría generar confusión.	aclarar	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem referido menciona características de seguridad que se deben tener en cuenta en la implementación de dicha herramienta, pero no es en sí una funcionalidad del servicio o capacidad a adquirir.
24	General	Sustancial	Cronograma	Respetuosamente solicitamos a la entidad confirmar el cronograma establecido para el presente proceso de licitación, indicando de manera precisa las fechas de cada etapa del proceso, incluyendo publicación de adendas (si aplica), cierre del proceso, evaluación de ofertas, subsanación, adjudicación y firma del contrato. Lo anterior, con el fin de garantizar la debida planeación y participación oportuna de los proponentes en condiciones de transparencia e igualdad. ¿Cual es el cronograma que corresponde a la versión definitiva del proceso y si se prevén modificaciones mediante adenda?	Solicitar información	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, los documentos y demás información concerniente al proceso se encuentra publicada en el link https://www.dian.gov.co/dian/Paginas/Fondo-DIAN.aspx, allí los interesados pueden descargarlos y dentro de los mismo se encuentra estipulado el respectivo cronograma del proceso.
25	General	Sustancial	Link de audiencia	Solicitamos a la entidad confirmar cual es el link de la audiencia virtual 15 de abril y proceso para informar el equipo que participara,	Solicitud	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el link o enlace es comunicado a cada uno de los participantes previa presentación del formato que manifiesta su intención de participación.
26	General	Sustancial	Indicador de Capital de Trabajo	Respetuosamente solicitamos a la entidad revisar el requisito habilitante relacionado con el indicador de capital de trabajo en relación con el presupuesto oficial del proceso, establecido en un valor mínimo de ≥ 0,05. Lo anterior, teniendo en cuenta que este nivel de exigencia puede resultar desproporcionado frente a la naturaleza del objeto contractual y limitar la pluralidad de oferentes, especialmente cuando se trata de servicios donde la ejecución no requiere una alta inversión inicial en capital de trabajo, sino que se soporta en capacidades técnicas, operativas y esquemas de prestación progresiva del servicio. En este sentido, consideramos que el indicador exigido podría restringir la participación de empresas idóneas que cuentan con la experiencia y capacidad técnica requerida, pero que no necesariamente reflejan altos niveles de capital de trabajo en proporción al presupuesto del proceso. Por lo anterior, solicitamos respetuosamente a la entidad considerar alguna de las siguientes alternativas:Disminuir el valor del indicador a un nivel más acorde con el objeto contractual (por ejemplo ≥ 0,02).Esta solicitud se realiza en el marco de los principios de pluralidad de oferentes, selección objetiva y libre concurrencia, buscando garantizar una mayor participación sin comprometer la adecuada ejecución del contrato.	Solicitud	En atención a la observación no se acepta la solicitud, el indicador se mantiene debido a la envergadura del proyecto.

27	2.9		Debe tener correlación cruzada de analítica de SOC y NOC con capacidades de correlación cruzada de eventos y datos analíticos provenientes tanto del Centro de Operaciones de Seguridad (SOC) como del Centro de Operaciones de Red (NOC). Esta funcionalidad permitirá una visión integral del estado de la infraestructura tecnológica, facilitando la detección de incidentes que involucren tanto aspectos de seguridad como de disponibilidad, rendimiento y operación de red. Características mínimas requeridas: -Integración nativa o mediante conectores con plataformas NOC (monitorización de red, gestión de fallos, rendimiento, etc.). -Capacidad de correlacionar eventos de seguridad (SOC) con métricas operativas (NOC) para mejorar el contexto de los incidentes. -Visualización unificada de alertas y eventos correlacionados. -Soporte para reglas de correlación personalizadas y aprendizaje automático. -Mejora de la capacidad de respuesta ante incidentes mediante análisis contextual enriquecido. Para el efecto se informa que actualmente la Entidad cuenta con la plataforma de monitoreo ORION	Amablemente se solicita a la entidad aclarar si la recolección solicitada del NOC debe ser de la misma marca que la del SOC	Se solicita que la ingesta entregada por los dispositivos del NOC se traten como una fuente de terceros o una integración mas que genera ingesta al SIEM	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en el referido ítem el NOC se trataría como una fuente más para el SIEM, para lo cual el futuro proveedor deberá hacer la integración con el NOC de la Entidad.
28	2.12		Debe tener monitoreo de transacciones sintéticas o tecnologías similares o equiparables. Una transacción sintética es la que permite simular interacciones críticas con aplicaciones, servicios y sistemas para evaluar su disponibilidad, rendimiento y comportamiento desde una perspectiva de usuario final. Estas simulaciones deben ejecutarse de forma programada y controlada, generando datos que puedan ser correlacionados con eventos de seguridad y operativos.	Amablemente se solicita a la entidad el por que LA solicitud que se esta realizando no esta diseñada para una plataforma de ciberseguridad, ya que estas no incluyen capacidades de monitoreo sintético de transacciones para simular interacciones de usuario final con aplicaciones y servicios. Las observaciones están dirigidas para una plataforma de observabilidad, probablemente alguna de las siguientes? •Datadog Synthetics – scripted browser & API tests •Dynatrace Synthetic Monitoring – simulación completa de navegador •New Relic Synthetics – monitores programados •AWS CloudWatch Synthetics (Canaries) – verificaciones sintéticas basadas en Lambda •Eatchpoint / Pingdom / UptimeRobot – testing de disponibilidad y transacciones	Se solicita aclarar si lo que requiere la institución es un SIEM o una plataforma de obserbabilidad	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem permite equivalencia al mencionar que las características solicitadas se pueden cumplir con herramientas similares o equiparables, sin embargo, para evitar equivocos en el requerimiento de la Entidad, el ítem en mención 2.12 será eliminado del respectivo anexo técnico, cambio que se verá reflejado en la adenda a publicar en los próximos días.
29	2.19		Contexto en tiempo real para análisis de seguridad que incluya como mínimo: - Actualización continua del contexto, de los dispositivos, su software y parches instalados, así como los servicios en ejecución. - Análisis del rendimiento de aplicaciones y sistemas junto con datos del entorno para identificar rápidamente problemas de seguridad. - Contexto de usuario, en tiempo real, con seguimiento de direcciones IP, cambios de identidad de usuario, contexto de datos de ubicación física y geo-localización. - Detección de dispositivos, aplicaciones de red y cambios de configuración no autorizados.	Amablemente se solicita a la entidad el por que LA solicitud que se esta realizando no esta diseñada para una plataforma de ciberseguridad, ya que estas no incluyen capacidades de monitoreo sintético de transacciones para simular interacciones de usuario final con aplicaciones y servicios. Las observaciones están dirigidas para una plataforma de observabilidad, probablemente alguna de las siguientes? •Datadog Synthetics – scripted browser & API tests •Dynatrace Synthetic Monitoring – simulación completa de navegador •New Relic Synthetics – monitores programados •AWS CloudWatch Synthetics (Canaries) – verificaciones sintéticas basadas en Lambda •Eatchpoint / Pingdom / UptimeRobot – testing de disponibilidad y transacciones	Se solicita aclarar si lo que requiere la institución es un SIEM o una plataforma de obserbabilidad	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el servicio o capacidad requerida por la Entidad es un SIEM.
30	2.19		Contexto del dispositivo y de la aplicación, como mínimo debe incluir los siguientes elementos: - Dispositivos de red incluyendo switches, routers, WLAN. - Dispositivos de seguridad - Firewalls, IPS de red, gateways Web/Mail, protección contra malware, escáneres de vulnerabilidades. - Servidores, incluyendo Windows, Linux, AIX, HP UX. - Servicios de infraestructura incluyendo DNS, DHCP, DFS, AAA, controladores de dominio. - Aplicaciones orientadas al usuario, incluidos servidores Web, servidores de aplicaciones, correo, bases de datos. - Dispositivos de almacenamiento como (revisar contra inventario) - Cloud Apps, incluyendo AWS, Azure. - Infraestructura de la nube incluyendo AWS. - Dispositivos ambientales como UPS, HVAC, hardware del dispositivo. - Infraestructura de virtualización incluyendo VMware ESX, Microsoft HyperVScalable .	Se habal de contexto, termino aplicado a OBSERVABILIDAD, amablemente solicitamos aclarar si lo que se esta solicitando en un SIEM o es una plataforma de OBSERVABILIDAD	Se habal de contexto, termino aplicado a OBSERVABILIDAD, amablemente solicitamos aclarar si lo que se esta solicitando en un SIEM o es una plataforma de OBSERVABILIDAD	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el servicio o capacidad requerida por la Entidad es un SIEM.
31	2.21		Informes de Cumplimiento Out-of-the-Box, como mínimo debe incluir los siguientes elementos: - Informes predefinidos listos para ser utilizados, que soporten una amplia gama de necesidades de auditoría y cumplimiento normativo, incluyendo: PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13 y SANS Critical Controls.	Amablemente solicitamos ala entidad que avlare cual de estas normativas les aplica y cual están interesados en cumplir	Retirar las normativas que no son de interés de la institución.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, tal como se indica en el respectivo requerimiento se deben cumplir con las normativas solicitadas.
32	2.22		Supervisión de rendimiento, como mínimo debe incluir los siguientes elementos: - Monitor de métricas de sistema (almacenamiento, rendimiento, memoria, etc.). - Estado del sistema a través de SNMP, WMI, PowerShell. - Estado de aplicaciones a través de JMX, WMI, PowerShell. - Supervisión de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster. - Monitorización del rendimiento de aplicaciones a medida. - Microsoft Active Directory y Exchange a través de WMI y Powershell. - Posibilidad de agregar métricas personalizadas.	Amablemente se solicita a la entidad, revisar erte requerimiento, ya que se esta solicitando recopilar información relacionada a eventos de maquina y no a Ciberseguridad	Retirar el requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible retirar este requerimiento.
33	2.25		Analitica - Búsqueda de eventos en real - sin necesidad de indexación. - Búsquedas por palabras clave basadas en atributos de eventos analizados. - Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API. - Match de patrones complejos en tiempo real. - Uso de objetos CMDB y datos de usuario/identidad y ubicación en búsquedas y reglas. - Programación de informes y entregas de resultados por correo electrónico a los principales interesados. - Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.). - Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico. - Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes. - Análisis escalable mediante la adición de nodos worker en caliente. - Posibilidad de priorización de los informes de incidentes.	Se solicita aclarar a la entidad el porque se solicita Escalabilidad mediante nodos worker en caliente, esto alica para soluciones en premisas y limita la pluralidad de oferentes	Se solicita amablemente retirar este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem será ajustado, para evitar equivocos en el requerimiento de la Entidad, quedando de la siguiente manera, cambio que se verá reflejado en la adenda a publicar en los próximos días: Analítica - Búsquedas por palabras clave basadas en atributos de eventos analizados. - Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API. - Match de patrones complejos en tiempo real. - Programación de informes y entregas de resultados por correo electrónico a los principales interesados. - Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.). - Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico. - Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes.. - Posibilidad de priorización de los informes de incidentes.
34	2.33		Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos: - Sistema de monitorización de estado - a través de Ping, SNMP, WMI, Uptime Analysis, interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento. - Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP. - Monitorización del hardware y del entorno. - Calendario para la programación de las ventanas de mantenimiento. - Cálculo de SLA – consideración de las horas normales de trabajo y fuera de horas.	Estos requisitos no son propios de una herramienta de ciberseguridad, sino que aplican a una herramienta de monitorización de operaciones IT (APM/NPM)	Se solicita ala entidad, retirar este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem refiere a la integración que debe tener este servicio con la plataforma de disponibilidad de la Entidad, sin embargo, para evitar equivocos en el requerimiento de la Entidad, el ítem en mención 2.33 será eliminado del respectivo anexo técnico, cambio que se verá reflejado en la adenda a publicar en los próximos días.

35	2.34		Almacenamiento - Soporte de archivado de logs tanto para NFS como HDFS. - Creación de políticas de retención de logs tanto por espacio como por periodos de tiempo.	Amablemente solicitamos a la entidad, que nos aclare porque solicita este tipo de formatos de almacenamiento, es decir si esto obedece a alguna necesidad puntual de la organización.	Se solicita retirar este requerimiento y que se permita contar con un sistema de almacenamiento nativo basado en infraestructura cloud	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible retirar este requerimiento.
36	3.13		Mostrar un dashboard de monitoreo de estado de integraciones y también el estado del sistema del motor SOAR.	Amablemente se solicita a la entidad que se tome como base para este requerimiento, el estado de salud general de la solución ofertada	Amablemente se solicita a la entidad que se tome como base para este requerimiento, el estado de salud general de la solución ofertada	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento es claro en cuanto a: "*Mostrar un dashboard de monitoreo de estado de integraciones y también el estado del sistema del motor SOAR",* por lo tanto, no es posible aceptar su sugerencia.
37	3.19		Las alertas y los incidentes deben manejarse por separado, cada uno en su propio módulo de interfaz de usuario. Las interfaces de gestión de alertas e incidentes deben ser personalizables para permitir una visualización flexible de la información, incluida la visualización de información de la alerta en sí más información adicional devuelta por los playbook de investigación.	La solución debe disponer de vistas diferenciadas para la gestión de alertas individuales y para la gestión de incidentes correlacionados, permitiendo al analista navegar entre ambas vistas sin perder el contexto de la investigación. Dichas vistas deben permitir filtrar, ordenar y configurar las columnas de información visualizada. La solución debe proveer registro auditado de las acciones y enriquecimientos ejecutados por los playbooks de automatización, accesible en el contexto del caso o incidente gestionado	La solución debe disponer de vistas diferenciadas para la gestión de alertas individuales y para la gestión de incidentes correlacionados, permitiendo al analista navegar entre ambas vistas sin perder el contexto de la investigación. Dichas vistas deben permitir filtrar, ordenar y configurar las columnas de información visualizada. La solución debe proveer registro auditado de las acciones y enriquecimientos ejecutados por los playbooks de automatización, accesible en el contexto del caso o incidente gestionado	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, para el ítem en cuestión se debe cumplir con lo solicitado, no es posible ajustarlo según sugerencia.
38	7.3		Se debe licenciar como mínimo para 25000 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web).	lo que eyo enccual es la cantidad de througput a inspeccionar y cantidad de segmentos de red debido a que no todas las soluciones se cotizan con cantidad de activosontre	Se debe licenciar un througput de XXx Gbytes como mínimo para 25000 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web)	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, lo requerido en este ítem es muy claro: "*Se debe licenciar como mínimo para 25000 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web)",* y esta información permite a los interesados dimensionar su ofrecimiento.
39	7.10		La herramienta debe utilizar modelos matemáticos probabilísticos de estimación, analizando y correlacionando múltiples dimensiones distintas dentro del paquete, con el fin de validar los comportamientos anómalos en la red.	no todas las tecnologías lo hacen por probabilidad, hay otras que lo hacen por firmas, por reputación , sanbox, porque cerrar el pliego a este tipo de detección	La herramienta deberá contar con capacidades avanzadas de analítica para la detección de comportamientos anómalos en la red, mediante el uso de modelos analíticos, estadísticos, probabilísticos, de aprendizaje automático y/o técnicas equivalentes. Estas capacidades deberán analizar y correlacionar múltiples dimensiones de telemetría, tráfico, eventos, entidades y contexto operativo, con el fin de identificar desviaciones, patrones sospechosos y actividades potencialmente maliciosas con un nivel adecuado de precisión y reducción de falsos positivos.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible ajustar según su sugerencia.
40	7.11		El servicio debe proporcionar visibilidad completa de la red, incluidas las tecnologías tradicionales (como servidores físicos, estaciones de trabajo, dispositivos de red, entre otros) y no tradicionales (como dispositivos IoT, entornos OT, servicios en la nube, contenedores, microservicios y aplicaciones SaaS, entre otros).	confirmar que equipos y protocolos tiene en entornos OT, IoT y en la nube, dar un poco mas de detalle sobre estas superficies de ataque	El servicio deberá proporcionar visibilidad integral y continua sobre los activos y superficies tecnológicas de la organización, incluyendo entornos tradicionales y modernos. Esto deberá contemplar, como mínimo, activos de TI convencionales (servidores físicos y virtuales, estaciones de trabajo, dispositivos de red, entre otros), así como activos no tradicionales o especializados, tales como dispositivos IoT, entornos OT/ICS, cargas de trabajo en nube pública o privada, contenedores, microservicios, aplicaciones SaaS y demás recursos conectados o administrados dentro del entorno corporativo. La visibilidad podrá obtenerse mediante mecanismos nativos o integraciones soportadas por el fabricante.	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el inventario de la infraestructura tecnológica se encuentra detallado tanto en el documento SDO (Solicitud de Oferta), así como también en el documento anexo de características técnicas mínimas.
41	7.14		Capacidad de realizar consultas a los datos capturados y almacenados en el hardware de uso específico (appliance) sin conectarse a la nube, como mínimo se debe tener un tiempo de retención de seis (6) meses.	es una solución full on-premise? O solo están restringiendo el ndr para uso de datos on-premise? El solución debe tener la posibilidad de llevar la información a la nube o de esta manera no se tendría pluralidad de oferentes	La solución deberá permitir la consulta, búsqueda, análisis e investigación de los datos capturados y almacenados por la plataforma desde una consola centralizada, sin requerir infraestructura dedicada tipo appliance como condición obligatoria. La solución podrá operar en modalidad SaaS, híbrida, virtual o equivalente, siempre que garantice acceso seguro a la información histórica y capacidades avanzadas de búsqueda e investigación. Como mínimo, deberá ofrecer una retención de datos de seis (6) meses, ya sea de forma nativa o mediante opciones de almacenamiento soportadas por el fabricante.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las soluciones solicitadas pueden ser de tipo onpremise, nube, SaaS o cualquier otra modalidad siempre y cuando se cumplan las características requeridas para dicho servicio.
42	7.15		La solución debe poder realizar una captura de paquetes en tiempo real que permita un monitoreo de incidentes en el momento de su ocurrencia, así como ofrecer la opción de análisis exhaustivo de paquetes tanto en Wireshark como dentro de su propia interfaz de usuario permitiendo hacer la extracción en formatos .pcap y otros, o sus equivalentes de acuerdo a las tecnologías ofrecidas.		La solución deberá contar con capacidades de captura, inspección, análisis y/o reconstrucción de tráfico de red en tiempo real o bajo demanda, que permitan apoyar el monitoreo e investigación de incidentes durante su ocurrencia o posterior análisis forense. Asimismo, deberá permitir la exportación de evidencias técnicas en formatos estándar del mercado (como .pcap u otros equivalentes) y/o	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible ajustar según su sugerencia.
43	7.16		La solución debe permitir la personalización y adaptación del aprendizaje automático a condiciones y características específicas de la red.	**el aprendizaje automática es de una solución específica y hace que las otras soluciones que lo hace por medio de firmas, reputación , sandbox no puedan participar , este requerimiento debería ser opcional**	Se solicita ala entidad, retirar este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible retirar este requerimiento.
44	7.17		Capacidad para identificar cualquier amenaza anómala en la red en tiempo real a través del aprendizaje automático e inteligencia artificial.	**el aprendizaje automática es de una solución específica y hace que las otras soluciones que lo hace por medio de firmas, reputación , sandbox no puedan participar , este requerimiento debería ser oocional**	Se solicita ala entidad, retirar este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible retirar este requerimiento.
45	7.18		El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 17727 dispositivos por (3) años.	cual es la cantidad de througput a inspeccionar y cantidad de segmentos de red debido a que no todas las soluciones se cotizan con cantidad de activos	Se solicita ala entidad, retirar este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la cantidad de dispositivos es 25000, para lo cual se procederá a modificar la cantidad expresada en este ítem quedando de la siguiente manera, cambio que se verá reflejado en la adenda a publicar en los próximos días: 7.18 El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 25000 dispositivos por (3) años.
46	7.20		Después del período de aprendizaje inicial, la tecnología debe proporcionar automáticamente un seguimiento de auditoría completo de todos los dispositivos en el entorno, clasificando previamente al menos el tipo de dispositivo, el nombre de host, la dirección MAC, la primera y la última vez que se detectó el dispositivo en la red	**el aprendizaje automática es de una solución específica y hace que las otras soluciones que lo hace por medio de firmas, reputación , sandbox no puedan participar , este requerimiento debería ser opcional**	Se solicita ala entidad, retirar este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible retirar este requerimiento.

47	7.23		La tecnología deberá proporcionar la capacidad de realizar procedimientos automatizados por parte del proveedor del servicio para la cacería de amenazas basados en inteligencia artificial con al menos las siguientes capacidades: - Procesos de Threat Hunting basados en anomalías de comportamiento detectadas por la inteligencia artificial. - Los procesos de Threat Hunting deberán indicar las fases del ciberataque en lo que se hayan visto la/las anomalías detectadas en el comportamiento. - El proceso de Threat Hunting deberá poder correlacionar anomalías detectadas dentro de la misma plataforma de IA e identificar si pertenecen o no a un ataque más complejo. Se deben validar con otras fuentes de información que llegan al correlacionador para dar mayor contexto a los hallazgos identificados por la inteligencia Artificial. - Se deberá poder integrar el proceso de Threat Hunting automatizado para que otros servicios vía API puedan solicitar informes de cacería de amenazas de manera automatizada. - Se deben poder solicitar investigaciones autónomas y a demanda a la inteligencia artificial, donde el disparador pueda ser una anomalía ya detectada o una simple investigación a demanda. - El proceso de Threat Hunting deberá proporcionar un informe base entregado por la inteligencia artificial y uno adicional con la información de contexto y otras investigaciones adicionales realizadas por los analistas humanos. - El proceso deberá tener la capacidad de realizar investigaciones continuas 24/7 y en tiempo real de las anomalías detectadas por la inteligencia artificial - Se deberán realizar procesos de Threat Hunting manuales basados en TTP's mitre de manera recurrente, identificando qué anomalías detectadas por la plataforma de Inteligencia Artificial hacen parte de las técnicas buscadas para	la cacería de amenazas basada solo en inteligencia artificial y en aprendizaje es un modelo que generar muchos falsos positivos si no queda bien entrenada y un mayor tiempo de protección , por lo que también se debería contemplar el uso de firmas o el uso de varias capas como sandbox para las detecciones	Se solicita ala entidad, retirar este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible retirar este requerimiento.
48	7.26		La solución debe ser una plataforma de autoaprendizaje y tener un enfoque adaptativo que utilice inteligencia artificial comprobada para aprender sobre el entorno en el que se encuentra, detectar y responder a las desviaciones de la línea de base normal de comportamiento, así: - La línea base de la red debe ser lo suficientemente adaptable y dinámica para adaptarse a cualquier cambio en el comportamiento del entorno - Debe funcionar completamente en función del comportamiento, donde no se permitan las tecnologías que hacen uso de reglas y / o firmas	**el aprendizaje automática es de una solución específica y hace que las otras soluciones que lo hace por medio de firmas, reputación , sandbox no puedan participar , este requerimiento debería ser opcional**	Se solicita ala entidad, retirar este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Ítem 7.26 será ajustado, para evitar equivocos en el requerimiento de la Entidad, quedando de la siguiente manera, cambio que se verá reflejado en la adenda a publicar en los próximos días: La solución debe ser una plataforma de autoaprendizaje y tener un enfoque adaptativo que utilice inteligencia artificial comprobada para aprender sobre el entorno en el que se encuentra, detectar y responder a las desviaciones de la línea de base normal de comportamiento, así: - La línea base de la red debe ser lo suficientemente adaptable y dinámica para adaptarse a cualquier cambio en el comportamiento del entorno. - Debe trabajar en función del comportamiento.
49	7.29		La solución debe utilizar varios algoritmos de inteligencia artificial, así como varias técnicas de Machine Learning como: Deep Learning, Machine Learning supervisado y Machine Learning no supervisado	**el aprendizaje automática es de una solución específica y hace que las otras soluciones que lo hace por medio de firmas, reputación , sandbox no puedan participar , este requerimiento debería ser opcional**	Se solicita ala entidad, retirar este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible retirar este requerimiento.
50	5.11.3		La solución ofertada deberá poseer capacidades de auto remediación.	en este caso la plataforma puede tomar ciertas acciones, aclaras que tipo de remediación se necesita	Se solicita ala entidad, retirar este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible retirar este requerimiento.
51	5.4.6		La solución ofertada deberá realizar una gestión de vulnerabilidades basadas en el riesgo, permitiendo una priorización dinámica de las tareas de remediación en función de las amenazas; permitiendo así el despliegue de parches o actualizaciones en aplicativos de endpoints y servidores, garantizando los flujos de aprobaciones requeridos para el despliegue automático de estas actualizaciones.	solicitamos sea retirado el ítem de despliegue de parches	Se solicita ala entidad, retirar este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible retirar este requerimiento.
52	5.4.10		La solución ofertada deberá soportar funcionalidades de seguridad de doble factor de autenticación.	se requiere que las funcionalidades sean para el acceso a la consola de gestión o para controlar el doble factor hacia usuarios?	Se solicita ala entidad, retirar este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible retirar este requerimiento.
53	5.4.11		La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	solicitamos sea retirado este ítem	Se solicita ala entidad, retirar este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible retirar este requerimiento.
54	3.22		Permitir definir las condiciones que se deben cumplir antes de que se pueda ejecutar un playbook y limitar los playbook que se muestran al analista a aquellos que son relevantes para la vista actual.	La solución debe permitir configurar lógica condicional en los playbooks de automatización (criterios de activación por severidad, tipo de detección, origen del sensor, programación horaria y resultados de pasos previos del propio playbook), de modo que las acciones de respuesta solo se ejecuten cuando se cumplan las condiciones predefinidas. El control de qué playbooks puede ver y ejecutar cada analista debe gestionarse mediante roles y permisos (RBAC), garantizando que cada perfil de analista acceda únicamente a los playbooks correspondientes a sus responsabilidades asignadas	La solución debe permitir configurar lógica condicional en los playbooks de automatización (criterios de activación por severidad, tipo de detección, origen del sensor, programación horaria y resultados de pasos previos del propio playbook), de modo que las acciones de respuesta solo se ejecuten cuando se cumplan las condiciones predefinidas. El control de qué playbooks puede ver y ejecutar cada analista debe gestionarse mediante roles y permisos (RBAC), garantizando que cada perfil de analista acceda únicamente a los playbooks correspondientes a sus responsabilidades asignadas	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible ajustar según su sugerencia.
55	1.2	Sustancial	Se debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá que cuente con las condiciones adecuadas para garantizar la continuidad operativa, la seguridad física y lógica, y el cumplimiento de las mejores prácticas del sector.	Con el objetivo de garantizar la resiliencia del servicio sin incurrir en exigencias de infraestructura física obsoletas, se recomienda respetuosamente a la Entidad flexibilizar y aclarar el alcance de la continuidad operativa. Se está de acuerdo con mantener la sede física principal de analistas en la ciudad de Bogotá o sus alrededores; sin embargo, en las arquitecturas modernas de ciberseguridad, la continuidad no depende de tener un segundo edificio con personal en otra ciudad, sino de contar con infraestructuras tecnológicas resilientes. Por lo tanto, solicitamos que se permita y valore que el Centro de Datos que soporta las plataformas (SIEM, SOAR, etc.) pueda estar distribuido en esquemas de alta disponibilidad, ya sea mediante centros de datos dispersos geográficamente o en arquitecturas de nube (Cloud). Asimismo, para el personal operativo (analistas), el cumplimiento se debe garantizar mediante un Plan de Continuidad de Negocio (BCP) que contemple esquemas de operación alterna o remota segura en caso de contingencia en la sede principal.	Se debe contar con un Centro de Operaciones de Seguridad - SOC principal ubicado en una locación física en la ciudad de Bogotá o sus alrededores, que cuente con las condiciones adecuadas de seguridad física y lógica. Para garantizar la continuidad operativa ante contingencias, el oferente deberá contar con un Plan de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP) estructurado. Dicho plan debe garantizar: 1) La continuidad de la operación del recurso humano (analistas) ante indisponibilidad de la sede principal; y 2) La alta disponibilidad de las plataformas tecnológicas que soportan el servicio, permitiendo que la infraestructura de procesamiento (Centros de Datos) opere de manera redundante, geográficamente dispersa o bajo modelos de nube (Cloud) que asegure la ininterrumpida del	a Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, tal como se indica en el requerimiento, el futuro proveedor de SOC puede entregar dos Centros de Operaciones en la ciudad de Bogotá u optar por tener uno en la Ciudad de Bogotá y otro en otra locación diferente a esta ciudad, aclarando que lo que se requiere es que el SOC (Personal, Infraestructura Física y Técnica, entre otros) esté en la Ciudad de Bogotá, más no el centro de datos que soporta dicha operación, en el entendido de que muchos SOC´s tienen su operación en la nube o en un centro de datos de terceros, sin embargo, para una mejor comprensión de lo solicitado y así evitar equivocos, se informa que se hará la respectiva modificación que se publicará en adenda en los próximos días, para los ítems 1.2 y 12.80 quedando de la siguiente manera: 1.2 Se debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá que cuente con las condiciones adecuadas para garantizar la continuidad operativa, la seguridad física y lógica, y el cumplimiento de las mejores prácticas del sector. Desde donde se administrarán todos los productos, capacidades, plataformas, soluciones y servicios, que sean requeridos para dar cumplimiento a lo solicitado en el anexo técnico y que le permitan realizar todas las actividades encomendadas en este documento por la DIAN. Aclarando que lo que se requiere es que el SOC (Personal, Infraestructura Física y Técnica, entre otros) esté en la Ciudad de Bogotá, más no el centro de datos que soporta dicha operación, en el entendido de que muchos SOC´s tienen su operación en la nube o en un centro de datos de terceros. Entendiéndose que el CONTRATISTA realizará toda la gestión, monitoreo, administración, optimización, actualización, acompañamiento, soporte y garantía de los mismos, cobijando toda la infraestructura tecnológica de la Entidad. Para el efecto debe tener la capacidad de detectar, escalar, informar, acompañar apoyar y soportar a la DIAN en la resolución de cada uno de los incidentes encontrados por el SOC durante el tiempo que dure el proyecto en mención. Los activos y demás características de estos se encuentran detallados en el apartado de inventarios y las especificaciones de cada una de las soluciones, plataformas, capacidades, servicios, soporte y garantía se encuentran en este anexo técnico de obligatorio cumplimiento. 12.80 El servicio del SOC deberá contar como mínimo con dos (2) centros de operaciones de seguridad geográficamente ubicados en diferentes lugares dentro de Bogotá D.C o uno de estos puede estar fuera de Bogotá, siendo este para contingencia o alta disponibilidad, así mismo se indica que lo que se requiere es que el SOC (Personal, Infraestructura Física y Técnica, entre otros) esté en la Ciudad de Bogotá, más no el centro de datos que soporta dicha operación, en el entendido de que muchos SOC´s tienen su operación en la nube o en un centro de datos de terceros.

57	2.8	Sustancial	Debe tener autoaprendizaje de inventario de activos (CMDB) contando con capacidades de descubrimiento automático para alimentar y mantener actualizada la Base de Datos de Gestión de Configuración (CMDB). Esto implica que el sistema debe ser capaz de identificar, clasificar y registrar de forma dinámica los activos tecnológicos presentes en la infraestructura, incluyendo servidores, estaciones de trabajo, dispositivos de red, aplicaciones y servicios, sin intervención manual constante. Para tal efecto se informa que actualmente la Entidad cuenta con un ITSM del fabricante ARANDA. Características mínimas requeridas: - Descubrimiento automático de nuevos activos en la red. - Actualización continua de la CMDB ante cambios en la infraestructura. - Integración con herramientas de escaneo de red y agentes locales. - Capacidad de correlación entre activos y eventos de seguridad. - Soporte para múltiples entornos (on-premise, nube, híbrido).	Se solicita respetuosamente a la Entidad la modificación de la exigencia que obliga al SIEM a contar con capacidades de autodescubrimiento para alimentar una CMDB propia. Exigir esta característica constituye una restricción injustificada a la pluralidad de oferentes y un direccionamiento hacia plataformas de nicho, excluyendo de tajo a los SIEM líderes mundiales en ciberseguridad, cuyo diseño arquitectónico se centra en la analítica avanzada de amenazas y no en el escaneo y descubrimiento de activos de TI. Adicionalmente, este requerimiento genera una duplicidad de funciones y contradice las mejores prácticas de gestión de servicios de TI (ITIL). Al confirmar que la Entidad ya cuenta con la solución ARANDA ITSM como su herramienta institucional para la gestión de la base de datos de configuración (CMDB), obligar al SIEM a construir y mantener una segunda CMDB paralela crearía 'silos de información' y rompería el principio de la 'Única Fuente de Verdad' (Single Source of Truth) corporativa. Por lo anterior, para garantizar la selección objetiva y la eficiencia operativa, solicitamos amablemente que el requerimiento se enfoque en la capacidad del SIEM para integrarse de manera nativa o vía API con la CMDB existente.	La solución debe integrarse bidireccionalmente y de manera automatizada con la Base de Datos de Gestión de Configuración (CMDB) de la Entidad (ARANDA ITSM) para enriquecer el contexto de los activos y eventos de seguridad de forma dinámica, o en su defecto, contar con capacidades de descubrimiento de activos integradas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, para una mejor comprensión y entendimiento del ítem en cuestión esta será ajustado de la siguiente manera, cambio que se verá reflejado en la adenda a publicar en los próximos días: La solución debe integrarse bidireccionalmente y de manera automatizada con la Base de Datos de Gestión de Configuración (CMDB) de la Entidad (ARANDA ITSM) para enriquecer el contexto de los activos y eventos de seguridad de forma dinámica, o en su defecto, contar con capacidades de descubrimiento de activos integradas.
58	2.9	Sustancial	Debe tener correlación cruzada de analítica de SOC y NOC con capacidades de correlación cruzada de eventos y datos analíticos provenientes tanto del Centro de Operaciones de Seguridad (SOC) como del Centro de Operaciones de Red (NOC). Esta funcionalidad permitirá una visión integral del estado de la infraestructura tecnológica, facilitando la detección de incidentes que involucren tanto aspectos de seguridad como de disponibilidad, rendimiento y operación de red. Características mínimas requeridas: -Integración nativa o mediante conectores con plataformas NOC (monitorización de red, gestión de fallos, rendimiento, etc.). -Capacidad de correlacionar eventos de seguridad (SOC) con métricas operativas (NOC) para mejorar el contexto de los incidentes. -Visualización unificada de alertas y eventos correlacionados. -Soporte para reglas de correlación personalizadas y aprendizaje automático. -Mejora de la capacidad de respuesta ante incidentes mediante análisis contextual enriquecido. Para el efecto se informa que actualmente la Entidad cuenta con la plataforma de monitoreo ORION	La Entidad ya cuenta con la plataforma SolarWinds ORION para el monitoreo de red (NOC) y métricas de rendimiento. Exigir que el SIEM realice tareas nativas de NOC como el monitoreo de transacciones sintéticas, métricas JMX, estados BGP/OSPF y supervisión de disponibilidad, duplica funciones ya existentes en la Entidad y restringe la pluralidad de oferentes al direccionar el pliego hacia herramientas híbridas (Ver https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortisiem-mssp.pdf página 2). Se sugiere eliminar los requisitos de monitoreo de disponibilidad/rendimiento nativo y, en su lugar, exigir la integración del SIEM con SolarWinds ORION.	El SIEM debe tener capacidad de correlación cruzada de analítica de SOC y NOC mediante integración con la plataforma de monitoreo NOC de la Entidad (SolarWinds ORION). Esto permitirá correlacionar eventos de seguridad con métricas operativas. Se eliminan los requerimientos de monitoreo nativo de disponibilidad, transacciones sintéticas y rendimiento dentro del SIEM.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en el referido ítem el NOC se trataría como una fuente más para el SIEM, para lo cual el futuro proveedor deberá hacer la integración con el NOC de la Entidad.
59	2.12	Sustancial	Debe tener monitoreo de transacciones sintéticas o tecnologías similares o equiparables. Una transacción sintética es la que permite simular interacciones críticas con aplicaciones, servicios y sistemas para evaluar su disponibilidad, rendimiento y comportamiento desde una perspectiva de usuario final. Estas simulaciones deben ejecutarse de forma programada y controlada, generando datos que puedan ser correlacionados con eventos de seguridad y operativos.	La Entidad ya cuenta con la plataforma SolarWinds ORION para el monitoreo de red (NOC) y métricas de rendimiento. Exigir que el SIEM realice tareas nativas de NOC como el monitoreo de transacciones sintéticas, métricas JMX, estados BGP/OSPF y supervisión de disponibilidad, duplica funciones ya existentes en la Entidad y restringe la pluralidad de oferentes al direccionar el pliego hacia herramientas híbridas (Ver https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortisiem-mssp.pdf página 2). Se sugiere eliminar los requisitos de monitoreo de disponibilidad/rendimiento nativo y, en su lugar, exigir la integración del SIEM con SolarWinds ORION.	El SIEM debe tener capacidad de correlación cruzada de analítica de SOC y NOC mediante integración con la plataforma de monitoreo NOC de la Entidad (SolarWinds ORION). Esto permitirá correlacionar eventos de seguridad con métricas operativas. Se eliminan los requerimientos de monitoreo nativo de disponibilidad, transacciones sintéticas y rendimiento dentro del SIEM.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem permite equivalencia al mencionar que las características solicitadas se pueden cumplir con herramientas similares o equiparables, sin embargo, para evitar equivocos en el requerimiento de la Entidad, el ítem en mención 2.12 será eliminado del respectivo anexo técnico, cambio que se verá reflejado en la adenda a publicar en los próximos días.
60	2.13	Sustancial	La solución debe estar en capacidad de instalarse en Azure, AWS, HyperV (en la versiones con que cuenta la entidad), VMware (en la versiones con que cuenta la entidad). (Revisar archivo anexo inventarios), se aclara que la Entidad cuenta con Windows Server 2012R2, Windows Server 2022 y VMware ESXi, 7.0.3	Con el fin de garantizar la escalabilidad y eficiencia operativa, se sugiere respetuosamente a la Entidad aceptar y priorizar plataformas SIEM en modalidad SaaS (Software as a Service). Obligar a que la solución se instale exclusivamente en la infraestructura local (VMware/Hyper-V) genera una fuerte carga de coadministración y una dependencia operativa constante hacia los equipos internos de virtualización de la Entidad. Adicionalmente, debido a la escasez global en la cadena de suministro de componentes de hardware, particularmente de memoria RAM, sostener el crecimiento de cómputo en premisas para una plataforma de tan alto consumo como un SIEM representa un riesgo operativo y de sobrecostos a mediano plazo. Adoptar un modelo SaaS elimina estos cuellos de botella, transfiriendo toda la responsabilidad de procesamiento, mantenimiento y alta disponibilidad directamente al fabricante.	La solución debe entregarse preferiblemente en modalidad SaaS (Software as a Service) nativa, alojada, procesada y administrada en la nube del fabricante, evitando el consumo de recursos de cómputo internos de la Entidad. Alternativamente, en caso de que la arquitectura ofertada requiera despliegue en la infraestructura del cliente, la solución debe estar en la capacidad de instalarse en Azure, AWS, HyperV o VMware (considerando las versiones con que cuenta la entidad: Windows Server 2012R2, Windows Server 2022 y VMware ESXi, 7.0.3).	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible ajustar según su sugerencia.
61	2.18	Sustancial	Una vez integrada toda la plataforma tecnológica, se debe configurar y afinar la herramienta de correlación para mejorar su funcionalidad, tomando como base al menos los siguientes eventos: - Actividades asociadas a la administración de cuentas de usuario final (UserID) - Actividades asociadas a cuentas de altos privilegios, automáticas de procesos o asignadas a usuarios administradores (root, sa, administrator). - Ejecución de comandos especiales sobre sistemas operativos - Ejecución de comandos especiales sobre bases de datos (dump,drop, delete, insert, update) - Cambios de parámetros técnicos, de configuración o de seguridad - Cambios de configuración horaria. - Cambios no autorizados en recursos tecnológicos críticos - Actividades de conexión de cuentas de usuario final o administradores. - Actividades asociadas a manipulación de bitácoras técnicas (LOGs) o interrupciones en el envío de los LOGs. - Actividades asociadas a conexión de acceso remoto. - Actividades asociadas a la no efectividad de controles en el ejercicio del monitoreo transaccional.	Respecto a la configuración de casos de uso para el monitoreo de cuentas de altos privilegios (root, sa, administrator), ejecución de comandos especiales y actividades de acceso remoto, solicitamos a la Entidad confirmar si actualmente cuenta con una solución de Gestión de Accesos Privilegiados (PAM). En caso negativo, se recomienda respetuosamente contemplar la adopción de una plataforma PAM a corto plazo. Depender exclusivamente de una herramienta de propósito general como un SIEM para supervisar identidades críticas representa un enfoque reactivo basado únicamente en logs (los cuales pueden ser evadidos o manipulados). Una solución PAM es la plataforma especializada idónea para gobernar, rotar y controlar estos accesos de manera preventiva, delegando al SIEM su función principal: la correlación de alertas de seguridad generadas por el PAM, evitando así falsos positivos y sobrecarga operativa.	Una vez integrada toda la plataforma tecnológica, se debe configurar y afinar la herramienta de correlación para mejorar su funcionalidad, tomando como base los eventos de seguridad de la infraestructura. Para las actividades asociadas a cuentas de altos privilegios, ejecución de comandos especiales (OS y Bases de Datos) y conexiones remotas administrativas, el SIEM deberá integrarse con la solución de Gestión de Accesos Privilegiados (PAM) de la Entidad para correlacionar sus alertas nativas. En caso de no contar con un PAM, el SIEM realizará el monitoreo a través de la correlación de logs transaccionales nativos de los sistemas origen, como medida mitigante.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible ajustar según su sugerencia.
62	2.25	Sustancial	Analítica - **Búsqueda de eventos en real - sin necesidad de indexación.** - Búsquedas por palabras clave basadas en atributos de eventos analizados. - Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API. - Match de patrones complejos en tiempo real. - **Uso de objetos CMDB y datos de usuario/identidad y ubicación en búsquedas y reglas.** - Programación de informes y entregas de resultados por correo electrónico a los principales interesados. - Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.). - Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico. - Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes. - **Análisis escalable mediante la adición de nodos worker en caliente.** - Posibilidad de priorización de los informes de incidentes.	Exigir que la búsqueda en tiempo real sea estrictamente 'sin necesidad de indexación' limita arquitecturas líderes del mercado que utilizan indexación en tiempo real de alta velocidad o procesamiento en streaming. Solicitamos modificar el requerimiento a: 'Búsqueda y correlación de eventos en tiempo real o en flujo (streaming analytics), independientemente del orden de la indexación en la arquitectura del fabricante'. Se solicita a la Entidad flexibilizar este requerimiento para aceptar el uso de datos de contexto, modelos de datos, listas enriquecidas o bases de datos de activos externos integrados, en lugar de restringirlo al uso exclusivo del término 'objetos CMDB', el cual hace alusión al fabricante Fortinet (Ver https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortisiem-mssp.pdf página 2]). Solicitamos a la Entidad modificar el término propietario 'nodos worker' por un término genérico de arquitectura, permitiendo que la solución escale el análisis mediante la adición de nodos de procesamiento, indexación o correlación, de acuerdo con la nomenclatura y arquitectura distribuida propia de cada fabricante, sin requerir reinicios (en caliente). Ver término en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSIEM.pdf		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem será ajustado, para evitar equivocos en el requerimiento de la Entidad, quedando de la siguiente manera, cambio que se verá reflejado en la adenda a publicar en los próximos días: Analítica - Búsquedas por palabras clave basadas en atributos de eventos analizados. - Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API. - Match de patrones complejos en tiempo real. - Programación de informes y entregas de resultados por correo electrónico a los principales interesados. - Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.). - Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico. - Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes.. - Posibilidad de priorización de los informes de incidentes.

63		2.33	Sustancial	Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos: - Sistema de monitorización de estado - a través de Ping, SNMP, WMI, Uptime Analysis, interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento. - Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP. - Monitorización del hardware y del entorno. - Calendario para la programación de las ventanas de mantenimiento. - Cálculo de SLA – consideración de las horas normales de trabajo y fuera de horas.	La Entidad ya cuenta con la plataforma SolarWinds ORION para el monitoreo de red (NOC) y métricas de rendimiento. Exigir que el SIEM realice tareas nativas de NOC como el monitoreo de transacciones sintéticas, métricas JMX, estados BGP/OSPF y supervisión de disponibilidad, duplica funciones ya existentes en la Entidad y restringe la pluralidad de oferentes al direccionar el pliego hacia herramientas hibridas (Ver https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortisiem-mssp.pdf página 2). Se sugiere eliminar los requisitos de monitoreo de disponibilidad/rendimiento nativo y, en su lugar, exigir la integración del SIEM con SolarWinds ORION.	El SIEM debe tener capacidad de correlación cruzada de analítica de SOC y NOC mediante integración con la plataforma de monitoreo NOC de la Entidad (SolarWinds ORION). Esto permitirá correlacionar eventos de seguridad con métricas operativas. Se eliminan los requerimientos de monitoreo nativo de disponibilidad, transacciones sintéticas y rendimiento dentro del SIEM.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem refiere a la integración que debe tener este servicio con la plataforma de disponibilidad de la Entidad, sin embargo, para evitar equivocos en el requerimiento de la Entidad, el ítem en mención 2.33 será eliminado del respectivo anexo técnico, cambio que se verá reflejado en la adenda a publicar en los próximos días.
64		2.34	Sustancial	Almacenamiento - Soporte de archivado de logs tanto para NFS como HDFS. - Creación de políticas de retención de logs tanto por espacio como por periodos de tiempo.	Exigir explícitamente el soporte de archivado de logs para 'HDFS' (Hadoop Distributed File System) describe la arquitectura subyacente de una solución y fabricante en particular. Los SIEM líderes utilizan motores de indexación y compresión propietarios o nativos de nube altamente eficientes. Se solicita que el requerimiento se enfoque en la capacidad y formato de retención, no en el sistema de archivos de un fabricante particular como Fortinet (https://docs.fortinet.com/document/fortisiem/7.5.0/hdfs-storage-guide/290385/setting-up-hdfs-for-fortisiem-event-archive).	Soporte de archivado de logs para sistemas de almacenamiento estándar de red (ej. NFS, SMB, S3) o bases de datos y sistemas de archivos propietarios del fabricante, garantizando la retención exigida y la inmutabilidad de los datos.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, varios SIEM (Security Information and Event Management) y herramientas de gestión de logs soportan el archivado y la ingesta de registros desde HDFS (Hadoop Distributed File System) para cumplir con requisitos de cumplimiento y análisis de seguridad. Sin embargo, se aclara, que las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no se acepta su observación.
65		2.35	Sustancial	Licenciamiento, como mínimo debe incluir los siguientes elementos: - El fabricante ofertante deberá disponer de un método de licenciamiento escalable. - Se deberá disponer de paquetes de licencia de agentes avanzados para monitorización de servidores críticos Windows y Linux, en ambientes híbridos (On-premise y Cloud). - Se deberá disponer de paquetes de licencia de agentes de UEBA para equipos Windows (según el inventario proporcionado por la entidad). Dichas licencias de UEBA no deberán conllevar consumo asociado ni de licencia de dispositivos ni de EPS. - Se deberá disponer de otras suscripciones como Indicadores de Compromiso (IoC). - Se deberá poder añadir EPS adicionales sin necesidad de contratar soporte asociado a los mismos. - Se podrán desplegar tantos colectores virtuales en ambientes híbridos como se quiera sin coste adicional.	El pliego exige que el módulo UEBA no consuma EPS/dispositivos, y que se puedan añadir 'nodos worker en caliente' o 'colectores virtuales' sin costo adicional. Estas especificaciones corresponden al modelo comercial exacto y la lista de precios de una marca en particular. Cada fabricante (líderes según Gartner) tiene métricas diferentes (GB/día, vCPU, EPS, Dispositivos). Se solicita flexibilizar el requisito para que el fabricante cumpla con la volumetría técnica requerida bajo su propio modelo comercial, garantizando que no haya costos ocultos para la Entidad.	El fabricante ofertante deberá disponer de un método de licenciamiento escalable que cubra la volumetría técnica total exigida (mínimo 2467 dispositivos y 25000 EPS, o su equivalente en GB/día o poder de cómputo). La oferta debe incluir las licencias necesarias para agentes, UEBA y el despliegue de la arquitectura requerida (colectores, indexadores o nodos) para ambientes híbridos, garantizando el cumplimiento de la solución integral ofertada sin costos de licenciamiento ocultos o adicionales para la Entidad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las cantidades solicitadas son los mínimos requeridos por la Entidad, para lo cual el interesado deberá dar estricto cumplimiento, teniendo en cuenta que, las características solicitadas por la Entidad obedecen a necesidades puntuales.
66		3.4	Sustancial	La solución ofertada debe estar licenciada como mínimo para tres (3) analistas.	Se solicita respetuosamente a la Entidad modificar el requerimiento, ya que exigir una métrica de licenciamiento específica ('por analista') direcciona el pliego hacia el modelo comercial de un fabricante en particular y limita la pluralidad de oferentes. Las plataformas líderes del mercado según Gartner licencian bajo métricas diferentes y más orientadas a la operación, tales como volumen de acciones automatizadas, cantidad de eventos (EPS) o capacidad de procesamiento, otorgando a menudo usuarios o analistas ilimitados. Se sugiere flexibilizar el texto para que el oferente garantice la concurrencia operativa de los tres (3) analistas requeridos, pero utilizando la métrica de licenciamiento nativa de su fabricante.	La solución ofertada debe contar con el dimensionamiento y licenciamiento necesario para soportar la operación y acceso simultáneo de como mínimo tres (3) analistas. El oferente deberá entregar este alcance utilizando el modelo de licenciamiento propio del fabricante (ya sea por usuarios nombrados/concurrentes, volumen de acciones, eventos, o nodos), garantizando el cumplimiento funcional sin costos adicionales u ocultos para la Entidad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad son mínimas y son homologables en este ítem a los diferentes modelos de licenciamiento de los fabricantes, para lo cual el interesado entregara su oferta siempre y cuando cumpla con los requerimientos de la Entidad.
67		3.19	Sustancial	Las alertas y los incidentes deben manejarse por separado, cada uno en su propio módulo de interfaz de usuario. Las interfaces de gestión de alertas e incidentes deben ser personalizables para permitir una visualización flexible de la información, incluida la visualización de información de la alerta en sí más información adicional devuelta por los playbook de investigación.	Exigir que las alertas y los incidentes se manejen 'cada uno en su propio módulo' restringe la arquitectura de base de datos de la solución a un fabricante en particular. Las plataformas SOAR líderes del mercado (reconocidas por Gartner) utilizan un enfoque de gestión de casos unificado basado en 'Tipos de Incidentes' (Incident Types), lo cual es más eficiente para el triaje y la investigación, garantizando igualmente la separación visual y funcional de alertas e incidentes. Se solicita flexibilizar el requisito para permitir diferentes arquitecturas tecnológicas.	Las alertas y los incidentes deben poder gestionarse, clasificarse y visualizarse de forma diferenciada. Las interfaces de gestión deben ser personalizables para permitir una visualización flexible de la información, ya sea mediante módulos separados o mediante un sistema unificado de gestión de casos con tipificación o categorización de incidentes.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no es posible ajustar según su sugerencia.
68		3.42	Sustancial	La solución debe tener la capacidad de crear módulos personalizados desde dentro de la GUI web, un módulo es un subsistema como: Alertas, Incidentes, indicadores... etc.	Requerir la creación de 'módulos personalizados' directamente desde la interfaz web (es decir, crear nuevas tablas de base de datos sin código) es una funcionalidad exclusiva de una marca específica. Las herramientas líderes en automatización logran la personalización requerida permitiendo a los analistas crear y modificar 'Tipos de Incidentes', 'Vistas/Layouts' y 'Campos Personalizados' (Custom Fields) desde la interfaz. Se solicita modificar el lenguaje para que evalúe la capacidad de personalización y no la nomenclatura de una arquitectura propietaria.	La solución debe tener la capacidad de adaptar la plataforma a diferentes casos de uso, permitiendo crear tipos de incidentes, vistas (layouts), agrupaciones o contenedores personalizados desde la interfaz gráfica para entidades como Alertas, Incidentes o Indicadores, sin necesidad de desarrollos a medida.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, varias plataformas SOAR (Security Orchestration, Automation, and Response) permiten la creación de módulos, aplicaciones e integraciones personalizadas directamente desde su interfaz gráfica de usuario (GUI) web. Sin embargo, se aclara que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no se acepta su observación.
69		3.66	Sustancial	La solución debe admitir el reinicio del playbook desde el paso del playbook fallido anteriormente.	El requerimiento de 'admitir el reinicio del playbook desde el paso del playbook fallido' describe el nombre exacto de un botón/funcionalidad de la plataforma del fabricante Fortinet (Playbook Recovery) (https://docs.fortinet.com/document/fortisoar/7.6.5/administration-guide/743805/application-configuration#Configuring_Playbook_Recovery). Otras soluciones líderes manejan el control de errores de forma robusta mediante manejo nativo de excepciones, reintentos automatizados, o la capacidad de re-ejecutar tareas específicas (Task re-run). Se sugiere abrir el alcance para permitir distintos enfoques de control de errores.	La solución debe contar con mecanismos integrados de control de errores y depuración, permitiendo a los analistas manejar excepciones, re-ejecutar tareas específicas fallidas, o retomar el flujo de un playbook tras la corrección de un error, garantizando la continuidad de la automatización.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, diferentes plataformas SOAR (Security Orchestration, Automation, and Response) modernas permiten reiniciar o reanudar playbooks desde el paso fallido, lo cual es fundamental para la resiliencia de la automatización. Sin embargo, se aclara que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no se acepta su observación.
70		3.86	Sustancial	Debe permitir que la granularidad del control de acceso sea a nivel de módulo, registro o campo ("Alertas", "máquina A con IP 1.2.3.4 infectada", "1.2.3.4" son respectivamente ejemplos de módulo, registro y campo).	Exigir que la granularidad del Control de Acceso Basado en Roles (RBAC) llegue 'a nivel de campo' individual dentro de un registro es un nivel de microsegmentación propio de un solo fabricante. La mayoría de los SOAR líderes de la industria garantizan la seguridad y confidencialidad aplicando RBAC a nivel de módulo, registro, etiqueta de datos (label) o tipo de incidente. Exigir RBAC por campo limita drásticamente la pluralidad de oferentes sin aportar un diferencial crítico de seguridad que no pueda lograrse con etiquetas de confidencialidad.	Debe permitir que la granularidad del control de acceso (RBAC) sea altamente configurable y flexible, permitiendo restringir la visibilidad, lectura y edición a nivel de módulo, registro, etiqueta (label), dominio o tipo de incidente, garantizando la separación de funciones.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem solicitado presenta varias opciones al mencionar modulo o registro o campo, en ningún momento se limita la granularidad a "campo", por lo tanto, su observación es imprecisa, así mismo, al revisar se encuentra que existen diferentes plataformas SOAR que permiten granularidad del Control de Acceso Basado en Roles (RBAC) a diferentes niveles. Sin embargo, se aclara que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no se acepta su observación.
71		3.59	Sustancial	Debería ser posible que la solución SOAR permita la ejecución simultánea de múltiples playbooks, garantizando la capacidad de respuesta ante varios incidentes de seguridad en paralelo, con nodos o licencias adicionales o su equivalente de acuerdo a la solución ofrecida, sin que ello implique costos adicionales para la Entidad, cumpliendo como mínimo: - Capacidad de ejecutar varios playbooks al mismo tiempo, sin afectar el rendimiento del sistema. - Soporte para playbooks anidados o encadenados, permitiendo modularizar tareas complejas. - **Arquitectura escalable que permita aumentar la capacidad de ejecución mediante la adición de nodos, instancias o licencias adicionales.** - Gestión eficiente de recursos para evitar cuellos de botella en la ejecución de automatizaciones. - Monitoreo y visualización del estado de ejecución de cada playbook en tiempo real.	Exigir que la plataforma soporte la ejecución simultánea de múltiples playbooks requiriendo 'nodos o licencias adicionales [...] sin que ello implique costos adicionales' direcciona el pliego hacia el modelo de licenciamiento de un solo fabricante (licenciamiento por usuario administrador). Fabricantes líderes licencian por 'Acciones automatizadas' o por 'Nodos/Motores de ejecución'. Se solicita que el proveedor demuestre la capacidad técnica y dimensione la oferta bajo su propio modelo comercial para garantizar el rendimiento sin costos ocultos.	La solución SOAR debe garantizar la ejecución simultánea de múltiples playbooks y la capacidad de respuesta en paralelo, sin afectar el rendimiento del sistema. El oferente deberá incluir en su propuesta técnica y económica la arquitectura requerida (nodos, motores, instancias) y el licenciamiento necesario para soportar la volumetría de la Entidad, de acuerdo con el modelo comercial propio del fabricante.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento solicitado en el mismo ítem admite equivalencia, tal como se indica en el parráfo siguiente resaltado en negrita y con una fuente más grande: Debería ser posible que la solución SOAR permita la ejecución simultánea de múltiples playbooks, garantizando la capacidad de respuesta ante varios incidentes de seguridad en paralelo, con nodos o licencias adicionales **o su equivalente de acuerdo a la solución ofrecida**, sin que ello implique costos adicionales para la Entidad. Acorde a lo anterior se indica al observante que no se acepta su solicitud.
72		5.4.11	Forma	La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	Respecto a la exigencia de que el fabricante de la solución de Gestión de Vulnerabilidades se encuentre en el cuadrante de líderes de Gartner o Forrester, se solicita respetuosamente a la Entidad eliminar dicho requerimiento. Si bien las evaluaciones de terceros son un referente valioso, exigir esta condición a una única tecnología y omitirla en soluciones críticas y estructurales del proyecto (como el SIEM, SOAR o Cacería de Amenazas) genera una inconsistencia técnica en los criterios de calidad del pliego y podría limitar injustificadamente la pluralidad de oferentes en esta categoría puntual. Para garantizar un proceso equitativo, objetivo y enfocado en el cumplimiento de los requerimientos técnicos del anexo, sugerimos retirar esta obligatoriedad, evaluando las soluciones por sus capacidades reales y no por reportes comerciales que no aplican de manera transversal a todo el proyecto.	Se solicita eliminar el presente requerimiento del anexo técnico, evaluando la idoneidad de la solución ofertada con base en el cumplimiento a cabalidad de las especificaciones funcionales y técnicas detalladas en esta sección, garantizando así la pluralidad de oferentes y la consistencia en los criterios de evaluación de todas las herramientas del proyecto.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no se acepta su solicitud.

73	6.4.2	Sustancial	El appliance, o solución, plataforma o servicio de decepción debe estar en capacidad de crear al menos 400 señuelos, en hasta 20 máquinas virtuales y desplegarse en mínimo 120 VLANs. o características similares o superiores en las tecnologías ofrecidas.	Se solicita a la Entidad flexibilizar la volumetría exigida ('hasta 20 máquinas virtuales y 400 señuelos'). Este dimensionamiento corresponde a la ficha técnica (Data Sheet) de los appliances de FortiDeceptor de Fortinet. Existen fabricantes líderes en decepción que logran la cobertura exigida (120 VLANs) con arquitecturas mucho más eficientes y modernas, utilizando menos máquinas virtuales (mediante forwarders o proyecciones ligeras) o sin límite estricto de señuelos. Se sugiere evaluar la capacidad de cobertura de la red y no la cantidad de máquinas virtuales que la marca requiera para lograrlo. Ver "características FORTIDECEPTOR VM" en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiDeceptor.pdf	La solución de decepción debe estar dimensionada y licenciada para dar cobertura y despliegue de señuelos en como mínimo 120 VLANs de la Entidad. El oferente deberá proporcionar la arquitectura necesaria (appliances, máquinas virtuales, forwarders o sensores) que garantice esta cobertura bajo el modelo de licenciamiento y mejores prácticas de su fabricante.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el mismo ítem permite equivalencias siempre y cuando se cumpla con las cantidades y características requeridas, y una vez revisado se encuentra que dichas características las cumplen diferentes proveedores de este tipo de servicios. Sin embargo, se aclara que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no se acepta su observación.
74	6.4.12	Sustancial	Debe integrarse con el Firewall de Nueva Generación de la entidad, de manera que se pueda tener en este último un dashboard centralizado con la información general del dispositivo y los señuelos desplegados.	Respecto al requerimiento de integrar la solución con el Firewall para 'tener en este último un dashboard centralizado', se solicita respetuosamente a la Entidad modificar este alcance. Requerir que la interfaz de administración de los señuelos viva 'dentro' de la interfaz del Firewall es una característica propietaria de un único ecosistema de fabricante cerrado (Fortinet). Las plataformas líderes del mercado en tecnología de decepción se integran con los firewalls perimetrales (como Palo Alto) mediante APIs estándar para enviar acciones automatizadas (bloqueos/cuarentenas), mientras mantienen la gestión y visibilidad centralizada en su propia consola, en el SIEM o en el SOAR. Mantener este texto limita la pluralidad de oferentes a una sola marca. Ver https://docs.fortinet.com/document/fortideceptor/6.2.1/administration-guide/894739/integrate-fortideceptor-with-fortigate-over-fabric-v7-2-4	La solución debe integrarse bidireccionalmente con el Firewall de Nueva Generación de la Entidad (mediante APIs estándar, Syslog o a través de la plataforma SOAR), garantizando el envío automatizado de acciones de bloqueo, cuarentena e indicadores de compromiso (IoCs) ante la detección de un ataque en los señuelos.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la unión de estas plataformas con NGFWs permite mover la inteligencia desde la detección pasiva a la prevención activa, permitiendo bloquear comportamientos maliciosos detectados por el sistema de caza de amenazas mediante reglas automáticas en el firewall. Varias plataformas avanzadas de caza de amenazas (Threat Hunting) y respuesta se integran con Firewalls de Nueva Generación (NGFW) para automatizar la detección y bloquear ataques en tiempo real. Sin embargo, se aclara que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no se acepta su observación.
75	6.5.1	Sustancial	Debe tener al menos 4 capas de decepción (o tecnología similar o superior), con la capacidad de crear como mínimo los siguientes elementos falsos: Señuelos de infraestructura (Sistemas operativos, cámaras, impresoras, bases de datos, etc.), de acuerdo a la cantidad de vlans (120). Carnadas o servicios falsos que se ejecuten sobre los señuelos (servidores web, aplicaciones, etc.), de acuerdo a la cantidad de vlans (120). Tráfico de red falso para detectar ataques de tipo MitM o app spoofing, entre otros. Tokens o recursos falsos desplegados sobre los señuelos (Credenciales, archivos, recursos compartidos, conexiones RDP, etc.).	Exigir textualmente que la herramienta tenga 'al menos 4 capas de decepción' y emule un 'Gateway de VPN SSL' restringe el pliego a la nomenclatura comercial y funcionalidades específicas del catálogo de un único fabricante. La industria clasifica las técnicas de engaño de diversas formas (Endpoint, Red, Directorio Activo, Datos). Se solicita generalizar el requerimiento hacia las capacidades técnicas reales esperadas para permitir la participación de otras soluciones líderes (reconocidas en el mercado) que logran el mismo objetivo de protección mediante técnicas y emulaciones equivalentes.	La solución debe proveer capacidades integrales de decepción para detectar amenazas avanzadas, incluyendo como mínimo la capacidad de crear: a) Señuelos de red/infraestructura (sistemas operativos, bases de datos), b) Servicios simulados (servidores web, SSH, portales de acceso remoto corporativo), c) Tráfico de red falso o proyecciones para detectar reconocimientos, y d) Tokens o datos falsos en los endpoints (credenciales, archivos).	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el mismo ítem permite equivalencias en el apartado donde menciona (tecnología similar o superior), siempre y cuando se cumpla con las cantidades y características requeridas, por lo tanto, no se acepta su observación.
76	7.4	Forma	Se debe suministrar una solución para Monitoreo de Red con Inteligencia Artificial con el objetivo de revisar el tráfico de red y alertar ciberamenazas que existan en la red de la entidad, favor tener en cuenta los procedimientos al respecto incluidos en el **Manual de políticas de seguridad de la información de la Entidad, con código MN-IIT-0072.**	En la documentación actualmente compartida este documento particular no se encuentra. Amablemente solicitamos a la entidad remitir o indicar donde es posible consultar (si es posible) el documento en mención, para alinear los procedimientos según lo requerido.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, link del correspondiente manual es el siguiente: https://www.dian.gov.co/atencionciudadano/LMDP/Informacion-Innovacion-y-Tecnologia/Seguridad-de-la-Informacion/Manuales/MN-IIT-0072.pdf Para lo cual el ítem en mención será ajustado y quedará de la siguiente manera, cambio que se verá reflejado en la adenda a publicar en los próximos días: Se debe suministrar una solución para Monitoreo de Red con Inteligencia Artificial con el objetivo de revisar el tráfico de red y alertar ciberamenazas que existan en la red de la entidad, favor tener en cuenta los procedimientos al respecto incluidos en el Manual de políticas de seguridad de la información de la Entidad, con código MN-IIT-0072, el cual puede ser consultado en el link https://www.dian.gov.co/atencionciudadano/LMDP/Informacion-Innovacion-y-Tecnologia/Seguridad-de-la-Informacion/Manuales/MN-IIT-0072.pdf
77	7.10	Sustancial	La herramienta debe utilizar modelos matemáticos probabilísticos de estimación, analizando y correlacionando múltiples dimensiones distintas dentro del paquete, con el fin de validar los comportamientos anómalos en la red.	Exigir que la herramienta utilice específicamente 'modelos matemáticos probabilísticos de estimación' direcciona el pliego hacia el algoritmo subyacente (inferencia bayesiana) utilizado por una única marca del mercado (Darktrace). El campo de la Inteligencia Artificial es amplio, y diferentes fabricantes líderes utilizan distintos enfoques matemáticos igual o más efectivos (como Redes Neuronales, Deep Learning, Analítica Cognitiva o Heurística avanzada) para el análisis de dimensiones del paquete. Se solicita neutralidad tecnológica, evaluando la capacidad de la herramienta para detectar anomalías mediante IA, independientemente de la fórmula matemática exacta que utilice su motor. Ver https://www.darktrace.com/news/invoke-capital-makes-first-investment-in-fundamental-cyber-security-technology	La herramienta debe utilizar algoritmos avanzados de Machine Learning e Inteligencia Artificial, analizando y correlacionando múltiples dimensiones dentro del tráfico de red para validar los comportamientos anómalos, de acuerdo con la arquitectura y los modelos analíticos propios del fabricante ofertado.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no se acepta su observación.
78	7.15	Sustancial	La solución debe poder realizar una captura de paquetes en tiempo real que permita un monitoreo de incidentes en el momento de su ocurrencia, así como ofrecer la opción de análisis exhaustivo de paquetes tanto en Wireshark como dentro de su propia interfaz de usuario permitiendo hacer la extracción en formatos .pcap y otros, o sus equivalentes de acuerdo a las tecnologías ofrecidas.	Se sugiere a la Entidad flexibilizar la obligatoriedad de que la solución realice captura completa de paquetes (Full Packet Capture) con almacenamiento PCAP por 6 meses directamente en el appliance. Las arquitecturas NDR modernas y líderes en el mercado basan gran parte de su analítica en metadatos avanzados y telemetría de red (ej. flujos enriquecidos, IPFIX), reservando la captura completa de paquetes solo para eventos críticos o mediante integraciones. Exigir Full Packet Capture por defecto para 25,000 activos obliga a dimensionar un hardware de almacenamiento masivo y costoso, excluyendo arquitecturas altamente eficientes orientadas a telemetría.	La solución debe realizar un análisis exhaustivo del tráfico mediante inspección profunda o análisis de telemetría y metadatos avanzados. Debe contar con la capacidad de ofrecer contexto detallado de las sesiones de red y ofrecer opciones para la captura y extracción de paquetes (ej. formato .pcap) cuando sea requerido para investigaciones profundas, ya sea de forma nativa o mediante integración.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el mismo ítem permite equivalencias en el apartado donde menciona (o sus equivalentes de acuerdo a las tecnologías ofrecidas.), siempre y cuando se cumpla con las cantidades y características requeridas, por lo tanto, no se acepta su observación.
79	7.26	Sustancial	La solución debe ser una plataforma de autoaprendizaje y tener un enfoque adaptativo que utilice inteligencia artificial comprobada para aprender sobre el entorno en el que se encuentra, detectar y responder a las desviaciones de la línea de base normal de comportamiento, así: - La línea base de la red debe ser lo suficientemente adaptable y dinámica para adaptarse a cualquier cambio en el comportamiento del entorno - Debe funcionar completamente en función del comportamiento, donde no se permitan las tecnologías que hacen uso de reglas y / o firmas	Se solicita a la Entidad eliminar la restricción que prohíbe el uso de tecnologías basadas en reglas o firmas. Las consultoras líderes de la industria (como Gartner) y las mejores prácticas de ciberseguridad recomiendan que las plataformas NDR utilicen un enfoque híbrido. Obligar a un motor de Inteligencia Artificial a deducir una amenaza ya conocida (ej. un beacon de ransomware documentado) basándose puramente en anomalías matemáticas genera latencia, mayor tiempo de exposición y consumo innecesario de cómputo. Permitir enfoques que combinen Machine Learning para el comportamiento anómalo (Zero-Days) con motores de firmas/reglas e Inteligencia de Amenazas (para detección inmediata de ataques conocidos) garantiza una respuesta mucho más rápida, menor tasa de falsos positivos y asegura la pluralidad de oferentes. Ver https://www.darktrace.com/news/under-the-radar-insider-threats-detected-by-darktrace	La línea base de la red debe ser adaptable para detectar desviaciones de comportamiento. La solución debe basarse en Inteligencia Artificial / Machine Learning para la detección de anomalías, permitiendo un enfoque híbrido que complemente esta analítica con el uso de reglas, firmas o inteligencia de amenazas (CTI) para garantizar la detección eficiente e inmediata de ciberataques conocidos.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem 7.26 será ajustado, para evitar equivocos en el requerimiento de la Entidad, quedando de la siguiente manera, cambio que se verá reflejado en la adenda a publicar en los próximos días: La solución debe ser una plataforma de autoaprendizaje y tener un enfoque adaptativo que utilice inteligencia artificial comprobada para aprender sobre el entorno en el que se encuentra, detectar y responder a las desviaciones de la línea de base normal de comportamiento, así: - La línea base de la red debe ser lo suficientemente adaptable y dinámica para adaptarse a cualquier cambio en el comportamiento del entorno. - Debe trabajar en función del comportamiento.
80	7.27	Sustancial	La Investigación basada en Inteligencia Artificial debe generar un reporte como resultado del proceso investigativo que contenga como mínimo: i. Una reconstrucción cronológica de los eventos que hacen parte del Incidente. **ii. Un resumen del incidente con una narrativa basada en procesamiento de lenguaje natural que describa a alto nivel los comportamientos evidenciados durante el incidente.** iii. Detalles técnicos relevantes a la investigación realizada como direcciones Ips, Hostnames, cuentas de usuario involucradas, saltos de conexión, cantidad de transferencia de datos, destinos externos, rareza de los destinos, rareza de las conexiones y resúmenes de conexiones.	Requerir que el resumen del incidente se entregue específicamente mediante una 'narrativa basada en procesamiento de lenguaje natural' es una característica comercial y de marketing exclusiva de un fabricante particular (Cyber AI Analyst de Darktrace). El objetivo operativo de la investigación de un incidente es brindar contexto claro y accionable al analista humano. Las plataformas líderes del mercado logran esto de manera altamente eficiente mediante tableros ejecutivos estructurados, líneas de tiempo gráficas (timelines) y mapas de correlación visual, sin necesidad de redactar la alerta como un texto conversacional. Se solicita evaluar el resultado (el contexto del incidente) y no el formato de presentación exclusivo de una marca. Ver https://www.koncisesolutions.com/wp-content/uploads/2021/06/wp-cyber-ai-analyst.pdf página 2	Un resumen ejecutivo y estructurado del incidente que describa claramente los comportamientos evidenciados, las alertas correlacionadas y los detalles técnicos de la investigación. Este resumen puede ser presentado mediante tableros de correlación avanzada, líneas de tiempo gráficas (timelines) o texto descriptivo, de acuerdo con la interfaz de la solución ofertada.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no se acepta su solicitud.
81	7.28	Sustancial	La solución debe ser OPEN API O API RESTFULL , que admita integraciones con otros elementos de seguridad al menos en los formatos, CEF, LEEF, JSON, SYSLOG, entre otros.	Respecto al requerimiento de formatos de integración, se solicita respetuosamente a la Entidad flexibilizar la lista obligatoria exigida. Formatos como CEF o LEEF son extensiones propietarias desarrolladas originalmente por fabricantes específicos de SIEM (ArcSight e IBM, respectivamente). Exigir el soporte nativo y obligatorio de todos estos formatos simultáneamente limita la pluralidad de oferentes, ya que las plataformas de seguridad, analítica y orquestación (SOAR) modernas y líderes del mercado logran una interoperabilidad total y superior utilizando estándares universales (como JSON vía API REST o Syslog estructurado), delegando a sus motores internos el parseo y normalización de la información. Se recomienda exigir la capacidad de integración mediante formatos estructurados reconocidos, sin obligar al soporte de dialectos propietarios.	La solución debe contar con una arquitectura de integración abierta (OPEN API o API RESTful), que admita la interoperabilidad y el intercambio de información con otros elementos de seguridad de la Entidad. Dicha integración debe soportarse mediante protocolos estándar y formatos de datos estructurados reconocidos por la industria (tales como JSON, SYSLOG, XML, CEF o LEEF), garantizando el correcto análisis y correlación de los eventos sin depender exclusivamente de un único formato propietario.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no se acepta su solicitud.

82	12.3	Forma	La administración, operación, gestión de los servicios y demás actividades de las plataformas, soluciones, software, hardware, entre otros, que hacen parte de las capacidades requeridas por la Entidad en este proyecto, deben ser realizadas por el futuro oferente, por el tiempo de duración del proyecto.	De manera respetuosa, solicitamos a la Entidad aclarar el plazo de ejecución total y la vigencia general del proyecto para la prestación del servicio administrado SOC. Actualmente existe una ambigüedad en el pliego, ya que se exige la administración de las plataformas 'por el tiempo de duración del proyecto', pero simultáneamente se establecen hitos de finalización desfasados para diferentes componentes (ej. licenciamiento del nuevo SIEM hasta agosto de 2030; Firewall de Base de Datos y NDR hasta enero de 2031). Esta diferencia de fechas genera incertidumbre técnica y financiera. Solicitamos aclarar si el servicio de gestión, administración y monitoreo por parte del recurso humano del SOC tendrá una duración general y unificada de tres (3) años contados a partir de la firma del acta de inicio (ej. 2026), o si se espera que el proveedor opere las plataformas de manera granular hasta el vencimiento de la última licencia en 2031 (lo que implicaría un proyecto de aproximadamente 5 años). Para un correcto dimensionamiento del servicio, sugerimos unificar el periodo de operación administrada a 3 años, dejando los remanentes de licenciamiento como derechos de uso a favor de la Entidad.	El plazo de ejecución general del proyecto y la prestación del servicio administrado de gestión, operación y monitoreo (SOC/NOC) será de tres (3) años, contados a partir de la firma del acta de inicio y la fase de implementación inicial (año 2026). Para aquellas soluciones tecnológicas con cronogramas de implementación diferidos o de renovación tecnológica (como el nuevo SIEM a partir de septiembre de 2027, y el Firewall de BD y NDR a partir de enero de 2028), el Contratista proveerá el licenciamiento, soporte de fábrica y garantía por un periodo granular de tres (3) años para cada una de ellas. En caso de que la vigencia de dicho licenciamiento supere el tiempo de duración del servicio general del proyecto, el Contratista transferirá los derechos de uso, soporte y actualizaciones de estas soluciones a favor de la Entidad hasta su respectiva fecha de caducidad (2030 y 2031), finalizando su responsabilidad de administración operativa una vez se cumplan los 3 años del contrato principal.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, la operación, seguimiento, gestión, monitoreo y administración por parte del futuro proveedor de todos los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho a uso, licenciamiento, suscripciones, actualizaciones, soporte y garantía irá por tres (3) años y sus periodos se contabilizarán a partir de la puesta en operación de cada uno de los servicios requeridos, incluyendo lo siguiente: Tener en cuenta que desde el inicio del contrato se deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 nuevo SIEM (solicitado en el ítem 2) que hace parte integral de este proyecto por el tiempo solicitado (Tres años) con licenciamiento soporte, garantía y derecho a uso hasta agosto 31 de 2030. La protección de bases de datos (Firewall de bases de datos) irá a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031. El futuro contratista deberá, recibir, gestionar, administrar y operar desde el inicio del contrato el actual firewall de bases de datos propiedad de la DIAN del fabricante IBM Referencia GUARDIUM hasta diciembre 31 de 2027 tiempo en el que termina el soporte de este dispositivo por parte del fabricante, una vez esto ocurra deberá implementar el nuevo firewall de bases de datos solicitado en las capacidades requeridas por la DIAN. Para la capacidad de NDR se deberá tener en cuenta que este comenzará a operar a partir de enero de 2028 previamente autorización de la DIAN, para lo cual deberá implementar, administrar, operar, soportar y garantizar el servicio mencionado, con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031.
83	12.7	Sustancial	Controles: El servicio de SOC ofrecido debe contemplar también el monitoreo de los siguientes controles tecnológicos pertenecientes al SGSI de la Entidad: Dispositivos de punto final de usuario Derechos de acceso privilegiado Restricción de acceso a la información Acceso al código fuente Autenticación segura Gestión de la capacidad Protección contra malware Gestión de vulnerabilidades técnicas Gestión de la configuración Eliminación de datos Enmascaramiento de datos Prevención de la fuga de datos Copia de seguridad de la información Redundancia de las instalaciones de procesamiento de información Inicio de sesión Actividades de seguimiento Sincronización del reloj Uso de programas de utilidad privilegiados Instalación de software en sistemas operativos Seguridad de redes Seguridad de los servicios de red Segregación de redes Filtrado web	Se observa que el pliego requiere el monitoreo de controles tecnológicos alineados al Anexo A de la norma ISO 27001:2022. Para garantizar la viabilidad y efectividad del monitoreo de controles como Derechos de acceso privilegiado (8.2), Acceso al código fuente (8.4), Copia de seguridad (8.13) y Uso de criptografía (8.24), solicitamos a la Entidad confirmar si proporcionará los logs de auditoría nativos de las plataformas externas correspondientes (Ej. herramientas PAM, Repositorios de Código, Sistemas de Backup y HSM/KMS). El alcance del servicio SOC ofertado respecto a estos controles estará sujeto a la capacidad de la Entidad para integrar y suministrar dicha telemetría hacia la plataforma SIEM, dado que soluciones como el SIEM o el EDR no pueden suplir la falta de plataformas de gestión especializada como un PAM.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, la Entidad proporcionará los logs necesarios para poder realizar el seguimiento solicitado en este ítem, sin embargo, se aclara que cualquier integración con los servicios SOC requeridos, la deberá realizar el futuro proveedor del SOC.
84	12.11	Forma	El SOC mediante el cual se prestarán los servicios debe ser miembro FIRST ™ , lo cual es estratégico para la Entidad por lo siguiente: 1.Interoperabilidad y confianza internacional: La membresía en FIRST™ garantiza que el SOC opera bajo estándares reconocidos globalmente en gestión de incidentes, lo que facilita la colaboración con otros CSIRTs y CERTs en situaciones críticas. 2.Acceso a inteligencia de amenazas de alta calidad: Los miembros de FIRST™ tienen acceso a canales exclusivos de intercambio de información sobre amenazas emergentes, vulnerabilidades y tácticas de ataque, lo que permite una respuesta más rápida y efectiva. 3.Capacidad técnica validada: Para ser aceptado como miembro, el SOC debe demostrar capacidades técnicas avanzadas, procesos maduros de gestión de incidentes, y un compromiso con la mejora continua en ciberseguridad. 4.Participación en ejercicios y foros especializados: La membresía permite participar en simulacros internacionales, capacitaciones y foros técnicos que fortalecen la preparación ante incidentes complejos y coordinados. 5.Cumplimiento de buenas prácticas y gobernanza: FIRST™ promueve principios de ética, confidencialidad y responsabilidad que son fundamentales para la operación segura y confiable de un SOC. Esta postura busca asegurar que los servicios prestados se alineen con los más altos estándares internacionales en ciberseguridad, sin comprometer la calidad ni la capacidad de respuesta ante incidentes.	De manera respetuosa, solicitamos a la Entidad aclarar una contradicción evidente entre las Especificaciones Técnicas y el Pliego de Condiciones General respecto a la certificación/membresía FIRST. En las especificaciones técnicas se indica de forma imperativa que el SOC 'debe ser miembro FIRST' (sugiriendo que es un requisito técnico habilitante y de obligatorio cumplimiento). Sin embargo, en los criterios de evaluación (410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf), esta misma vinculación se enlista como una certificación para lograr puntuación (otorgando puntos si se presentan varias certificaciones y 0 puntos si no se presentan). Un mismo criterio no puede ser habilitante y puntuable a la vez, ya que esto genera inseguridad jurídica. Solicitamos aclarar si la membresía FIRST es un requisito habilitante obligatorio para poder participar, o si es un criterio puntuable opcional que solo otorga puntaje adicional en la evaluación.	Se valorará y otorgará puntuación adicional a los oferentes cuyo SOC cuente con vinculación directa y activa como miembro FIRST ™ (Forum Incident Response and Security Teams), de acuerdo con lo establecido en la matriz de evaluación del Pliego de Condiciones. Esta membresía es estratégica para la Entidad ya que promueve la interoperabilidad internacional, el acceso a inteligencia de amenazas y el cumplimiento de buenas prácticas; por lo tanto, será calificada como un diferencial técnico dentro del proceso.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem en mención que solicita certificación FIRST para el SOC donde se prestarán los servicios es puntuable, no es una certificación obligatoria, por lo tanto, para evitar equivocos en el entendimiento de la característica solicitada, este ítem (12.11) será ajustado en el anexo técnico mediante adenda que se publicará en en los próximos días quedando de la siguiente manera: Es deseable (opcional) para la Entidad que el SOC mediante el cual se prestarán los servicios debe ser miembro FIRST ™, para lo cual el interesado presentará la respectiva certificación con doce (12) meses de antiguedad y se hará acreedor a la respectiva puntuación explicada en sección III criterios de evaluación, es importante resaltar los beneficios que representa para Entidad el tener un SOC certificado: 1.Interoperabilidad y confianza internacional: La membresía en FIRST™ garantiza que el SOC opera bajo estándares reconocidos globalmente en gestión de incidentes, lo que facilita la colaboración con otros CSIRTs y CERTs en situaciones críticas. 2.Acceso a inteligencia de amenazas de alta calidad: Los miembros de FIRST™ tienen acceso a canales exclusivos de intercambio de información sobre amenazas emergentes, vulnerabilidades y tácticas de ataque, lo que permite una respuesta más rápida y efectiva. 3.Capacidad técnica validada: Para ser aceptado como miembro, el SOC debe demostrar capacidades técnicas avanzadas, procesos maduros de gestión de incidentes, y un compromiso con la mejora continua en ciberseguridad. 4.Participación en ejercicios y foros especializados: La membresía permite participar en simulacros internacionales, capacitaciones y foros técnicos que fortalecen la preparación ante incidentes complejos y coordinados. 5.Cumplimiento de buenas prácticas y gobernanza: FIRST™ promueve principios de ética, confidencialidad y responsabilidad que son fundamentales para la operación segura y confiable de un SOC. Esta postura busca asegurar que los servicios prestados se alineen con los más altos estándares internacionales en ciberseguridad, sin comprometer la calidad ni la capacidad de respuesta ante incidentes.
85	12.11	Sustancial	El SOC mediante el cual se prestarán los servicios debe ser miembro FIRST ™ , lo cual es estratégico para la Entidad por lo siguiente: 1.Interoperabilidad y confianza internacional: La membresía en FIRST™ garantiza que el SOC opera bajo estándares reconocidos globalmente en gestión de incidentes, lo que facilita la colaboración con otros CSIRTs y CERTs en situaciones críticas. 2.Acceso a inteligencia de amenazas de alta calidad: Los miembros de FIRST™ tienen acceso a canales exclusivos de intercambio de información sobre amenazas emergentes, vulnerabilidades y tácticas de ataque, lo que permite una respuesta más rápida y efectiva. 3.Capacidad técnica validada: Para ser aceptado como miembro, el SOC debe demostrar capacidades técnicas avanzadas, procesos maduros de gestión de incidentes, y un compromiso con la mejora continua en ciberseguridad. 4.Participación en ejercicios y foros especializados: La membresía permite participar en simulacros internacionales, capacitaciones y foros técnicos que fortalecen la preparación ante incidentes complejos y coordinados. 5.Cumplimiento de buenas prácticas y gobernanza: FIRST™ promueve principios de ética, confidencialidad y responsabilidad que son fundamentales para la operación segura y confiable de un SOC. Esta postura busca asegurar que los servicios prestados se alineen con los más altos estándares internacionales en ciberseguridad, sin comprometer la calidad ni la capacidad de respuesta ante incidentes.	– Requisito de Membresía FIRST™ Respetuosamente solicitamos a la entidad aclarar que el requisito de membresía en FIRST™ no se limite exclusivamente al SOC físicamente ubicado en Bogotá. La membresía en FIRST™ valida las capacidades técnicas, la interoperabilidad internacional y el acceso a inteligencia de amenazas, pero dichas condiciones pueden estar soportadas en infraestructura y centros de datos ubicados en otras geografías o en la nube, siempre que cumplan con las certificaciones y estándares internacionales requeridos. En este sentido, el requisito debería enfocarse en que el SOC que presta los servicios a la DIAN sea miembro activo de FIRST™, independientemente de la localización física de la infraestructura tecnológica, garantizando que el equipo de monitoreo y operación asignado al proceso sí esté disponible en Bogotá para atender las necesidades de la entidad. De esta manera, se asegura el cumplimiento de los más altos estándares internacionales en ciberseguridad, sin restringir innecesariamente la participación de oferentes que cuentan con SOC certificados en FIRST™ en otras ubicaciones, pero que pueden garantizar operación local y soporte directo en Bogotá.	Aclaración del requerimiento FIRTS del SOC no es exclusivo en Bogotá pueden estar soportadas en infraestructura y centros de datos ubicados en otras geografías o en la nube, siempre que cumplan con las certificaciones y estándares internacionales requeridos.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem en mención que solicita certificación FIRST para el SOC donde se prestarán los servicios es puntuable, no es una certificación obligatoria, por lo tanto, para evitar equivocos en el entendimiento de la característica solicitada, este ítem (12.11) será ajustado en el anexo técnico mediante adenda que se publicará en en los próximos días quedando de la siguiente manera: Es deseable (opcional) para la Entidad que el SOC mediante el cual se prestarán los servicios debe ser miembro FIRST ™, para lo cual el interesado presentará la respectiva certificación con doce (12) meses de antiguedad y se hará acreedor a la respectiva puntuación explicada en sección III criterios de evaluación, es importante resaltar los beneficios que representa para Entidad el tener un SOC certificado: 1.Interoperabilidad y confianza internacional: La membresía en FIRST™ garantiza que el SOC opera bajo estándares reconocidos globalmente en gestión de incidentes, lo que facilita la colaboración con otros CSIRTs y CERTs en situaciones críticas. 2.Acceso a inteligencia de amenazas de alta calidad: Los miembros de FIRST™ tienen acceso a canales exclusivos de intercambio de información sobre amenazas emergentes, vulnerabilidades y tácticas de ataque, lo que permite una respuesta más rápida y efectiva. 3.Capacidad técnica validada: Para ser aceptado como miembro, el SOC debe demostrar capacidades técnicas avanzadas, procesos maduros de gestión de incidentes, y un compromiso con la mejora continua en ciberseguridad. 4.Participación en ejercicios y foros especializados: La membresía permite participar en simulacros internacionales, capacitaciones y foros técnicos que fortalecen la preparación ante incidentes complejos y coordinados. 5.Cumplimiento de buenas prácticas y gobernanza: FIRST™ promueve principios de ética, confidencialidad y responsabilidad que son fundamentales para la operación segura y confiable de un SOC. Esta postura busca asegurar que los servicios prestados se alineen con los más altos estándares internacionales en ciberseguridad, sin comprometer la calidad ni la capacidad de respuesta ante incidentes.

86	12.59	Sustancial	Prestar el servicio desde un centro de operaciones de seguridad (SOC) ubicado en la ciudad de Bogotá D.C. (Colombia), cuya comunicación con la infraestructura de la Dian, se hará utilizando los canales de la Entidad.	Con el objetivo de garantizar la resiliencia del servicio sin incurrir en exigencias de infraestructura física obsoletas, se recomienda respetuosamente a la Entidad flexibilizar y aclarar el alcance de la continuidad operativa. Se está de acuerdo con mantener la sede física principal de analistas en la ciudad de Bogotá o sus alrededores; sin embargo, en las arquitecturas modernas de ciberseguridad, la continuidad no depende de tener un segundo edificio con personal en otra ciudad, sino de contar con infraestructuras tecnológicas resilientes. Por lo tanto, solicitamos que se permita y valore que el Centro de Datos que soporta las plataformas (SIEM, SOAR, etc.) pueda estar distribuido en esquemas de alta disponibilidad, ya sea mediante centros de datos dispersos geográficamente o en arquitecturas de nube (Cloud). Asimismo, para el personal operativo (analistas), el cumplimiento se debe garantizar mediante un Plan de Continuidad de Negocio (BCP) que contemple esquemas de operación alterna o remota segura en caso de contingencia en la sede principal.	Se debe contar con un Centro de Operaciones de Seguridad - SOC principal ubicado en una locación física en la ciudad de Bogotá o sus alrededores, que cuente con las condiciones adecuadas de seguridad física y lógica. Para garantizar la continuidad operativa ante contingencias, el oferente deberá contar con un Plan de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP) estructurado. Dicho plan debe garantizar: 1) La continuidad de la operación del recurso humano (analistas) ante indisponibilidad de la sede principal; y 2) La alta disponibilidad de las plataformas tecnológicas que soportan el servicio, permitiendo que la infraestructura de procesamiento (Centros de Datos) opere de manera redundante, geográficamente dispersa o bajo modelos de nube (Cloud) que aseguren la ininterrupción del servicio y el cumplimiento de las mejores prácticas del sector.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que tal como se indica en el requerimiento, el futuro proveedor de SOC puede entregar dos Centros de Operaciones en la ciudad de Bogotá u optar por tener uno en la Ciudad de Bogotá y otro en otra locación diferente a esta ciudad, tal como se indica en el respectivo numeral, por lo tanto, no se acepta su sugerencia, en el entendido que dicho requerimiento permite pluralidad y da diferentes opciones para los interesados.
87	12.81	Forma	Se deberá prestar el servicio de acompañamiento, asesoramiento, generación de planes de remediación entre otros para la solución de todas las vulnerabilidades e incidentes encontrados durante el tiempo que dure el contrato, para lo cual deberá contar con personal en sitio (mínimo un Ingeniero) en el horario laboral entre semana (8x5) y si por alguna circunstancia fortuita o de acuerdo a la necesidad de la DIAN (bajo demanda de la Entidad), se podrán coordinar sesiones en horario no hábil.	Amablemente solicitamos aclarar si este rol esta considerado dentro del "Equipo Mínimo de Trabajo" definido en el anexo técnico o se debe considerar un rol adicional y dedicado a este propósito.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el rol esta considerado dentro del equipo mínimo de trabajo.
88	13.17	Sustancial	Para la plataforma de gestión de vulnerabilidades, se debe tener el servicio de gestión y remediación según lo reportado en la herramienta , de modo que sirva de apoyo al área de DIGIT, para resolver todos los casos a remediar según los informes y dashboards que muestre la respectiva herramienta. Se debe poner a disposición el recurso humano para generar planes de acción sobre la información reportada en la herramienta, y realizar el apoyo, soporte y acompañamiento durante la remediación de todas las vulnerabilidades encontradas en la prestación del servicio y la ejecución del contrato.	Con el fin de garantizar la estabilidad de los servicios de la Entidad y alinearse con las mejores prácticas de la industria (como ITIL y la separación de funciones en ISO 27001), solicitamos respetuosamente aclarar el alcance de las labores de 'remediación'. El rol de un Centro de Operaciones de Seguridad (SOC) y sus analistas es consultivo y de auditoría: se encarga de la detección, priorización basada en riesgo, generación de planes de acción, asesoramiento técnico y verificación posterior a la remediación. Sin embargo, la ejecución directa de los cambios en los sistemas de producción (ej. aplicación de parches del sistema operativo, modificaciones de código fuente en aplicaciones o cambios de configuración en bases de datos) debe recaer estrictamente sobre el área de TI/Infraestructura de la Entidad, quienes son los dueños y administradores de los activos. Se sugiere ajustar la redacción para establecer claramente que el recurso humano ofertado realizará un acompañamiento experto, consultivo y de seguimiento, sin asumir la responsabilidad de ejecutar los cambios directamente sobre la infraestructura productiva del cliente.	Para la plataforma de gestión de vulnerabilidades, se debe tener el servicio de gestión, seguimiento y apoyo a la remediación, de modo que sirva de apoyo al área de DIGIT para gestionar los casos a resolver según los informes de la herramienta. Se debe poner a disposición el recurso humano para priorizar las vulnerabilidades, generar planes de acción técnicos, y realizar el apoyo, soporte y acompañamiento consultivo durante todo el ciclo de mitigación en la ejecución del contrato. Se aclara que la ejecución material de los parches, actualizaciones y cambios de configuración sobre los activos tecnológicos será responsabilidad del área de tecnología de la Entidad, previa ventana de mantenimiento. Para estas labores, el contratista deberá prestar el servicio de acompañamiento, asesoramiento, priorización y verificación post-remediación para todas las vulnerabilidades e incidentes encontrados, para lo cual deberá contar con personal en sitio (mínimo un Ingeniero) en el horario laboral entre semana (8x5) y, de requerirse por necesidades de la Entidad, coordinar sesiones de acompañamiento	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, las remediaciones y la intervenciones a las que haya lugar en la infraestructura propia de la Entidad, las realizará el personal de la DIAN, el futuro proveedor del SOC deberá realizar el acompañamiento desde el inicio y hasta la solución de las mismas, tal como se indica en el anexo técnico: 8.17 Apoyar con los recursos necesarios (personal idóneo) constantemente a la Dian realizando el respectivo acompañamiento, apoyo, experticia, experiencia, conocimiento en la resolución y remediación de todas y cada una de las vulnerabilidades encontradas durante la ejecución del contrato, se aclara que el personal de la Dian estará al frente de dichas actividades.
89	14.1	Sustancial	Se deberán realizar cinco (5) capacitaciones para cinco (5) ingenieros cada una, designados por la DIAN, con sus respectivos vouchers de certificación, dictadas en un centro de capacitación certificado, en temas de o sus equivalentes: A. Curso preparatorio en Gestión de Seguridad de la información - CISM de ISACA B. Profesional de arquitectura de seguridad de sistemas de información - CISSP ISACA C. Seguridad de Cisco Certified Network Associate - CCNA D. Especialista Certificado en Cifrado – ECouncil - ECES E. Hacker ético certificado (CEH) Los centros de enseñanza deben ser sitios óptimos para las capacitaciones, con los recursos necesarios, tales como material de estudio, video Beam o proyector, televisor, puestos de estudio, apuntador y demás elementos que garanticen un sitio cómodo para recibir los cursos.	De manera respetuosa, solicitamos a la Entidad realizar dos precisiones técnicas en el listado de capacitaciones y certificaciones requeridas, con el fin de alinearlas con la oferta vigente de los fabricantes a nivel mundial: La certificación CISSP (Profesional de Arquitectura de Seguridad de Sistemas de Información) es propiedad exclusiva de la organización ISC2, no de ISACA. Solicitamos corregir el fabricante en el pliego. La certificación CCNA Security fue retirada oficialmente por Cisco en el año 2020. Solicitamos a la Entidad actualizar este requerimiento y confirmar si se debe ofertar el actual CCNA (200-301), el cual ya incluye módulos de seguridad, o en su defecto, la certificación Cisco Certified CyberOps Associate, que es el estándar vigente de Cisco para operaciones de seguridad.	Se deberán realizar cinco (5) capacitaciones para cinco (5) ingenieros cada una, designados por la DIAN, con sus respectivos vouchers de certificación, dictadas en un centro de capacitación certificado, en temas de o sus equivalentes: A. Curso preparatorio en Gestión de Seguridad de la información - CISM de ISACA B. Profesional de arquitectura de seguridad de sistemas de información - CISSP ISC2 C. Cisco Certified Network Associate - CCNA O Cisco Certified CyberOps Associate D. Especialista Certificado en Cifrado – ECouncil - ECES E. Hacker ético certificado (CEH) Los centros de enseñanza deben ser sitios óptimos para las capacitaciones, con los recursos necesarios, tales como material de estudio, video Beam o proyector, televisor, puestos de estudio, apuntador y demás elementos que garanticen un sitio cómodo para recibir los cursos.	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, en efecto la certificación CISSP es del Consorcio ISC2, en este ítem se presenta un error de digitación, pero se aclara que debe ser CISSP de ISC2, en este punto se aclara que aplica equivalencia de la certificación, en caso de que esta ya no sea ofrecida por el mercado, teniendo en cuenta que debe ser igual o de mejores características que al solicitada.
90	14.2	Sustancial	Se deberá realizar un programa para apropiación de competencias en seguridad de la información para la conformación de un equipo de excelencia en ciberseguridad dirigido a los grupos específicos que la Supervisión del contrato indique, para mínimo veinte (20) funcionarios por capacitación. Las capacitaciones deben ser oficiales y certificables en estándares internacionales de seguridad informática incluyendo entre otros los siguientes: A. Cybersecurity fundamentals certificate – ISACA (Information Systems Audit and Control Association). B. Cybersecurity audit certificate - ISACA. C. Profesional certificado en seguridad en la nube - CCSP – ISACA. D. Marco de ciberseguridad del NIST Cybersecurity Framework (NCSF) Foundation. E. Certificado en fundamentos NCSF. F. Certificado como auditor interno en ISO 27001:2022 o superior. G. Certificado como Líder Gestor de Ciberseguridad ISO 27032:2023 o superior. H. Certificado como Auditor interno en la gestión de servicios ISO/IEC 20000-1:2018 o superior. I. Certificado como Auditor interno ISO 22301:2019 Sistema de Gestión de continuidad del negocio. J. CompTIA PenTest+ - CompTIA . K. Cybersecurity Practitioner - CSX-P - ISACA. NOTA 1. Las capacitaciones listadas en el punto anterior, deben permitir a los funcionarios de la DIAN que participen en las mismas, estar en la capacidad de presentar exámen de certificación de forma posterior, si es de su interés.	De manera respetuosa, solicitamos a la Entidad realizar ajustes y precisiones técnicas en el listado de capacitaciones y certificaciones requeridas, debido a inconsistencias con la oferta actual del mercado global de ciberseguridad: Certificación Retirada: La certificación indicada en el literal K (Cybersecurity Practitioner - CSX-P - ISACA) fue descontinuada y retirada oficialmente por el fabricante ISACA. Solicitamos eliminar este requerimiento, ya que es materialmente imposible adquirirla o presentarla en la actualidad. Error de Fabricante: En el literal C, se solicita la certificación CCSP (Profesional certificado en seguridad en la nube) atribuyéndola a ISACA. Aclaramos que el CCSP es propiedad exclusiva de la organización ISC2. Solicitamos corregir el fabricante en el pliego. Redundancia de Certificaciones: Los literales D (NIST NCSF Foundation) y E (Certificado en fundamentos NCSF) hacen referencia al mismo nivel de certificación básica del marco NIST. Solicitamos unificar ambos ítems en uno solo para no generar sobrecostos injustificados en la propuesta económica. Política de Segundos Intentos (Retakes): Solicitamos confirmar si los vouchers de certificación exigidos deben incluir obligatoriamente el derecho a un segundo intento (Retake). Cabe resaltar que fabricantes como ISACA, ISC2 y CompTIA no incluyen esta opción por defecto, lo que requeriría la cotización de paquetes especiales.	Se deberá realizar un programa para apropiación de competencias en seguridad de la información para la conformación de un equipo de excelencia en ciberseguridad dirigido a los grupos específicos que la Supervisión del contrato indique, para mínimo veinte (20) funcionarios por capacitación. Las capacitaciones deben ser oficiales y certificables en estándares internacionales de seguridad informática incluyendo entre otros los siguientes: A. Cybersecurity fundamentals certificate – ISACA (Information Systems Audit and Control Association). B. Cybersecurity audit certificate - ISACA. C. Profesional certificado en seguridad en la nube - CCSP – ISC2. D. Marco de ciberseguridad del NIST Cybersecurity Framework (NCSF) Foundation. E. Certificado en fundamentos NCSF. F. Certificado como auditor interno en ISO 27001:2022 o superior. G. Certificado como Líder Gestor de Ciberseguridad ISO 27032:2023 o superior. H. Certificado como Auditor interno en la	La Dirección de Impuestos y Aduanas Nacionales - DIAN, informa al observante que, el ítem 14.2 será modificado quedando de la siguiente manera, para lo cual se publicará una adenda en los próximos días con el cambio en mención: Se deberá realizar un programa para apropiación de competencias en seguridad de la información para la conformación de un equipo de excelencia en ciberseguridad dirigido a los grupos específicos que la Supervisión del contrato indique, para mínimo veinte (20) funcionarios por capacitación. Las capacitaciones deben ser oficiales y certificables en estándares internacionales de seguridad informática incluyendo entre otros los siguientes: A. Cybersecurity fundamentals certificate – ISACA (Information Systems Audit and Control Association). B. Cybersecurity audit certificate - ISACA. C. Profesional certificado en seguridad en la nube - CCSP – ISC2. D. Marco de ciberseguridad del NIST Cybersecurity Framework (NCSF) Foundation o Certificado en fundamentos NCSF. E. Certificado como auditor interno en ISO 27001:2022 o superior. F. Certificado como Líder Gestor de Ciberseguridad ISO 27032:2023 o superior. G. Certificado como Auditor interno en la gestión de servicios ISO/IEC 20000-1:2018 o superior. H. Certificado como Auditor interno ISO 22301:2019 Sistema de Gestión de continuidad del negocio. I. CompTIA PenTest+ - CompTIA . NOTA 1. Las capacitaciones listadas en el punto anterior, deben permitir a los funcionarios de la DIAN que participen en las mismas, estar en la capacidad de presentar exámen de certificación de forma posterior, si es de su interés. NOTA 2. Se debe suministrar al menos 2 vouchers de certificación por capacitación siendo opcional el derecho a segundo intento para estos vouchers.

91	Equipo Mínimo de Trabajo	Sustancial	Threat Hunter / Analista de Ciber inteligencia
Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines.
Posgrado en Gerencia de proyectos o Seguridad Informática
Certificaciones vigentes:
• Licensed Penetration Tester (LPT)
Mínimo cinco (5) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales tres (3) años con participación en proyectos de seguridad de la información, plan de recuperación de desastres o continuidad de negocio, demostrados en al menos dos(2) proyectos de esta naturaleza | De manera respetuosa, solicitamos a la Entidad actualizar y ampliar el requerimiento de la certificación 'Licensed Penetration Tester (LPT)'. Actualmente, el fabricante EC-Council ha migrado este esquema: el título actual es LPT (Master) y solo se otorga a los candidatos que logren un puntaje superior al 90% en el examen CPENT (Certified Penetration Testing Professional), lo que la convierte en una certificación de extrema escasez en el mercado laboral.

Para garantizar la pluralidad de oferentes, la disponibilidad de recursos altamente cualificados y evitar declarar desierto este perfil, solicitamos amablemente que el requerimiento se modifique para aceptar el examen base CPENT de EC-Council, o en su defecto, homologar y aceptar certificaciones equivalentes de la industria que demuestren el mismo o mayor nivel de experticia práctica en Ethical Hacking avanzado, como lo es la certificación OSCP (Offensive Security Certified Professional) de OffSec. | Threat Hunter / Analista de Ciber inteligencia
Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines.
Posgrado en Gerencia de proyectos o Seguridad Informática
Certificaciones vigentes:
• Licensed Penetration Tester (LPT), LPT (Master), CPENT o OSCP (Offensive Security Certified Professional)
Mínimo cinco (5) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales tres (3) años con participación en proyectos de seguridad de la información, plan de recuperación de desastres o continuidad de negocio, demostrados en al menos dos(2) proyectos de | La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, después de validar la infomación, el ítem en mención será ajustado en el anexo técnico mediante adenda que se publicará en en los próximos días, quedando de la siguiente manera:

Threat Hunter / Analista de Ciber inteligencia
Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines.
Posgrado en Gerencia de proyectos o Seguridad Informatica
Certificaciones vigentes:
• Licensed Penetration Tester (LPT), CPENT o LPT (Master).
Mínimo cinco (5) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales tres (3) años con participación en proyectos de seguridad de la información, plan de recuperación de desastres o continuidad de negocio, demostrados en al menos dos(2) proyectos de esta naturaleza |
| 92 | 410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf | Sustancial | 6.
Contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá, con las condiciones adecuadas para garantizar la continuidad operativa, la seguridad física y lógica, y el cumplimiento de las mejores prácticas del sector., | Con el objetivo de garantizar la resiliencia del servicio sin incurrir en exigencias de infraestructura física obsoletas, se recomienda respetuosamente a la Entidad flexibilizar y aclarar el alcance de la continuidad operativa. Se está de acuerdo con mantener la sede física principal de analistas en la ciudad de Bogotá o sus alrededores; sin embargo, en las arquitecturas modernas de ciberseguridad, la continuidad no depende de tener un segundo edificio con personal en otra ciudad, sino de contar con infraestructuras tecnológicas resilientes. Por lo tanto, solicitamos que se permita y valore que el Centro de Datos que soporta las plataformas (SIEM, SOAR, etc.) pueda estar distribuido en esquemas de alta disponibilidad, ya sea mediante centros de datos dispersos geográficamente o en arquitecturas de nube (Cloud). Asimismo, para el personal operativo (analistas), el cumplimiento se debe garantizar mediante un Plan de Continuidad de Negocio (BCP) que contemple esquemas de operación alterna o remota segura en caso de contingencia en la sede principal. | Se debe contar con un Centro de Operaciones de Seguridad - SOC principal ubicado en una locación física en la ciudad de Bogotá o sus alrededores, que cuente con las condiciones adecuadas de seguridad física y lógica. Para garantizar la continuidad operativa ante contingencias, el oferente deberá contar con un Plan de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP) estructurado.

Dicho plan debe garantizar: 1) La continuidad de la operación del recurso humano (analistas) ante indisponibilidad de la sede principal; y 2) La alta disponibilidad de las plataformas tecnológicas que soportan el servicio, permitiendo que la infraestructura de procesamiento (Centros de Datos) opere de manera redundante, geográficamente dispersa o bajo modelos de nube (Cloud) que aseguren la ininterrupción del servicio y el cumplimiento de las mejores prácticas del sector. | La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que tal como se indica en el requerimiento, el futuro proveedor de SOC puede entregar dos Centros de Operaciones en la ciudad de Bogotá u optar por tener uno en la Ciudad de Bogotá y otro en otra locación diferente a esta ciudad, tal como se indica en el respectivo numeral, por lo tanto, no se acepta su sugerencia, en el entendido que dicho requerimiento permite pluralidad y da diferentes opciones para los interesados. |
| 93 | 410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf | Sustancial | Desde el inicio del contrato y hasta las fechas mencionadas en las viñetas anteriores, el contratista deberá realizar la operación, administración y gestión de las soluciones con las que cuenta actualmente la Entidad IBM QRadar e IBM GUARDIUM. La solución de inteligencia de amenazas es administrada y operada por la Entidad hasta el 31 de diciembre de 2027.
Lo anterior incluye la monitorización, análisis, generación de informes y soporte técnico, asegurando la continuidad del servicio sin interrupciones. | De manera respetuosa, solicitamos a la Entidad definir y delimitar el alcance técnico del requerimiento asociado a la gestión, administración y operación de las soluciones heredadas propiedad de la Entidad (ej. IBM QRadar e IBM Guardium). Teniendo en cuenta que estas plataformas no fueron proveidas ni implementadas por el futuro contratista, asumir labores de 'soporte profundo' o resolución de fallas de núcleo (core) sin contar con el respaldo del fabricante representa un alto riesgo operativo para los servicios de la Entidad. Por políticas de los fabricantes de ciberseguridad, los contratos de soporte técnico y actualización de software (OEM) solo pueden ser gestionados por el proveedor que vendió la solución o directamente por el cliente final.

Por lo anterior, solicitamos aclarar que el alcance del futuro oferente sobre estas plataformas preexistentes se limitará a la administración, operación y configuración de casos de uso (Niveles 1 y 2), y que la Entidad garantizará la vigencia de los contratos de soporte de fábrica con IBM, así como los canales de escalamiento autorizados, para que el nuevo SOC pueda reportar incidentes de Nivel 3 (bugs de software, fallas de hardware o parches críticos) directamente al fabricante. | El Contratista deberá recibir, gestionar, administrar y operar (operación de Nivel 1 y 2, monitoreo, creación de reglas/políticas y afinamiento) las plataformas de seguridad actuales propiedad de la Entidad (como el SIEM IBM QRadar y el Firewall de Base de Datos IBM Guardium) hasta la fecha de caducidad de sus respectivas licencias.

Para garantizar la continuidad del servicio ante fallas mayores, la Entidad será la responsable de mantener vigentes los contratos de soporte técnico, mantenimiento y garantía de fábrica (OEM) sobre dichas plataformas heredadas. El Contratista brindará acompañamiento para el diagnóstico inicial y apoyará en el escalamiento de los casos (Nivel 3) hacia las mesas de ayuda del fabricante o del canal proveedor original, pero no asumirá responsabilidad por daños de hardware, bugs de software o actualizaciones de firmware que dependan exclusivamente de la suscripción de soporte de fábrica de un tercero. | La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las plataformas en mención (QRADAR y GUARDIUM de IBM) cuenta con el respectivo soporte del fabricante hasta las fechas mencionadas en el anexo técnico. |
| 94 | 410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf | Sustancial | A partir del vencimiento del contrato, la DIAN utilizará estas herramientas por cuenta propia o a través de un tercero, de acuerdo con lo que defina la DIAN. | De manera respetuosa, solicitamos a la Entidad confirmar si nuestro entendimiento es correcto respecto al plazo de ejecución de los servicios operativos. Entendemos que las labores de administración de las plataformas, el monitoreo SOC, la gestión de vulnerabilidades y, en general, la dedicación exclusiva de todos los perfiles exigidos en el 'Equipo Mínimo de Trabajo', tendrán una duración estricta de tres (3) años (36 meses) contados a partir de la firma del acta de inicio (ej. junio de 2026 a junio de 2029).

Comprendemos que, una vez finalizado este periodo de 36 meses, cesarán todas las obligaciones operativas, laborales y contractuales asociadas a la prestación de servicios profesionales por parte del contratista, transfiriendo la administración y gestión directa de las plataformas a la Entidad (o a quien esta designe), independientemente de que los derechos de uso o licenciamiento de algunas tecnologías tengan vigencias superiores (ej. 2030/2031). ¿Es correcto nuestro entendimiento? | | La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, la operación, seguimiento, gestión, monitoreo y administración (con el equipo y/o perfiles de trabajo solicitados) por parte del futuro proveedor de todos los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho a uso, licenciamiento, suscripciones, actualizaciones, soporte y garantía irá por tres (3) años y sus periodos se contabilizarán a partir de la puesta en operación de cada uno de los servicios requeridos, incluyendo lo siguiente:

Tener en cuenta que desde el inicio del contrato se deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 nuevo SIEM (solicitado en el ítem 2) que hace parte integral de este proyecto por el tiempo solicitado (Tres años) con licenciamiento soporte, garantía y derecho a uso hasta agosto 31 de 2030.

La protección de bases de datos (Firewall de bases de datos) irá a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031. El futuro contratista deberá, recibir, gestionar, administrar y operar desde el inicio del contrato el actual firewall de bases de datos propiedad de la DIAN del fabricante IBM Referencia GUARDIUM hasta diciembre 31 de 2027 tiempo en el que termina el soporte de este dispositivo por parte del fabricante, una vez esto ocurra deberá implementar el nuevo firewall de bases de datos solicitado en las capacidades requeridas por la DIAN.

Para la capacidad de NDR se deberá tener en cuenta que este comenzará a operar a partir de enero de 2028 previamente autorización de la DIAN, para lo cual deberá implementar, administrar, operar, soportar y garantizar el servicio mencionado, con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031.
" |
| 95 | 410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf | Sustancial | El tiempo esperado para la implementación del proyecto SOC (Levantamiento de información, planeación y diseño, pruebas y puesta en producción) es de máximo cuatro meses. | De manera respetuosa, solicitamos a la Entidad aclarar el criterio de evaluación y aceptación para el tiempo de implementación de cuatro (4) meses, considerando los cronogramas diferidos establecidos en el pliego. Dado que el Nuevo SIEM iniciará operaciones en septiembre de 2027, y el Firewall de Base de Datos y el NDR en enero de 2028 (12 a 16 meses después del inicio del proyecto), es materialmente imposible implementar 'todo el proyecto SOC' en los primeros 4 meses. Solicitamos confirmar que este plazo máximo aplicará única y exclusivamente a la 'Fase Inicial' (soluciones de despliegue inmediato), y que existirá un periodo de implementación independiente para las soluciones diferidas.

Adicionalmente, advertimos respetuosamente a la Entidad sobre un impacto operativo importante: mantener el SIEM heredado (IBM QRadar) hasta agosto de 2027 obligará al futuro contratista a realizar un reproceso de ingeniería (doble trabajo). Primero, deberá integrar todas las nuevas soluciones (SOAR, Deception, Análisis de código, etc.) al QRadar actual; y meses después, deberá realizar una nueva integración, migración de logs y reconstrucción de reglas de correlación hacia el Nuevo SIEM. Solicitamos confirmar si este doble esfuerzo de integración es el escenario deseado y obligatorio (para que todos los oferentes lo costeen en su propuesta económica), o si la Entidad evaluará habilitar la implementación anticipada del Nuevo SIEM para evitar este desgaste técnico y optimizar los recursos del proyecto. | El tiempo esperado para la implementación de la Fase Inicial del proyecto SOC (Levantamiento de información, planeación, diseño, pruebas y puesta en producción de las soluciones de inicio inmediato) es de máximo cuatro (4) meses contados a partir de la firma del acta de inicio.

Para las soluciones tecnológicas con fechas de inicio diferidas (Nuevo SIEM, NDR y Firewall de Bases de Datos), se acordará en el plan de trabajo un periodo de implementación y transición proporcional, previo a su respectiva fecha de salida a producción (septiembre 2027 y enero 2028). El Contratista deberá contemplar dentro de su alcance el esfuerzo técnico de integrar inicialmente las fuentes de datos al SIEM actual (IBM QRadar) y la posterior reintegración, migración de casos de uso y puesta a punto hacia la nueva plataforma SIEM una vez comience su fase de despliegue. | La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en efecto todos los servicios solicitados deberán ser implementados durante los primeros cuatro (4) meses del contrato, se exceptúan de estas labores los servicios que tienen fechas diferidas tales como el SIEM, FIREWALL DE BASES DE DATOS e INTELIGENCIA DE AMENAZAS, para lo cual el futuro contratista deberá tener en cuentas las fechas detalladas en el alcance técnico y proyectar así su posterior implementación. |

96	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	7. El CONTRATISTA deberá contar con tableros balanceados con información en línea sobre el estado del Ecosistema de la DIAN en temas de seguridad de la información, los cuales podrán ser consultado por la DIAN vía web. Dichos tableros deberán incluir mecanismos de autenticación, trazabilidad de acceso, conservación de histórico y evidencia para auditoría.	De manera respetuosa, solicitamos a la Entidad aclarar el alcance tecnológico del requerimiento asociado a la presentación de 'tableros balanceados'. Las plataformas core solicitadas en este proyecto (particularmente el SIEM y el SOAR) cuentan de manera nativa con consolas web, tableros personalizables (dashboards) a nivel ejecutivo y técnico, control de acceso basado en roles (RBAC) y trazabilidad de auditoría. Para realizar un correcto dimensionamiento técnico y económico, solicitamos confirmar si la visualización centralizada a través de las capacidades y tableros nativos de las plataformas de ciberseguridad ofertadas (SIEM/SOAR) es suficiente para dar cumplimiento a este punto, o si por el contrario, la Entidad exige la provisión, licenciamiento e integración de una herramienta externa de observabilidad o Inteligencia de Negocios (BI) dedicada exclusivamente para este propósito.	El CONTRATISTA deberá disponer de tableros de control (dashboards) ejecutivos y operativos con información en línea sobre el estado del Ecosistema de la DIAN en temas de seguridad de la información, los cuales podrán ser consultados por la Entidad vía web. Para dar cumplimiento a este requerimiento, el contratista podrá hacer uso de las capacidades nativas de visualización y reportería incluidas en las plataformas tecnológicas ofertadas (tales como el SIEM o el SOAR). Los accesos a estas consolas deberán incluir mecanismos de autenticación segura, trazabilidad de acceso, conservación de histórico y evidencia para auditoría.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, para dar cumplimiento a este requerimiento, el futuro contratista podrá hacer uso de las capacidades nativas de visualización y reportería incluidas en las plataformas tecnológicas ofertadas o de cualquier otra herramienta con la que cuente el proveedor, siempre y cuando se cumpla con lo solicitado en este ítem.
97	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	16. Deberá ejecutar lo planificado para el cierre de las vulnerabilidades identificadas, de acuerdo con la estrategia definida y teniendo en cuenta la criticidad de estas, probabilidad de explotación e impacto en caso de materialización.	De manera respetuosa, solicitamos a la Entidad aclarar el alcance de la obligación de 'ejecutar lo planificado'. En alineación con las mejores prácticas de ciberseguridad, gestión de servicios (ITIL) y separación de funciones (Segregation of Duties), el alcance del SOC y del equipo de gestión de vulnerabilidades debe ser de carácter consultivo, estratégico y de verificación. El contratista se encargará de identificar, priorizar (basado en riesgo e impacto), planificar y generar las recomendaciones de remediación. Sin embargo, la ejecución material de dichos cambios (aplicación de parches, modificaciones en código, cambios de configuración en servidores o bases de datos) recae única y exclusivamente bajo la responsabilidad de los administradores de TI o dueños de la plataforma de la Entidad. Solicitamos ajustar el requerimiento para que el contratista sea el encargado de hacer el seguimiento y la comprobación final, y no el ejecutor directo sobre la infraestructura productiva.	El CONTRATISTA deberá gestionar, hacer seguimiento y auditar lo planificado para el cierre de las vulnerabilidades identificadas, de acuerdo con la estrategia definida y teniendo en cuenta la criticidad de estas, probabilidad de explotación e impacto en caso de materialización. La ejecución material de las acciones de remediación (tales como la instalación de parches o cambios de configuración en ambientes productivos) será responsabilidad exclusiva de la Entidad a través de sus administradores de plataforma. Una vez la Entidad ejecute los cambios, el Contratista deberá realizar las pruebas de verificación correspondientes para dar por cerrada la vulnerabilidad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, las remediaciones y la intervenciones a las que haya lugar en la infraestructura propia de la Entidad, las realizará el personal de la DIAN, el futuro proveedor del SOC deberá realizar el acompañamiento desde el inicio y hasta la solución de las mismas, tal como se indica en el anexo técnico: 8.17 Apoyar con los recursos necesarios (personal idóneo) constantemente a la Dian realizando el respectivo acompañamiento, apoyo, experticia, experiencia, conocimiento en la resolución y remediación de todas y cada una de las vulnerabilidades encontradas durante la ejecución del contrato, se aclara que el personal de la Dian estará al frente de dichas actividades.
98	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Forma	8 Ver características en el ítem 9 del anexo técnico	Entendemos que este pago corresponde a la implementación de la plataforma de "Protección de Marca (Deep&Dark Web)". ¿Es correcto nuestro entendimiento?	8 Solución de Protección de Marca (Deep&Dark Web) Ver características en el ítem 9 del anexo técnico	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, su entendimiento es preciso, el pago se refiere a la implementación y puesta en operación del respectivo servicio o capacidad.
99	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Forma	12 Garantía y Soporte técnico de tres (3) años Al recibo a satisfacción de los entregables de esta capacidad De acuerdo con los valores ofertados (Ver características en el ítem 13 del anexo técnico)	De manera respetuosa, solicitamos a la Entidad modificar la condición de 'Pago único (general)' para el rubro de Garantía y Soporte técnico, alineándolo con el cronograma de implementación técnica exigido en el pliego. Como se ha establecido en los requerimientos, el proyecto contempla un despliegue diferido: un grupo de soluciones inicia su implementación al firmar el contrato, mientras que otras (como el SIEM, NDR y Firewall de BD) inician su operación entre 12 y 16 meses después. Mantener un pago único general genera una inconsistencia financiera y operativa, ya que obligaría al contratista a proveer licenciamiento, infraestructura y soporte por más de un año sin percibir la remuneración correspondiente, o viceversa. Para garantizar la viabilidad financiera del proyecto y el flujo de caja, solicitamos que el pago asociado a hardware, licenciamiento, soporte y garantía se realice de manera individual o fraccionada, atado a la firma del acta de recibo a satisfacción y puesta en producción de cada una de las soluciones.	Garantía y Soporte técnico de tres (3) años. Pago fraccionado por solución: El pago correspondiente al hardware, licenciamiento, garantía y soporte técnico se realizará de manera individual por cada capacidad o solución tecnológica implementada. Este pago se efectuará una vez se genere el recibo a satisfacción y la puesta en producción de la respectiva solución, de acuerdo con los valores ofertados y respetando el cronograma de entregas diferidas del proyecto (Fase Inicial y Fases Posteriores). (Ver características en el Ítem 13 del anexo técnico).	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los pagos se realizarán a medida de que el futuro proveedor de SOC vaya realizando la implementación y puesta en operación de cada uno de los servicios y capacidades SOC requeridas por la Entidad.
100	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Forma	11 Servicios de Monitoreo y operación de SOC con el personal mínimo requerido Informes mensuales de monitoreo y operación SOC **Pagos mensuales hasta el agotamiento de los recursos**	De manera respetuosa, solicitamos a la Entidad aclarar y modificar la condición de pago establecida como 'Pagos mensuales hasta el agotamiento de los recursos' para el rubro de Servicios de Monitoreo y operación de SOC. En el pliego se exige la disposición de un Equipo Mínimo de Trabajo dedicado y la prestación del servicio durante un periodo estricto de treinta y seis (36) meses. Establecer un modelo de pago 'hasta agotar recursos' genera una grave incertidumbre financiera y laboral. Si el presupuesto estimado por la Entidad se agota antes del mes 36, el contratista se vería imposibilitado para sostener la nómina del equipo humano exigido, poniendo en riesgo la continuidad de la operación de ciberseguridad y generando contingencias laborales. Para garantizar la viabilidad del proyecto, solicitamos que este rubro se defina como un servicio de tracto sucesivo con pagos mensuales fijos y garantizados durante los 36 meses de ejecución del servicio, alineando el presupuesto oficial con la duración real exigida.	Servicios de Monitoreo y operación de SOC con el personal mínimo requerido. Pago mensual por el servicio prestado: El pago de este rubro se realizará mediante actas parciales de cobro mensual, previa entrega y recibo a satisfacción de los Informes mensuales de monitoreo y operación SOC. Estos pagos mensuales se garantizarán de manera fija y recurrente durante los treinta y seis (36) meses de duración del servicio operativo, o hasta la finalización del plazo de ejecución contractual estipulado, garantizando así la cobertura salarial y operativa del Equipo Mínimo de Trabajo exigido.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, la operación, seguimiento, gestión, monitoreo y administración (con el equipo y/o perfiles de trabajo solicitados) por parte del futuro proveedor de todos los servicios requeridos irá hasta el 31 de octubre de 2028. (Tal como lo indica la nota 6 del archivo Formulario 1 Lista de precios). El derecho a uso, licenciamiento, suscripciones, actualizaciones, soporte y garantía irá por tres (3) años y sus periodos se contabilizarán a partir de la puesta en operación de cada uno de los servicios requeridos.
101	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Forma	1.1. Asignación de puntaje: b. Nivel de partner más alto en las capacidades ofertadas (ítems 2 al 9 del anexo técnico).	De manera respetuosa, solicitamos a la Entidad revisar y ampliar el alcance del criterio de calificación 'b. Nivel de partner más alto en las capacidades ofertadas'. En la industria de ciberseguridad, el nivel de partnership es una métrica de relacionamiento comercial entre el integrador y el fabricante, pero no garantiza la madurez técnica ni la eficacia de la herramienta. Mantener este criterio de forma exclusiva favorece enfoques de un único fabricante y penaliza arquitecturas especializadas (Best-of-Breed), donde se integran soluciones líderes indiscutibles en su respectivo dominio. Para garantizar que la Entidad adquiera las herramientas más robustas y con mejor reputación del mercado, solicitamos que este criterio se equilibre, otorgando el puntaje ya sea por el nivel de canal comercial del oferente, o bien, por la demostración de que la tecnología ofertada se encuentra posicionada en los niveles superiores de evaluaciones técnicas especializadas e independientes (tales como el cuadrante de Líderes de Gartner, Forrester Wave o equivalentes) para las categorías correspondientes.	b. Nivel comercial y técnico de las capacidades ofertadas (ítems 2 al 9 del anexo técnico). El oferente obtendrá puntuación si demuestra que, para cada capacidad evaluada, cumple con al menos una de las siguientes dos condiciones: 1. El oferente cuenta con el nivel de partner más alto otorgado por el fabricante de la solución. 2. La solución tecnológica ofertada se encuentra posicionada como Líder en su respectiva categoría según la última evaluación vigente de firmas analistas reconocidas internacionalmente (Ej. Gartner Magic Quadrant o Forrester Wave). 1 a 2 capacidades que cumplan alguna condición: 3 puntos 3 capacidades que cumplan alguna condición: 7 puntos 4 o más capacidades que cumplan alguna condición: 12 puntos	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el literal b es un ítem puntuable, para el caso en específico, la Entidad da una puntuación en caso de que el futuro interesado acredite pertenecer al nivel de parner más alto en las capacidades o servicios solicitados puntuando desde el que tenga dos (2) y hasta cuatro (4) o más membresías, así las cosas el futuro interesado podrá hacerse a esta puntuación según lo comentado anteriormente, por lo tanto, no se acepta su sugerencia en el entendido que la puntuación requerida ofrece equilibrio para el proyecto.
102	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	Razón de endeudamiento | Pasivo total / Activo total Menor o igual a 0,6	En relación con el requisito financiero de la Sección III, que establece una razón de endeudamiento (Pasivo total / Activo total ≤ 0,6), consideramos que dicho umbral resulta restrictivo frente a la realidad financiera de empresas del sector tecnológico y de servicios especializados en ciberseguridad. Estas compañías, por la naturaleza de sus operaciones y la dinámica de contratación de proyectos de gran escala, suelen manejar niveles de endeudamiento superiores sin que ello comprometa su solvencia ni capacidad de ejecución. Adicionalmente, el presente proceso corresponde a un contrato de aproximadamente USD 13 millones, lo cual asegura que los oferentes que cumplen con los demás indicadores de liquidez, patrimonio y capital de trabajo no son empresas pequeñas, sino organizaciones con capacidad financiera sólida y trayectoria comprobada. Por lo anterior, se solicita ajustar el criterio a un nivel de Pasivo total / Activo total ≤ 0,7, manteniendo un estándar prudente de control financiero, pero ampliando la participación de oferentes con capacidad técnica y financiera comprobada, garantizando mayor pluralidad y competitividad en el proceso.	Razón de endeudamiento | Pasivo total / Activo total Menor o igual a 0,7	En atención a la observación no se acepta la solicitud, el indicador se mantiene debido a la envergadura del proyecto.

103	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	Apalancamiento a corto plazo | Pasivo Corriente/Patrimonio Menor o igual a 0,5	En relación con el requisito financiero de la Sección III, que establece un apalancamiento a corto plazo (Pasivo corriente / Patrimonio ≤ 0,5), consideramos que este límite resulta excesivamente restrictivo y no refleja la realidad de empresas que, aun con un mayor nivel de pasivos corrientes, mantienen una estructura patrimonial sólida y capacidad de respuesta frente a sus obligaciones. El monto del proceso, cercano a USD 13 millones, garantiza que los oferentes que cumplen con los demás indicadores financieros son compañías de gran tamaño y con respaldo suficiente, por lo que flexibilizar este indicador no compromete la solvencia ni la estabilidad del proceso. Por lo anterior, se solicita ajustar el criterio a un nivel de Pasivo corriente / Patrimonio ≤ 0,8, lo cual mantiene un estándar razonable de prudencia financiera, pero permite ampliar la concurrencia de oferentes calificados, fortaleciendo la competitividad y garantizando la adecuada ejecución	Apalancamiento a corto plazo | Pasivo Corriente/Patrimonio Menor o igual a 0,8	En atención a la observación no se acepta la solicitud, el indicador se mantiene debido a la envergadura del proyecto.
104	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Forma	1 Índice de liquidez Activo | corriente/Pasivo corriente Mayor o igual a 1 2 Razón de endeudamiento | Pasivo total / Activo total Menor o igual a 0,6 3 Patrimonio en relación al presupuesto estimado del proceso | Patrimonio/Presupuesto estimado Mayor o igual a 0,1 4 Capital de trabajo en relación al presupuesto estimado del proceso | (Activo Corriente - Pasivo Corriente) /Presupuesto estimado Mayor o igual a 0,05 5 Apalancamiento a corto plazo | Pasivo Corriente/Patrimonio Menor o igual a 0,5	Se solicita respetuosamente a la entidad que publique de manera explícita las fórmulas utilizadas para el cálculo de los indicadores financieros en los casos de participación mediante asociaciones, consorcios o uniones temporales (APCA). Esto con el fin de garantizar transparencia y uniformidad en la interpretación de los criterios, evitando posibles errores o discrepancias por parte de los oferentes al momento de presentar sus propuestas.	Publicación de las respectivas formulas	En atención a la observación, a continuación se detallan las fórmulas para la evaluación de las APCAS: **Indicador** — **Fórmula de cálculo APCA** Índice de liquidez: $(AC_{socio1}*\%P_{socio1}) + (AC_{socio2}*\%P_{socio2})$ / $(PC_{socio1}*\%P_{socio1}) + (PC_{socio2}*\%P_{socio2})$ donde: AC= Activo corriente, PC=Pasivo corriente, %P= Porcentaje participación Razón de endeudamiento: $(P_{socio1}*\%P_{socio1}) + (P_{socio2}*\%P_{socio2})$ / $(A_{socio1}*\%P_{socio1}) + (A_{socio2}*\%P_{socio2})$ donde: A= Activo total, P=Pasivo total, %P= Porcentaje participación Patrimonio en relación al presupuesto estimado del proceso: $(Pt_{socio1}*\%P_{socio1}) + (Pt_{socio2}*\%P_{socio2})$ / PE donde: Pt = Patrimonio, PE=Presupuesto Estimado, %P= Porcentaje participación Capital de trabajo en relación al presupuesto estimado del proceso: $[(AC_{socio1}*\%P_{socio1}) + (AC_{socio2}*\%P_{socio2})] - [(PC_{socio1}*\%P_{socio1}) + (PC_{socio2}*\%P_{socio2})]$ / PE donde: AC= Activo corriente, PC=Pasivo corriente, PE=Presupuesto Estimado, %P= Porcentaje participación Apalancamiento a corto plazo: $[(PC_{socio1}*\%P_{socio1}) + (PC_{socio2}*\%PC_{socio2})]$ / $[(Pt_{socio1}*\%P_{socio1}) + (Pt_{socio2}*\%P_{socio2})]$ donde: PC=Pasivo Corriente, Pt= Patrimonio, %P= Porcentaje participación Los porcentajes de participación de cada firma por criterio (Activo total o corriente, pasivo total o corriente y patrimonio) se calculan sobre la sumatoria de esos mismos criterios para el APCA que se presenta. Esto significa que, por ejemplo: %P para Activo= Asocio1/(Asocio1+Asocio2)
105	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Forma	La fecha límite para presentar las ofertas es: Fecha: 14 de mayo de 2026 Hora: hasta las 10:00 am (hora legal colombiana) Los Oferentes podrán presentar sus ofertas electrónicamente (de manera virtual).	Solicitamos respetuosamente a la entidad aclarar y publicar un cronograma detallado de actividades del proceso, dado que actualmente no resulta claro cuál es la fecha límite para solicitar el enlace de presentación de la oferta. Asimismo, se requiere precisar si en el caso de participación mediante asociaciones, consorcios o uniones temporales (APCA) esta condición debe manifestarse expresamente en la solicitud del	Aclaración por parte de la entidad	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, los documentos y demás información concerniente al proceso se encuentra publicada en el link https://www.dian.gov.co/dian/Paginas/Fondo-DIAN.aspx, allí los interesados pueden descargarlos y dentro de los mismos se encuentra estipulado el respectivo cronograma del proceso.
106	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Forma	La fecha límite para presentar las ofertas es: Fecha: 14 de mayo de 2026 Hora: hasta las 10:00 am (hora legal colombiana) Los Oferentes podrán presentar sus ofertas electrónicamente (de manera virtual).	Solicitamos confirmar si para la solicitud del enlace se debe cumplir con algún requisito previo, como experiencia, presentación de estados financieros u otro criterio específico, con el fin de garantizar transparencia y evitar interpretaciones erróneas por parte de los posibles oferentes.	Aclaración por parte de la entidad	En atención a la observación presentada, para la solicitud de enlace no se requiere el cumplimiento de ningun requisito previo.
107	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	27. Liquidación por Daños y Perjuicios 27.1 Con excepción de lo que se establece en la Cláusula 32 de las CGC, si el Proveedor no cumple con la entrega de la totalidad o parte de los Bienes en la(s) fecha(s) establecida(s) o con la prestación de los Servicios Conexos dentro del período que el Comprador tenga en virtud del Contrato, éste podrá deducir del Precio del Contrato por concepto de liquidación de daños y perjuicios, una suma equivalente al porcentaje del precio de entrega de los Bienes atrasados o de los servicios no prestados establecido en las CEC por cada semana o parte de la semana de retraso hasta alcanzar el máximo del porcentaje especificado en las CEC. Al alcanzar el máximo establecido, el Comprador podrá dar por terminado el Contrato de conformidad con la Cláusula 35 de las CGC.	Se solicita precisar que la aplicación de la liquidación de daños y perjuicios prevista en la Cláusula 27 únicamente proceda cuando el incumplimiento sea imputable al Proveedor, excluyendo aquellos eventos derivados de causas no atribuibles a este,	Aclaración por parte de la entidad	En atención a la observación presentada, se precisa que la aplicación de la cláusula de liquidación de daños y perjuicios prevista en la Cláusula 27 de las CGC se realizará previa verificación por parte del Comprador de las circunstancias que dieron lugar al eventual incumplimiento. En este sentido, se evaluará si dicho incumplimiento es efectivamente imputable al Proveedor, teniendo en cuenta los soportes y justificaciones que este aporte, así como las condiciones de ejecución del contrato.
108	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	28.5 Tan pronto reciba el Proveedor dicha comunicación, y dentro del plazo establecido en las CEC, deberá reparar o reemplazar los Bienes defectuosos, o sus partes sin ningún costo para el Comprador.	Se solicita que el plazo para la reparación o reemplazo de los bienes defectuosos sea definido y acordado previamente entre las partes,	Aclaración por parte de la entidad	De acuerdo con las Condiciones Especiales del Contrato (CEC) indican que el numeral 28.5 no aplica para las condiciones del presente proceso.
109	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial		Solicitar la inclusión expresa de una causal de terminación anticipada a favor del Proveedor, cuando la ejecución del contrato se torne objetiva o jurídicamente inviable por causas no imputables al Proveedor, incluyendo cambios normativos, restricciones legales, decisiones del Comprador o circunstancias de fuerza mayor o caso fortuito.	Aclaración por parte de la entidad	Las causales de terminación de las Condiciones Generales del Contrato No. 35 - Terminación - no son susceptibles de modificación al ser condiciones establecidas por el Banco Interamericano de Desarrollo BID.
110	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	Deberá realizar una primera etapa de complemento y levantamiento de información donde detalle algunos aspectos no incluidos en este documento y el anexo de características técnicas para el diagnóstico de las condiciones actuales con el fin de realizar el diseño de acuerdo con las capacidades y servicios requeridos y según la infraestructura tecnológica a monitorear y supervisar.	De manera respetuosa, solicitamos a la Entidad aclarar la expectativa con relación al tiempo de ejecución de esta fase de levantamiento, y si se considerará algún periodo de transición para iniciar con la medición formal de indicadores del Servicio mientras se completan las etapas de afinamiento inicial del Servicio.	Por favor especificar tiempos esperados para completar cada fase y condiciones contractuales de periodo de transición inicial.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el tiempo máximo de implementación es de cuatro (4) meses, y dentro de este tiempo el futuro proveedor debe contemplar un levantamiento de información.
111	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	El contratista deberá presentar un Plan de calidad, enfocado en Asegurar la calidad de los servicios de monitoreo, detección y respuesta a incidentes, de modo que cumplan con los requisitos técnicos y de seguridad. El plan debe tener en cuenta como mínimo los siguientes aspectos y sin limitarse a:	De manera respetuosa, agradecemos a la entidad confirmar en que momento se debe entregar este Plan de Calidad y si es requerida la conformación de un Comité de Calidad que realice el monitoreo a la ejecución del plan durante la vigencia del Contrato		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el plan de calidad deberá entregarse por parte del futuro contratista antes de la respectiva implementación.
112	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	Serán parte del diseño, entre otras, la identificación e integración inicial de las fuentes de eventos a monitorear, y de las sucesivas que la DIAN solicite a lo largo del contrato, el modelado de amenazas, la definición y desarrollo de los casos de uso de monitoreo, la generación y ejecución de los planes de vulnerabilidades, ethical hacking, la alta disponibilidad y DRP de las soluciones de seguridad de la información entregadas en por el CONTRATISTA en el actual proyecto.	Con relación a estos ítem, se requerirá involucrar al Equipo de Ingeniería ya que lo más probable es que impliquen la generación de nuevas propuestas de diseño de Producto o Servicio. Agradecemos a la entidad confirmar si para estos Servicios adicionales especializados se usará una Bolsa de horas adicional a la propuesta, lo cual podría generar un desequilibrio económico al Proyecto, ya que no pueden ser dimensionados en la etapa pre contractual.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, todas las actividades solicitadas en este ítem y los demás que componen y se describen en los documentos propios del proceso, hacen parte integral del proyecto, por ende los futuros interesados deben considerarlos dentro de su oferta, se aclara que no son servicios adicionales, y que la Entidad en ningún momento ha considerado una bolsa de horas para tales propósitos.
113	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	Deberá realizar y entregar el plan de trabajo detallado para la operación de forma anualizada y por cada uno de los temas asociados a la operación. Este plan deberá contemplar indicadores verificables, responsables, mecanismos de reporte y trazabilidad sobre las acciones ejecutadas.	El Plan de Trabajo anualizado se entiende como un documento de planeación y seguimiento de alto nivel, estructurado por dominios o temas de operación del SOC. Esto conlleva a que no se requiere la elaboración de planes detallados a nivel de actividad diaria ni la replanificación continua, salvo ante cambios formales de alcance solicitados por la DIAN. De manera respetuosa, agradecemos a la entidad confirmar si es correcto nuestro entendimiento.	El CONTRATISTA deberá elaborar y entregar un Plan de Trabajo anual para la operación del Servicio de SOC, el cual deberá estar alineado exclusivamente con el alcance contractual del servicio y estructurarse por cada uno de los temas o dominios asociados a la operación (por ejemplo: monitoreo, detección, respuesta a incidentes, gestión de alertas, mejora continua, entre otros). El Plan de Trabajo tendrá un enfoque de planeación, seguimiento y control a nivel operativo – táctico, sin requerir la definición de actividades a nivel de microgestión ni la planificación detallada de tareas diarias. El Plan deberá contemplar, como mínimo: - Actividades incluidas, claramente asociadas al alcance del servicio contratado. - Indicadores de desempeño y calidad, medibles y verificables, alineados con los SLA y KPI definidos contractualmente. - Responsables, identificando los roles del CONTRATISTA encargados de la ejecución y el seguimiento, así como las dependencias que corresponden a la DIAN cuando aplique.	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el plan solicitado debe cumplir con los requerimientos mínimos solicitados en este ítem, el futuro contratista deberá tenerlos en cuenta, y desde allí diseñar su propuesta con los respectivos valores agregados de acuerdo a la experticia del interesado.

114	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	Deberá realizar y entregar el plan de trabajo detallado para la operación de forma anualizada y por cada uno de los temas asociados a la operación. Este plan deberá contemplar indicadores verificables, responsables, mecanismos de reporte y trazabilidad sobre las acciones ejecutadas.	Para que el plan de trabajo sea consistente con la operación, los indicadores incluidos en el mismo deberán ser medibles, verificables y alineados con los niveles de servicio (SLA y KPI) definidos en el contrato. Esto conlleva a que no se considerarán indicadores que dependan exclusivamente de decisiones, accesos, herramientas o tiempos de respuesta de la DIAN o de terceros. De manera respetuosa, agradecemos a la entidad confirmar si es correcto nuestro entendimiento.	El CONTRATISTA deberá elaborar y entregar un Plan de Trabajo anual para la operación del Servicio de SOC, el cual deberá estar alineado exclusivamente con el alcance contractual del servicio y estructurarse por cada uno de los temas o dominios asociados a la operación (por ejemplo: monitoreo, detección, respuesta a incidentes, gestión de alertas, mejora continua, entre otros). El Plan de Trabajo tendrá un enfoque de planeación, seguimiento y control a nivel operativo – táctico, sin requerir la definición de actividades a nivel de microgestión ni la planificación detallada de tareas diarias. El Plan deberá contemplar, como mínimo: - Actividades incluidas, claramente asociadas al alcance del servicio contratado. - Indicadores de desempeño y calidad, medibles y verificables, alineados con los SLA y KPI definidos contractualmente. - Responsables, identificando los roles del CONTRATISTA encargados de la ejecución y el seguimiento, así como las dependencias que correspondan a la DIAN cuando aplique.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el plan solicitado debe cumplir con los requerimientos mínimos solicitados en este ítem, el futuro contratista deberá tenerlos en cuenta, y desde allí diseñar su propuesta con los respectivos valores agregados de acuerdo a la experticia del interesado.
115	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	Deberá incluir en el diseño de la estrategia de presentación del servicio SOC las alertas tempranas para todos los incidentes de seguridad de la información y/o vulnerabilidades, incluso de día cero, que puedan poner en peligro la seguridad de la información de la DIAN.	De manera respetuosa, agradecemos a la entidad confirmar si es correcto nuestro entendimiento, con relación a que las alertas tempranas se generarán únicamente sobre los activos, sistemas y aplicaciones previamente integrados al SOC y formalmente definidos dentro del alcance del servicio. Esto quiere decir que quedarían excluidos los activos no monitoreados, partes no integradas o tecnologías no soportadas por las herramientas del SOC.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, su entendimiento es correcto, las alertas tempranas se generarían únicamente sobre la infraestructura tecnológica monitoreada desde el futuro centro de operaciones de seguridad - SOC, a cargo del futuro contratista.
116	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	Deberá realizar el análisis y reporte del Retorno de la Inversión en Seguridad de la Información (ROSI) incorporando un desarrollo y/o herramienta que permita tener una visión global de servicio SOC, independiente de las consolas de las plataformas para análisis y generación de reportes, que permita obtener información sobre el posible impacto económico de la prevención del riesgo de seguridad digital (no materialización), así como obtener el impacto económico de la materialización del riesgo de seguridad digital.	El análisis y reporte del Retorno de la Inversión en Seguridad de la Información (ROSI) se realizará bajo un enfoque referencial y estimado, basado en metodologías reconocidas, supuestos razonables y la información disponible del servicio SOC. Dicho análisis no constituirá una medición financiera exacta ni una garantía de ahorro económico real para la DIAN, y estará sujeto a las limitaciones propias de la información provista por la DIAN y a la información de los eventos de seguridad observados o detectados. De manera respetuosa, agradecemos a la entidad confirmar si es correcto nuestro entendimiento.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, su entendimiento es correcto, dicho análisis no constituirá una medición financiera exacta ni una garantía de ahorro económico real para la DIAN, y estará sujeto a las limitaciones propias de la información provista por la DIAN y a la información de los eventos de seguridad observados o detectados.
117	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Sustancial	El CONTRATISTA deberá contar con un equipo mínimo de trabajo (especificado en el anexo de características mínimas) exclusivo asignado al SOC este equipo se encargará de la gerencia, operación y relacionamiento entre el SOC y la DIAN; el CONTRATISTA deberá describir su conformación indicando como mínimo el rol, sus responsabilidades y tiempo asignado; esta estructura deberá ser presentada a la DIAN para su aprobación y deberá mantenerse durante la ejecución del proyecto.	De manera respetuosa, agradecemos a la entidad confirmar si el dimensionamiento del equipo mínimo del SOC estará directamente asociado a la cantidad, criticidad y tipología de los activos de información efectivamente integrados y gestionados por el SOC, y si, en caso de que dicha cantidad supere los umbrales definidos durante el diseño inicial del servicio, se podrá replantear el modelo operativo del SOC, considerando un incremento en el tamaño del equipo dedicado		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, todas las condiciones consignadas en los documentos propios del proceso son características mínimas solicitadas por la Entidad, en el caso del equipo de trabajo, es el mínimo exigido por la Entidad, si el futuro contratista estima conveniente adicionar más personal a dicho equipo, lo podrá hacer siempre y cuando no genere valores o cargos adicionales a la Entidad.
118	Sección III	Formal	(ii) Experiencia y capacidad técnica general: Contratos terminados o iniciados (mínimo 40% de ejecución) dentro de los últimos siete (7) años con entidades públicas y/o privadas, nacionales o internacionales, relacionados con las siguientes actividades: • Servicios de diseño, planeación e implementación de Centros de Operaciones de Seguridad (SOC) y/o servicios avanzados de protección en ciberseguridad. • Suministro de hardware y software especializado en seguridad informática de nivel empresarial. • Servicios de implementación, integración y configuración de soluciones avanzadas de ciberseguridad. Presentar máximo seis (6) contratos. La sumatoria de los contratos debe ser mínimo de seis (6) millones de dólares. Entre los contratos presentados se debe cumplir que: - Al menos uno (1) debe haber sido ejecutado para el sector Gubernamental. - Al menos uno (1) debe haber sido ejecutado para el sector Financiero. - Al menos uno (1) incluya actividades de prestación de servicios de SOC, por un valor mayor a un (1) millón de dólares. Nota: Si el contrato presentado corresponde a una APCA: asociación en participación, consorcio, unión temporal, asociación o cualquier otra figura asociativa en la que se responda solidariamente por la ejecución del contrato, se tendrá como válido el valor del total del contrato multiplicado por el porcentaje de participación del interesado, para el efecto, las certificaciones	Teniendo en cuenta que la figura de Red Global de Firmas Miembro permite a sus integrantes tener acceso ilimitado a profesionales, capital intelectual, experiencias, metodologías, aceleradores a nivel global y normas de calidad para ofrecer servicios integrados a clientes en todo el mundo. Cada Firma Miembro, sus entidades afiliadas y subsidiarias, son entidades independientes que operan bajo la legislación y normatividad vigente en su respectiva jurisdicción y, a su vez, se rigen y orientan bajo la marca, las prácticas compartidas y los estándares de servicio al cliente que, entre otros protocolos y directrices, las distinguen e identifican como Deloitte.	De acuerdo con la observación, solicitamos amablemente se especifique en la solicitud esa referencia cuando se trata de red global de firmas miembro: "RED INTERNACIONAL DE FIRMAS Cuando el OFERENTE pertenezca a una red internacional de firmas, podrá acreditar experiencia por otras firmas que pertenezcan a la misma red. Se entiende por red internacional de firmas el conjunto de empresas que, aun siendo sociedades independientes y sin relaciones de propiedad entre ellas, se presentan ante el público como una misma organización empresarial por compartir marcas, emblemas y otros símbolos distintivos".	No se acepta la observación. Existe una diferencia entre sucursal y filial en relación con la acreditación de la experiencia. Filiales: Al tratarse de sociedades legalmente constituidas en Colombia o en el país donde operan, cuentan con personalidad jurídica propia, independencia y autonomía administrativa respecto de la casa matriz. En consecuencia, la experiencia que haya adquirido la matriz no puede trasladarse ni acumularse a favor de la filial, puesto que se trata de entes jurídicos distintos. Sucursales: A diferencia de las filiales, no constituyen una nueva persona jurídica, sino que son una extensión de la casa matriz en otro territorio. Por tanto, las obligaciones, derechos y, en particular, la experiencia adquirida por la matriz sí son plenamente atribuibles a la sucursal, en la medida en que ambas forman parte de un mismo sujeto jurídico.
119	Sección III	Formal	5.1 Criterios de Calificación (IAO 38.1) (i) El Oferente deberá proporcionar prueba documental que demuestre que cumple los siguientes requisitos financieros: ... Indicador: Apalancamiento a corto plazo. Fórmula: Pasivo Corriente/Patrimonio Valor del indicador: Menor o igual a 0,5	Modificación del indicador Apalancamiento a corto plazo	5.1 Criterios de Calificación (IAO 38.1) (i) El Oferente deberá proporcionar prueba documental que demuestre que cumple los siguientes requisitos financieros: ... Indicador: Apalancamiento a corto plazo. Fórmula: Pasivo Corriente/Patrimonio Valor del indicador: Menor o igual a **0,6.** De manera atenta, se sugiere a la Entidad evaluar la conveniencia de establecer el valor máximo del indicador de apalancamiento a corto plazo en **0,6**, en lugar de 0,5, como una referencia financiera alineada con las condiciones reales del mercado. Esta consideración se sustenta en la sólida trayectoria financiera demostrada por Deloitte durante los últimos cinco (5) años, periodo en el cual ha mantenido niveles adecuados de liquidez, estabilidad patrimonial y cumplimiento oportuno de sus obligaciones, sin registrar impactos negativos en su desempeño financiero. El ajuste propuesto no desvirtúa el carácter	En atención a la observación no se acepta la solicitud, el indicador se mantiene debido a la envergadura del proyecto.

120	Sección III	Formal	(ii) Experiencia y capacidad técnica general: Contratos terminados o iniciados (mínimo 40% de ejecución) dentro de los últimos siete (7) años con entidades públicas y/o privadas, nacionales o internacionales, relacionados con las siguientes actividades: • Servicios de diseño, planeación e implementación de Centros de Operaciones de Seguridad (SOC) y/o servicios avanzados de protección en ciberseguridad. • Suministro de hardware y software especializado en seguridad informática de nivel empresarial. • Servicios de implementación, integración y configuración de soluciones avanzadas de ciberseguridad.	Modificación experiencia	(ii) Experiencia y capacidad técnica general: Contratos terminados o iniciados (mínimo 40% de ejecución) dentro de los últimos siete (7) años con entidades públicas y/o privadas, nacionales o internacionales, relacionados con **alguna de** las siguientes actividades: • Servicios de diseño, planeación e implementación de Centros de Operaciones de Seguridad (SOC) y/o servicios avanzados de protección en ciberseguridad. • Suministro de hardware y software especializado en seguridad informática de nivel empresarial. • Servicios de implementación, integración y configuración de soluciones avanzadas de ciberseguridad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el requerimiento es claro en cuando a la experiencia solicitada, la cual se enmarca entre las opciones presentadas por el mismo ítem, por lo tanto, no es posible aceptar su sugerencia. Ahora bien, mediante Adenda se incluirá la siguiente Nota 2 en el numeral ii) - Experiencia y Capacidad Técnica General del numeral 5. Calificación del Oferente (IAO 38), la cual dispondrá lo siguiente: Nota 2: En caso de APCA, la experiencia podrá ser sumada, no obstante, todos los integrantes deberán haber celebrado al menos uno de los contratos exhibidos.
121	Sección III	Formal	En el caso de las diferentes figuras asociativas, se realizará un promedio ponderado de cada uno de los conceptos relacionados en la tabla anterior (Activos, pasivos y patrimonio) a partir de la información de los Estados financieros de cada una de las firmas integrantes y se aplicará la fórmula.	Aclaración	En párrafo menciona que se aplicará la formula; sin embargo, solicitamos publicar a los oferentes la fórmula con la respectiva explicación de cada componente de la fórmula.	En atención a la observación, a continuación se detallan las fórmulas para la evaluación de las APCAS: **Indicador** — **Fórmula de cálculo APCA** Índice de liquidez: $\frac{(AC_{Socio1}*\%P_{socio1}) + (AC_{Socio2}*\%P_{socio2})}{(PC_{Socio1}*\%P_{socio1}) + (PC_{Socio2}*\%P_{socio2})}$ — donde: AC= Activo corriente, PC=Pasivo corriente, %P= Porcentaje participación Razón de endeudamiento: $\frac{(P_{socio1}*\%P_{socio1}) + (P_{socio2}*\%P_{socio2})}{(A_{socio1}*\%P_{socio1}) + (A_{socio2}*\%P_{socio2})}$ — donde: A= Activo total, P=Pasivo total, %P= Porcentaje participación Patrimonio en relación al presupuesto estimado del proceso: $\frac{(Pt_{socio1}*\%P_{socio1}) + (Pt_{socio2}*\%P_{socio2})}{PE}$ — donde: Pt = Patrimonio, PE=Presupuesto Estimado, %P= Porcentaje participación Capital de trabajo en relación al presupuesto estimado del proceso: $\frac{[(AC_{socio1}*\%P_{socio1}) + (AC_{socio2}*\%P_{socio2})] - [(PC_{socio1}*\%P_{socio1}) + (PC_{socio2}*\%P_{socio2})]}{PE}$ — donde: AC= Activo corriente, PC=Pasivo corriente, PE=Presupuesto Estimado, %P= Porcentaje participación Apalancamiento a corto plazo: $\frac{[(PC_{Socio1}*\%P_{socio1}) + (PC_{Socio2}*\%P_{socio2})]}{[(Pt_{socio1}*\%P_{socio1}) + (Pt_{socio2}*\%P_{socio2})]}$ — donde: PC=Pasivo Corriente, Pt= Patrimonio, %P= Porcentaje participación Los porcentajes de participación de cada firma por criterio (Activo total o corriente, pasivo total o corriente y patrimonio) se calculan sobre la sumatoria de esos mismos criterios para el APCA que se presenta. Esto significa que, por ejemplo: %P para Activo= Asocio1/(Asocio1+Asocio2)
122	Sección III	Formal	Entre los contratos presentados se debe cumplir que: - Al menos uno (1) debe haber sido ejecutado para el sector Gubernamental. - Al menos uno (1) debe haber sido ejecutado para el sector Financiero. - Al menos uno (1) incluya actividades de prestación de servicios de SOC, por un valor mayor a un (1) millón de dólares.	Modificación de la cantidad de experiencias.	Entre los contratos presentados se debe cumplir que **se cumplan al menos dos de las siguientes condiciones**: - Al menos uno (1) debe haber sido ejecutado para el sector Gubernamental. - Al menos uno (1) debe haber sido ejecutado para el sector Financiero. - Al menos uno (1) incluya actividades de prestación de servicios de SOC, por un valor mayor a un (1) millón de dólares. Nota: Si el contrato presentado corresponde a una APCA: asociación en participación, consorcio, unión temporal, asociación o cualquier otra figura asociativa en la que se responda solidariamente por la ejecución del contrato, se tendrá como válido el valor del total del contrato multiplicado por el porcentaje de participación del interesado, para el efecto, las certificaciones allegadas deben especificar el porcentaje de participación y que esta sea verificable	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, en el mismo ítem se encuentra la correspondiente nota, la cual se muestra al final de esta respuesta, por lo tanto, no se acepta su sugerencia. Nota: Si el contrato presentado corresponde a una APCA: asociación en participación, consorcio, unión temporal, asociación o cualquier otra figura asociativa en la que se responda solidariamente por la ejecución del contrato, se tendrá como válido el valor del total del contrato multiplicado por el porcentaje de participación del interesado, para el efecto, las certificaciones allegadas deben especificar el porcentaje de participación y que esta sea verificable
123	Sección VI	Formal	Consideraciones Herramientas SIEM, Protección de bases de datos e Inteligencia de amenazas. Actualmente, la DIAN cuenta con las siguientes soluciones: •Una solución SIEM IBM QRadar contratada hasta el 31 de agosto de 2027. •Un firewall de bases de datos IBM GUARDIUM contratado hasta diciembre 31 de 2027. •Solución de Inteligencia de Amenazas contratada hasta diciembre 31 de 2027.	Definición de expectativa y migración: Respecto a la transición del SIEM, vemos que solicitan operar el IBM QRadar actual hasta agosto de 2027, pero piden implementar el nuevo SOAR desde el inicio del contrato. ¿La expectativa es que integremos el nuevo SOAR con el QRadar actual durante esos tres años y luego volvamos a configurar los playbooks para el nuevo SIEM? Adicionalmente, al hacer el cambio de SIEM en 2027, ¿se debe migrar la data y logs históricos de QRadar a la nueva plataforma, o el nuevo SIEM iniciará desde cero?	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el futuro contratista deberá integrar el nuevo SOAR con el QRadar actual por el tiempo requerido en los documentos del proceso, así mismo, deberá implementar el nuevo SIEM, configurando los playbooks y migrar la data y logs históricos de QRadar a la nueva plataforma.
124	6.4.2	Formal	Ítem 6.4.2 El appliance, o solución, plataforma o servicio de decepción debe estar en capacidad de crear al menos 400 señuelos, en hasta 20 máquinas virtuales y desplegarse en mínimo 120 VLANs. o características similares o superiores en las tecnologías ofrecidas.	En el ítem 6, denominado "Caza de Amenazas", los requerimientos técnicos (como la creación de 400 señuelos y trampas en 120 VLANs) apuntan estrictamente a tecnología de Engaño (Deception Technology). ¿La entidad aceptará propuestas de Caza de Amenazas basadas en metodologías de analítica avanzada e Inteligencia Artificial (SIEM/EDR), o es obligatorio ofertar una solución nativa y especializada en Decetion?	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem solicita o requiere una solución de caza de amenazas o su equivalente, por lo tanto, es valido ofrecer soluciones o servicios equivalentes o similares siempre y cuando se cumpla con las características técnicas mínimas solicitadas en los documentos del proyecto.
125	5.3.1	Formal	Ítem 1.2 Se debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá que cuente con las condiciones adecuadas para garantizar la continuidad operativa, la seguridad física y lógica, y el cumplimiento de las mejores prácticas del sector. Donde instalará todos los productos, capacidades, plataformas, soluciones y servicios, que sean requeridos alojar allí para dar cumplimiento a lo solicitado en el anexo técnico y que le permitan realizar todas las actividades encomendadas en este documento por la DIAN. Entendiéndose que el CONTRATISTA realizará toda la gestión, monitoreo, administración, optimización, actualización, acompañamiento, soporte y garantía de los mismos, cobijando toda la infraestructura tecnológica de la Entidad. Para el efecto debe tener la capacidad de detectar, escalar, informar, acompañar apoyar y soportar a la DIAN en la resolución de cada uno de los incidentes encontrados por el SOC durante el tiempo que dure el proyecto en mención. Los activos y demás características de estos se encuentran detallados en el apartado de inventarios y las especificaciones de cada una de las soluciones, plataformas, capacidades, servicios, soporte y garantía se encuentran en este anexo técnico de obligatorio cumplimiento. Ítem 5.3.1 Debe ser en modalidad software como servicio. (SaaS), con capacidad de aprovisionamiento rápido y elasticidad automática de servicios. No se aceptan soluciones de código abierto o similares. Debe integrarse con las plataformas SIEM, SOAR a considerar en el Proyecto. El servicio SaaS incluye la operación y mantenimiento de la plataforma, su monitoreo, actualizaciones, soporte técnico con ingeniero de fabricante dedicado con Tecnical Account Manager TAMv optimización continua	Notamos una posible contradicción respecto a la ubicación de las soluciones: el ítem 1.2 exige que el SOC esté en Bogotá y allí se instale todo, pero ítems como el 5 y 8 exigen plataformas en la nube (SaaS). Para plataformas nativas de nube como el SIEM o el SOAR, ¿existe alguna restricción de soberanía de datos que obligue a almacenar los logs físicamente en Colombia, o es totalmente válido que la información resida en las regiones globales de nube del fabricante?	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, es válido que la información resida en las regiones globales de nube del fabricante
126	7.3	Formal	Ítem 7.3 Se debe licenciar como mínimo para 25000 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web).	Para la capacidad de NDR (Ítem 7), donde se requiere analizar el tráfico de red de 25.000 activos a través de puertos pasivos (SPAN), nos gustaría entender la topología actual: ¿La DIAN ya cuenta con un concentrador de tráfico o Packet Broker centralizado en su Data Center principal donde podamos conectar los sensores del NDR, o será necesario contemplar el despliegue de equipos físicos en las diferentes sedes regionales del país?	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro contratista deberá contemplar todos y cada uno de los elementos necesarios para dar cumplimiento a los requerimientos del proceso, en el caso particular se informa que no se cuenta con un concentrador de tráfico, por ende los interesados deberán contemplar lo necesario para realizar los respectivos despliegues en las sedes a nivel nacional de la Entidad.

127	Sección III	Formal	En el caso de las diferentes figuras asociativas, se realizará un promedio ponderado de cada uno de los conceptos relacionados en la tabla anterior (Activos, pasivos y patrimonio) a partir de la información de los Estados financieros de cada una de las firmas integrantes y se aplicará la fórmula.	Entendemos que el promedio ponderado se realizará con relación al porcentaje de participación, sin embargo al no indicarlo explícitamente podría dar lugar a confusiones.	En el caso de las diferentes figuras asociativas, se realizará un promedio ponderado con relación al porcentaje de participación de cada uno de los conceptos relacionados en la tabla (Activos, pasivos y patrimonio)	En atención a la observación, a continuación se detallan las fórmulas paraa la evaluación de las APCAS: **Indicador** — **Fórmula de cálculo APCA** Índice de liquidez: $\frac{(AC_{asocio1}*\%P_{asocio1}) + (AC_{asocio2}*\%P_{asocio2})}{(PC_{asocio1}*\%P_{asocio1}) + (PC_{asocio2}*\%P_{asocio2})}$ — donde: AC= Activo corriente, PC=Pasivo corriente, %P= Porcentaje participación Razón de endeudamiento: $\frac{(P_{asocio1}*\%P_{asocio1}) + (P_{asocio2}*\%P_{asocio2})}{(A_{asocio1}*\%P_{asocio1}) + (A_{asocio2}*\%P_{asocio2})}$ — donde: A= Activo total, P=Pasivo total, %P= Porcentaje participación Patrimonio en relación al presupuesto estimado del proceso: $\frac{(PT_{asocio1}*\%P_{asocio1}) + (PT_{asocio2}*\%P_{asocio2})}{PE}$ — donde: Pt = Patrimonio, PE=Presupuesto Estimado, %P= Porcentaje participación Capital de trabajo en relación al presupuesto estimado del proceso: $\frac{[(AC_{asocio1}*\%P_{asocio1}) + (AC_{asocio2}*\%P_{asocio2})] - [(PC_{asocio1}*\%P_{asocio1}) + (PC_{asocio2}*\%P_{asocio2})]}{PE}$ — donde: AC= Activo corriente, PC=Pasivo corriente, PE=Presupuesto Estimado, %P= Porcentaje participación Apalancamiento a corto plazo: $\frac{[(PC_{asocio1}*\%P_{asocio1}) + (PC_{asocio2}*\%PC_{asocio2})]}{[(Pt_{asocio1}*\%P_{asocio1}) + (Pt_{asocio2}*\%P_{asocio2})]}$ — donde: PC=Pasivo Corriente, Pt= Patrimonio, %P= Porcentaje participación Los porcentajes de participación de cada firma por criterio (Activo total o corriente, pasivo total o corriente y patrimonio) se calculan sobre la sumatoria de esos mismos criterios para el APCA que se presenta. Esto significa que, por ejemplo: %P para Activo= Asocio1/(Asocio1+Asocio2)
128	Proyecto SOC DIAN	Formal	Licenciamiento para 25000 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, usuarios de directorio activo, plataformas alojadas en nube publica, entre otros y 260 aplicaciones web).	Se pide a a la entidad aclarar el detalle de los 25.000 activos; ya que 15.000 PCs + 2.467 activos de infraestructura + 260 aplicaciones web son un total de 17.727. ¿cuáles son los 7.223 activos restantes?	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las cantidades mencionadas contemplan las respectivas proyecciones hechas por la Entidad, tener en cuenta que el máximo de elementos o activos a cubrir por el SOC es de 25000.
129	5.9.1	Formal	La solución debe realizar el escaneo para la detección de vulnerabilidades locales y remotas sin la necesidad de un agente en el dispositivo de destino.	Para poder hacer un correcto dimensionamiento para este ITEM se solicita especificar la periodicidad de los escaneos a ejecutar para los 25.000 activos. Ejm: mínimo 1 mensual		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los escaneos solicitados son ilimitados, es decir se deben realizar programados, por demanda en cualquier momento requerido por la entidad. Para el caso de la capacidad de aseguramiento de directorio activo este debe ser en tiempo real para la totalidad del directorio activo sin ningún limite durante la duración del licenciamiento ofertado. Para el caso de la capacidad de seguridad en nube publica esta debe ser en todas sus funcionalidades en tiempo real y conectada con las nubes publicas de la DIAN para lograr un aseguramiento continuo e integral sin ningún limite durante la duración del licenciamiento ofertado. Para el caso de las capacidades de escaneo de aplicaciones web se requieren escaneo ilimitado sin ningún limite durante la duración del licenciamiento ofertado.
130	5.9.2	Formal	Debe tener la funcionalidad de realizar pruebas con agentes para la detección de vulnerabilidad local sin costo adicional.	En el numeral 5.9.2, el pliego indica que la solución "debe tener la funcionalidad de realizar pruebas con agentes para la detección de vulnerabilidad local sin costo adicional", y en el numeral 5.3.2 se establece un licenciamiento para 25.000 activos. Agradecemos a la Entidad aclarar si el requerimiento de "sin costo adicional" implica que: El licenciamiento para 25.000 activos debe incluir también la instalación y uso de agentes en todos esos activos, sin incremento en el valor ofertado, independientemente del modelo de licenciamiento del fabricante, o La funcionalidad de agentes se considera opcional o limitada a un subconjunto de activos, siempre que el licenciamiento total no supere los 25.000 activos definidos en el alcance. Esta aclaración es necesaria debido a que, en modelos comerciales ampliamente utilizados en el mercado (por ejemplo, soluciones con escaneo basado en agente), el licenciamiento por agente puede representar un costo incremental significativo.	No aplica.	La DIAN se permite aclarar que sea con agente o no, el valor debe estar considerado en la oferta y no debe generar costos adicionales para la entidad. En todo caso la tecnología ofertada debe soportar su funcionalidad y cumplimiento con información publica del fabricante.
131	Proyecto SOC DIAN	Formal	Especificaciones Técnicas herramienta de protección de Bases de Datos	Se solicita respecto a este ITEM 4 para la protección de Bases de Datos suministrar: - Inventario de BD / Cantidades - Numero de instancias - Fabricante(s) - Versiones de cada fabricante - Ubicación (on-premise / Cloud)	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el inventario requerido de bases de datos se encuentra detallado en el archivo Solicitud de Oferta - SDO del presente proceso.
132	8.3	Formal	Especificaciones Técnicas Solución de análisis de código estático y dinámico para aplicaciones 8.3 La entidad requiere de una herramienta de software como servicio (SaaS), para el análisis de código estático tipo SATS y análisis de código dinámico tipo DAST para un total de cincuenta (50) aplicaciones.	Con el objetivo de dimensionar correctamente la herramienta de análisis de código solicitada, agradeceríamos confirmar la siguiente información: - Tamaño aproximado de las aplicaciones (líneas de código – LOC o rangos estimados). - Lenguajes de programación utilizados. - Tipo de aplicaciones (web, APIs, microservicios, móviles). - Si las aplicaciones cuentan con autenticación y roles (relevante para DAST).	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en los documentos publicados se encuentra la información amplia y suficiente para que el futuro contratista pueda realizar su dimensionamiento.
133	7.3 7.18	Formal	Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas 7.3 Se debe licenciar como mínimo para 25000 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web). 7.18 El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 17727 dispositivos por (3) años.	En el marco del análisis técnico para la correcta dimensión y cotización de la solución de Network Detection and Response (NDR), hemos identificado una posible ambigüedad en las cantidades descritas en el alcance, específicamente entre los numerales 7.3 y 7.18. En el numeral 7.3 se indica que la solución debe licenciarse como mínimo para 25.000 activos, incluyendo 15.000 PCs, 2.467 activos de infraestructura y 260 aplicaciones web. Sin embargo, en el numeral 7.18 se solicita un licenciamiento total para 17.727 dispositivos por un período de tres (3) años. Con el fin de realizar un dimensionamiento técnico adecuado y una estimación económica precisa, agradecemos por favor nos puedan confirmar lo siguiente: - ¿Cuál es la cantidad final de activos/dispositivos que debe considerarse para el licenciamiento del NDR? - ¿El valor de 25.000 activos corresponde a un mínimo contractual, a un escalón de licenciamiento del fabricante, o incluye otros activos no detallados? - ¿Las aplicaciones web deben ser consideradas como activos independientes para efectos de licenciamiento del NDR? - ¿Se espera crecimiento del número de activos durante la vigencia del contrato (3 años)? Esta información es clave para garantizar que la solución propuesta cumpla con el alcance técnico esperado y evite desviaciones en costos o capacidades.	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la cantidad de dispositivos es 25000 (allí están referenciados todos los activos tecnológicos de la Entidad incluyendo aplicaciones web) para lo cual se procederá a la modificación de la cantidad expresada en este ítem quedando de la siguiente manera, cambio que se verá reflejado en la adenda a publicar en los próximos días: 7.18 El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 25000 dispositivos por (3) años.

134	9	Formal	9. Especificaciones Técnicas Protección de Marca (Deep&Dark Web)	Para la solución de Protección de Marca (Deep & Dark Web), hemos identificado que algunos requerimientos podrían interpretarse de dos formas complementarias, por lo cual agradecemos su validación para asegurar una correcta alineación de la propuesta. En particular, el numeral 9.3 menciona el licenciamiento mínimo para 260 activos públicos, y los numerales 9.4 y 9.5 hacen referencia al rastreo y monitoreo continuo de la presencia en línea, así como a la identificación de usos no autorizados e infracciones relacionadas con la marca. Dado lo anterior, agradeceríamos nos puedan confirmar: ¿Los "activos públicos" hacen referencia exclusivamente a activos asociados a la reputación de marca (nombre, logotipo, dominios oficiales, redes sociales), o ¿Se espera también incluir capacidades de gestión de superficie de ataque externa (External Attack Surface Management – EASM), tales como: Descubrimiento automatizado de dominios, subdominios, IPs y servicios expuestos a Internet Identificación de activos olvidados o no inventariados Detección de configuraciones erróneas o exposiciones técnicas desde la perspectiva de un atacante Priorización de riesgos mediante integración con inteligencia de amenazas (CTI) Esta aclaración nos permitirá definir correctamente si la solución debe cubrir únicamente monitoreo de marca y reputación, o si debe incorporar adicionalmente capacidades de gestión de superficie de ataque externa, lo cual tendría impacto directo en el dimensionamiento técnico y el modelo de licenciamiento.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el ítem referido hace mención a capacidades de protección, monitoreo y protección de marca en las cantidades requeridas por la Entidad.
135	Sección III	Formal	El oferente deberá acreditar su pertenencia a la más alta membresía por parte de las fabricantes de los productos, servicios, plataformas o licenciamientos ofrecidos y requeridos por la DIAN, para tal efecto, el oferente deberá informar los mecanismos suficientes para corroborar dicha información.	La consideración b establece que el oferente deberá acreditar su pertenencia a la más alta membresía por parte de los fabricantes de los productos, servicios, plataformas o licenciamientos ofrecidos y requeridos por la DIAN, así como informar los mecanismos suficientes para corroborar dicha información. Al respecto, se solicita respetuosamente a la Entidad evaluar el alcance de este requisito, considerando que: En los esquemas habituales de relacionamiento de los fabricantes de tecnologías, los niveles de membresía o categorización de aliados suelen responder, entre otros factores, a variables de índole comercial tales como volúmenes de facturación, metas de ventas, inversiones conjuntas en mercadeo o cobertura comercial, además de ciertos requisitos técnicos y de certificación. En consecuencia, el nivel más alto de membresía no siempre resulta determinante para garantizar la correcta implementación, operación o soporte de las soluciones tecnológicas ofrecidas. Para efectos de la prestación de los servicios requeridos por la DIAN, lo esencial es que el oferente cuente con una relación formal, vigente y reconocida por el fabricante, que lo habilite para: - Comercializar y licenciar las tecnologías propuestas. - Implementar y operar las capacidades requeridas. - Acceder a actualizaciones, soporte técnico y escalamiento cuando sea necesario. Dichas condiciones pueden acreditarse mediante distintos niveles de membresía, siempre que exista autorización expresa por parte del fabricante.	El oferente deberá acreditar que cuenta con una relación formal, vigente y reconocida con los fabricantes de los productos, servicios, plataformas o licenciamientos ofrecidos y requeridos por la DIAN, que lo habilite para su comercialización, licenciamiento, implementación, operación y soporte, según aplique. Para tal efecto, el oferente deberá presentar certificaciones, constancias o documentos equivalentes emitidos por los respectivos fabricantes, en los que se evidencie su condición de partner, proveedor autorizado, reseller u otra figura equivalente, independientemente del nivel de membresía o categorización asignado por cada fabricante. Así mismo, el oferente deberá informar los mecanismos suficientes que permitan a la Entidad corroborar la veracidad y vigencia de dicha relación durante el proceso de evaluación y durante la ejecución del contrato.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el literal b es un ítem puntuable, para el caso en específico, la Entidad da una puntuación en caso de que el futuro interesado acredite pertenecer al nivel de parner más alto en las capacidades o servicios solicitados puntuando desde el que tenga dos (2) y hasta cuatro (4) o más membresías, así las cosas el futuro interesado podrá hacerse a esta puntuación según lo comentado anteriormente, por lo tanto, no se acepta su sugerencia en el entendido que la puntuación requerida ofrece equilibrio para el proyecto.
136	Sección III	Formal	c. El futuro interesado deberá acreditar que el fabricante de las capacidades ofrecidas entregue el servicio de TAM (Thecnical Account Manager) para el soporte a dichas capacidades por el tiempo estipulado para el proyecto y que no ocasione ningún costo adicional para la Entidad.	La consideración c establece que el futuro interesado deberá acreditar que el fabricante de las capacidades ofrecidas provea el servicio de TAM (Technical Account Manager) para el soporte de dichas capacidades durante el tiempo estipulado para el proyecto, sin que ello ocasione ningún costo adicional para la Entidad. Al respecto, se solicita respetuosamente a la Entidad considerar los siguientes aspectos: En los modelos habituales de soporte de los fabricantes de tecnologías, la asignación de un servicio de TAM depende de diferentes variables, tales como el tipo de licenciamiento contratado, el alcance de la solución, el nivel de soporte seleccionado o las condiciones comerciales globales del acuerdo, sin que exista un esquema único o estándar aplicable a todos los fabricantes. El acompañamiento del fabricante, cuando se ofrece a través de un TAM, constituye un mecanismo de soporte especializado de segundo o tercer nivel, que complementa, pero no sustituye, la responsabilidad principal del proveedor del servicio SOC en la operación, gestión y soporte continuo de las capacidades implementadas. Exigir la provisión de un TAM específico, bajo la condición de que no genere costo adicional para la Entidad, podría limitar la participación de oferentes que cuentan con modelos equivalentes de soporte del fabricante, igualmente efectivos para el cumplimiento del objeto contractual, pero estructurados de manera distinta a la figura formal de un TAM dedicado.	**Soporte técnico especializado para las capacidades ofrecidas.** El oferente deberá acreditar que, durante el tiempo estipulado para la ejecución del proyecto, la Entidad contará con acceso permanente a soporte técnico especializado para las capacidades, productos, servicios, plataformas o licenciamientos ofrecidos. Dicho soporte podrá ser provisto directamente por el fabricante de las soluciones ofrecidas o por el proveedor del servicio, a través de esquemas de acompañamiento técnico de segundo y/o tercer nivel, incluyendo, cuando aplique, figuras como Technical Account Manager (TAM) u otros mecanismos de soporte equivalente, siempre que se garantice la atención oportuna y especializada requerida para la adecuada operación de las capacidades implementadas. El oferente deberá acreditar que el soporte técnico especializado descrito no generará costos adicionales para la Entidad durante la vigencia del proyecto y deberá informar los mecanismos mediante los cuales la DIAN podrá solicitar, acceder y escalar dicho soporte cuando sea necesario.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el literal c es un ítem puntuable, para el caso en específico, la Entidad da una puntuación en caso de que el futuro interesado oferte servicios de TAM en las capacidades o servicios solicitados, puntuando desde el que tenga dos (2) y hasta cinco (5) o más, así las cosas el futuro interesado podrá hacerse a esta puntuación según lo comentado anteriormente. No obstante se aclara que los servicios TAM constituyen un mecanismo de soporte especializado de segundo o tercer nivel, que complementa, pero no sustituye, la responsabilidad principal del proveedor del servicio SOC en la operación, gestión y soporte continuo de las capacidades implementadas.
137	Sección VI	Formal	Sección VI. Requisitos de los Bienes y Servicios Conexos: A la fecha de finalización del servicio se debe entregar la data de los logs de los últimos seis (6) meses de prestación del servicio en formato estándar para ser leído por cualquier plataforma	En la descripción de la Fase 4 – Entrega del servicio para el control de la DIAN, se establece que "a la fecha de finalización del servicio se debe entregar la data de los logs de los últimos seis (6) meses de prestación del servicio en formato estándar para ser leído por cualquier plataforma". Al respecto, se solicita a la Entidad aclarar el alcance específico de los logs objeto de entrega, indicando de manera expresa si dicha obligación corresponde exclusivamente a: Los logs administrados, procesados o almacenados en la plataforma o solución SIEM provista por el proponente o proveedor de los servicios SOC como parte del alcance contractual, o si, por el contrario, Incluye logs provenientes de otras plataformas, sistemas o infraestructuras de la DIAN que no formen parte de las herramientas implementadas o gestionadas por el proveedor del servicio SOC. La presente aclaración resulta necesaria para delimitar de forma precisa el alcance técnico, operativo y contractual de la fase de cierre del servicio y para la adecuada estructuración de las propuestas por parte de los interesados.	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el ítem se refiere a logs de las capacidades, servicios y/o plataformas implementados, administrados y operados por el futuro contratista.

138	Sección VII	Formal	11.1 El Proveedor permitirá, y realizará todos los trámites para que sus Subcontratistas permitan, que el Banco y/o las personas designadas por el Banco inspeccionen todas las cuentas y registros contables del Proveedor y sus Subcontratistas relacionados con el proceso de licitación y la ejecución del contrato y realice auditorías por medio de auditores designados por el Banco, si así lo requiere el Banco. El Proveedor y los Subcontratistas deberán prestar atención a lo estipulado en la Cláusula 3 de las CGC "Prácticas Prohibidas", según la cual las actuaciones dirigidas a obstaculizar significativamente el ejercicio por parte del Banco de los derechos de inspección y auditoría consignados en ésta Subcláusula 11.1 constituye una Práctica Prohibida que podrá resultar en la terminación del contrato (al igual que en la declaración de inelegibilidad de acuerdo a los procedimientos vigentes del Banco).	Equipo FONDO DIAN, dada la naturaleza del servicio del presente pliego es de carácter técnico en ciberseguridad, y por tanto entendemos que el requerimiento es aplicable para contratos con alcances contables o financieros, que están fuera del alcance de este proceso. Por este motivo sugerimos redactar el texto de la siguiente forma: 11.1 El Proveedor permitirá, y realizará todos los trámites para que sus Subcontratistas igualmente permitan, que el Banco y/o las personas designadas por este inspeccionen los servicios prestados a la DIAN relacionados con el proceso de licitación y la ejecución del contrato, así como la realización de auditorías por parte de auditores designados por el Banco, cuando este así lo requiera. Lo anterior aplicará exclusivamente para el servicio SOC, para el cual el Proveedor deberá suministrar la información requerida por la DIAN. El Proveedor y los Subcontratistas deberán prestar atención a lo estipulado en la Cláusula 3 de las CGC "Prácticas Prohibidas", según la cual las actuaciones dirigidas a obstaculizar significativamente el ejercicio por parte del Banco de los derechos de inspección y auditoría consignados en ésta Subcláusula 11.1 constituye una Práctica Prohibida que podrá resultar en la terminación del contrato (al igual que en la declaración de inelegibilidad de acuerdo a los procedimientos vigentes del Banco).	No es posible modificar este apartado ya que es un estandar del Banco y aplicable a este tipo de procesos. Vale señalar que estas revisiones están relacionada con las prácticas prohibidas, razón por la cual, no es un mecanismo utilizado con frecuencia por el BID.
139	Sección VI	Formal	Inteligencia de Amenazas (NDR) a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031.	Solicitamos al FONDO DIAN informar el nombre de la tecnología NDR tienen actualmente implementado, cantidad de licencias, fecha de vencimiento (DD/MM/AAAA) y características de la tecnología NDR para tenerlo en cuenta en la implementación.	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, actualmente la Entidad cuenta con la plataforma TREND VISION ONE con licenciamiento hasta diciembre de 2027, después de esta fecha el futuro proveedor deberá implementar el nuevo servicio de NDR de Inteligencia de Amenazas con el licenciamiento de acuerdo a las cantidades estipuladas por la Entidad.
140	Sección VI	Formal	Consideraciones Herramientas SIEM, Protección de bases de datos e Inteligencia de amenazas. Actualmente, la DIAN cuenta con las siguientes soluciones: • Una solución SIEM IBM QRadar contratada hasta el 31 de agosto de 2027. • Un firewall de bases de datos IBM GUARDIUM contratado hasta diciembre 31 de 2027. • Solución de Inteligencia de Amenazas contratada hasta diciembre 31 de 2027.	Solicitamos informar las características y capacidades de la solución SIEM IBM QRadar actual de la DIAN.	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, las características de la plataforma SIEM de la Entidad: Qradar Licenciado: 110K flujos por minuto 25K eventos por segundo Versión desplegada 7.5.0 UpdatePackage 14 (Build 20251017194912) Retención: 30 días en caliente y 1.3 años en frio
141	Sección VI	Formal	Consideraciones Herramientas SIEM, Protección de bases de datos e Inteligencia de amenazas. Actualmente, la DIAN cuenta con las siguientes soluciones: • Una solución SIEM IBM QRadar contratada hasta el 31 de agosto de 2027. • Un firewall de bases de datos IBM GUARDIUM contratado hasta diciembre 31 de 2027. • Solución de Inteligencia de Amenazas contratada hasta diciembre 31 de 2027.	Solicitamos informar las características, capacidades de la solución firewall de bases de datos IBM GUARDIUM actual de la DIAN. Cuántas bases de datos requiere la DIAN configurar en la solución firewall de base de datos a partir del 01 de septiembre del 2028.	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, las características de la plataforma Firewall de Bases de Datos de la Entidad: Guardium Licenciado 240 Licencias -100 resource units Actualmente desplegados 1 CM y 16 colectores. 16 clientes desplegados, 12 clientes pendientes por desplegar. Versión desplegada 12.2.2.0_r123402_main_1-el96-20260323_1749, Latest patch number:5007 Retención: 1 semana en el colector y 4 años en el GDBI.
142	Sección VI	Formal	Consideraciones Herramientas SIEM, Protección de bases de datos e Inteligencia de amenazas. Actualmente, la DIAN cuenta con las siguientes soluciones: • Una solución SIEM IBM QRadar contratada hasta el 31 de agosto de 2027. • Un firewall de bases de datos IBM GUARDIUM contratado hasta diciembre 31 de 2027. • Solución de Inteligencia de Amenazas contratada hasta diciembre 31 de 2027.	Solicitamos informar la marca, las características y capacidades de la solución Solución de Inteligencia de Amenazas actual de la DIAN.	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, actualmente la Entidad cuenta con la plataforma TREND VISION ONE con licenciamiento hasta diciembre de 2027, después de esta fecha el futuro proveedor deberá implementar el nuevo servicio de NDR de Inteligencia de Amenazas con el licenciamiento de acuerdo a las cantidades estipuladas por la Entidad.
143	Sección VI	Formal	El servicio de monitoreo deberá preservar la cadena de custodia de evidencias digitales, conforme a estándares como ISO/IEC 27037, y permitir su uso en auditorías internas, investigaciones disciplinarias o procesos judiciales.	El criterio establece que "el servicio de monitoreo deberá preservar la cadena de custodia de evidencias digitales, conforme a estándares como ISO/IEC 27037, y permitir su uso en auditorías internas, investigaciones disciplinarias o procesos judiciales." Al respecto, se solicita respetuosamente a la Entidad precisar el alcance de la expresión "permitir su uso en auditorías internas", teniendo en cuenta que, conforme a las políticas internas de reputación y riesgo de Deloitte, no permiten las auditorías, revisiones, inspecciones o evaluaciones técnicas directas por parte de clientes o terceros sobre controles, sistemas, metodologías, políticas o procesos propios de Deloitte. No obstante lo anterior, el se pueden coordinar visitas de verificación de controles implementados en materia de seguridad de la información, limitadas al objetivo de los servicios contratados, bajo las siguientes condiciones generales: 1. Las visitas se orientan exclusivamente a la verificación de la existencia y aplicación de controles, sin actividades de auditoría técnica. 2. No se contempla la entrega, copia, extracción ni acceso a información del proveedor, ni a sus sistemas internos. Las visitas requieren solicitud previa y coordinación, dentro de los plazos y condiciones definidos por la política interna del proveedor. En ese sentido, se solicita aclarar si el cumplimiento de este requisito se entiende satisfecho mediante: La preservación adecuada de la cadena de custodia de las evidencias digitales generadas en el marco del servicio, conforme a estándares reconocidos como ISO/IEC 27037; y La disponibilidad	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem menciona que en caso de requerirse por parte de la DIAN, el proveedor de los servicios SOC deberá permitir el uso de evidencias digitales en auditorías internas, investigaciones disciplinarias o procesos judiciales, teniendo presente que únicamente se refiere a información que se desprende de los servicios del futuro SOC, no a procesos internos del proveedor y ajenos a dicha operación.
144	Proyecto SOC DIAN	Formal	El appliance, o solución, plataforma o servicio de decepción debe estar en capacidad de crear al menos 400 señuelos, en hasta 20 máquinas virtuales y desplegarse en mínimo 120 VLANs. o características similares o superiores en las tecnologías ofrecidas.	¿Para dar cumplimiento al despliegue en las 120 VLANs, la entidad acepta plataformas con arquitectura de proyección centralizada (basada en software/túneles), la cual permite desplegar los señuelos requeridos sin la necesidad de instalar appliance o hardware dedicado en cada segmento de red?"	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la Entidad permite soluciones equivalente de iguales o mejores características siempre y cuando se cumpla con los requerimientos de la Entidad que están detallados en el anexo técnico.
145	Proyecto SOC DIAN	Formal	El licenciamiento de la solución debe ser como mínimo ciento veinte (120) vlans.	¿La entidad acepta esquemas de licenciamiento basados en capacidad (por número total de activos, usuarios o IPs) siempre y cuando el dimensionamiento propuesto garantice la cobertura técnica y la proyección de señuelos sobre las 120 VLANs solicitadas?"	No aplica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la Entidad permite soluciones equivalente de iguales o mejores características siempre y cuando se cumpla con los requerimientos de la Entidad que están detallados en el anexo técnico.

146	Equipo Mínimo	Sustancial	Tres (03) Analistas SOC Nivel I Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 2 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: - Cédula de Ciudadanía - Tarjeta Profesional - Certificación vigente como analista o profesional o especialista o arquitecto en seguridad de operaciones o su equivalente en las soluciones ofertadas (SIEM, SOAR, caza de amenazas o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. - Certificación en Plataformas de Gestión de la Superficie de Ataque. - Certificaciones de experiencia mínima de dos (2) años en implementación y/o soporte y/o administración de soluciones de seguridad. NOTA: Estos tres perfiles (analista I) deben cumplir los ANS de 7x24x365	Se sugiere esta modificación por transparencia e inclusión, ya que un perfil de analista, son profesionales recién graduados que desean vengan trabajando o iniciando en seguridad, no se recomienda solicitar certificados puntuales, ya que en este nivel se busca que las personas puedan iniciar como carrera la parte del SOC, aunque si pudieran tener experiencia	**Tres (03) Analistas SOC Nivel I** Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de **1 año** a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: -Cédula de Ciudadanía -Tarjeta Profesional -**DESEABLE**: Certificación vigente como analista o profesional o especialista o arquitecto en seguridad de operaciones o su equivalente en las soluciones ofertadas (SIEM, SOAR, caza de amenazas o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. - **DESEABLE**: Certificación en Plataformas de Gestión de la Superficie de Ataque. - Certificaciones de experiencia mínima de **un (1)** años en implementación y/o soporte y/o administración de soluciones de seguridad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los perfiles solicitados para el equipo de trabajo obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su modificación.
147	Equipo Mínimo	Sustancial	Un (01) Analista SOC Nivel II Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 3 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: - Cédula de Ciudadanía - Tarjeta Profesional - Certificación vigente como analista o profesional o especialista o arquitecto en seguridad de redes o su equivalente en las soluciones ofertadas (SIEM o SOAR o Caza de Amenazas o NDR o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. - Certificación en Plataformas Gestión de la Superficie de Ataque. - Certificaciones de experiencia mínima de tres (3) años en implementación y/o soporte y/o administración de soluciones de seguridad.	Las cerficaciones se requieren a medida que el perfil tiene mayor nivel de responsabilidad y complejidad que el rol de analista por ello deseable.	**Un (01) Analista SOC Nivel II** Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 3 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: -Cédula de Ciudadanía -Tarjeta Profesional -**DESEABLE:** Certificación vigente como analista o profesional o especialista o arquitecto en seguridad de redes o su equivalente en las soluciones ofertadas (SIEM o SOAR o Caza de Amenazas o NDR o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. - Certificación en Plataformas Gestión de la Superficie de Ataque. - Certificaciones de experiencia mínima de **dos (2)** años en implementación y/o soporte y/o administración de soluciones de seguridad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los perfiles solicitados para el equipo de trabajo obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su modificación.
148	Equipo Mínimo	Sustancial	Un (01) Analista SOC Nivel III Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 5 años a partir de la emisión de la Tarjeta Profesional: - Cédula de Ciudadanía - Tarjeta Profesional – Postgrado en seguridad informática. - Certificación vigente como analista o profesional o arquitecto en seguridad de redes o su equivalente en las soluciones ofertadas (SIEM, SOAR, Caza de Amenazas, NDR o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. - Certificación en gestión o administración de plataformas de seguridad informática. Certificaciones de experiencia mínima de 5 años en implementar y/o soportar y/o administrar soluciones de seguridad.	Las certificaciones se requieren a medida que el perfil tiene mayor nivel de responsabilidad y complejidad	**Un (01) Analista SOC Nivel III** Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 5 años a partir de la emisión de la Tarjeta Profesional: -Cédula de Ciudadanía -Tarjeta Profesional - **DESEABLE:** Postgrado en seguridad informática. -Certificación vigente como analista o profesional o arquitecto en seguridad de redes o su equivalente en las soluciones ofertadas (SIEM, SOAR, Caza de Amenazas, NDR o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. -Certificación en gestión o administración de plataformas de seguridad informática. Certificaciones de experiencia mínima de 5 años en implementar y/o soportar y/o administrar soluciones de seguridad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los perfiles solicitados para el equipo de trabajo obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su modificación.
149	Equipo Mínimo	Sustancial	Especialista de Respuesta a Incidentes (IR) Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Seguridad Informática Certificaciones vigentes: • ITIL V3 o superior. Mínimo cinco (5) años de experiencia profesional en proyectos de tecnologías de la información de los cuales tres (3) años con participación en proyectos de seguridad de la información, plan de recuperación de desastres o continuidad de negocio, demostrados en al menos dos(2) proyectos de esta naturaleza. NOTA: Este perfil debe estar en sitio de la Entidad Sede Ministerio de Hacienda, trabajando en una disponibilidad de 8 x 5, con los conocimientos necesarios y suficientes en las plataformas, servicios, y capacidades entregadas e implementadas. Debe estar en la sede principal de la DIAN Bogotá, para realizar el acompañamiento y asesoramiento frente al tema de las remediaciones a las posibles vulnerabilidades encontradas en el monitoreo y las demás halladas en las actividades que hacen parte de este anexo técnico.	Las certificaciones se requieren a medida que el perfil tiene mayor nivel de responsabilidad y complejidad	**Especialista de Respuesta a Incidentes (IR)** Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Seguridad Informática Certificaciones vigentes: **•ITI**L V3 o superior. *** Al menos una de las siguientes certificaciones: GCIH (GIAC Certified Incident Handler), ECIH (EC-Council Certified Incident Handler) y CySA+ de CompTIA.** Mínimo cinco (5) años de experiencia profesional en proyectos de tecnologías de la información de los cuales tres (3) años con participación en proyectos de seguridad de la información, plan de recuperación de desastres o continuidad de negocio **NOTA: Este perfil debe estar en sitio de la Entidad Sede Ministerio de Hacienda, trabajando en una disponibilidad de 8 x 5, con los conocimientos necesarios y suficientes en las plataformas, servicios, y capacidades entregadas e implementadas. Debe estar en la sede principal de la DIAN Bogotá, para realizar el acompañamiento y asesoramiento frente al tema de las remediaciones a las posibles**	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los perfiles solicitados para el equipo de trabajo obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su modificación.

150	Equipo Mínimo	Sustancial	Threat Hunter / Analista de Ciber inteligencia Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Gerencia de proyectos o Seguridad Informática Certificaciones vigentes: • Licensed Penetration Tester (LPT) Mínimo cinco (5) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales tres (3) años con participación en proyectos de seguridad de la información, plan de recuperación de desastres o continuidad de negocio, demostrados en al menos dos(2) proyectos de esta naturaleza	Tiene más valor una especialización en seguridad que en Gerencia de proyectos dado los temas de enfoque de la persona, no es normal que alguien se enfoque en lo técnico y también en gerencia de proyectos.	**Threat Hunter / Analista de Ciber inteligencia** Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado Seguridad Informática Certificaciones vigentes: **• Dos de las siguientes certificaciones: GCIH (GIAC Certified Incident Handler), ECIH (EC-Council Certified Incident Handler), CySA+ de CompTIA, Licensed Penetration Tester (LPT)** Mínimo cinco (5) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales tres (3) años con participación en proyectos de seguridad de la información, plan de recuperación de desastres o continuidad de negocio	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los perfiles solicitados para el equipo de trabajo obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su modificación.
151	Equipo Mínimo	Sustancial	Líder /Coordinador SOC Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Gerencia de proyectos Certificaciones vigentes: • PMP Mínimo seis (6) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales tres (3) años en Gerencia de proyectos de seguridad de la información, plan de recuperación de desastres o continuidad de negocio, demostrados en al menos dos(2) proyectos de esta naturaleza	El rol de Líder del SOC debe ser asumido por un profesional especialista en ciberseguridad, con experiencia directa en la operación de servicios de monitoreo y respuesta a incidentes. Este perfil debe contar con la capacidad de analizar amenazas, priorizar eventos de seguridad y tomar decisiones técnicas en tiempo real, garantizando la efectividad del servicio. Las habilidades de liderazgo son clave, pero deben estar fundamentadas en un conocimiento técnico sólido que permita dirigir al equipo y responder de manera adecuada ante escenarios de riesgo.	**Líder /Coordinador SOC** Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Seguridad informática o afines Deseable Maestría en seguridad de la información o afines Certificaciones vigentes: •ISO 27001 Mínimo seis (6) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales tres (3) años en Gerencia de proyectos de seguridad de la información, plan de recuperación de desastres o continuidad de negocio	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los perfiles solicitados para el equipo de trabajo obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su modificación.
152	Equipo Mínimo	Sustancial	Gerente de Proyecto Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Gerencia de proyectos Certificaciones vigentes: • PMP • Scrum Master Mínimo diez (10) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales cinco (5) años en Gerencia de proyectos de seguridad de la información , plan de recuperación de desastres o continuidad de negocio, demostrados con al menos dos (2) proyectos de esta naturaleza.	Para el rol de Gerente de Proyectos del SOC, se requiere un perfil con sólida experiencia en ciberseguridad que le permita comprender el contexto técnico y operativo del servicio, gestionar adecuadamente los riesgos asociados y tomar decisiones informadas frente a incidentes y requerimientos del negocio. Si bien las habilidades de PMP y gerencia de proyectos son fundamentales, estas deben estar respaldadas por un conocimiento profundo en seguridad de la información, asegurando así una adecuada coordinación entre la estrategia, la operación y la gestión del riesgo.	**Gerente de Proyecto** Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Seguridad informática o afines Maestría en seguridad de la información o afines Certificaciones vigentes: •ISO 27001 Mínimo diez (10) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales cinco (5) años en Gerencia de proyectos de seguridad de la información , plan de recuperación de desastres o continuidad de negocio	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los perfiles solicitados para el equipo de trabajo obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su modificación.
153	Sección VII	Sustancial	La solución debe estar en capacidad de instalarse en	Se solicita instalación de producto.	Permitir el uso de plataforma SaaS. S/N	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la Entidad permite soluciones equivalente de iguales o mejores características, ya sea SaaS o cualquier otra presentación, siempre y cuando se cumpla con los requerimientos de la Entidad que están detallados en el anexo técnico.
154	Sección VII	Sustancial	(Revisar archivo anexo inventarios)	Se menciona un archivo anexo.	Enviar / aclarar cuál es el 'archivo anexo inventarios'.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el grueso del inventario de la infraestructura tecnológica de la Entidad se encuentra detallado en la sección VI del documento Solicitud de Oferta o SDO, y su complemento está especificado en una de las hojas del archivo anexo de características técnicas mínimas.
155	Sección VII	Sustancial	Se debe realizar la integración y monitoreo	Se menciona realización de integración.	Indicar si esta integración hace referencia a desarrollo de software?	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, las integraciones a la que se refiere el ítem son las que tienen que ver con las fuentes de infraestructura tecnológica que debe monitorear el servicio de SIEM, para lo cual el futuro proveedor de SOC deberá contar con la experticia para poder realizar dichas actividades, en ningún momento se habla de desarrollo de software.
156	Sección VII	Sustancial	Informes de Cumplimiento Out-of-the-Box	Se solicita condición Out-of-the-Box, incluyendo reporte GPG13.	Indicar alternativa para requerimiento Out-of-the-Box. ¿Se trata de GPG13 ó GPR13?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem indica GPG13.
157	Sección VII	Sustancial	Mostrar un dashboard de monitoreo de estado de integraciones	Se piden integraciones para el motor SOAR.	Para este y los demás componentes del proyecto (Inventario: SIEM actual, NGFW, AV/EDR, sandbox, ticketing), indicar la integraciones mínimas exigidas?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las integraciones mínimas exigidas están descritas en el respectivo ítem 3.5 (En la solución SOAR entregada como mínimo debe integrar el SIEM, firewalls, plataforma antivirus y las demás plataformas de seguridad de la Entidad y que sean susceptibles de integración, para lo cual el oferente se apoyará en los inventarios incluidos en el archivo excel Anexo Técnico Proyecto SOC DIAN).
158	Sección VII	Sustancial	Mostrar un dashboard de monitoreo de estado de integraciones	Se piden integraciones para el motor SOAR.	Indicar¿ qué método de integración se acepta (API, syslog, webhook, Kafka, email)?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en el item 3.70 se detalla lo solicitado que a la letra dice: "La solución SOAR debe contar con una amplia biblioteca de conectores de integración preexistentes, que permitan la interoperabilidad con diversas herramientas de seguridad, infraestructura, nube, gestión de incidentes, inteligencia de amenazas, y otros sistemas relevantes. Estos conectores deben facilitar la automatización de tareas, el intercambio de información y la ejecución de acciones dentro de los playbooks, cumpliendo como mínimo con lo siguiente: -La solución debe incluir al menos 300 conectores de integración preconfigurados o funcionalidades equivalentes, que cubran herramientas de seguridad, TI, nube, mensajería, bases de datos, APIs REST, entre otros. - Los conectores deben estar documentados y actualizados regularmente por el fabricante o comunidad. - La solución debe permitir el desarrollo de nuevos conectores a demanda, utilizando herramientas de desarrollo, SDKs o APIs proporcionadas por el fabricante, sin que esto implique nuevos costos para la Entidad. - La solución debe contar con los conectores necesarios para integrar los sistemas actuales de la DIAN, así como tener la flexibilidad para integrar sistemas futuros, mediante desarrollo propio o expansión de la biblioteca existente. - Debe existir soporte para conectores personalizados, autenticación segura, y gestión de versiones.
159	Sección VII	Sustancial	Las políticas granulares para	Se solicitan 21 condiciones muy específicas.	Para todo el pliego, permitir cumplimiento mínimo del 90% cuando haya más de 10 ítems solicitados en una pregunta.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su solicitud, sin embargo el cumplimiento se puede presentar mediante equivalencias de iguales o mejores características.
160	Sección III	Sustancial	Los oferentes deberán allegar como parte de la	Se menciona antigüedad de la certificación FIRST	Reducir la antigüedad; alternativa: solicitar mínimo 6 meses.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la certificación FIRST para que sea puntuable y se le puedan otorgar puntos debe tener una antiguedad de 12 meses, por lo tanto, no se acepta su sugerencia.
161	Sección III	Sustancial	Presentar máximo seis (6) contratos.	Se limita hasta en 6 contratos la presentación de la experiencia.	Ampliar cumplimiento de experiencia: hasta diez (10) contratos.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento es claro frente al número de contratos (6), por lo tanto, no es posible acceder a su sugerencia.
162	Sección III	Sustancial	Al menos uno (1) incluya actividades de prestación de servicios de SOC.	Se piden al menos un contrato de 1 millón de dólares.	Reducir requerimiento; alternativa: proyecto mínimo de 200 mil dólares.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los valores solicitados para experiencia permiten validar la robustez y la experiencia del interesado frente al presupuesto del proyecto, por lo tanto, no es posible aceptar su sugerencia.
163	Sección VII	Sustancial	13. ANEXOS. ANEXO 1. Característica Técnicas mínimas	Hoja en blanco, sin Anexo 1.	Indicar cuál es el documento 'ANEXO CARACTERÍSTICAS TÉCNICAS MÍNIMAS'.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el documento se encuentra publicado con el nombre Anexo Técnico Proyecto SOC.
164	Sección V	Sustancial	NOTA 1: Para costear los diferentes	Se indica: "tener en cuenta los requerimientos del ANEXO CARACTERÍSTICAS TÉCNICAS MÍNIMAS".	Indicar cuál es el documento 'ANEXO CARACTERÍSTICAS TÉCNICAS MÍNIMAS'; no está en la documentación oficial del proyecto.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el documento se encuentra publicado con el nombre Anexo Técnico Proyecto SOC.
165	Sección V	Sustancial	NOTA 5: El SIEM debe ser cotizado a tres (3) años	Se indican las condiciones de uso y transición del SIEM.	Cumpliendo las condiciones técnicas, se permite el uso de IBM QRADAR en su nueva versión y/o fabricante, bajo una nueva implementación? S/N	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, si se permite, siempre y cuando se cumplan las características técnicas solicitadas, así como también sea una nueva implementación de una nueva plataforma de la marca referenciada o cualquier otro fabricante.
166	Sección V	Sustancial	NOTA 7: La protección de bases de datos (Firewall de bases de datos	Se indican las condiciones de uso y transición de la DB de firewall.	Cumpliendo las condiciones técnicas, se permite el uso de IBM GUARDIUM en su nueva versión, bajo una nueva implementación? S/N	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, si se permite, siempre y cuando se cumplan las características técnicas solicitadas, así como también sea una nueva implementación de una nueva plataforma de la marca referenciada o cualquier otro fabricante.

168	18.2	Sustancial	"Certificación de fabricante por solución, plataforma, servicios y dispositivos solicitados indicando que está en alguno de los tres niveles de membresía más altos ante el fabricante de las soluciones y plataformas ofertadas"	Respetuosamente solicitamos analizar y modificar este requerimiento habilitante y permitir que como requisito habilitante solo se requiera que el oferente aporte una carta de distribuidor autorizado sin que tenga que pertenecer a los tres niveles más altos de las membresías de cada fabricante. Lo anterior obedece a que por la naturaleza y magnitud del proceso se debe acreditar más de 8 capacidades en cerca de cuatro o cinco fabricantes. Pero los integradores de tecnología con capacidad de participar en este proceso centran su estrategia comercial en un par de fabricantes y es ahí donde centran todos sus esfuerzos por obtener los niveles de membresía más alto en ese o esos dos fabricantes. Es prácticamente imposible que un integrandor tenga de los niveles más altos de membresía en los cuatro o cinco fabricantes requeridos en el pliego de condiciones. Por lo anterior, solicitamos a la entidad reevaluar dicho requerimiento y de esta forma garantizar la pluralidad de oferentes permitiendo que en las marcas se presente algún nivel de certificación de distribución y si es el caso , que mínimo en una de ellas sea de los tres nieveles más altos.	"Certificación de cada fabricante por capacidades ofrecidas, indicando que el oferente es distribuidor autorizado de la marca de los productos y servicios de las plataformas ofertadas", indicando el número de la licitación, dirigida a la entidad y que indique su nivel de membresía si tiene".	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento permite pluralidad al referir que el interesado debe certificar que está rankeado en los tres niveles más altos de las capacidades ofrecidas, permitiendo esto asegurar idoneidad y experticia para las dimensiones del proyecto SOC en mención. Se aclara que, es perfectamente viable y común que los proveedores de un Centro de Operaciones de Seguridad (SOC) cumplan con el requerimiento de presentar una certificación de fabricante que acredite su nivel de membresía. Este tipo de exigencia es una práctica estándar en licitaciones y contratos de servicios gestionados de ciberseguridad para garantizar que el proveedor cuenta con el respaldo técnico y comercial directo del fabricante. Propósito de la certificación El objetivo principal de este requerimiento es asegurar que el proveedor no solo sea un revendedor, sino que posea una relación estratégica con el fabricante que garantice la calidad del servicio, sostenibilidad en el tiempo y la experticia necesaria de acuerdo a la robustez del proyecto. Al exigir estar en uno de los niveles de membresía más altos como por ejemplo Platinum, Gold o Elite), plata, bronce y otros la entidad contratante obtiene las siguientes garantías: ▪Soporte especializado: Acceso directo a ingenieros de soporte del fabricante en caso de incidentes críticos o configuraciones complejas. ▪Actualización y capacitación: Obligación del personal del proveedor de estar certificado técnica y comercialmente sobre las herramientas, garantizando que el SOC opere con personal experto. ▪Autenticidad y licenciamiento: Validación de que los servicios, plataformas y dispositivos son legítimos, cuentan con licenciamiento vigente y seguirán siendo soportados durante toda la duración del contrato.
169	Ficha técnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	Sustancial	En toda la capacidad 4 del pliego de condiciones (protección de Bases de datos)	Respetuosamente solicitamos a la entidad permitir la participación de Guardian de IBM para la protección de bases de datos, aboliendo o cambiando la forma de redacción de los siguientes requerimientos: 4.3 4.8 4.15 4.23 4.33 4.37 4.39 4.54.3 4.54.4 4.54.7 De no ser tenida en cuenta nuestra observación en estos ítems, Guardiam de IBM quedaría por fuera del proceso toda vez que no se evidencia el cumplimiento de estos ítems, y no tendría sentido que Guardium no pueda participar cuando justamente es la herramienta actual. Recomendamos a la entidad que esta información pueda ser ser confirmada directamente con el fabricante	eliminar y/o modificar la redacción del requerimiento, a fin que se permita la participación de IBM con su herramienta de protección de Bases de datos Guardiam (el que tiene actualmente la entidad). A continuación enlistamos la recomendación para cada ítem del sistema de protección de Bases de datos	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no se acepta su observación.
170	Ficha técnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	Sustancial		Teniendo en cuenta que la entidad requiere que en un período inicial del contrato se administre y opere con un SIEM y un firewall de protección de base de datos con el licenciamiento actual que provee la entidad, **es correcto concluir que la entidad no exigirá al nuevo contratista cumplir un imposible si el licenciamiento provisto por ésta no permite la nueva funcionalidad requerid?, e inclusive que aunque esta nueva funcionalidad esté pedida en esta ficha técnica pero no lo permite el licenciamiento actual provisto por la entidad, no será de obligatorio cumplimiento para el contratista?.** **Esta solicitud aclaratoria se hace, toda vez que desconocemos todas las funcionalidades adquiridas y licenciadas con las que cuenta la entidad en el caso de Guardium, y como ya les indicamos, algunos requerimientos no permiten la participación de esta herramienta de IBM, motivo por el cual no sabemos si la ficha técnica de este proceso lo cumple 100% las herramientas con que cuenta la DIAN en la actualidad.**		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los requerimientos solicitados obedecen a necesidades puntuales de la Entidad, en este caso se informa que las características requeridas (SIEM y FIREWALL DE BASES DE DATOS) aplican para el nuevo servicio o capacidad, no son de obligatorio cumplimiento para las plataformas actuales propiedad de la Entidad y que deben ser administradas por el futuro proveedor.
171	Ficha técnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	Sustancial	"La entidad requiere adquirir […] una Herramienta de protección de bases de datos (Firewall de bases de datos).”"	El ítem 4 describe una solución de Database Activity Monitoring (DAM) / Database Firewall de propósito específico, con características que corresponden a un mercado de nicho muy especializado (IBM Guardium, Imperva Data Security, Oracle Audit Vault). El pliego no especifica ningún fabricante para este componente, lo cual es correcto. Sin embargo, se solicita confirmar explícitamente que: (i) se acepta que este componente sea provisto por un fabricante diferente al del SIEM y el SOAR, siempre que la integración con dichas plataformas esté garantizada; y (ii) la gestión centralizada de alertas del DAM desde el SIEM y la respuesta automatizada desde el SOAR son suficientes para acreditar el cumplimiento de los ítems de integración. Esto garantiza que el oferente pueda proponer el fabricante de DAM más idóneo sin estar forzado a una marca única que concentre todos los componentes.	Respetuosamente recomendamos a la entidad "La herramienta de protección de bases de datos podrá ser de un fabricante diferente al SIEM y SOAR, siempre que se garantice integración vía API o Syslog para el reenvío de alertas al SIEM y la ejecución de respuestas automatizadas desde el SOAR. El oferente deberá demostrar la integración funcional entre todos los componentes durante las pruebas de aceptación."	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en ninguno de los ítems que hacen parte del anexo técnico del presente proceso se solicita un fabricante en específico, y mucho menos se requiere que dichas capacidades o servicios sea de un solo fabricante, los posibles interesados podrán cumplir los requerimientos con diferentes fabricantes, siempre y cuando cumplan con las características requeridas para cada servicio.
172	4.3	Sustancial	"La solución deberá contar con tecnología de autoaprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo esquemas, objetos, tablas, sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario; todo esto para el establecimiento de un comportamiento base de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta."	En aras de la pluralidad de marcas, respetuosamente solicitamos a la entidad aboliir esta parte del requerimiento:	" El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.”"	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su observación.
173	4.8	Sustancial	"La solución no deberá requerir el instalar agentes de software en los servidores a monitorear, pero deberá tener la opción en caso de ser necesario."	En aras de la pluralidad de marcas, respetuosamente solicitamos a la entidad que este requerimiento quede así: "	La solución deberá permitir el monitoreo de actividad en las bases de datos mediante diversos mecanismos, como uso de agente y/o agentless"	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su observación.
174	4.15	Sustancial	Proveer un servicio de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.	En aras de la pluralidad de marcas, respetuosamente solicitamos a la entidad eliminar este requerimiento, ***toda vez que esto es una característica técnica que solo cumple Imperva*** , y justamente este requerimiento fue el que nos motivó a escribir nuestra observación **3 "Que la entidad nos asegure que no nos exigirá el cumplimiento de lo imposible con las herramientas otorgadas por la entidad, pues Guardium no cumple este requerimiento.** **No entendemos como si el nuevo contratista debe prestar su servicio con Guardium (la herramienta que proporciona la entidad) para la renovación no le permiten la participación.**		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su observación.

175	4.23	Sustancial	Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios deberán de poder usarse en cualquier número y cualquier combinación: - Número de registros a regresar por la consulta (SQL Query) - Número de registros afectados - Tipo de datos accedido (financiero, recursos humanos, inventarios, o cualquier definición personalizada) - Acceso a datos marcados como sensibles - Base de Datos, Esquema, Tabla y Columna accedida - Estado de autenticación de la sesión - Usuario y/o grupo de usuarios de Base de Datos conectado - Usuario conectado en la capa aplicativo, a diferencia del usuario conectado a la base de datos - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier personalización por expresiones regulares) - Autenticación (login, logout) y tareas (quering) - Direcciones IP origen y destino - Nombre de Host origen, usuario firmado en el host origen - Aplicación usada para la conexión a la base de datos - Tiempo de respuesta/procesamiento de las tareas - Errores en el manejador de SQL - Número de ocurrencias en intervalos de tiempo definidos - Por operaciones básicas (Select, Insert, Update, Delete) - Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export)	En aras de la pluralidad de marcas, respetuosamente solicitamos a la entidad abolir este requerimiento: "**Si existe evento asignado de cambio (ticket)**; toda vez que esto no corresponde al alcance natural de una solución de protección de base de datos		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, una vez revisado el ítem en mención se ajusta en su redacción y será publicado en adenda en los próximos días quedando de la siguiente manera: 4.23 Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios deberán de poder usarse en cualquier número y cualquier combinación: - Número de registros a regresar por la consulta (SQL Query) - Número de registros afectados - Tipo de datos accedido (financiero, recursos humanos, inventarios, o cualquier definición personalizada) - Acceso a datos marcados como sensibles - Base de Datos, Esquema, Tabla y Columna accedida - Estado de autenticación de la sesión - Usuario y/o grupo de usuarios de Base de Datos conectado - Usuario conectado en la capa aplicativo, a diferencia del usuario conectado a la base de datos - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier personalización por expresiones regulares) - Autenticación (login, logout) y tareas (quering) - Direcciones IP origen y destino - Nombre de Host origen, usuario firmado en el host origen - Aplicación usada para la conexión a la base de datos - Tiempo de respuesta/procesamiento de las tareas - Errores en el manejador de SQL - Número de ocurrencias en intervalos de tiempo definidos - Por operaciones básicas (Select, Insert, Update, Delete) - Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export) - Por Stored Procedure o función utilizada - Fecha y hora del evento
176	4.33	Sustancial	La solución deberá analizar los eventos generados desde diferentes bases de datos. El análisis deberá contemplar los siguientes criterios: - Deberá mostrar el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos. - Deberá contar con un sistema de correlación basado en la dirección de los ataques. Deberá determinar si los ataques provienen desde dentro de la organización hacia afuera de la misma o viceversa. - Deberá realizar una correlación automática y en tiempo real de eventos, vulnerabilidades y bases de datos. - Deberá ejecutar una correlación que permita identificar usuarios de aplicación asociados con consultas –y determinadas actividades– en bases de datos específicas sin necesidad de alterar aplicaciones o instalar APIs. - Deberá correlacionar eventos como número de errores inusuales de sentencias de SQL o al momento de hacer autenticación a las bases de datos.	En aras de la pluralidad de marcas, respetuosamente solicitamos a la entidad abolirdo de los cinco siguientes requerimientos: ". Deberá contar con un sistema de correlación basado en la dirección de los ataques. Deberá determinar si los ataques provienen desde dentro de la organización hacia afuera de la misma o viceversa. - Deberá realizar una correlación automática y en tiempo real de eventos, vulnerabilidades y bases de datos" y a que esto hace parte de la herramienta de propósito específico SIEM que corresponde a la capacidad 2 de la ficha técnica y justamente esta funcionalidad fue la que nos incitó a escribir nuestra observación 24.. **(que la entidad nos asegure que no nos exigirá el cumplimiento de lo imposible con las herramientas otorgadas por la entidad, pues Guardium no cumple este requerimiento).** **No entendemos como si el nuevo contratista debe prestar su servicio con Guardium (la herramienta que proporciona la entidad) para la renovación no le permiten la participación.**	La solución deberá analizar los eventos generados desde diferentes bases de datos. El análisis deberá contemplar los siguientes criterios: - Deberá mostrar el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos. - Deberá ejecutar una correlación que permita identificar usuarios de aplicación asociados con consultas –y determinadas actividades– en bases de datos específicas sin necesidad de alterar aplicaciones o instalar APIs. - Deberá correlacionar eventos como número de errores inusuales de sentencias de SQL o al momento de hacer autenticación a las bases de datos.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, una vez revisado se encuentra que las características en mención por parte del interesado para este ítem, las cumplen diferentes herramientas en el mercado, por lo tanto no se acepta su solicitud.
177	4.37	Sustancial	La solución deberá contar con una base de datos de vulnerabilidades predefinida para las siguientes regulaciones: - CIS - DISA (STIG) - FISMA - HIPAA - PCI-DSS	Teniendo en cuenta que: - CIS y DISA (STIG) no son regulaciones, son marcos de referencia - FISMA aplica para agencias federales de USA - HIPAA es para protección de datos de Salud en USA - PCI-DSS aplicaría solamente si almacenan, procesan o transmiten información de tarjetahabientes. Por o anteriormente expuesto, y en aras de la pluralidad de marcas, recomendamos a la entidad requerir lo que se ajusta a su necesidad, esd eliminar CIS y DISA (STIG)	La solución deberá contar con una base de datos de vulnerabilidades predefinida para las siguientes regulaciones: - FISMA - HIPAA - PCI-DSS	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su observación.
178	4.39	Sustancial	Deberá ser capaz de monitorear al menos las siguientes plataformas de bases de datos: - Oracle (Including NDE/ASO, SSL) - Oracle Exadata - Microsoft SQL Server - IBM DB2 para Linux, z/OS y DB2/400 - IBM IMS para z/OS - IBM Informix - IBM Netezza - SAP Sybase (ASE, IQ, SQL Anywhere) - SAP-HANA - Teradata - MySQL - PostgreSQL - Progress OpenEdge - Maria DB	En aras de la pluralidad de marcas, y justamente dejar participar a Guardium que es la herramienta que tiene la DIAN, respetuosamente solicitamos a la entidad dejar así: Deberá ser capaz de monitorear al menos las siguientes plataformas de bases de datos: - Oracle (Including NDE/ASO, SSL) - Oracle **(eliminar la palabra Exadata)** - Microsoft SQL Server - IBM DB2 para Linux, z/OS y DB2/400 - IBM IMS para z/OS - IBM Informix - IBM Netezza - SAP Sybase (ASE, IQ, SQL (**eliminar la palabra Anywhere**) - SAP-HANA - Teradata - MySQL - PostgreSQL - Progress **(Eliminar la palabra OpenEdge)** - Maria DB	Deberá ser capaz de monitorear al menos las siguientes plataformas de bases de datos: - Oracle (Including NDE/ASO, SSL) - Oracle - Microsoft SQL Server - IBM DB2 para Linux, z/OS y DB2/400 - IBM IMS para z/OS - IBM Informix - IBM Netezza - SAP Sybase (ASE, IQ, SQL) - SAP-HANA - Teradata - MySQL - PostgreSQL - Progress - Maria DB	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, una vez revisado se encuentra que las características en mención por parte del interesado para este ítem, las cumplen diferentes herramientas en el mercado, por lo tanto no se acepta su solicitud.
179	4.54.3	Sustancial	En el modo monitoreo el administrador podrá visualizar alertas, ataques, errores de servidor y otra actividad no autorizada.	Respetuosamente recomendamos a la entidad cambiar esta redacción toda vez que como está escrito está enfocado a una funcionalidad de la solución y no a una necesidad. Por lo anteriormente expuesto, y en aras de la pluralidad de marcas, recomendamos a la entidad cambiar la redacción y que quede así: "La solución deberá asignar roles específicos para el acceso a la gestión y a la administración, es decir, asociados con la consola de administración y monitoreo de las bases de datos"		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su observación.
180	4.54.4	Sustancial	En el modo de cumplimiento de políticas, la solución deberá bloquear ataques proactivamente.	Respetuosamente recomendamos a la entidad cambiar esta redacción toda vez que como está escrito está enfocado a una funcionalidad de la solución y no a una necesidad. Por lo anteriormente expuesto, y en aras de la pluralidad de marcas, recomendamos a la entidad cambiar la redacción y que quede así: "De acuerdo a los roles definidos en el acceso a las consolas de administración y monitoreo de las Bases de datos, se deberá proporcionar de acuerdo al rol del usuario la investigación de amenazas proactivamente"	"De acuerdo a los roles definidos en el acceso a las consolas de administración y monitoreo de las Bases de datos, se deberá proporcionar de acuerdo al rol del usuario la investigación de amenazas proactivamente"	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su observación.
181	4.54.7	Sustancial	En modo analizador de paquetes, la solución deberá ser capaz de enviar un paquete TCP-RST a ambos extremos de la conexión. Alternativamente, si así se configura, la solución podrá reportar el comportamiento anómalo, pero no tomar acción alguna.	En aras de la pluralidad de marcas, respetuosamente solicitamos a la entidad eliminar este requerimiento, ***toda vez que esto es una característica técnica que solo cumple Imperva*** , y justamente este requerimiento fue el que nos incitó a escribir nuestra observación **3.. (que la entidad nos asegure que no nos exige el cumplimiento de lo imposible con las herramientas otorgadas por la entidad, pues Guardium no cumple este requerimiento).** **No entendemos como si el nuevo contratista debe prestar su servicio con Guardium (la herramienta que proporciona la entidad) para la renovación no le permiten la participación.**		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, una vez revisado se encuentra que las características en mención por parte del interesado para este ítem, las cumplen diferentes herramientas en el mercado, por lo tanto no se acepta su solicitud.
182	V. Formularios de la Oferta IAO 15.2	Formal	"...El Oferente podrá expresar el Precio de su Oferta en cualquier moneda. Si el Oferente desea recibir el pago en una combinación de montos en diferentes monedas, podrá cotizar su precio en las monedas que correspondan. Sin embargo, no podrá incluir más de tres monedas extranjeras además de la del País del Comprador."	Respetuosamente solicitamos a la entidad indicar si podemos cambiar el formato de la oferta económica para determinar cuál ítem está en pesos y cual en dólares o en una tercera moneda.		Se aclara que se podrá incluir la moneda de la preferencia dentro de la lista de precios, no obstante, se precisa que no se podrá modificar el formulario de lista de precios ni los otros formularios incluidos en la Solicitud de Oferta.
183	V. Formularios de la Oferta IAO 15.2	Formal	"...El Oferente podrá expresar el Precio de su Oferta en cualquier moneda. Si el Oferente desea recibir el pago en una combinación de montos en diferentes monedas, podrá cotizar su precio en las monedas que correspondan. Sin embargo, no podrá incluir más de tres monedas extranjeras además de la del País del Comprador."	Respetuosamente solicitamos a la entidad indicarnos con cuál TRM se liquidarán los ítems que se coticen en una moneda diferente a pesos a fin que el proveedor reciba su pago?		En caso de que el contrato se suscriba en dólares de los Estados Unidos de América y se requiera el pago en pesos colombianos se cancelará el valor en esta moneda tomando como base la conversión de los dólares a pagar convertidos a pesos según la TRM publicada por el Banco de la República para la fecha de emisión de cada factura, de acuerdo con el procedimiento interno de pagos.

184	V. Formularios de la Oferta IAO 15.2	Formal	"...El Oferente podrá expresar el Precio de su Oferta en cualquier moneda. Si el Oferente desea recibir el pago en una combinación de montos en diferentes monedas, podrá cotizar su precio en las monedas que correspondan. Sin embargo, no podrá incluir más de tres monedas extranjeras además de la del País del Comprador."	Respetuosamente solicitamos a la entidad indicárnosla metodología que usarán para liquidar los ítems que se coticen en una moneda diferente a pesos, de tal manera que las ofertas sean comparables al momento de su evaluación económica y poder identificar la más económica para asignarle la máxima puntuación. Favor tener presente que la evaluación económica pesa 50 % de la evaluación completa		De acuerdo con lo establecido en la IAO 32.1 de la Sección de Datos de la Licitación, se indica el procedimiento para la comparación de los valores así: *La única moneda para la conversión de todos los precios expresados en varias monedas en una sola es: el dólar* *La fuente oficial de la tasa de cambio tipo vendedor es: la superintendencia Financiera de Colombia.* *https://www.superfinanciera.gov.co/publicaciones/60819/informes-y-cifrasifrasestablecimientos-de-creditoinformacion-periodicadiariatasa-de-cambio-representativa-del-mercado-trm-60819/* *La fecha de las tasas de cambio es: Una (1) semana antes de la fecha límite definida para la presentación de propuestas.*
185	V. Formularios de la Oferta IAO 15.2	Formal	"...El Oferente podrá expresar el Precio de su Oferta en cualquier moneda. Si el Oferente desea recibir el pago en una combinación de montos en diferentes monedas, podrá cotizar su precio en las monedas que correspondan. Sin embargo, no podrá incluir más de tres monedas extranjeras además de la del País del Comprador."	Respetuosamente solicitamos a la entidad indicar la metodología de comparación de ofertas en su oferta económica cuando tiene dos o tres monedas		De acuerdo con lo establecido en la IAO 32.1 de la Sección de Datos de la Licitación, se indica el procedimiento para la comparación de los valores así: *La única moneda para la conversión de todos los precios expresados en varias monedas en una sola es: el dólar* *La fuente oficial de la tasa de cambio tipo vendedor es: la superintendencia Financiera de Colombia.* *https://www.superfinanciera.gov.co/publicaciones/60819/informes-y-cifrasifrasestablecimientos-de-creditoinformacion-periodicadiariatasa-de-cambio-representativa-del-mercado-trm-60819/* *La fecha de las tasas de cambio es: Una (1) semana antes de la fecha límite definida para la presentación de propuestas.*
186	II: Datos de la licitación (DDL)	Sustancial	El idioma utilizado será Español	Teniendo en cuenta que en algunos puntos se demostrará el cumplimiento técnico con un link del fabricante, respetuosamente solicitamos a la entidad seleccionar el idioma español en su navegador a fin que si se toma un idioma diferente a este, no se rechace la oferta		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, para la revisión de las diferentes ofertas se tendrá en cuenta su comentario.
187	II: Datos de la licitación (DDL)	Sustancial	EEFF de 2024	Debido a que hay 2 indicadores que involucran el presupuesto (Patrimonio en relación con el presupuesto estimado: y Capital de trabajo en relación al presupuesto estimado del proceso) , favor indicar como se calcula el indicador financiero en caso de APCA . Favor publicar un ejemplo. ES decir, el presupuesto también se multiplica por el porcentaje de participación?		En atención a la observación, a continuación se detallan las fórmulas paraa la evaluación de las APCAS: **Indicador** — **Fórmula de cálculo APCA** Índice de liquidez: $\frac{(AC_{socio1}*\%P_{socio1}) + (AC_{socio2}*\%P_{socio2})}{(PC_{socio1}*\%P_{socio1}) + (PC_{socio2}*\%P_{socio2})}$ donde: AC= Activo corriente, PC=Pasivo corriente, %P= Porcentaje participación Razón de endeudamiento: $\frac{(P_{socio1}*\%P_{socio1}) + (P_{socio2}*\%P_{socio2})}{(A_{socio1}*\%P_{socio1}) + (A_{socio2}*\%P_{socio2})}$ donde: A= Activo total, P=Pasivo total, %P= Porcentaje participación Patrimonio en relación al presupuesto estimado del proceso: $\frac{(Pt_{socio1}*\%P_{socio1}) + (Pt_{socio2}*\%P_{socio2})}{PE}$ donde: Pt = Patrimonio, PE=Presupuesto Estimado, %P= Porcentaje participación Capital de trabajo en relación al presupuesto estimado del proceso: $\frac{[(AC_{socio1}*\%P_{socio1}) + (AC_{socio2}*\%P_{socio2})] - [(PC_{socio1}*\%P_{socio1}) + (PC_{socio2}*\%P_{socio2})]}{PE}$ donde: AC= Activo corriente, PC=Pasivo corriente, PE=Presupuesto Estimado, %P= Porcentaje participación Apalancamiento a corto plazo: $\frac{[(PC_{socio1}*\%P_{socio1}) + (PC_{socio2}*\%P_{socio2})]}{[(Pt_{socio1}*\%P_{socio1}) + (Pt_{socio2}*\%P_{socio2})]}$ donde: PC=Pasivo Corriente, Pt= Patrimonio, %P= Porcentaje participación Los porcentajes de participación de cada firma por criterio (Activo total o corriente, pasivo total o corriente y patrimonio) se calculan sobre la sumatoria de esos mismos criterios para el APCA que se presenta. Esto significa que, por ejemplo: %P para Activo= Asocio1/(Asocio1+Asocio2)
188	II: Datos de la licitación (DDL) AIO 17.2 ©	Sustancial	Con el fin de establecer la conformidad de los Bienes y Servicios Conexos con el documento de licitación, los Oferentes deberán proporcionar, como parte de su Oferta, prueba documental que acredite que los Bienes cumplen con las especificaciones técnicas y los estándares especificados en la Sección VI, "Requisitos de los Bienes y Servicios Conexos".	Favor indicarnos cómo se debe acreditar el cumplimiento		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, con el cumplimiento del anexo técnico.
189	II: Datos de la licitación (DDL) AIO 22.1	Sustancial	Las firmas participantes deberán informar al correo adquisiciones@fondodian.gov.co , que presentarán oferta dentro del proceso para que el Fondo Dian para Colombia -FDC remita un Link para cada oferente interesado en el que podrán cargar las ofertas de acuerdo con el protocolo de presentación que se adjunta a la SdO. Cada oferente realizará el cargue de su oferta así:	Favor indicar el plazo máximo para hacer esta solicitud		Los interesados deberán solicitar el enlace para el cargue del enlace por lo menos con 7 días calendario anterior a la fecha del cierre del proceso.
190	Sección III. Criterios de evaluación	Sustancial	"c. El futuro interesado deberá acreditar que el fabricante de las capacidades ofrecidas entregue el servicio de TAM (Thecnical Account Manager) para el soporte a dichas capacidades por el tiempo estipulado para el proyecto y que no ocasione ningún costo adicional para la Entidad."	Respetuosamente recomendamos a la entidad reemplazar la frase futuro interesado por interesado u oferente o contratista según coinciden	"c. El oferente deberá acreditar que el fabricante de las capacidades ofrecidas entregue el servicio de TAM (Thecnical Account Manager) para el soporte a dichas capacidades por el tiempo estipulado para el proyecto y que no ocasione ningún costo adicional para la Entidad."	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la frase que indica el futuro interesado ofrece el significado amplio y suficiente para que los proponentes puedan entregar lo solicitado, por lo tanto no se acepta su solicitud.
191	(ii) Experiencia y capacidad técnica general	Sustancial	"• Servicios de diseño, planeación e implementación de Centros de Operaciones de Seguridad (SOC) y/o servicios avanzados de protección en ciberseguridad. • Suministro de hardware y software especializado en seguridad informática de nivel empresarial. • Servicios de implementación, integración y configuración de soluciones avanzadas de ciberseguridad."	¿es correcto nuestro entendimiento al deducir, que los contratos que tengan por objeto el diseño y operación de un CSIRT con el suministro como servicio de herramientas de ciberseguridad, cumple con lo requerido por la entidad en el numeral 3 experiencia y capacidad técnica general?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, su entendimiento es correcto y se aplicaría equivalencia por experiencia SOC.
192	4. 410-Formulario-1-lista-de-precios-VSD	Sustancial	Servicios de Monitoreo y operación de SOC con el personal mínimo requerido (Ver características en el ítem 12 del anexo).: 30 meses	ES correcto nuestro entendimiento que los meses de monitoreo corresponden a los meses desde el primer día del contrato y no que luego tenga que coincidir con la fecha de vencimiento de las licencias del SIEM vendidas?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la operación, seguimiento, gestión, monitoreo y administración por parte del futuro proveedor de todos los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho a uso, licenciamiento, suscripciones, actualizaciones, soporte y garantía irá por tres (3) años y sus periodos se contabilizarán a partir de la puesta en operación de cada uno de los servicios requeridos, incluyendo lo siguiente: Tener en cuenta que desde el inicio del contrato se deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 nuevo SIEM (solicitado en el ítem 2) que hace parte integral de este proyecto por el tiempo solicitado (Tres años) con licenciamiento soporte, garantía y derecho a uso hasta agosto 31 de 2030. La protección de bases de datos (Firewall de bases de datos) irá a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031. El futuro contratista deberá, recibir, gestionar, administrar y operar desde el inicio del contrato el actual firewall de bases de datos propiedad de la DIAN del fabricante IBM Referencia GUARDIUM hasta diciembre 31 de 2027 tiempo en el que termina el soporte de este dispositivo por parte del fabricante, una vez esto ocurra deberá implementar el nuevo firewall de bases de datos solicitado en las capacidades requeridas por la DIAN. Para la capacidad de NDR se deberá tener en cuenta que este comenzará a operar a partir de enero de 2028 previamente autorización de la DIAN, para lo cual deberá implementar, administrar, operar, soportar y garantizar el servicio mencionado, con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031.

193	4. 410-Formulario-1-lista-de-precios-VSD	Sustancial	Servicios de Monitoreo y operación de SOC con el personal mínimo requerido (Ver características en el ítem 12 del anexo).: 30 meses	Es correcto nuestro entendimiento que los meses de monitoreo corresponden a los meses desde el primer día del contrato y no que luego tenga que coincidir con la fecha de vencimiento de las licencias del Firewall de Protección de base de datos vendido?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, la operación, seguimiento, gestión, monitoreo y administración por parte del futuro proveedor de todos los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho a uso, licenciamiento, suscripciones, actualizaciones, soporte y garantía irá por tres (3) años y sus periodos se contabilizarán a partir de la puesta en operación de cada uno de los servicios requeridos, incluyendo lo siguiente: Tener en cuenta que desde el inicio del contrato se deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 el nuevo SIEM (solicitado en el ítem 2) que hace parte integral de este proyecto por el tiempo solicitado (Tres años) con licenciamiento soporte, garantía y derecho a uso hasta agosto 31 de 2030. La protección de bases de datos (Firewall de bases de datos) irá a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031. El futuro contratista deberá, recibir, gestionar, administrar y operar desde el inicio del contrato el actual firewall de bases de datos propiedad de la DIAN del fabricante IBM Referencia GUARDIUM hasta diciembre 31 de 2027 tiempo en el que termina el soporte de este dispositivo por parte del fabricante, una vez esto ocurra deberá implementar el nuevo firewall de bases de datos solicitado en las capacidades requeridas por la DIAN. Para la capacidad de NDR se deberá tener en cuenta que este comenzará a operar a partir de enero de 2028 previamente autorización de la DIAN, para lo cual deberá implementar, administrar, operar, soportar y garantizar el servicio mencionado, con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031.
194	Ficha técnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	Sustancial	La protección de bases de datos (Firewall de bases de datos) irá a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031. El futuro contratista deberá, recibir, gestionar, administrar y operar desde el inicio del contrato el actual firewall de bases de datos propiedad de la DIAN del fabricante IBM Referencia GUARDIUM hasta diciembre 31 de 2027 tiempo en el que termina el soporte de este dispositivo por parte del fabricante, una vez esto ocurra deberá implementar el nuevo firewall de bases de datos solicitado en las capacidades requeridas por la DIAN.	Respetuosamente solicitamos a la entidad indicarnos si este SIEM está operando y adicionalmente compartirnos el pantallazo o evidencia que el licenciamiento está activo hasta la fecha indicada por la entidad		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el SIEM de la Entidad está operativo con derecho a uso, soporte y garantía por parte del fabricante, se aclara que desde el inicio del contrato el proveedor del SOC deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 el nuevo SIEM (solicitado en el ítem 2) que hace parte integral de este proyecto por el tiempo solicitado (Tres años) con licenciamiento soporte, garantía y derecho a uso hasta agosto 31 de 2030.
195	1.3	Sustancial	Para la capacidad de NDR se deberá tener en cuenta que este comenzará a operar a partir de enero de 2028 previamente autorización de la DIAN, para lo cual deberá implementar, administrar, operar, soportar y garantizar el servicio mencionado, con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031.	ES correcto nuestro entendimiento cuando concluimos que el NRD no lo tiene actualmente la entidad pero el nuevo contratista deberá proveerlo e implementarlo en enero de 2028?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la Entidad cuenta actualmente con servicio de NDR administrado y operado hasta la diciembre de 2027, a partir de enero de 2028 deberá ser puesto en operación el nuevo servicio de NDR ofrecido por el proveedor del SOC.
196	2.4	Sustancial	Se debe licenciar como mínimo para 2467 dispositivos (2056 que están estipulados en el inventario anexo más el 20% de incremento adicional) o unidad equivalente o superior de acuerdo con la tecnología ofrecida.	El pliego contempla la expresión "o unidad equivalente o superior de acuerdo con la tecnología ofrecida", lo cual es positivo. Sin embargo, para garantizar la comparabilidad de las ofertas y evitar interpretaciones restrictivas durante la evaluación, se solicita que la entidad precise en los datos de la licitación (DDL) la metodología de equivalencia entre el modelo de licenciamiento por dispositivos y el modelo por Eventos por Segundo (EPS), que es el estándar de industria utilizado por los fabricantes líderes de SIEM. Una equivalencia sugerida: 2.467 dispositivos con un promedio de 10 EPS/dispositivo = 24.670 EPS = 25.000 EPS (ítem 2.5). Confirmar que ambas métricas satisfacen el requisito.	Recomendamos a la entidad cambiar el requerimiento así: "Se debe licenciar como mínimo para 2.467 dispositivos o 25.000 EPS, o cualquier unidad de medida equivalente o superior según la tecnología ofrecida. El oferente deberá justificar documentalmente la equivalencia de la unidad propuesta respecto al número de dispositivos del inventario."	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, una vez revisado se encuentra que el detalle dado en el ítem en cuestión es amplio y suficiente para que los interesados puedan confeccionar sus ofrecimientos de acuerdo a los requerimientos de la Entidad, por lo tanto, no se acepta su sugerencia.
197	2.8	Sustancial	"...Para tal efecto se informa que actualmente la Entidad cuenta con un ITSM del fabricante ARANDA"	El requerimiento indica que la solución SIEM debe integrarse con el ITSM ARANDA de la entidad. Se solicita aclarar si esta integración debe ser mediante conector certificado y nativo del fabricante SIEM, o si se acepta integración vía API REST estándar, webhooks o protocolos de intercambio abiertos (JSON/HTTP). La mayoría de fabricantes líderes de SIEM no cuentan con un conector nativo certificado para ARANDA, pero sí permiten integraciones bidireccionales a través de APIs estándar que funcionalmente cumplen el mismo propósito. Exigir conector nativo certificado para un ITSM de uso exclusivamente local limitaría artificialmente el número de proponentes elegibles.	Por lo anteriormente expuesto, recomendamos a la entidad dejar el requerimiento así: "La integración con el ITSM ARANDA podrá realizarse mediante conector nativo del fabricante o mediante integración vía API REST, webhooks o protocolos de intercambio estándar (JSON/HTTP/SOAP), siempre que se garantice la funcionalidad de creación, actualización y cierre bidireccional de tickets."	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, la integración se puede hacer mediante el método considerado por el proponente de acuerdo a su experticia, siempre y cuando se cumpla con lo requerido por la Entidad.
198	2.13	Sustancial	""La solución debe estar en capacidad de instalarse en Azure, AWS, HyperV, VMware. Se aclara que la Entidad cuenta con Windows Server 2012R2, Windows Server 2022 y VMware ESXi 7.0.3."	Windows Server 2012 R2 alcanzó su fin de soporte extendido en octubre de 2023 (Microsoft End of Life). Exigir compatibilidad garantizada con esta versión puede constituir un requisito técnico que ningún fabricante de SIEM vigente puede acreditar mediante documentación oficial de soporte, dado que el propio fabricante del sistema operativo ya no lo soporta. Se solicita aclarar si: (i) se acepta que la solución opere sobre Windows Server 2012 R2 a riesgo de la entidad sin garantía del fabricante del SIEM, o (ii) la entidad contempla migrar esos servidores a una versión soportada (WS 2019/2022) durante la vigencia del contrato, condición que el oferente podrá acompañar. Esto evita descalificaciones injustificadas por documentación de soporte que ningún fabricante puede proveer para un OS en EOL.	Respetuosamente solicitamos a la entidad permitir que el requerimiento sea así: ""La solución debe soportar despliegue en VMware ESXi 7.x o superior, Hyper-V sobre Windows Server 2019/2022, Azure y AWS. Para activos con sistemas operativos en fin de soporte (ej. WS 2012 R2), el monitoreo se realizará mediante colectores remotos o reenvío de logs, sin que ello implique garantía de soporte por parte del fabricante del SIEM sobre el sistema operativo subyacente."	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, las opciones de integración las debe dar el proponente siempre y cuando se cumpla con los requerimientos técnicos solicitados por la Entidad para este ítem.
199	2.27	Sustancial	"Integración basada en API a sistemas externos de ticketing - Aranda, ServiceNow, Salesforce, ConnectWise, Remedy y Jira".	"El ítem 2.27 menciona ARANDA en la lista de sistemas de ticketing, lo cual es coherente con el ítem 2.8. Se reitera la solicitud de confirmar **(ver OBSERVACIÓN-30** de este documento referente al ITSM ARANDA) que la integración vía API REST estándar cumple este requerimiento, dado que ARANDA no figura como conector nativo certificado en los catálogos de los principales fabricantes de SIEM a nivel global. La funcionalidad requerida (creación y actualización de tickets desde el SIEM) es plenamente alcanzable mediante API."		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, la integración se puede hacer mediante el método considerado por el proponente de acuerdo a su experticia, siempre y cuando se cumpla con lo requerido por la Entidad para este ítem.
200	3.4	Sustancial	"La solución ofertada debe estar licenciada como mínimo para tres (3) analistas."	Se solicita confirmar que el número de tres (3) analistas es el mínimo requerido y no un tope máximo, de manera que el oferente pueda proponer licenciamiento para un mayor número de analistas (o usuarios concurrentes) si la arquitectura de la solución lo permite por diseño, sin que ello implique costo adicional para la entidad. Algunas plataformas SOAR de mercado incluyen usuarios ilimitados en su licencia base, lo que representa un mayor valor para la DIAN.	Respetuosamente recomendamos a la entidad permitir requerirlo así: "La solución ofertada debe estar licenciada como mínimo para tres (3) analistas. El oferente podrá proponer un licenciamiento de mayor alcance (usuarios adicionales o ilimitados) si la plataforma lo permite, lo cual será valorado positivamente."	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los requerimientos solicitados son requerimientos mínimos, por lo tanto, para la cantidad en mención tres (3) analistas es lo mínimo y el proveedor del SOC puede ofrecer más de la cantidad solicitada.
201	3.70	Sustancial	"La solución debe tener al menos 300 playbooks preconfigurados." "La solución debe incluir al menos 300 conectores de integración preconfigurados."	Se propone que la entidad incorpore en la Sección III (Criterios de Evaluación) un criterio adicional de ponderación técnica que asigne puntaje diferencial a las soluciones que superen los mínimos requeridos de playbooks y conectores. Esto permitirá diferenciar objetivamente soluciones de mayor madurez y cobertura, evitando que ofertas que apenas alcanzan el mínimo obtengan el mismo puntaje que plataformas con ecosistemas de automatización significativamente más amplios. Esta adición beneficia directamente la calidad del servicio de SOC para la DIAN y evita que le ofrezcan herramientas open source o que eno tengan la madurez para atender un SOC como el de la DIAN, porque sus principales riesgos se pueden estar materializando en una fuga masiva de información sensible	Criterio técnico sugerido para la Sección III: "Cantidad de playbooks preconfigurados certificados por el fabricante: [300-399: X puntos] [400-499: X+Y puntos] [500 o más: X+2Y puntos]. Igual escala para conectores certificados."	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los criterios de evaluación están establecidos por la Entidad y obedecen a necesidades puntuales de la Entidad, por lo tanto su sugerencia no se acepta.
202	5.4.11	Sustancial	"La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management)."	Se solicita confirmar que este requisito aplica exclusivamente al fabricante del componente de Gestión de Vulnerabilidades (ítem 5) y no al integrador del SOC ni al fabricante de las demás plataformas (SIEM, SOAR, NDR, etc.). De lo contrario, se estaría exigiendo implícitamente que un único fabricante sea líder en Gartner en múltiples mercados distintos simultáneamente (SIEM, SOAR, VM, NDR), lo cual ningún fabricante del mundo cumple en su totalidad y restringiría la competencia de forma ilegítima.	Respetuosamente recomendamos a la entidad reemplazar el requerimiento de la siguiente manera ""El fabricante de la solución de Gestión de Vulnerabilidades (ítem 5) deberá estar posicionado en el cuadrante de Líderes del Magic Quadrant de Gartner o en Forrester Wave para la categoría Vulnerability Risk Management o Exposure Management, en su edición más reciente disponible a la fecha de cierre de la licitación.""	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento es para el fabricante de la solución de gestión de vulnerabilidades, y aplica para el ítem en mención.

203	5.11.1	Sustancial	"La solución ofertada deberá Gestionar las Vulnerabilidades de todas las cargas de trabajo (CWPP), Gobierno y Cumplimiento de la infraestructura nube (CSPM), Gobierno de Identidades (CIEM)... bajo una arquitectura CNAPP"	Se propone adicionar como requerimiento que la plataforma CNAPP (Item 5.11) tenga capacidad de enviar alertas y hallazgos directamente al SIEM y al SOAR ofertados, de manera nativa o mediante API documentada, para que los incidentes de seguridad en cloud sean tratados dentro del flujo de respuesta automatizada del SOC. Esta adición eleva la madurez del SOC y garantiza visibilidad unificada.	Por lo anteriormente expuesto, recomendamos Adicionar al ítem 5.11: "La plataforma CNAPP deberá integrarse con el SIEM y el SOAR ofertados para el envío automático de alertas y la ejecución de playbooks de respuesta ante incidentes de seguridad en cloud"	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los requerimientos obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
204	6.4.2	Sustancial	"El appliance, o solución, plataforma o servicio de decepción debe estar en capacidad de crear al menos 400 señuelos, en hasta 20 máquinas virtuales y desplegarse en mínimo 120 VLANs o características similares o superiores en las tecnologías ofrecidas."	El pliego ya contempla la expresión "características similares o superiores", lo cual es adecuado. Se solicita confirmar que la evaluación de equivalencia de capacidades se realizará sobre la funcionalidad operativa (capacidad de cobertura de la red, profundidad de la decepción y calidad de los IOCs generados) y no exclusivamente sobre los parámetros numéricos literales (400 señuelos, 20 VMs, 120 VLANs). Plataformas de última generación pueden lograr una cobertura superior con arquitecturas diferentes que no se expresan en los mismos términos métricos. Respetuosamente recomendamos a la entidad permitir y dejarlo así: ""...o características similares o superiores en las tecnologías ofrecidas. El oferente deberá justificar documentalmente la equivalencia funcional de la capacidad ofrecida respecto a los parámetros mínimos indicados, demostrando cobertura equivalente de la superficie de ataque de la entidad.""	Por lo anteriormente expuesto, recomendamos a la entidad dejar el requerimiento así: "...o características similares o superiores en las tecnologías ofrecidas. El oferente deberá justificar documentalmente la equivalencia funcional de la capacidad ofrecida respecto a los parámetros mínimos indicados, demostrando cobertura equivalente de la superficie de ataque de la entidad."	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento solicitado es amplio y suficiente de acuerdo a lo especificado en este ítem, por lo tanto, no se acepta su sugerencia.
205	6.4.12	Sustancial	"Debe integrarse con el Firewall de Nueva Generación de la entidad, de manera que se pueda tener en este último un dashboard centralizado con la información general del dispositivo y los señuelos desplegados."	Este requerimiento es técnicamente exigente y muy relevante. Se propone que la entidad incluya en los criterios de evaluación (Sección III) puntaje adicional para soluciones que demuestren integración nativa certificada por el fabricante (no solo vía API genérica) entre la plataforma de deception y el NGFW de la entidad, incluyendo: (i) visibilidad del estado de señuelos directamente en la consola del firewall, (ii) automatización de bloqueo de IPs atacantes en el NGFW desde la plataforma de deception sin intervención manual, y (iii) generación de políticas de cuarentena automática. Esta capacidad reduce significativamente el MTTR ante ataques detectados por la capa de deception.	Adicionar criterio técnico diferenciador: "La integración entre la plataforma de Caza de Amenazas/Deception y el NGFW que incluya automatización de bloqueo y cuarentena sin intervención manual, certificada por el fabricante, recibirá [X] puntos adicionales en la evaluación técnica."	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento solicitado es amplio y suficiente de acuerdo a lo especificado en este ítem, por lo tanto, no se acepta su sugerencia.
206	6.5.14	Sustancial	La solución se debe integrar como mínimo con los siguientes elementos: [...] BitDefender, Solución de detección y respuesta en el endpoint (EDR).	BitDefender es el nombre de un fabricante específico de antivirus/EDR. Incluirlo como requerimiento de integración obligatoria puede interpretarse como una exigencia de marca que discrimina a soluciones equivalentes o superiores. Se solicita aclarar si BitDefender es la plataforma AV/EDR actualmente desplegada en la DIAN y si la integración requerida es con la plataforma AV/EDR existente en general, aceptándose cualquier mecanismo de integración estándar (CEF/Syslog/API) independientemente del fabricante del conector.	Por lo anteriormente expuesto recomendamos a la entidad que el requerimiento quede así"La solución debe integrarse con la plataforma de protección de endpoints (AV/EDR) desplegada en la entidad, mediante API, CEF, Syslog u otro mecanismo de integración estándar documentado. El oferente indicará el mecanismo de integración propuesto con la solución AV/EDR vigente en la entidad."	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, bitdefender es la plataforma actual de la Entidad, por ende, se solicita la respectiva integración.
207	7.3-7.18	Sustancial	Ítem 7.3: "Se debe licenciar como mínimo para 25.000 activos." Ítem 7.18: "El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 17.727 dispositivos por 3 años."	Existe una discrepancia numérica entre los ítems 7.3 (25.000 activos) y 7.18 (17.727 dispositivos) para la misma solución NDR. Esta inconsistencia puede dar lugar a interpretaciones diferentes durante la evaluación de las propuestas y generar controversias contractuales. Se solicita a la entidad unificar el número de dispositivos licenciados para NDR en una sola cifra, indicando si se trata de dispositivos monitoreados, flujos de red o una métrica diferente, y cuál prevalece en caso de discrepancia.	Por lo anteriormente expuesto, recomendamos que el requerimiento quede así: "La solución NDR deberá licenciarse para [número unificado] dispositivos/flujos de red por un período de tres (3) años, con capacidad de escalamiento hasta 25.000 activos sin costo adicional de licencia."	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la cantidad de dispositivos es 25000 (allí están referenciados todos los activos tecnológicos de la Entidad incluyendo aplicaciones web) para lo cual se procederá a la modificación de la cantidad expresada en este ítem quedando de la siguiente manera, cambio que se verá reflejado en la adenda a publicar en los próximos días: 7.18 El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 25000 dispositivos por (3) años.
208	7.26	Sustancial	"Debe funcionar completamente en función del comportamiento, donde no se permitan las tecnologías que hacen uso de reglas y/o firmas."	Esta redacción es técnicamente imprecisa y excluiría de facto a TODOS los fabricantes líderes del mercado NDR reconocidos por Gartner y Forrester (Darktrace, Vectra AI, ExtraHop, Cisco Stealthwatch, Fortinet FortiNDR), dado que todas las plataformas maduras de NDR complementan su motor principal de ML con firmas o reglas para la detección de amenazas conocidas, mejorando la precisión y reduciendo los falsos positivos. Exigir detección basada EXCLUSIVAMENTE en comportamiento, sin ningún apoyo en firmas, es contrario a las mejores prácticas de seguridad (NIST SP 800-94, MITRE ATT&CK) y podría resultar en una solución con mayor tasa de falsos negativos para amenazas conocidas. Se propone ajustar la redacción para reflejar el estándar de mercado.	Por lo anteriormente expuesto, recomendamos a la entidad dejar el requerimiento así: ""El motor principal de detección de la solución NDR debe basarse en análisis de comportamiento e inteligencia artificial (Machine Learning supervisado, no supervisado y/o Deep Learning), sin depender exclusivamente de firmas o reglas estáticas para la detección de amenazas desconocidas (Zero Day, APT, movimiento lateral). La solución podrá complementar su capacidad de detección con firmas para amenazas conocidas, siempre que el componente de ML/IA sea el motor primario de análisis de comportamiento."	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem 7.26 será ajustado, para evitar equivocos en el requerimiento de la Entidad, quedando de la siguiente manera, cambio que se verá reflejado en la adenda a publicar en los próximos días: La solución debe ser una plataforma de autoaprendizaje y tener un enfoque adaptativo que utilice inteligencia artificial comprobada para aprender sobre el entorno en el que se encuentra, detectar y responder a las desviaciones de la línea de base normal de comportamiento, así: - La línea base de la red debe ser lo suficientemente adaptable y dinámica para adaptarse a cualquier cambio en el comportamiento del entorno. - Debe trabajar en función del comportamiento.
209	12.8	Sustancial	"Se deberá realizar la integración de la herramienta GRC de NOVASEC propiedad de la DIAN con la plataforma SOAR."	Para que el oferente pueda garantizar esta integración en su propuesta técnica y dimensionar el esfuerzo de desarrollo del conector, se solicita a la entidad: (i) confirmar si NOVASEC expone una API REST documentada o algún mecanismo de integración estándar (webhooks, SOAP, base de datos), (ii) indicar si la documentación técnica de dicha API estará disponible para los proponentes durante el período de preguntas, y (iii) aclarar el alcance funcional mínimo esperado de la integración (lectura/escritura de riesgos, actualización de estado de controles, generación de alertas). Sin esta información, cualquier compromisos de integración en la oferta sería especulativo.	Respetuosamente recomendamos a la entidad dejar el requerimiento así: ""La DIAN pondrá a disposición de los oferentes, durante el período de preguntas y respuestas, la documentación técnica de la API de NOVASEC GRC necesaria para el diseño de la integración con el SOAR. El desarrollar del conector será responsabilidad del contratista, usando el SDK o APIs provistas por el fabricante del SOAR."	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento es viable con el fabricante de la solución GRC, por lo tanto, el proveedor del SOC podrá hacerlo mediante API.
210	12.37	Sustancial	"El servicio debe incluir Threat Intelligence o Inteligencia Global, que permita usar un servicio mundial de amenazas identificadas."	Se propone que la entidad precise que el servicio de Threat Intelligence incluido en la oferta puede ser el propio del fabricante del SIEM/SOAR (p. ej. feeds de amenazas propietarios del fabricante actualizados en tiempo real) o de un tercero integrado, siempre que cumpla los criterios de calidad. Fabricantes como Fortinet (FortiGuard Labs, con más de 1.000 investigadores globales) ofrecen inteligencia de amenazas de primera calidad integrada nativamente en sus plataformas, lo que elimina la necesidad de licencias adicionales de TI de terceros y reduce costos. Excluir implícitamente los feeds propietarios del fabricante penalizaría ofertas de mayor valor integrado.	Por lo anteriormente expuesto, recomendamos dejar el requerimiento así: "El servicio de Threat Intelligence Global podrá ser provisto por el fabricante de las plataformas del SOC o por un proveedor especializado de terceros. En cualquier caso, deberá demostrar: cobertura global, actualización en tiempo real (máximo 24 horas), cobertura de IOCs (IPs, dominios, URLs, hashes, CVEs) y documentación del volumen de indicadores gestionados. La fuente de inteligencia nativa del fabricante del SIEM que cumpla estos criterios se considerará equivalente a un servicio de TI de terceros."	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la característica hace mención al servicio de monitoreo solicitado en el anexo técnico, el cual debe ser ofrecido por el proveedor del SOC apoyado por el o los fabricantes de las capacidades solicitadas y operadas por dicho proveedor.
211	Equipo Mínimo de Trabajo	Sustancial	NOTA 2:Todo el personal del SOC requerido para la implementación, operación, gestión, monitoreo, soporte, garantía, entre otros, deberá ser propio evitando figuras de tercerización, sin embargo se aclara que el CONTRATISTA se podrá apoyar con recursos (personal) directamente del fabricante para la etapa de implementación.	El personal mínimo requerido debe ser presentado con la oferta?, o lo debe proveer solo el contratista?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el personal junto con sus hojas de vida lo debera presentar el contratista o el proponente ganador en la etapa de adjudicación. Esta cambio se hará mediante adenda en los próximos días y se verá reflejado en el documento anexo de características técnicas, hoja equipo mínimo de trabajo, y quedará de la siguiente manera: NOTA 3: El personal mínimo de trabajo y sus hojas de vida deberán ser presentados por el oferente ganador cuando se adjudique el contrato.
212	Equipo Mínimo de Trabajo	Sustancial	NOTA 2:Todo el personal del SOC requerido para la implementación, operación, gestión, monitoreo, soporte, garantía, entre otros, deberá ser propio evitando figuras de tercerización, sin embargo se aclara que el CONTRATISTA se podrá apoyar con recursos (personal) directamente del fabricante para la etapa de implementación.	Teniendo en cuenta que los fabricantes para los servicios de implementación regularmente cuentan con los ingenieros que tienen sus partners especializados en servicios, respetuosamente solicitamos a la entidad indicar si el personal mínimo requerido para la implementación puede ser personal especializado con certificados de las fábricas, toda vez que difícilmente el personal que el fabricante muestra como "suyo" es de su nómina aunque si puede ser "propio" a través de contratos de prestación de servicios a través de terceros		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el proveedor del SOC deberá entregar el equipo de trabajo mínimo requerido por la Entidad para realizar las labores propias de implementación, gestión y operación. Adicional a este equipo si el futuro proveedor de SOC lo considera podrá apoyarse en personal del fabricante o fabricantes, siempre y cuando se cumpla con los requerimientos mínimos para este ítem (equipo mínimo).
213	All	Formal	N/A	Confirmar el presupuesto asignado para la ejecución del proyecto en SECOP II se asignan 13 Millones de Pesos M/c, es esto correcto?	Ajustar Secop	Es preciso indicar que la publicación de la documentación que se realiza en SECOP II es de manera publicitaria, sin embargo, la interacción del proceso se realiza a través del correo adquisiciones@fondodian.gov.co, tal como se señala en la IAO 7.1. de la Sección II de Datos de la Licitación. Ahora bien, el valor estimado del proceso de acuerdo con la CGC 15.1 se establece en hasta TRECE MILLONES DOS MIL OCHOCIENTOS VEINTICINCO DOLARES ESTADOUNIDENSES (USD $13.002.825).

214	20.2	Formal	Entregar las licencias a perpetuidad de las herramientas o recursos tecnológicos para los casos donde aplique, utilizados en la operación del SOC , a nombre de la DIAN implementadas y configuradas durante el proyecto con las capacidades en las que se encuentren en operación en el momento de la devolución del servicio con soporte actualizado por mínimo un año.	Frente al requerimiento que establece la obligación de entregar licencias a perpetuidad de las herramientas o recursos tecnológicos utilizados en la operación del SOC, a nombre de la DIAN, respetuosamente solicitamos a la Entidad evaluar su eliminación o ajuste. Lo anterior considerando que el modelo de prestación del servicio de SOC, de acuerdo con las mejores prácticas internacionales, se basa cada vez más en esquemas de servicios gestionados y soluciones Software as a Service (SaaS), en los cuales el valor principal no radica en la propiedad de licencias perpetuas, sino en la capacidad operativa, la actualización continua, la escalabilidad, la seguridad y los niveles de servicio garantizados durante la vigencia contractual. La exigencia de licencias a perpetuidad limita de manera significativa la participación de oferentes que operan bajo modelos SaaS o de seguridad gestionada, ampliamente utilizados en proyectos de ciberseguridad de naturaleza similar, incluso en entornos gubernamentales y bajo esquemas de financiamiento internacional, sin que ello implique una reducción en los niveles de control, seguridad o continuidad del servicio. Así mismo, los estándares y marcos de referencia aplicables a la operación de un SOC, tales como ISO/IEC 27001, NIST Cybersecurity Framework y NIST 800-61, no establecen como requisito la transferencia de licencias perpetuas, sino la garantía de controles efectivos, trazabilidad, custodia de la información, continuidad operativa y adecuada gestión de los activos durante la prestación del servicio. En este sentido, solicitamos considerar mecanismos alternativos que permitan la prestación del servicio mediante soluciones SaaS o esquemas de licenciamiento temporal asociados al servicio, garantizando a la DIAN el acceso a la información, la continuidad operativa y un soporte adecuado durante el periodo de transición o cierre del contrato."	"Entregar a la DIAN el acceso, uso y aprovechamiento de las herramientas o recursos tecnológicos, para los casos donde aplique, utilizados en la operación del SOC, implementados y configurados durante el proyecto con las capacidades que se encuentren en operación al momento de la finalización del servicio, bajo esquemas de licenciamiento, suscripción o servicios Software as a Service (SaaS), según corresponda."	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el requerimiento es claro en el sentido que menciona "para los casos donde aplique", es claro que si el ofrecimiento del proveedor del SOC no los contempla o presenta otro tipo de servicio o licenciamiento, no tendría que entregar licenciamiento alguno.
215	1.2	Formal	Se debe contar con un Centro de Operaciones de Seguridad - SOC **ubicado en una locación física en la ciudad de Bogotá** que cuente con las condiciones adecuadas para garantizar la continuidad operativa, la seguridad física y lógica, y el cumplimiento de las mejores prácticas del sector. Donde instalará todos los productos, capacidades, plataformas, soluciones y servicios, que sean requeridos alojar allí para dar cumplimiento a lo solicitado en el anexo técnico y que le permitan realizar todas las actividades encomendadas en este documento por la DIAN. Entendiéndose que el CONTRATISTA realizará toda la gestión, monitoreo, administración, optimización, actualización, acompañamiento, soporte y garantía de los mismos, cobijando toda la infraestructura tecnológica de la Entidad. Para el efecto debe tener la capacidad de detectar, escalar, informar, acompañar apoyar y soportar a la DIAN en la resolución de cada uno de los incidentes encontrados por el SOC durante el tiempo que dure el proyecto en mención. Los activos y demás características de estos se encuentran detallados en el apartado de inventarios y las especificaciones de cada una de las soluciones, plataformas, capacidades, servicios, soporte y garantía se encuentran en este anexo técnico de obligatorio cumplimiento.	Considerando que este proceso se adelanta mediante una Licitación Pública Internacional, entendemos que el objetivo del requerimiento relacionado con la ubicación del SOC es garantizar el control, la supervisión y la seguridad de la información, y no necesariamente la presencia física del centro en la ciudad de Bogotá. En ese sentido, entendemos que la Entidad considerará como válidos modelos de operación de SOC distribuidos o híbridos, ampliamente utilizados a nivel internacional, siempre que se garantice el cumplimiento de la normativa aplicable, la supervisión por parte de la DIAN, la trazabilidad, la custodia de la información y los niveles de servicio requeridos. Así mismo, este tipo de esquemas de operación de SOC distribuidos o híbridos han sido aceptados y utilizados por otras entidades públicas en la contratación de servicios de ciberseguridad, incluso en proyectos de naturaleza similar y bajo esquemas de financiamiento internacional, siempre que se asegure el cumplimiento de los requisitos normativos, contractuales y de control exigidos, así como la adecuada supervisión y trazabilidad del servicio. Por lo anterior, agradecemos confirmar si nuestro entendimiento es correcto. En en el evento en que no lo sea y que se requiera contar físicamente con el SOC localmente, dado los argumentos antes expuestos y los que fueron mencionados en la audiencia de aclaración por diferentes interesados, solicitamos sea flexibilizado este requisito y en esa medida el centro pueda operar de forma hibrida.	Se debe contar con un Centro de Operaciones de Seguridad – SOC que disponga de una infraestructura tecnológica, física y lógica adecuada para garantizar la continuidad operativa, la seguridad de la información y el cumplimiento de las mejores prácticas del sector, bajo los lineamientos y supervisión de la DIAN. El SOC deberá contar con las capacidades necesarias para instalar, operar y administrar los productos, plataformas, soluciones y servicios que deban ser alojados para dar cumplimiento a lo solicitado en el anexo técnico, permitiendo la ejecución integral de todas las actividades encomendadas en el presente documento. El CONTRATISTA será responsable de realizar la gestión, monitoreo, administración, optimización, actualización, acompañamiento, soporte y garantía de dichas capacidades y servicios, cubriendo la totalidad de la infraestructura tecnológica de la Entidad, independientemente de que esta se encuentre en ambientes locales, distribuidos o en esquemas hibridos. Para tal efecto, el CONTRATISTA deberá tener la capacidad de detectar, escalar, informar,	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, tal como se indica en el requerimiento, el futuro proveedor de SOC puede entregar dos Centros de Operaciones en la ciudad de Bogotá u optar por tener uno en la Ciudad de Bogotá y otro en otra locación diferente a esta ciudad, tal como se indica en el respectivo numeral, por lo tanto, es claro que el centro de operaciones de seguridad (personal, monitoreo, operación, locación física, entre otros), debe estar en la ciudad de Bogotá.
216	12.34	Formal	El oferente debe tener al menos tres (3) años, prestando el servicio, con SOC propietario, dentro del territorio nacional.	Frente al requerimiento que establece que 'el oferente debe tener al menos tres (3) años, prestando el servicio, con SOC propietario, dentro del territorio nacional', respetuosamente solicitamos a la Entidad evaluar su eliminación o ajuste. Lo anterior considerando que el proceso se adelanta mediante una Licitación Pública Internacional, la cual busca promover la libre concurrencia y la competencia efectiva entre oferentes nacionales e internacionales, permitiendo la participación de firmas con experiencia global comprobada en la prestación de servicios de SOC, incluso en entornos gubernamentales y de infraestructura crítica. El requisito de contar específicamente con un SOC propietario operando dentro del territorio nacional por un período mínimo de tres años introduce una restricción geográfica y temporal que no resulta proporcional al objetivo del servicio contratado, y podría limitar injustificadamente la participación de oferentes extranjeros o de firmas con modelos de operación distribuidos o híbridos, ampliamente aceptados y utilizados en proyectos de ciberseguridad de naturaleza similar y bajo esquemas de financiamiento internacional. Desde el punto de vista técnico, los estándares y mejores prácticas aplicables a la operación de un SOC —como ISO/IEC 27001, NIST Cybersecurity Framework y NIST 800-61— no condicionan la madurez, calidad o capacidad del servicio a la ubicación territorial del SOC, sino al cumplimiento de controles, procesos, capacidades operativas, niveles de servicio, trazabilidad y mecanismos de supervisión. En ese sentido, consideramos que la experiencia requerida podría acreditarse mediante la prestación previa de servicios de SOC, con independencia de la ubicación física del centro, siempre que se demuestre el cumplimiento de los requisitos técnicos, normativos, contractuales y de control exigidos por la DIAN	Eliminar el requerimiento	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, tal como se indica en el requerimiento, el futuro proveedor de SOC puede entregar dos Centros de Operaciones en la ciudad de Bogotá u optar por tener uno en la Ciudad de Bogotá y otro en otra locación diferente a esta ciudad, aclarando que lo que se requiere es que el SOC (Personal, Infraestructura Física y Técnica, entre otros) esté en la Ciudad de Bogotá, más no el centro de datos que soporta dicha operación, en el entendido de que muchos SOC´s tienen su operación en la nube o en un centro de datos de terceros, dicho requerimiento obedece a necesidades propias de la Entidad, por lo tanto no se acepta su sugerencia.
217	Sección II - 11.j	Formal	N/A	Para oferentes que son APCA con un extranjero, ¿qué documentos equivalentes se consideran válidos para acreditar existencia legal, representación y facultades del firmante, y si estos deben venir apostillados o legalizados?	N/A	En el caso de oferentes extranjeros, se podrán presentar documentos equivalentes a los certificados de existencia y representación legal o registro mercantil, expedidos por la autoridad competente en el país de origen, siempre que permitan verificar, como mínimo, la constitución de la firma, su vigencia, objeto social, así como las facultades de representación del firmante. . Si hay documentos emitidos en el extranjero que acompañen la oferta no requieren ser apostillados. Si están en otro idioma pueden ser presentados en traducción simple al español. En caso de adjudicación, se podrán solicitar documentos apostillados.
218	Sección II - 14.6	Formal	Los precios cotizados corresponderán al menos al 100% de los servicios especificados. Es decir, los precios deberán incluir honorarios, gastos de viaje, logística para la movilización, uso de equipamiento y software, gastos de comunicación, combustible, impresiones, impuestos y en general todos los costos directos e indirectos, gastos administrativos, así como cualquier otro gasto o impuesto que sea necesario para la implementación de la totalidad de los servicios de no consultoría requeridos	¿La Entidad puede confirmar si el precio total ofertado debe contemplar exclusivamente los costos asociados al alcance definido en el Anexo Técnico, sin considerar ampliaciones futuras o servicios adicionales no explícitamente solicitados?	Hacer la claridad dentro del la sección de ser necesario.	De acuerdo con la CGC 15.1 se establece que el valor estimado del proceso ha sido establecido en el entendido de que incluye el IVA y todos los costos y utilidades, así como cualquier obligación tributaria a que esté sujeto el Contratista al momento de suscribir el contrato. Es decir, el valor incluye todos los costos asociados al proyecto especificado en la Solicitud de Oferta. La proyección de estos costos debe tener en cuenta en los valores a 2028.
219	1.1	Formal	La Dian requiere adquirir, instalar, configurar....	¿El modelo final es licencia perpetua + soporte, suscripción, o modelo híbrido? ¿Qué sucede con las licencias SaaS que no pueden transferirse legalmente (ej. TI feeds, UEBA cloud, reputación IP, sandboxing cloud)?	Ajustar con base a la respuesta	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el requerimiento es claro en el sentido que menciona "para los casos donde aplique", es claro que si el ofrecimiento del proveedor del SOC no los contempla o presenta otro tipo de servicio o licenciamiento, no tendría que entregar licenciamiento alguno.
220	1.2	Formal	Se debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá...	Es posible que DIAN informe un Límite cuantitativo (activos actuales vs futuros), por posibles cambios de alcance por crecimiento orgánico (nuevas sedes, proyectos TI, nube). ¿Se exigen certificaciones físicas (TIA-942, ISO 22301, etc.)?	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, tal como se indica en el requerimiento, el futuro proveedor de SOC puede entregar dos Centros de Operaciones en la ciudad de Bogotá u optar por tener uno en la Ciudad de Bogotá y otro en otra locación diferente a esta ciudad, tal como se indica en el respectivo numeral, por lo tanto, es claro que el centro de operaciones de seguridad (personal, monitoreo, operación, locación física, entre otros), debe estar en la ciudad de Bogotá.
221	1.3	Formal	...el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra..	¿Quién asume riesgos de obsolescencia o límites de soporte extendido?	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el SIEM de la Entidad al que hace referencia este ítem cuenta con soporte, garantía, derecho a uso, actualizaciones por parte del fabricante hasta la fecha especificada, por ende no habría riesgos de obsolescencia.
222	4.35	Formal	Contar con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de estas.	¿Este servicio se refiere a feeds/documentación del fabricante o a un servicio humano especializado?	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, es una característica propia de la herramienta, capacidad o servicio requerido, se aclara que las herramientas modernas de gestión de vulnerabilidades integran servicios de investigación e inteligencia de amenazas (Threat Intelligence) para identificar, priorizar y corregir debilidades en tiempo real. Combinan escaneo, análisis de riesgos y fuentes externas para prever cómo los atacantes podrían explotar fallos
223	6.5.7	Formal	La solución debe poder crear señuelos para ambientes OT (Tecnología Operacional) y para redes SCADA (PLC, HMI, Sensores IoT, entre otros).	¿Puede confirmarse si actualmente la DIAN cuenta con entornos OT o SCADA que deban ser cubiertos?¿Cuántos hay o se tiene proyectados tener?	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, actualmente no se cuenta con entornos OT, la característica se solicita para futuros proyectos, sin embargo, se aclara que el servicio solicitado debe cumplir con esta característica.

224	7.14	Formal	Capacidad de realizar consultas a los datos capturados y almacenados en el hardware de uso específico (appliance) sin conectarse a la nube, como mínimo se debe tener un tiempo de retención de seis (6) meses.	¿Puede la Entidad suministrar una estimación de tráfico agregado para dimensionar el almacenamiento requerido?	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el futuro proveedor debe estar en la capacidad de realizar las estimaciones necesarias con base en los datos dados por la Entidad, en este caso 25000 usuarios o activos, y una retención de seis meses.
225	9.7	Formal	La herramienta/servicio debe realizar la creación y gestión de casos para seguir el progreso de las acciones tomadas contra infractores, incluidas las comunicaciones legales, las medidas de cumplimiento y las soluciones	¿La gestión de casos se limita al seguimiento técnico y documental sin acciones de representación legal directas?	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, su entendimiento es correcto.
226	11.18	Formal	Todas las plataformas y soluciones entregadas deberán ser de propósito específico, no se aceptan soluciones genéricas.	Muchas plataformas modernas son XDR/XSIAM/CNAPP, por lo tanto podrían estar excluidas. ¿Se aceptan plataformas multipropósito siempre que cumplan funcionalmente el propósito requerido?	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el requerimiento es claro en el sentido que menciona que deben ser plataformas, soluciones o servicios de propósito específico, lo cual obedece a necesidades propias de la Entidad.
227	12.7	Formal	Controles: El servicio de SOC ofrecido debe contemplar también el monitoreo de los siguientes controles tecnológicos pertenecientes al SGSI de la Entidad: ….	¿El monitoreo de controles se limita a evidencias técnicas y no a auditoría formal de cumplimiento?	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el requerimiento hace mención a seguimiento de los controles mediante evidencias técnicas ofrecidas con los servicios del SOC solicitados.
228	12.81	Formal	Se deberá prestar el servicio de acompañamiento, asesoramiento, generación de planes de remediación entre otros para la solución de todas las vulnerabilidades e incidentes encontrados durante el tiempo que dure el contrato, para lo cual deberá contar con personal en sitio (mínimo un Ingeniero) en el horario laboral entre semana (8x5) y si por alguna circunstancia fortuita o de acuerdo a la necesidad de la DIAN (bajo demanda de la Entidad), se podrán coordinar sesiones en horario no hábil.	¿El ingeniero en sitio está considerado dentro del requerimiento de equipo mínimo de trabajo requerido o es un recurso complementario?	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, el perfil solicitado para este ítem está incluido en el equipo mínimo de trabajo.
229	Equipo Mínimo de Trabajo	Formal	Especialista de Respuesta a Incidentes (IR)|| Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Seguridad Informática Certificaciones vigentes: •ITIL V3 o superior.|| Mínimo cinco (5) años de experiencia profesional en proyectos de tecnologías de la información de los cuales tres (3) años con participación en proyectos de seguridad de la información, plan de recuperación de desastres o continuidad de negocio, demostrados en al menos dos(2) proyectos de esta naturaleza. NOTA: Este perfil debe estar en sitio de la Entidad Sede Ministerio de Hacienda, trabajando en una disponibilidad de 8 x 5, con los conocimientos necesarios y suficientes en las plataformas, servicios, y capacidades entregadas e implementadas. Debe estar en la sede principal de la DIAN Bogotá, para realizar el acompañamiento y asesoramiento frente al tema de las remediaciones a las posibles vulnerabilidades encontradas en el monitoreo y las demás halladas en las actividades que hacen parte de este anexo técnico.	De manera atenta y en ejercicio del principio de planeación y eficiencia que rige la contratación estatal, solicitamos a la Entidad reconsiderar la exigencia contenida en la NOTA del perfil "Especialista de Respuesta a Incidentes (IR)", específicamente la disponibilidad presencial 8x5 en la sede indicada. La naturaleza de la respuesta a incidentes de seguridad —especialmente ante eventos de alta criticidad— requiere capacidades operativas y de decisión que se consolidan mediante la atención continua y recurrente de incidentes de alto impacto en distintos entornos y para múltiples clientes, lo cual permite mantener vigentes las competencias técnicas, tácticas y metodológicas del recurso. En ese sentido, exigir un esquema 8x5 en sitio no agrega valor proporcional al objetivo del servicio, pues limita la exposición del especialista a escenarios reales de crisis y reduce la efectividad esperada en contención, erradicación y recuperación. Por el contrario, una capacidad de IR efectiva se sustenta en un equipo especializado con cobertura extendida (24x7 o bajo demanda según severidad), con disponibilidad de desplazamiento y presencia en sitio cuando la criticidad del evento o la fase de respuesta así lo requiera, sin restringir indebidamente el modelo de prestación del servicio. En consecuencia, solicitamos se ajuste la redacción de la NOTA para que el requisito se enfoque en resultados y niveles de servicio (tiempos de atención, escalamiento, intervención y acompañamiento), en lugar de imponer una presencialidad fija 8x5, garantizando así la idoneidad y el valor agregado del componente de respuesta a incidentes.	Sugerimos retirar este perfil del pliego de condiciones, en tanto la función de Respuesta a Incidentes (IR) no se materializa como una actividad de acompañamiento presencial 8x5, sino como una capacidad especializada que debe activarse y operar conforme a la criticidad y ocurrencia real de incidentes. En caso de requerirse soporte a remediaciones de vulnerabilidades, éste puede cubrirse mediante un perfil de Gestión de Vulnerabilidades/Seguridad Operativa, o mediante el equipo SOC, con SLAs definidos. Alternativamente, si la Entidad considera indispensable mantener la capacidad IR, recomendamos reemplazar el requisito por: "La capacidad de Respuesta a Incidentes (IR) será provista por un equipo especializado con cobertura 24x7 (o bajo demanda conforme a la severidad), asegurando tiempos máximos de atención y escalamiento. La presencia en sitio en Bogotá se realizará únicamente cuando el incidente sea crítico o cuando la fase de contención/erradicación/recuperación lo requiera, según coordinación con la Entidad."	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los perfiles solicitados obedecen a necesidades especificas de la Entidad, acorde a su misionalidad, por lo tanto, no se acepta su observación.
230	Equipo Mínimo de Trabajo	Formal	Tres (03) Analistas SOC Nivel I Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 2 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: -Cédula de Ciudadanía -Tarjeta Profesional -Certificación vigente como analista o profesional o especialista o arquitecto en seguridad de operaciones o su equivalente en las soluciones ofertadas (SIEM, SOAR, caza de amenazas o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. - Certificación en Plataformas de Gestión de la Superficie de Ataque. - Certificaciones de experiencia mínima de dos (2) años en implementación y/o soporte y/o administración de soluciones de seguridad. NOTA: Estos tres perfiles (analista I) deben cumplir los ANS de 7x24x365	De manera respetuosa, solicitamos a la Entidad revisar la suficiencia del requerimiento asociado a "Tres (03) Analistas SOC Nivel I" para el cumplimiento de ANS 7x24x365. En la práctica, una cobertura continua (24 horas, 7 días, 365 días) exige un esquema de turnos, relevos, tiempos de descanso, capacitaciones, contingencias, ausencias y vacaciones que hace materialmente inviable garantizar la prestación ininterrumpida del servicio con únicamente tres (3) recursos. En consecuencia, el requerimiento, tal como está redactado, puede generar un riesgo de incumplimiento de los ANS y de afectación a la continuidad operativa del SOC. Por ello, resulta más idóneo que el pliego exija la "atención" 7x24x365 bajo niveles de servicio verificables (tiempos de respuesta, escalamiento y resolución), en lugar de limitar la obligación a un número fijo de perfiles.	Sugerimos ajustar el requisito para que se solicite la prestación del servicio SOC Nivel I 7x24x365 (atención continua) con ANS definidos, dejando a cargo del Contratista la asignación de la capacidad humana necesaria para cumplirlos. Redacción sugerida: "El Contratista deberá garantizar la atención del SOC Nivel I en modalidad 7x24x365, cumpliendo los ANS establecidos. Para tal efecto, deberá presentar y mantener un plan de operación que incluya turnos, número de analistas por turno, esquema de relevos y personal de respaldo, asegurando continuidad del servicio ante ausencias, vacaciones y contingencias. La Entidad evaluará el cumplimiento por resultados y ANS, no por la asignación de un número fijo de (3) perfiles."	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los perfiles solicitados obedecen a necesidades especificas de la Entidad, acorde a su misionalidad, por lo tanto, no se acepta su observación.
231	Equipo Mínimo de Trabajo	Formal	**Un (01) Analista SOC Nivel II** Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 3 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: -Cédula de Ciudadanía -Tarjeta Profesional -Certificación vigente como analista o profesional o especialista o arquitecto en seguridad de redes o su equivalente en las soluciones ofertadas (SIEM o SOAR o Caza de Amenazas o NDR o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. - Certificación en Plataformas Gestión de la Superficie de Ataque. - Certificaciones de experiencia mínima de tres (3) años en implementación y/o soporte y/o administración de soluciones de seguridad.	De manera respetuosa, solicitamos a la Entidad revisar la suficiencia del requerimiento de "Un (01) Analista SOC Nivel II" para atender la demanda operativa y técnica de un Centro de Operaciones de Seguridad (SOC) con las capacidades y el nivel de criticidad descritos en el Anexo Técnico. En la práctica, el Nivel II asume funciones de análisis avanzado, correlación y priorización de eventos, triage de alertas escaladas desde Nivel I, validación de falsos positivos, coordinación de contención con áreas técnicas y escalamiento hacia fabricantes/terceros; actividades que, por su naturaleza, se presentan de forma concurrente y no se restringen a un horario determinado. En ese orden, la asignación de un único recurso para dicho rol incrementa el riesgo de cuellos de botella, acumulación de casos, demoras en escalamiento y afectación del cumplimiento de ANS, especialmente en picos de alertamiento, incidentes simultáneos o ventanas de mantenimiento. Por lo anterior, estimamos que el requisito, tal como está planteado, podría resultar insuficiente para garantizar continuidad y oportunidad en la operación del SOC.	Sugerimos ajustar el pliego para exigir la "capacidad de atención" del Nivel II (cobertura y oportunidad) mediante ANS verificables (tiempos máximos de análisis, validación, escalamiento y soporte a contención), dejando al Contratista la responsabilidad de dimensionar el número de recursos necesarios (incluyendo esquema de turnos, relevos y respaldo). En caso de mantenerse la definición por perfiles mínimos, se recomienda considerar al menos dos (2) Analistas SOC Nivel II (o un esquema equivalente de cobertura) que permita continuidad operativa, manejo de simultaneidad y reemplazos por ausencias/vacaciones, sin afectar los ANS del servicio.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los perfiles solicitados obedecen a necesidades especificas de la Entidad, acorde a su misionalidad, por lo tanto, no se acepta su observación.
232	Equipo Mínimo de Trabajo	Formal	**Un (01) Analista SOC Nivel III** Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 5 años a partir de la emisión de la Tarjeta Profesional: -Cédula de Ciudadanía -Tarjeta Profesional - Postgrado en seguridad informática. -Certificación vigente como analista o profesional o arquitecto en seguridad de redes o su equivalente en las soluciones ofertadas (SIEM, SOAR, Caza de Amenazas, NDR o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. -Certificación en gestión o administración de plataformas de seguridad informática. Certificaciones de experiencia mínima de 5 años en implementar y/o soportar y/o administrar soluciones de seguridad.	De manera respetuosa, solicitamos a la Entidad revisar la suficiencia del requerimiento de "Un (01) Analista SOC Nivel III" para atender la demanda operativa y estratégica de un Centro de Operaciones de Seguridad (SOC) con el alcance, criticidad y volumen de eventos que se infiere del Anexo Técnico. El rol de Nivel III, por su naturaleza, concentra responsabilidades de mayor complejidad y decisión (análisis especializado, dirección técnica de la investigación, coordinación de respuesta avanzada, definición de cursos de acción, apoyo a contención/erradicación, y articulación con fabricantes/terceros), las cuales suelen presentarse de forma simultánea y en ventanas no restringidas a horario. En ese sentido, la asignación de un único recurso para dicho rol incrementa el riesgo de indisponibilidad, dependencia crítica, retrasos en escalamiento, fatiga operativa y afectación del cumplimiento de ANS, especialmente ante incidentes concurrentes o picos de alertamiento. Por lo anterior, consideramos que el requisito, tal como se encuentra formulado, puede resultar insuficiente para garantizar oportunidad, continuidad y calidad técnica en la operación del SOC.	Sugerimos ajustar el pliego para exigir la "capacidad de atención" del Nivel III mediante ANS verificables (p. ej., tiempos máximos de escalamiento, análisis especializado, dirección técnica de la investigación y apoyo a contención), dejando al Contratista la obligación de dimensionar y sostener los recursos necesarios (incluyendo turnos/guardias, relevos y personal de respaldo) para asegurar continuidad. En caso de mantenerse la definición por perfiles mínimos, recomendamos considerar al menos dos (2) Analistas SOC Nivel III (o un esquema equivalente de cobertura, como guardias rotativas con respaldo), que permita atender simultaneidad, asegurar reemplazos por ausencias/vacaciones y mitigar el riesgo de dependencia de una sola persona, sin comprometer los ANS del servicio.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los perfiles solicitados obedecen a necesidades especificas de la Entidad, acorde a su misionalidad, por lo tanto, no se acepta su observación.

233	1.2	Formal	Tener en cuenta que desde el inicio del contrato se deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 nuevo SIEM (solicitado en el ítem 2) que hace parte integral de este proyecto por el tiempo solicitado (Tres años) con licenciamiento soporte, garantía y derecho a uso hasta agosto 31 de 2030.	Durante el periodo de coexistencia entre QRadar (IBM) y el nuevo SIEM, ¿se espera un equipo mayor de trabajo? Debido a que van a haber tareas de gestión, administración y operación del SIEM actual, y en paralelo se deben realizar trabajos de migración al nuevo SIEM	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, para la implementación, gestión, operación, soporte, administración y demás actividades propias del SOC se requiere un equipo mínimo de trabajo al futuro proveedor, si para cumplir con dichas actividades el proveedor del SOC requiere adicionar personal al mínimo exigido, lo puede hacer siempre y cuando no implique costos adicionales para la Entidad.
234	2.7	Formal	Debe manejar tasa de retención de doce (12) meses en línea y doce (12) meses fuera de línea.	¿la infraestructura de almacenamiento debe ser provista en su totalidad por el contratista o la DIAN suministrará recursos?	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la infraestructura de almacenamiento la debe proveer en su totalidad el contratista del SOC.
235	2.30	Formal	Para tal efecto se informa que actualmente la Entidad cuenta con un ITSM del fabricante ARANDA.	1. Favor especificar la versión actual de Aranda para que el proveedor evalué la compatibilidad. 2. ¿Aranda actualmente es la CMDB de la DIAN y la nueva herramienta del proveedor la reemplazará o serán un complemento el uno del otro?	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el servicio de correlación de eventos (SIEM) deberá integrarse con el ITSM ARANDA de la Entidad.
236	VII	Formal		Solicitamos amablemente a la entidad informarnos el licenciamiento actual del siem qradar con el que cuentan actualmente, en donde se especifique: -Cantidad de EPs (eventos por segundo) o Gb/day -cantidad licenciamiento UEBA (Solo si aplica) -cantidad licenciamiento FIM (Solo si aplica) -retención en caliente -retención en frio		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, las características de la plataforma SIEM de la Entidad: Qradar Licenciado: 110K flujos por minuto 25K eventos por segundo Versión desplegada 7.5.0 UpdatePackage 14 (Build 20251017194912) Retención: 30 días en caliente y 1.3 años en frio
237	2.9	Formal		Solicitamos amablemente a la entidad confirmarnos si es responsabilidad del contratista prestar el servicio de NOC desde la herramienta ORION o se deberá contemplar alguna herramienta adicional.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclarar que el servicio de NOC es operado por la Entidad, de ser necesario y de acuerdo a la arquitectura de la solución planteada deben tenerse en cuenta estas interacciones.
238	2.9	Formal		Es de nuestro entendimiento que el licenciamiento de la herramienta ORION es responsabilidad de la DIAN, agradecemos confirmar si nuestro entendimiento es correcto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclarar que el servicio de NOC es operado por la Entidad, por lo tanto es responsabilidad de la DIAN este licenciamiento
239	5.4.8	Formal		Solicitamos amablemente a la entidad confirmarnos si al referirse a "Protección de la infraestructura" se refiere a una solución que cumpla el principio de CNAPP (Cloud native application protection platform) que combine herramientas como CSPM, CWPP y CIEM, de ser así, agradecemos nos confirmen que la cantidad de activos en nube (ejemplo: cargas de trabajo, aplicaciones, servicios, otros), tipo de activos (repositorios, infraestructura como código) y nubes donde se encuentren.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el plan solicitado debe cumplir con los requerimientos mínimos solicitados en este ítem, el futuro contratista deberá tenerlos en cuenta, y desde allí diseñar su propuesta con los respectivos valores agregados de acuerdo a la experticia y expertiz del interesado.
240	5.3.2	Formal		Solicitamos amablemente a la entidad por favor especificar de los 2467 activos cuantos son servidores o máquinas virtuales.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el inventario requerido se encuentra detallado en el archivo Solicitud de Oferta - SDO del presente proceso.
241	5.4.19	Formal		Se solicita amablemente a la entidad que se permita la implementación y despliegue de las soluciones ofertadas pueda ser ejecutada por partners autorizados o certificados por el fabricante, siempre que estos acrediten experiencia comprobada en proyectos de implementación de la misma naturaleza. Lo anterior, considerando que dichos partners cuentan con capacidades técnicas, metodologías y recursos especializados que garantizan una adecuada puesta en marcha de la solución. De manera alternativa, en caso de mantenerse la necesidad de participación del fabricante, se solicita que se habilite un esquema en el cual el partner realice la implementación y, posteriormente, el fabricante ejecute un ejercicio de aseguramiento de calidad (QA), validación o revisión post-despliegue, con el fin de verificar que la solución haya sido implementada conforme a las mejores prácticas y lineamientos técnicos definidos.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica que, la solución o servicio debe ser implementada por el proveedor del SOC y apoyado por el fabricante del servicio o solución.
242	5.5.1	Formal		Solicitamos amablemente a la entidad confirmarnos cuanto tiempo (tiempo en meses) desean retener la información almacenada.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara que para la Gestión y Monitoreo de Vulnerabilidades, en concordancia con los demás requerimientos debe ser de 6 meses
243	5.7.3	Formal		Con el objetivo de tener un alcance preciso en el modo de implementación, tiempos y recursos para este despliegue, solicitamos amablemente a la entidad confirmarnos si la solución deberá estar en nube del fabricante o en maquina virtual o si se debe contemplar las dos opciones iniciando por nube del fabricante y guardando el recurso de una posible migración en el tiempo a máquina virtual.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se debe cumplir con lo requerido, para este ítem 5.7.3 la necesidad es muy clara: La solución debe admitir múltiples motores de escaneo distribuidos geográficamente y administrados por una consola central. En el caso de que la DIAN requiera desplegar el servicio de escaneo de manera local para reducir el impacto a nivel de red, la solución debe permitir dicho despliegue mediante una máquina virtual o agentes que reporten a la consola central.
244	5.11.3-5.11.4-5.11.5	Formal		Es de nuestro entendimiento que la entidad requiere únicamente gestión de vulnerabilidades y no protección tipo CNAPP, agradecemos a la entidad confirmarnos si es correcto nuestro entendimiento.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento es muy claro a que se debe trabajar bajo arquitectura CNAPP: La solución ofertada deberá Gestionar las Vulnerabilidades de todas las cargas de trabajo (CWPP), Gobierno y Cumplimiento de la infraestructura nube (CSPM), Gobierno de Identidades (CIEM), Análisis e Identificación de Comportamiento Malicioso (CDR), Postura de Seguridad de los Datos (DSPM) y Gobierno de Infraestructura como Código (IaC / DevSecOps) de la entidad, bajo una arquitectura CNAPP; provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades y hacer parte de una plataforma de gestión de ciberexposición.
245	6.4.12	Formal		Solicitamos amablemente a la entidad informarnos de que fabricante es el firewall.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que en la actualidad cuenta con Firewall marca Paloalto
246	5.12.1	Formal		Se solicita amablemente a la entidad permitir el cumplimiento del requerimiento mediante mecanismos agentless o semi-agentless, incluyendo el uso de sensores, conectores, collectors o agentes livianos instalados únicamente sobre componentes críticos o servidores de soporte del entorno, siempre que no se requiera un despliegue masivo en toda la infraestructura y que la solución garantice auditoría, visibilidad y gestión de la postura de seguridad del Directorio Activo.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se debe cumplir con lo exigido en el requerimiento, por lo tanto, no se acepta su sugerencia.
247	5.12.3	Formal		Se solicita aceptar soluciones que provean monitoreo de seguridad del Directorio Activo en modalidad continua, cuasi continua o por ciclos automáticos programados de alta frecuencia, siempre que permitan identificar exposiciones, detectar técnicas de ataque relevantes, emitir alertas, generar recomendaciones de remediación y evidenciar rutas de escalamiento o caminos de ataque hacia objetos críticos, aun cuando algunas analíticas avanzadas dependan de correlación, enriquecimiento o evaluaciones periódicas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se debe cumplir con lo exigido en el requerimiento, por lo tanto, no se acepta su sugerencia.
248	5.12.6	Formal		Solicitamos amablemente a la entidad informarnos cuales son los antivirus específicos para los que se requiere auditoria de paquetes.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara que en la actualidad cuenta con la solución de antivirus Bitdefender.
249	6.4.2	Formal		Solicitamos amablemente a la entidad confirmarnos la cantidad de señuelos tipo máquina virtual con sistema operativo Windows y office.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara que esta definición es parte de la solución que se debe ofrecer de acuerdo con el conocimiento técnico ,experiencia y habilidades del proponente para que se ajuste a las necesidades de la entidad, por lo tanto, es valido ofrecer soluciones o servicios equivalentes o similares siempre y cuando se cumpla con las características técnicas mínimas solicitadas en los documentos del proyecto.
250	9.1-9.2-9.3	Formal		Solicitamos amablemente a la entidad confirmarnos de los 260 activos cuantos son dominios y subdominios.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que los activos a monitorear corresponden a los activos que exponen servicios de la marca DIAN bajo el dominio DIAN y sus subdominios que afecten su reputación digital
251	11.4	Formal		Es de nuestro entendimiento que la entidad suministrará energía, conexiones a internet.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el contrato es bajo la modalidad llave en mano, por lo cual el oferente deberá suministrar, instalar y poner en operación todos los elementos requeridos para la implementación de la solución, incluyendo infraestructura, hardware, software, racks, cableado y demás recursos necesarios. No obstante lo anterior, se entiende que la Entidad dispondrá de los servicios básicos de infraestructura en sus sedes, particularmente suministro de energía eléctrica y conectividad a Internet, los cuales estarán disponibles para la correcta operación de la solución implementada.
252	8.16-8.17-8.19-8.20-8.21	Formal		Se solicita amablemente a la entidad ajustar la especificación técnica para que la evaluación de la solución se realice con base en capacidades funcionales equivalentes y no en la coincidencia exacta de nombres comerciales de módulos, componentes o flujos de gestión propios de un fabricante en particular. En ese sentido, se solicita aceptar soluciones SaaS de seguridad de aplicaciones que integren SAST, DAST, SCA/OSS, gestión de SBOM, detección de secretos, panel unificado de hallazgos, priorización de riesgos, integraciones CI/CD, API y capacidades de gestión y seguimiento de vulnerabilidades, aun cuando dichas funcionalidades se presenten bajo una arquitectura, nomenclatura o flujo operativo diferente al descrito en el pliego. Lo anterior garantizaría pluralidad de oferentes y permitiría la participación de otros fabricantes, cuya cobertura funcional atiende el objetivo técnico requerido, aunque no utilice exactamente los mismos nombres de módulos o estados de vulnerabilidad allí indicados.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem solicita o requiere una solución de análisis de código estático y dinámico para aplicaciones o su equivalente, por lo tanto, es valido ofrecer soluciones o servicios equivalentes o similares siempre y cuando se cumpla con las características técnicas mínimas solicitadas en los documentos del proyecto.

253	7.1-7.2-7.3	Formal		Solicitamos amablemente a la entidad confirmarnos el throughtput que se desea monitorear y que abarca el total de los activos esperados por la entidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, lo requerido en este ítem es muy claro: *"Se debe licenciar como mínimo para 25000 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web)",* y esta información permite a los interesados dimensionar su ofrecimiento.
254	VII	Formal		Se solicita amablemente a la Entidad incorporar dentro de los requisitos técnicos o criterios de evaluación que la solución SIEM ofertada haya sido reconocida en la categoría de Líder en el Gartner Magic Quadrant for Security Information and Event Management 2025, en The Forrester Wave™: Security Analytics Platforms, Q2 2025, y en el IDC MarketScape: Worldwide SIEM for Enterprise 2024 Vendor Assessment. Lo anterior permitiría asegurar que la plataforma propuesta cuente con un nivel de madurez, capacidad de ejecución, visión estratégica, robustez funcional y posicionamiento de mercado validados de manera consistente por firmas analistas internacionales de amplio reconocimiento. La solicitud se fundamenta en que Gartner Magic Quadrant evalúa y posiciona proveedores con base en su Ability to Execute y Completeness of Vision; Forrester Wave se define como una guía de compra con comparativos detallados entre proveedores para apoyar decisiones de selección; e IDC MarketScape utiliza una metodología de valoración cuantitativa y cualitativa sobre capacidades y estrategia de los fabricantes. En una contratación crítica como la de un SIEM, exigir presencia consistente en esos estudios reduce el riesgo tecnológico y de ejecución, fortalece la probabilidad de adquirir una solución con mayor estabilidad, innovación, soporte, escalabilidad y continuidad de hoja de ruta, y aporta un criterio objetivo adicional para la selección de una plataforma estratégica para la operación del SOC.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, los requerimientos hechos por la Entidad para el presente proceso se consideran amplios y suficientes, por lo tanto, no se acepta su sugerencia.
255	VII	Formal		Solicitamos amablemente a la entidad incorporar dentro de los requisitos técnicos habilitantes que la solución SOAR ofertada se encuentre clasificada como Líder en el informe SPARK Matrix™: Security Orchestration, Automation and Response (SOAR), Q1 2025, emitido por QKS Group. Lo anterior permitiría asegurar que la plataforma propuesta haya sido evaluada y reconocida por una firma analista especializada bajo criterios objetivos de mercado y capacidades tecnológicas. Esta solicitud se justifica en que el marco SPARK Matrix™ de QKS Group evalúa a los fabricantes con base en dos dimensiones clave: Technology Excellence y Customer Impact. Adicionalmente, QKS Group indica que su metodología considera fuentes primarias como sesiones con analistas, RFI, demostraciones de producto y encuestas estructuradas a clientes, así como investigación secundaria y base de conocimiento propia, y precisa además que la inclusión en el análisis no depende de la participación o consentimiento del fabricante. En ese sentido, exigir que la solución se encuentre en la categoría de Líder permite a la entidad orientar el proceso hacia plataformas con un nivel comprobado de madurez, robustez funcional, posicionamiento competitivo y validación en el mercado, reduciendo el riesgo técnico en la selección de una herramienta crítica para la automatización y orquestación de la operación de ciberseguridad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, los requerimientos hechos por la Entidad para el presente proceso se consideran amplios y suficientes, por lo tanto, no se acepta su sugerencia.
256	VII	Formal		Entendemos que toda solución propuesta debe contar con tres (3) años de soporte y licenciamiento, y que dentro de dicho periodo de licenciamiento se encuentra contemplado el tiempo de implementación. Agradecemos, por favor, nos informen si nuestro entendimiento es correcto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, el tiempo de implementación no esta inmerso dentro de los tres años de soporte y licenciamiento, estos tiempos contarán a partir de la puesta en operación de cada una de las capacidades requeridas, por lo tanto, su entendimiento no es correcto. Aclarando que la operación, seguimiento, gestión, monitoreo y administración (con el equipo y/o perfiles de trabajo solicitados) por parte del futuro proveedor de todos los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho a uso, licenciamiento, suscripciones, actualizaciones, soporte y garantía irá por tres (3) años y sus periodos se contabilizarán a partir de la puesta en operación de cada uno de los servicios requeridos, incluyendo lo siguiente: Tener en cuenta que desde el inicio del contrato se deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 nuevo SIEM (solicitado en el ítem 2) que hace parte integral de este proyecto por el tiempo solicitado (Tres años) con licenciamiento soporte, garantía y derecho a uso hasta agosto 31 de 2030. La protección de bases de datos (Firewall de bases de datos) irá a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031. El futuro contratista deberá, recibir, gestionar, administrar y operar desde el inicio del contrato el actual firewall de bases de datos propiedad de la DIAN del fabricante IBM Referencia GUARDIUM hasta diciembre 31 de 2027 tiempo en el que termina el soporte de este dispositivo por parte del fabricante, una vez esto ocurra deberá implementar el nuevo firewall de bases de datos solicitado en las capacidades requeridas por la DIAN. Para la capacidad de NDR se deberá tener en cuenta que este comenzará a operar a partir de enero de 2028 previamente autorización de la DIAN, para lo cual deberá implementar, administrar, operar, soportar y garantizar el servicio mencionado, con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031.
257	VII	Formal		Se solicita amablemente a la entidad ajustar la especificación técnica para que la evaluación de la solución de protección de bases de datos se realice con base en el cumplimiento funcional sobre el inventario real de bases de datos de la Entidad y no sobre la coincidencia literal de la totalidad de motores, métodos de despliegue o capacidades accesorias descritas en el pliego. En ese sentido, se solicita aceptar soluciones DAM que ofrezcan monitoreo y auditoría de actividad en tiempo real, correlación de eventos, análisis de vulnerabilidades, políticas de alerta y bloqueo, virtual patching, soporte de despliegue con o sin agentes, administración centralizada, trazabilidad forense e integración con otras herramientas de seguridad, siempre que el proponente garantice cobertura efectiva sobre las plataformas de bases de datos que conforman el ambiente de la Entidad y acredite dicha compatibilidad mediante fichas técnicas, matriz de soporte del fabricante y compromiso formal de implementación. Lo anterior promovería la pluralidad de oferentes y permitiría la participación de otros fabricantes, cuya arquitectura y alcance funcional atienden el objetivo de protección, monitoreo y control de bases de datos requerido, aun cuando la solución no coincida de manera exacta con cada uno de los componentes o plataformas listadas de forma taxativa en la especificación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la solución a entregar debe cumplir los requerimientos técnicos a través de herramientas con características similares o superiores siempre y cuando se cumpla con los requerimientos.
258	VII	Formal		En relación a: Especificaciones Técnicas herramienta de protección de Bases de Datos, solicitamos amablemente a la entidad confirmarnos: - Cantidad de base de datos - Cantidad de instancias - Tipo y versión de cada base datos.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la información requerida se encuentra en los documentos del proceso en la sección de inventario. Adicionalmente la entidad entregará con mayor nivel de detalle técnico los inventarios y activos de información a tener en cuenta en este proceso
259	VII	Formal		Solicitamos amablemente a la Entidad incluir dentro de los requisitos habilitantes o técnicos del proceso que el SOC del proponente cuente con certificación vigente ISO/IEC 27001:2022, y que dicha certificación sea presentada como parte de la oferta, expedida por un organismo de certificación acreditado. Lo anterior, con el fin de asegurar que la operación del servicio se encuentra soportada en un Sistema de Gestión de Seguridad de la Información formalmente implementado, auditado y alineado con buenas prácticas internacionales, garantizando así mayores niveles de confidencialidad, integridad, disponibilidad, gestión de riesgos, control operativo y mejora continua en la prestación del servicio.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que en la Sección III numeral 2 2. Estrategia de implementación páginas 58 y 59 del documento des solitud de Oferta /SDO , se le asigna puntaje a proponente que presente certificaciones vigentes de certificaciones internacionales y reconocidas de SOC relevantes entre las que se tienen ISO 27001:2022, ISO 22301:2019 o superior, entre otras.

260	VII	Formal	<table><tr><th>No.</th><th>Indicador</th><th>Fórmula de cálculo</th><th>Valor del indicador</th></tr><tr><td>1</td><td>Índice de liquidez</td><td>Activo corriente/Pasivo corriente</td><td>Mayor o igual a 1</td></tr><tr><td>2</td><td>Razón de endeudamiento</td><td>Pasivo total / Activo total</td><td>Menor o igual a 0,6</td></tr><tr><td>3</td><td>Patrimonio en relación al presupuesto estimado del proceso</td><td>Patrimonio/ Presupuesto estimado</td><td>Mayor o igual a 0,1</td></tr><tr><td>4</td><td>Capital de trabajo en relación al presupuesto estimado del proceso</td><td>(Activo Corriente - Pasivo Corriente) /Presupuesto estimado</td><td>Mayor o igual a 0,05</td></tr><tr><td>5</td><td>Apalancamiento a corto plazo</td><td>Pasivo Corriente/Patrimonio</td><td>Menor o igual a 0,5</td></tr></table>	Respetuosamente, solicitamos a la entidad considerar la modificación del indicador de endeudamiento establecido en el pliego de condiciones, proponiendo que este sea ajustado a un valor de **menor o igual al 0,69.** La presente solicitud se fundamenta en los principios de la contratación estatal consagrados en la Ley 80 de 1993 y la Ley 1150 de 2007, particularmente en lo relacionado con la pluralidad de oferentes, la libre concurrencia y la selección objetiva, los cuales buscan garantizar la participación amplia y equitativa de proponentes idóneos. Si bien el indicador de endeudamiento es un mecanismo válido para medir la capacidad de una organización para responder por sus obligaciones financieras, es importante señalar que un nivel de endeudamiento superior no necesariamente representa un riesgo financiero, especialmente en sectores como el de tecnología. En este sector, es habitual mantener niveles de endeudamiento más altos debido a las inversiones constantes en investigación, desarrollo e innovación, necesarias para asegurar la competitividad y sostenibilidad de las compañías. En este sentido, el análisis financiero debe contemplar no solo el nivel de endeudamiento, sino también la capacidad de generación de ingresos, flujo de caja y rentabilidad de los proyectos financiados. En nuestro caso particular, el endeudamiento responde a estrategias de crecimiento y ejecución de proyectos con alto potencial de retorno, los cuales generan ingresos suficientes para garantizar el cumplimiento de las obligaciones adquiridas sin comprometer la estabilidad financiera de la compañía. Por lo anterior, consideramos que un ajuste del indicador a un nivel de hasta el **0,69** permitiría una evaluación más acorde con la realidad del mercado, promoviendo la participación de un mayor número de oferentes que cumplen con condiciones técnicas y financieras adecuadas, sin afectar la debida selección de contratistas idóneos. En consecuencia, solicitamos amablemente a la entidad revisar la estructuración de los		En atención a la observación no se acepta la solicitud, el indicador se mantiene debido a la envergadura del proyecto.
261	VII	Formal	<table><tr><th>No.</th><th>Indicador</th><th>Fórmula de cálculo</th><th>Valor del indicador</th></tr><tr><td>1</td><td>Índice de liquidez</td><td>Activo corriente/Pasivo corriente</td><td>Mayor o igual a 1</td></tr><tr><td>2</td><td>Razón de endeudamiento</td><td>Pasivo total / Activo total</td><td>Menor o igual a 0,6</td></tr><tr><td>3</td><td>Patrimonio en relación al presupuesto estimado del proceso</td><td>Patrimonio/ Presupuesto estimado</td><td>Mayor o igual a 0,1</td></tr><tr><td>4</td><td>Capital de trabajo en relación al presupuesto estimado del proceso</td><td>(Activo Corriente - Pasivo Corriente) /Presupuesto estimado</td><td>Mayor o igual a 0,05</td></tr><tr><td>5</td><td>Apalancamiento a corto plazo</td><td>Pasivo Corriente/Patrimonio</td><td>Menor o igual a 0,5</td></tr></table>	Respetuosamente, solicitamos a la entidad revisar el indicador financiero de patrimonio en relación con el presupuesto estimado del proceso, establecido en el pliego de condiciones en un valor mínimo de 0,1 (10 %), teniendo en cuenta su impacto en la pluralidad de oferentes y en la adecuada estructuración de los requisitos habilitantes. La presente solicitud se fundamenta en los principios que rigen la contratación estatal en Colombia, consagrados en la Ley 80 de 1993 y la Ley 1150 de 2007, en particular los principios de libre concurrencia, pluralidad de oferentes, transparencia y selección objetiva, los cuales exigen que los requisitos habilitantes sean proporcionales, razonables y directamente relacionados con el objeto contractual. En igual sentido, el Decreto 1082 de 2015 dispone que la verificación de la capacidad financiera debe responder a condiciones reales del mercado, evitando la imposición de exigencias que restrinjan de manera injustificada la participación de proponentes idóneos. En este contexto, el indicador de patrimonio debe analizarse no solo desde su valor porcentual, sino también considerando la estructura financiera propia de los sectores productivos. En industrias como la tecnología y los servicios especializados, la composición patrimonial suele ser más dinámica, como resultado de modelos de negocio basados en la reinversión, el apalancamiento operativo y el uso eficiente del capital de trabajo, sin que ello afecte la capacidad real de cumplimiento contractual. Bajo este análisis, nuestra compañía presenta un indicador de patrimonio equivalente al **9 % (0,09)**, el cual refleja de manera consistente la estructura financiera del negocio y su capacidad para respaldar la ejecución del objeto contractual, sin que se evidencie un riesgo financiero que comprometa el cumplimiento de las obligaciones derivadas del contrato. Por lo anterior, respetuosamente solicitamos a la entidad ajustar el valor mínimo del indicador de patrimonio, por ejemplo a **0,09 (9 %)**, o, en su defecto, revisar su exigencia dentro de los requisitos habilitantes, con el fin de promover una mayor pluralidad de oferentes, manteniendo criterios financieros adecuados, razonables y acordes con la realidad del mercado. La presente solicitud tiene como finalidad fortalecer los principios de la contratación pública,		En atención a la observación no se acepta la solicitud, el indicador se mantiene debido a la envergadura del proyecto.
262	VII	Formal	<table><tr><th>No.</th><th>Indicador</th><th>Fórmula de cálculo</th><th>Valor del indicador</th></tr><tr><td>1</td><td>Índice de liquidez</td><td>Activo corriente/Pasivo corriente</td><td>Mayor o igual a 1</td></tr><tr><td>2</td><td>Razón de endeudamiento</td><td>Pasivo total / Activo total</td><td>Menor o igual a 0,6</td></tr><tr><td>3</td><td>Patrimonio en relación al presupuesto estimado del proceso</td><td>Patrimonio/ Presupuesto estimado</td><td>Mayor o igual a 0,1</td></tr><tr><td>4</td><td>Capital de trabajo en relación al presupuesto estimado del proceso</td><td>(Activo Corriente - Pasivo Corriente) /Presupuesto estimado</td><td>Mayor o igual a 0,05</td></tr><tr><td>5</td><td>Apalancamiento a corto plazo</td><td>Pasivo Corriente/Patrimonio</td><td>Menor o igual a 0,5</td></tr></table>	Respetuosamente, solicitamos a la entidad revisar el indicador financiero de apalancamiento a corto plazo establecido en el pliego de condiciones, definido como Pasivo Corriente sobre Patrimonio, con un umbral de menor o igual a 0,5, en atención a su impacto en la participación de oferentes. La presente solicitud se fundamenta en los principios de la contratación estatal consagrados en la Ley 80 de 1993 y la Ley 1150 de 2007, especialmente en los principios de libre concurrencia, pluralidad de oferentes, transparencia y selección objetiva, los cuales exigen que los requisitos habilitantes sean proporcionales al objeto contractual y no restrinjan injustificadamente la participación. Asimismo, conforme a lo dispuesto en el Decreto 1082 de 2015, los indicadores financieros deben establecerse de acuerdo con las condiciones del mercado y la naturaleza del sector económico, garantizando que estos reflejen de manera adecuada la capacidad real de ejecución de los proponentes. En este sentido, el indicador de apalancamiento a corto plazo, en el nivel actualmente exigido, puede resultar restrictivo para empresas cuya estructura financiera responde a esquemas de financiación propios del sector, particularmente en industrias como tecnología y servicios, donde el uso de apalancamiento es una práctica habitual para el desarrollo de proyectos e inversiones operativas, sin que ello comprometa la capacidad de cumplimiento contractual. Por lo anterior, solicitamos respetuosamente a la entidad ajustar el indicador a un nivel de **menor o igual a 1,27**, valor que consideramos más acorde con la realidad del mercado y que permite mantener la evaluación de la capacidad financiera sin limitar la pluralidad de oferentes, o en su defecto, evaluar su eliminación como requisito habilitante. Lo anterior en garantía de los principios de contratación pública, resguardo condiciones de		En atención a la observación no se acepta la solicitud, el indicador se mantiene debido a la envergadura del proyecto.
263	VII	Formal		Respetuosamente, solicitamos a la entidad confirmar que el año fiscal a tener en cuenta para la verificación del cumplimiento de la capacidad financiera de los indicadores habilitantes establecidos en el presente proceso de selección corresponde al último año fiscal cerrado, es decir, el año 2025. Lo anterior, con el fin de asegurar una correcta interpretación de los requisitos financieros exigidos en el pliego de condiciones y presentar la información conforme a los criterios definidos por la entidad.		Los Estados financieros para verificar requisitos financieros corresponden a los del último año fiscal cerrado, para el caso de las firmas residentes fiscales en Colombia, a 31 de diciembre de 2025. En caso países cuyos cierres fiscales correspondan a otros meses deberán aportar el último aprobado por la Junta directiva o quien haga sus veces aportando la normatividad que sustenta dicha fecha de cierre.Los Estados financieros para verificar requisitos financieros corresponden a los del último año fiscal cerrado, para el caso de las firmas residentes fiscales en Colombia, a 31 de diciembre de 2025. En caso países cuyos cierres fiscales correspondan a otros meses deberán aportar el último aprobado por la Junta directiva o quien haga sus veces aportando la normatividad que sustenta dicha fecha de cierre.
264	VII	Formal		Se solicita amablemente a la entidad aclarar si, para la presente licitación, no se requiere el Registro Único de Proponentes (RUP) como medio para la acreditación y validación de las certificaciones y/o contratos de experiencia.		En atención a la observación presentada, se aclara que para el presente proceso no se exige la presentación del Registro Único de Proponentes (RUP) como requisito para la acreditación de la experiencia. En este sentido, los proponentes podrán presentar los documentos que consideren pertinentes para demostrar el cumplimiento de los requisitos de experiencia exigidos, tales como certificaciones contractuales, actas de liquidación, contratos u otros documentos equivalentes, siempre que estos permitan verificar de manera clara las condiciones requeridas, incluyendo, entre otros aspectos, la vigencia del contrato, su estado de ejecución o finalización, el alcance de las actividades desarrolladas y los valores asociados.

265	VII	Formal	**(ii) Experiencia y capacidad técnica general:** Contratos terminados o iniciados (mínimo 40% de ejecución) dentro de los últimos siete (7) años con entidades públicas y/o privadas, nacionales o internacionales, relacionados con las siguientes actividades: • Servicios de diseño, planeación e implementación de Centros de Operaciones de Seguridad (SOC) y/o servicios avanzados de protección en ciberseguridad. • Suministro de hardware y software especializado en seguridad informática de nivel empresarial. • Servicios de implementación, integración y configuración de soluciones avanzadas de ciberseguridad. Presentar mínimo seis (6) contratos. La sumatoria de los contratos debe ser mínimo de seis (6) millones de dólares. Entre los contratos presentados se debe cumplir que: - Al menos uno (1) debe haber sido ejecutado para el sector Gubernamental. - Al menos uno (1) debe haber sido ejecutado para el sector Financiero. - Al menos uno (1) incluya actividades de prestación de servicios de SOC, por un valor mayor a un (1) millón de dólares.	Respetuosamente, solicitamos a la entidad revisar los requisitos de experiencia establecidos en el pliego de condiciones, en particular lo relacionado con la sumatoria mínima de contratos y la exigencia de ejecución en el sector gubernamental. La presente solicitud se fundamenta en los principios de la contratación estatal consagrados en la Ley 80 de 1993 y la Ley 1150 de 2007, especialmente en los principios de libre concurrencia, pluralidad de oferentes, transparencia y selección objetiva, los cuales establecen que los requisitos habilitantes deben ser proporcionales al objeto contractual y no generar restricciones injustificadas a la participación. En este sentido, la exigencia actual de una sumatoria mínima de seis (6) millones de dólares en contratos de experiencia puede limitar la participación de proponentes idóneos que cuentan con experiencia relevante y especializada, pero estructurada en proyectos de menor cuantía, sin que ello implique una afectación en su capacidad técnica o operativa para la ejecución del contrato. Adicionalmente, la obligación de contar con al menos un contrato ejecutado para el sector gubernamental puede resultar restrictiva, en la medida en que la experiencia en la prestación de servicios tecnológicos y de SOC es transferible entre sectores, siempre que se acredite idoneidad técnica, calidad y cumplimiento en la ejecución de proyectos de similar complejidad. Por lo anterior, respetuosamente solicitamos a la entidad ajustar el requisito de experiencia, estableciendo una sumatoria mínima de contratos de dos millones quinientos mil (2.500.000) dólares, y que la experiencia en el sector gubernamental sea considerada opcional y no obligatoria, manteniendo como criterio esencial la acreditación de experiencia en servicios de SOC por un valor superior a un (1) millón de dólares. Lo anterior permitiría ampliar la pluralidad de oferentes, garantizar condiciones de competencia efectiva y asegurar la selección de proponentes con experiencia técnica comprobada, sin		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la experiencia solicitada se considera amplia y suficiente de acuerdo al tamaño y robustez del proyecto SOC, así como el presupuesto del proceso, por lo tanto, no es posible aceptar su observación.
266	VII	Formal	Imagen	Respetuosamente, solicitamos a la entidad que para la validación de los contratos en ejecución aportados como experiencia en el presente proceso de selección, se establezca de manera expresa que se tendrá en cuenta el valor total del contrato, siempre y cuando este tenga una ejecución mayor al 40%. Por lo anterior, solicitamos amablemente a la entidad que se confirme y se establezca de forma expresa que los contratos en ejecución serán tenidos en cuenta por su valor total contratado, sin aplicar reducción proporcional por porcentaje de ejecución.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la experiencia solicitada se considera amplia y suficiente de acuerdo al tamaño y robustez del proyecto SOC, así como el presupuesto del proceso, por lo tanto, no es posible aceptar su observación.
267	Equipo Mínimo de Trabajo	Formal		Respetuosamente, solicitamos a la entidad que la acreditación del equipo mínimo de trabajo requerido se exija únicamente al proponente adjudicatario, y no como requisito habilitante de presentación de hojas de vida y soportes por parte de todos los oferentes dentro del proceso. La presente solicitud se fundamenta en los principios de la contratación estatal consagrados en la Ley 80 de 1993 y la Ley 1150 de 2007, especialmente en los principios de transparencia, economía, selección objetiva y libre concurrencia, los cuales buscan evitar cargas innecesarias que puedan restringir la participación de proponentes. Adicionalmente, conforme al Decreto 1082 de 2015, la entidad debe estructurar los requisitos habilitantes de manera proporcional y adecuada al objeto contractual, evitando exigir documentación que no resulte indispensable para la comparación de las ofertas. En este sentido, la exigencia anticipada de hojas de vida y soportes del personal puede implicar la divulgación de información sensible y de carácter reservado, así como generar cargas administrativas innecesarias para los proponentes. Por tal motivo, resulta más adecuado que los proponentes presenten una carta de compromiso suscrita por el representante legal, en la cual se garantice la disponibilidad del equipo mínimo de trabajo requerido, y que la verificación documental correspondiente sea realizada exclusivamente al proponente adjudicatario antes de la suscripción del contrato. Lo anterior permite garantizar la idoneidad del equipo propuesto, sin afectar la confidencialidad de la información ni la eficiencia del proceso de selección, en concordancia con los principios que rigen la contratación pública.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el personal junto con sus hojas de vida lo debera presentar el contratista o el proponente ganador en la etapa de adjudicación. Este cambio se hará mediante adenda en los próximos días y se verá reflejado en el documento anexo de características técnicas, hoja equipo mínimo de trabajo, y quedará de la siguiente manera: NOTA 3: El personal mínimo de trabajo y sus hojas de vida deberán ser presentados por el oferente ganador para su evaluación cuando se adjudique el contrato.
268	VII - 10	Formal		Respetuosamente, solicitamos a la entidad aclarar la forma de pago establecida para el presente proceso, toda vez que en el cuadro económico se indican cantidades y valores, pero no se especifica si el pago se realizará en un solo desembolso o mediante pagos parciales asociados a entregables, hitos o periodos de ejecución.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la formade pago se encuentra descrita en la sección IV , numeral 10 "Forma de Pago". En esta sección se describen los pagos en función de las capacidades implementadas, entregables, hitos de pago y el valor a pagar. se debe tener en cuenta que" Los pagos no estarán sujetos únicamente a documentos en calidad de entregables, se debe tener en cuenta que se requiere de la recepción a conformidad de los entregables, implementación y puesta en operación de las capacidades y los servicios efectivamente prestados."
269	GCC 16.5	Formal	GCC 16.5 El plazo de pago después del cual el Comprador deberá pagar interés al Proveedor es de 90 días. La tasa de interés que se aplicará es: El interés bancario corriente para crédito de consumo y ordinario efectivo anual menos un punto básico, publicado por la Superintendencia Financiera de Colombia. Para efectos del pago, esta tasa se convertirá a tasa mensual y se reconocerá por cada mes de atraso contado a partir de los 90 días calendario posteriores a la aprobación y radicación de la totalidad de los documentos requeridos para el cobro, por parte del supervisor.	Respetuosamente, solicitamos a la entidad revisar el plazo de pago establecido en el pliego de condiciones, teniendo en cuenta que la cláusula que dispone que el reconocimiento de intereses por mora se causa a partir de los noventa (90) días calendario posteriores a la aprobación y radicación de la totalidad de los documentos requeridos para el cobro, implica en la práctica un plazo de pago de hasta 90 días. Si bien la redacción hace referencia al momento a partir del cual se generan intereses, resulta claro que dicho término constituye el plazo máximo dentro del cual la entidad puede efectuar el pago sin reconocimiento de intereses, lo cual tiene un impacto relevante en el flujo de caja y en el equilibrio económico del contrato para los proveedores. En este sentido, plazos de pago extensos pueden afectar la pluralidad de oferentes y la participación efectiva de proponentes idóneos, especialmente en contratos de ejecución continua y con alto componente operativo, como el objeto del presente proceso, sin que ello necesariamente represente un beneficio proporcional para la entidad. Por lo anterior, respetuosamente solicitamos a la entidad evaluar la posibilidad de reducir el plazo de pago, por ejemplo a treinta (30) o sesenta (60) días calendario, contados a partir de la aprobación y radicación completa de los documentos de cobro, manteniendo condiciones financieras razonables, acordes con las prácticas del mercado y con los principios de eficiencia, equilibrio económico del contrato y pluralidad de oferentes que rigen la contratación pública.		En atención a la observación presentada, la Entidad se permite indicar que no se acepta la solicitud, toda vez que el plazo establecido fue definido con base en la revisión de los procedimientos internos de gestión financiera, así como en los tiempos requeridos para la validación y trámite de los pagos. No obstante, se precisa que dicho término corresponde al momento a partir del cual se causan intereses por mora, y no implica que los pagos se realicen en ese plazo máximo. En la práctica, el tiempo entre la radicación de las cuentas con todos los soportes y el pago es muy reducido, siendo en la mayoría de los casos de apenas unos pocos días, siempre que la documentación esté completa.
270	II	Formal		Respetuosamente, solicitamos a la entidad indicar si existen limitaciones para la participación de los proponentes bajo la modalidad de consorcio o unión temporal en el presente proceso de selección y, en caso afirmativo, precisar de manera expresa cuáles son dichas limitaciones. Lo anterior, con el fin de garantizar una adecuada interpretación de las reglas del proceso y asegurar la presentación de las propuestas conforme a lo establecido en el pliego de condiciones.		En atención a la observación, la IAO 4.4 de la Sección II - Datos de la Licitación señala que no existe un límite en la conformación del APCA. Así mismo, se debe revisar a detalle las reglas generales de la Sección III - Criterios de Evaluación y Calificación que trata sobre la presentación de la oferta de manera individual o en Asociación en Participación, consorcio o asoción - APCA. Ahora bien, mediante Adenda se realizará la inclusión de la siguiente nota No. 3 en el numeral 2.1 Asignación de Puntajes, la cual dispondrá lo siguiente: Nota 3: En caso de APCA y para la asignación del puntaje del recuadro de las certificaciones vigentes del oferente, (literal c), las certificaciones presentadas por uno o alguno(s) de los miembros permitirá la asignación de los puntajes relacionados.
271	II	Formal		Respetuosamente, solicitamos a la entidad compartir las observaciones formuladas por los demás oferentes, junto con sus respectivas respuestas, con el fin de garantizar la adecuada comprensión de las condiciones del proceso y contar con información completa y uniforme para la correcta preparación de las propuestas.		Tal como fue mencionado en la audiencia de aclaración del 15-04-2026, todas las respuestas a las observaciones serán compartidas por los interasados omitiendo la fuente de la observación. Estas respuestas serán publicadas en el portal del micrositio Fondo DIAN y SECOP II.
272	II	Formal		Respetuosamente, solicitamos a la entidad compartir los formatos y/o anexos requeridos para el diligenciamiento de la presente licitación, en caso de que existan, o confirmar expresamente si los mismos se encuentran incluidos dentro del documento de la Solicitud de Oferta. Lo anterior, con el fin de asegurar la correcta preparación y presentación de la propuesta conforme a los requisitos establecidos en el proceso.		En el documento de Solicitud de Oferta, en la sección V - Formularios de la Oferta, se encuentran los formatos que se deben presentar para la oferta. Así mismo, es necesario que el interesado de lectura completa del documento de Solicitud de Oferta ya que dentro del mismo se señalan otros documentos que deben acompañar la oferta, como los mencionados en la IAO 11.1 (j) de la Sección II - Datos de la Licitación, Sección III - Criterios de Evaluación y Calificación entre otros acápites.

Original firmado

Original firmado

CARLOS JAVIER OSORIO BELTRÁN
Gestor III - OSI

JAVIER EDGARDO SOTO ARGEL
Consultor Fondo DIAN

Original firmado
ÁNGELA MARÍA BUSTAMANTE RODRÍGUEZ
Especialista Líder de Adquisiciones - UCP

Original firmado
DIEGO FERNANDO PALACIOS SÁNCHEZ
Especialista de Adquisiciones - UCP

Audiencia Aclaración de dudas proceso
Fecha: 15/04/2026
Hora: 10:30am

Ítem	N°	Pregunta	Respuesta
	1	Buenos días, pero no me queda claro cual es el plazo maximo para presentar observaciones?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en la IAO 7.1 se indica que el plazo máximo para presentar observaciones será 20 días calendario antes de la fecha de presentación límite de la oferta.
	2	¿se tiene alguna fecha límite para que se publiquen las respuestas a las observaciones, posterior al 24 de abril? y para las adendas que resulten, en caso dado?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, lo más pronto posible se publicarán las respuestas a las observaciones. Dependerá del número de las observaciones que se reciban.
	3	Se observa que el requisito establecido en el literal b, al exigir que el oferente acredite su pertenencia al máximo nivel de membresía para todos los fabricantes de las tecnologías ofertadas, resulta desproporcionado y restrictivo frente a la realidad del mercado. Este tipo de exigencia, aplicada de manera acumulativa sobre la totalidad de las soluciones requeridas, limita de forma significativa la participación, toda vez que en la práctica son muy pocos los integradores que alcanzan simultáneamente el nivel más alto de certificación con múltiples fabricantes. Mantener esta condición para todas las tecnologías genera un efecto excluyente, al reducir el universo de posibles oferentes a un número muy limitado de canales —incluso potencialmente uno o dos—, lo que afecta directamente la pluralidad de oferentes y puede comprometer la selección objetiva del proceso. Esta situación no necesariamente garantiza una mejor ejecución contractual, sino que introduce una barrera comercial que no está directamente relacionada con la capacidad técnica real del proponente. En ese sentido, se considera que la exigencia debe ser proporcional al objeto del contrato y orientada a garantizar el respaldo del fabricante sin restringir la competencia. Por ello, se solicita respetuosamente a la entidad ajustar el requisito, permitiendo que el oferente acredite el máximo nivel de membresía al menos en una de las tecnologías principales ofertadas, y para las demás soluciones se habiliten mecanismos alternativos de validación, tales como certificaciones de partner autorizado o cartas de respaldo del fabricante. Este ajuste permite mantener un estándar alto de idoneidad y respaldo técnico, sin generar un sesgo en el proceso, promoviendo así una mayor participación, mejores condiciones competitivas y una selección alineada con los principios de transparencia, economía y pluralidad de oferentes en la contratación estatal.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el literal b es un ítem puntuable, para el caso en especifico, la Entidad da una puntuación en caso de que el futuro interesado acredite pertenecer al nivel de parner más alto en las capacidades o servicios solicitados puntuando desde el que tenga dos (2) y hasta cuatro (4) o más membresías, así las cosas el futuro interesado podrá hacerse a esta puntuación según lo comentado anteriormente, por lo tanto, no se acepta su sugerencia en el entendido que la puntuación requerida ofrece equilibrio para el proyecto.
	4	Solicitamos a la entidad, confirmar la fecha de respuesta de las observaciones a partir del 24 de Abril y confirmar si existe la posibilidad de extensión de oferta debido a que se requieren las respuestas para realizar un dimensionamiento correcto.	En atención a la obsevación y teniendo en cuenta la cantidad de las osbervaciones, se remitirán las respuestas presentadas en el menor tiempo posible.
Página 112	5	En la fase 2 "Implementación SOC" habría servicios de operación como Atención de Incidentes?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la capacidad "Gestión de Incidentes " debe ser tenido en cuenta desde el principio y hasta el final del proyecto.
Pagina 165	6	Solicitamos a la entidad confirmar si el plazo de ejecución es de 27 meses, teniendo en cuenta que el RFI de 2024 se solicitó un total de 36 meses. Agradecemos aclarar, según el cronograma que mostraron en la sesión	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, la operación, seguimiento, gestión, monitoreo y administración por parte del futuro proveedor de todos los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho a uso, licenciamiento, suscripciones, actualizaciones, soporte y garantía irá por tres (3) años y sus periodos se contabilizarán a partir de la puesta en operación de cada uno de los servicios requeridos, incluyendo lo siguiente: Tener en cuenta que desde el inicio del contrato se deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 nuevo SIEM (solicitado en el ítem 2) que hace parte integral de este proyecto por el tiempo solicitado (Tres años) con licenciamiento soporte, garantía y derecho a uso hasta agosto 31 de 2030. La protección de bases de datos (Firewall de bases de datos) irá a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031. El futuro contratista deberá, recibir, gestionar, administrar y operar desde el inicio del contrato el actual firewall de bases de datos propiedad de la DIAN del fabricante IBM Referencia GUARDIUM hasta diciembre 31 de 2027 tiempo en el que termina el soporte de este dispositivo por parte del fabricante, una vez esto ocurra deberá implementar el nuevo firewall de bases de datos solicitado en las capacidades requeridas por la DIAN. Para la capacidad de NDR se deberá tener en cuenta que este comenzará a operar a partir de enero de 2028 previamente autorización de la DIAN, para lo cual deberá implementar, administrar, operar, soportar y garantizar el servicio mencionado, con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031.
	7	Cuanto tiempo se tardan en publicar la evaluación después de entregada la oferta?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, no se publica la evaluación, se publica el resultado y de acuerdo con los pasos procesales, el plazo suspensivo que se contempla en la etapa de notificación de intención de adjudicación será la etapa para que los oferentes presenten sus quejas para revisar la evaluación adelantada. Sin embargo, bajo las políticas del proceso, no hay un cronograma.
	8	El proceso requiere que cada oferente solicite el link de carga de su oferta pero el documento no establece en cuánto tiempo el Fondo DIAN debe remitir ese link una vez recibida la solicitud. Si el link llega muy tarde entonces el oferente podría quedarse sin tiempo suficiente para cargar su propuesta antes de la fecha límite del 14 de mayo de 2026. Solicitud: Establecer un plazo mínimo dentro del cual el Fondo DIAN debe enviar el link de cargue al oferente que lo solicite.	Los interesados deberán solicitar el enlace para el cargue del enlace por lo menos con 7 días calendario anterior a la fecha del cierre del proceso. Dentro de este término, el Fondo DIAN creará el enlace e informará al interesado el protocolo para el cargue de la propuesta.
	9	Cual es el plazo limite de respuesta a observaciones?, que debe ser anterior al plazo limite de manifestación de interés	En atención a la obsevación y teniendo en cuenta la cantidad de las osbervaciones, se remitirán las respuestas presentadas en el menor tiempo posible.
Página 106	10	Con base en el cronograma mostrado por la entidad, agradecemos confirmar si la Fase 2 correspondiente a la implementación del SOC contempla también las herramientas cuya puesta en marcha está prevista para los años 2027 y 2028.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara Tener en cuenta que, desde el inicio del contrato se deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 nuevo SIEM (solicitado en el ítem 2) que hace parte integral de este proyecto por el tiempo solicitado (Tres años) con licenciamiento soporte, garantía y derecho a uso hasta agosto 31 de 2030. La protección de bases de datos (Firewall de bases de datos) irá a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031. El futuro contratista deberá, recibir, gestionar, administrar y operar desde el inicio del contrato el actual firewall de bases de datos propiedad de la DIAN del fabricante IBM Referencia GUARDIUM hasta diciembre 31 de 2027 tiempo en el que termina el soporte de este dispositivo por parte del fabricante, una vez esto ocurra deberá implementar el nuevo firewall de bases de datos solicitado en las capacidades requeridas por la DIAN. Para la capacidad de NDR se deberá tener en cuenta que este comenzará a operar a partir de enero de 2028 previamente autorización de la DIAN, para lo cual deberá implementar, administrar, operar, soportar y garantizar el servicio mencionado, con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031.
	11	Nos permitimos solicitar que la presentación sea enviada a todos los participantes de esta audiencia	Tal como fue mencionado en la audiencia de aclaración del 15-04-2026, todas las respuestas a las observaciones serán compartidas por los interasados omitiendo la fuente de la observación. Estas respuestas serán publicadas en el portal del micrositio Fondo DIAN y SECOP II.

Página 106	12	Con base en el cronograma presentado por la entidad, entendemos que, en la Fase 3 correspondiente a la operación del SOC, las herramientas QRadar y Guardium deben entrar en operación desde el día uno durante un periodo de 23 meses. Agradecemos confirmar si dicha operación se encuentra efectivamente contemplada dentro de esta fase.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, la operación, seguimiento, gestión, monitoreo y administración por parte del futuro proveedor de todos los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho a uso, licenciamiento, suscripciones, actualizaciones, soporte y garantía irá por tres (3) años y sus periodos se contabilizarán a partir de la puesta en operación de cada uno de los servicios requeridos, incluyendo lo siguiente: Tener en cuenta que desde el inicio del contrato se deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 nuevo SIEM (solicitado en el ítem 2) que hace parte integral de este proyecto por el tiempo solicitado (Tres años) con licenciamiento soporte, garantía y derecho a uso hasta agosto 31 de 2030. La protección de bases de datos (Firewall de bases de datos) irá a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031. El futuro contratista deberá, recibir, gestionar, administrar y operar desde el inicio del contrato el actual firewall de bases de datos propiedad de la DIAN del fabricante IBM Referencia GUARDIUM hasta diciembre 31 de 2027 tiempo en el que termina el soporte de este dispositivo por parte del fabricante, una vez esto ocurra deberá implementar el nuevo firewall de bases de datos solicitado en las capacidades requeridas por la DIAN. Para la capacidad de NDR se deberá tener en cuenta que este comenzará a operar a partir de enero de 2028 previamente autorización de la DIAN, para lo cual deberá implementar, administrar, operar, soportar y garantizar el servicio mencionado, con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031.
	13	Es mandatorio que las marcas que de deben utilizar son las que mencionan o podemos proponer otra solucion?	La Dirección de Impuestos y Aduanas Nacionales (DIAN) aclara al observante que las herramientas Guardium y Q Radar mencionadas en el documento son tecnologías con las que la entidad ya cuenta y que actualmente se encuentran en operación. Las fechas descritas en el documento corresponden al licenciamiento adquirido y vigente por la DIAN, el cual deberá ser operado por el futuro proponente. Transcurrido el tiempo del licenciamiento el proveedor deberá mantener /garantizar el funcionamiento de las capacidades a través de la misma o mejores tecnologias que mantengan el servicio/capacidad operando. Es valido ofrecer soluciones o servicios equivalentes o similares siempre y cuando se cumpla con las características técnicas mínimas solicitadas en los documentos del proyecto.
	14	Ficha copiada Tad3. Fichas copiadas y limitan la participación.	La Dirección de Impuestos y Aduanas Nacionales (DIAN) aclara al observante que, no está clara la pregunta.
	15	El SOC Bogotá sea Fisrt. Esto limita la participación, que no sea en Bogotá.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem en mención que solicita certificación FIRST para el SOC donde se prestarán los servicios es puntuable, no es una certificación obligatoria, por lo tanto, para evitar equivocos en el entendimiento de la característica solicitada, este ítem (12.11) será ajustado en el anexo técnico mediante adenda que se publicará en en los próximos días quedando de la siguiente manera: Es deseable (opcional) para la Entidad que el SOC mediante el cual se prestarán los servicios debe ser miembro FIRST ™, para lo cual el interesado presentará la respectiva certificación con doce (12) meses de antiguedad y se hará acreedor a la respectiva puntuación explicada en sección III criterios de evaluación, es importante resaltar los beneficios que representa para Entidad el tener un SOC certificado: 1.Interoperabilidad y confianza internacional: La membresía en FIRST™ garantiza que el SOC opera bajo estándares reconocidos globalmente en gestión de incidentes, lo que facilita la colaboración con otros CSIRTs y CERTs en situaciones críticas. 2.Acceso a inteligencia de amenazas de alta calidad: Los miembros de FIRST™ tienen acceso a canales exclusivos de intercambio de información sobre amenazas emergentes, vulnerabilidades y tácticas de ataque, lo que permite una respuesta más rápida y efectiva. 3.Capacidad técnica validada: Para ser aceptado como miembro, el SOC debe demostrar capacidades técnicas avanzadas, procesos maduros de gestión de incidentes, y un compromiso con la mejora continua en ciberseguridad. 4.Participación en ejercicios y foros especializados: La membresía permite participar en simulacros internacionales, capacitaciones y foros técnicos que fortalecen la preparación ante incidentes complejos y coordinados. 5.Cumplimiento de buenas prácticas y gobernanza: FIRST™ promueve principios de ética, confidencialidad y responsabilidad que son fundamentales para la operación segura y confiable de un SOC. Esta postura busca asegurar que los servicios prestados se alineen con los más altos estándares internacionales en ciberseguridad, sin comprometer la calidad ni la capacidad de respuesta ante incidentes.
	16	Estados Financieros 2023-2024 (los del año 2025 ya están habilitados)	Los Estados financieros para verificar requisitos financieros corresponden a los del último año fiscal cerrado, para el caso de las firmas residentes fiscales en Colombia, a 31 de diciembre de 2025. En caso países cuyos cierres fiscales correspondan a otros meses deberán aportar el último aprobado por la Junta directiva o quien haga sus veces aportando la normatividad que sustenta dicha fecha de cierre.
	17	Subir el índice de apalancamiento ya que es muy robusto, pasar de 0.5 a 0.8.	En atención a la observación. no se acepta la solicitud, el indicador se mantiene debido a la envergadura del proyecto.
	18	18. Quisiera dejar una observación frente al requisito del literal b, relacionado con la exigencia de contar con el máximo nivel de membresía del fabricante. Considero que esta condición resulta restrictiva, ya que limita la pluralidad de oferentes y la libre competencia. En la práctica, no solo favorece a ciertos fabricantes que cumplen las especificaciones técnicas, sino que además les traslada la facultad de definir qué canales pueden participar, al ser ellos quienes otorgan estas certificaciones. Esto implica que la participación no depende únicamente de la capacidad técnica o la experiencia del proponente, sino de una habilitación comercial de un tercero, lo cual constituye una barrera de acceso injustificada y puede afectar principios como la transparencia y la selección objetiva. Por lo anterior, respetuosamente solicito ajustar este requisito, eliminando la exigencia del nivel máximo de membresía y permitiendo, en su lugar, una carta de respaldo del fabricante por cada tecnología ofertada, que garantice el acompañamiento técnico y comercial durante la ejecución del contrato.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el literal b es un ítem puntuable, para el caso en especifico, la Entidad da una puntuación en caso de que el futuro interesado acredite pertenecer al nivel de parner más alto en las capacidades o servicios solicitados puntuando desde el que tenga dos (2) y hasta cuatro (4) o más membresías, así las cosas el futuro interesado podrá hacerse a esta puntuación según lo comentado anteriormente, por lo tanto, no se acepta su sugerencia en el entendido que la puntuación requerida ofrece equilibrio para el proyecto.
	19	Se comparte a los oferentes el conjunto de respuestas de observaciones realizadas por todos los interesados?	Tal como fue mencionado en la audiencia de aclaración del 15-04-2026, todas las respuestas a las observaciones serán compartidas por los interasados omitiendo la fuente de la observación. Estas respuestas serán publicadas en el portal del micrositio Fondo DIAN y SECOP II.

18.2	20	El numeral 18.2 de la ficha técnica. Niveles de Membresía altos. Se solicita modificar ese requisito.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento permite pluralidad al referir que el interesado debe certificar que está rankeado en los tres niveles más altos de las capacidades ofrecidas, permitiendo esto asegurar idoneidad y experticia para las dimensiones del proyecto SOC en mención. Se aclara que, es perfectamente viable y común que los proveedores de un Centro de Operaciones de Seguridad (SOC) cumplan con el requerimiento de presentar una certificación de fabricante que acredite su nivel de membresía. Este tipo de exigencia es una práctica estándar en licitaciones y contratos de servicios gestionados de ciberseguridad para garantizar que el proveedor cuenta con el respaldo técnico y comercial directo del fabricante. Propósito de la certificación El objetivo principal de este requerimiento es asegurar que el proveedor no solo sea un revendedor, sino que posea una relación estratégica con el fabricante que garantice la calidad del servicio, sostenibilidad en el tiempo y la experticia necesaria de acuerdo a la robustez del proyecto. Al exigir estar en uno de los niveles de membresía más altos como por ejemplo Platinum, Gold o Elite), plata, bronce y otros la entidad contratante obtiene las siguientes garantías: ▪Soporte especializado: Acceso directo a ingenieros de soporte del fabricante en caso de incidentes críticos o configuraciones complejas. ▪Actualización y capacitación: Obligación del personal del proveedor de estar certificado técnica y comercialmente sobre las herramientas, garantizando que el SOC opere con personal experto. ▪Autenticidad y licenciamiento: Validación de que los servicios, plataformas y dispositivos son legítimos, cuentan con licenciamiento vigente y seguirán siendo soportados durante toda la duración del contrato.
	21	Respecto a los estados financieros, según las indicaciones dadas, los requisitos no son habilitantes, sino que se asigna puntaje; sin embargo en el documento no se indica un puntaje específico para el cumplimiento de los indicadores de los estados financieros. Por lo anterior se solicita aclarar si estos indicadores son mandatorios o no?	Los indicadores relacionados en la sección III, numeral 5 (IAO 38), numeral 5.1 (IAO 38.1) pemitirán validar la capacidad financiera y experiencia de la firma o APCA que haya obtenido el mayor puntaje, por lo cual, la revisión se hará a partir del análisis de los índices presentados.
	22	22. Acreditación de Experiencia: Estado de Ejecución de los Contratos Objeto de la observación Se solicita respetuosamente a la entidad contratante que modifique el requisito habilitante actualmente consignado en el pliego de condiciones, el cual establece como válidos los "contratos terminados o iniciados con un mínimo del 40% de ejecución", para que en su lugar se exija la acreditación de contratos ejecutados y finalizados al 100% dentro del plazo contractual pactado. Fundamento de la observación La aceptación de contratos con un avance de ejecución de apenas el 40% como criterio habilitante de experiencia resulta insuficiente para acreditar de manera confiable la capacidad técnica, operativa y de gestión del proponente, tal como se expone a continuación. En primer lugar, un contrato que registra únicamente el 40% de avance no permite verificar que el oferente haya cumplido de manera integral con el objeto contractual. Las fases críticas de un contrato —tales como la estabilización del servicio, el cierre operativo, la entrega definitiva de productos y el cumplimiento cabal de los resultados esperados— se materializan en las etapas finales de ejecución. Admitir experiencias parciales impide a la entidad evaluar si el proponente cuenta con la capacidad probada para llevar a término la totalidad de las obligaciones asumidas. En segundo lugar, un nivel de ejecución del 40% representa una etapa temprana del contrato que no refleja la gestión integral de los riesgos inherentes a la prestación del servicio, ni el cumplimiento sostenido de los Acuerdos de Niveles de Servicio (ANS), ni la correcta administración de los recursos técnicos, humanos y financieros a lo largo de todo el ciclo contractual. La experiencia adquirida en esa fase inicial no es equiparable a la que se obtiene al ejecutar y concluir satisfactoriamente la totalidad del contrato. En tercer lugar, los indicadores de calidad y satisfacción del contratante se consolidan y verifican al momento de la finalización y liquidación del contrato. Un contrato que no ha sido completado no cuenta con la certificación de cumplimiento definitiva ni con el acta de liquidación que acredite la conformidad de la entidad con los bienes o servicios recibidos. Prescindir de estos elementos de verificación debilita la rigurosidad del proceso de evaluación. En cuarto lugar, admitir experiencias con niveles de ejecución parcial podría generar asimetrías injustificadas en la evaluación de los proponentes, en tanto que contratos ejecutados al 40% recibirían el mismo tratamiento habilitante que contratos finalizados en su totalidad. Esta equiparación no resulta razonable ni proporcional, pues desconoce la diferencia sustancial en el grado de complejidad, compromiso y responsabilidad que implica la ejecución completa de un contrato frente a una ejecución incipiente. Solicitud: Con fundamento en las razones expuestas, se solicita a la entidad que modifique el requisito habilitante de experiencia para que únicamente se consideren válidos los contratos ejecutados y finalizados al 100% dentro del plazo contractual establecido. Esta modificación permitirá a la entidad contar con elementos de juicio sólidos y objetivos para verificar la capacidad real de los proponentes, asegurando que quienes resulten habilitados hayan demostrado, de manera comprobable, su aptitud para ejecutar de forma completa, oportuna y satisfactoria el objeto del contrato.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la experiencia solicitada se considera amplia y suficiente de acuerdo al tamaño y robustez del proyecto SOC, así como el presupuesto del proceso, por lo tanto, no es posible aceptar su observación.
	23	Igualmente se solicita aclarar la ponderación que se dará a las experiencias requeridas	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, este requisito no lleva ponderación sólo se valida que el interesado cuente con la respectiva experiencia solicitada.
	24	Qué TRM debe utilizarse para el cálculo de indicadores financieros, toda vez que algunos están atados al presupuesto, que está establecido en dólares	Se aplicará la TRM vigente publicada por la Superintendencia Financiera de Colombia al cierre de vigencia fiscal de los Estados Financieros, para el caso de residentes en Colombia, el 31 de diciembre de 2025.
	25	Observación técnica – Enfoque de integración y tendencia de la industria de ciberseguridad Desde una perspectiva técnica y alineada con las tendencias actuales de la industria de ciberseguridad, se considera que la entidad debería priorizar y otorgar mayor puntos en calidad de oferta técnica a aquellas propuestas que integren múltiples capacidades dentro de un mismo fabricante o plataforma unificada, en lugar de promover esquemas altamente fragmentados entre múltiples marcas. La evolución del mercado ha demostrado que los modelos basados en múltiples herramientas aisladas (silos tecnológicos) generan riesgos operativos significativos, ampliamente documentados en la industria, tales como: falta de visibilidad integral, dificultades en la correlación de eventos, aumento en los tiempos de respuesta ante incidentes y mayores costos de operación e integración. Este enfoque fragmentado limita la capacidad real de un SOC para detectar y responder de manera efectiva a amenazas avanzadas. En contraste, las plataformas modernas están migrando hacia esquemas consolidados y orientados a XDR, gestión de exposición (CTEM/CREM) y analítica unificada, donde un mismo fabricante provee capacidades integradas de detección, respuesta, inteligencia de amenazas y gestión del riesgo. Este modelo permite correlación nativa, reducción de falsos positivos, automatización efectiva y una operación más eficiente, aspectos críticos para entidades como la DIAN. En ese sentido, más que exigir condiciones que incentiven la dispersión de soluciones, se recomienda que la entidad incorpore criterios de evaluación que valoren positivamente la consolidación tecnológica, premiando aquellas ofertas que logren cubrir múltiples dominios de seguridad bajo una misma plataforma o fabricante, garantizando interoperabilidad real, eficiencia operativa y una postura de ciberseguridad más robusta. Este enfoque no solo se alinea con las mejores prácticas internacionales, sino que reduce riesgos estructurales en la operación del SOC y maximiza el retorno de la inversión en ciberseguridad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que se ha analizado la observación presentada y agradece los aportes realizados, los cuales contribuyen al fortalecimiento técnico del proceso. Al respecto, se considera pertinente precisar lo siguiente: La Entidad es consciente de que dicha exigencia no siempre refleja la realidad del mercado ni las capacidades técnicas efectivas de los oferentes, por lo cual no se busca establecer barreras de acceso que afecten la libre concurrencia, sino garantizar que los proponentes cuenten con el respaldo y la idoneidad necesarios para la correcta ejecución del contrato. En este sentido, la Entidad aclara que los servicios y capacidades objeto de la contratación buscan el mejor aprovechamiento de las capacidades tecnológicas existentes, promoviendo su correcta integración, operación y optimización. Por tanto, no se pretende limitar la participación a una tecnología, fabricante o plataforma específica, ni condicionar la eficiencia del proyecto a esquemas cerrados o dependientes de un único proveedor. El enfoque adoptado privilegia la interoperabilidad, la continuidad tecnológica y la sostenibilidad operativa, permitiendo que distintas soluciones puedan integrarse de forma coherente y eficiente dentro del ecosistema de la Entidad. Este enfoque permite garantizar la idoneidad del proponente sin trasladar de manera implícita a los fabricantes la definición de quién puede o no participar en el proceso, preservando la objetividad y transparencia de la evaluación. Si bien la Entidad reconoce que las tendencias actuales de la industria de ciberseguridad promueven arquitecturas integradas y plataformas con múltiples capacidades, dicho enfoque no se establece como una condición excluyente, sino como un posible valor agregado dentro de la evaluación técnica. Las propuestas basadas en plataformas unificadas o en esquemas multivendedor serán valoradas en función de: • Su capacidad de integración con la arquitectura existente. • Su contribución a la eficiencia operativa. • Su alineación con la estrategia de ciberseguridad de la Entidad. En todo caso, no se limita ni se favorece de manera anticipada a un fabricante, tecnología o modelo de solución específico, en estricto cumplimiento del principio de selección objetiva. De esta forma la Entidad ratifica que el proceso de contratación se estructura bajo los principios de pluralidad, eficiencia y selección objetiva, buscando un equilibrio entre el respaldo del fabricante, la realidad del mercado y la necesidad de garantizar soluciones técnicamente sólidas, interoperables y sostenibles, sin generar restricciones injustificadas a la participación.

	26	Se le solicita amablemente a la entidad que las respuestas a las observaciones se publiquen por lo menos con una semana de antelación a la fecha de la presentación de la oferta, para prepararla teniendo en cuenta esas claridades Se solicita se informe cuales son los plazos en los que se harán los cortes para presentar observaciones de forma previa, se propone que sean 2 cortes, y plazo de publicacion de las respuesta, toda vez que dentro del principio de planeación es necesario un cronograma, claro que permita a los interesados obtener la información y respuesta claras en tiempos oportunos. Cordialmente, Ivonne Sossa - COMCEL S.A.	En atención a la obsevación y teniendo en cuenta la cantidad de las osbervaciones, se remitirán las respuestas presentadas en el menor tiempo posible. Así mismo, tal como fue mencionado en la audiencia de aclaración del 15-04-2026, se señaló dos cortes para la atención de las respuestas. Un primer corte con las observaciones recibidas hasta el 15-04-2026cuyas respuestas se estarán dando en el menor tiempo posible y un segundo corte con las observaciones que se han recibido con posterioridad a la fecha señalada.
	27	Observación técnica – Continuidad operativa y mitigación de riesgos en la implementación (Proceso BID – SdO SOC DIAN) En el marco de la presente Solicitud de Ofertas (SdO) para la prestación del SOC de la DIAN, financiado por el Banco Interamericano de Desarrollo, se evidencia que el objeto contractual incluye no solo el suministro de herramientas, sino también la operación continua de los instrumentos de seguridad existentes y nuevos . En este contexto, resulta fundamental que las condiciones del proceso contemplen criterios que minimicen riesgos de transición tecnológica y garanticen la continuidad de la operación. Desde una perspectiva técnica y de mejores prácticas en la industria de ciberseguridad, es ampliamente reconocido que los procesos de reemplazo total ("rip and replace") de plataformas críticas como SIEM, NDR, EDR o herramientas de monitoreo, incrementan significativamente el riesgo operativo, especialmente en entidades con alta criticidad como la DIAN. Estos riesgos incluyen, entre otros: pérdida de visibilidad temporal, errores en la correlación de eventos, retrasos en la afinación de reglas, y exposición ante amenazas durante la curva de aprendizaje e implementación. En ese sentido, se solicita respetuosamente a la entidad que se incorpore una condición que permita que, cuando un proponente decida mantener dentro de su oferta la(s) solución(es) del fabricante actualmente implementado, desde la fecha definida en el proceso, esta aproximación sea considerada viable y valorada técnicamente, en la medida en que reduce el riesgo de interrupciones, facilita la continuidad operativa y optimiza los tiempos de transición. De igual forma, para aquellas soluciones que el proponente decida reemplazar o complementar con otras marcas, se deberá exigir el cumplimiento pleno de las especificaciones técnicas ya definidas en el anexo, garantizando así que cualquier cambio tecnológico se realice bajo criterios objetivos de calidad, desempeño y funcionalidad. Este enfoque híbrido —que combina continuidad controlada con evolución tecnológica— permite: Reducir el riesgo de fallas en la implementación. Evitar dejar a la entidad en estados de vulnerabilidad durante la transición. Asegurar una operación estable del SOC desde el inicio del contrato. Promover competencia real sin sacrificar la seguridad operativa. En conclusión, se recomienda que la entidad ajuste el enfoque del proceso para permitir que los oferentes puedan mantener tecnologías existentes cuando esto represente menor riesgo, y complementar o reemplazar únicamente donde se garantice el cumplimiento técnico, asegurando así una implementación progresiva, controlada y alineada con las mejores prácticas internacionales en operación de SOC.	La Dirección de Impuestos y Aduanas Nacionales (DIAN) agradece la observación presentada y aclara que, en el marco de la presente Solicitud de Ofertas (SdO), los oferentes cuentan con plena libertad para contemplar dentro de sus propuestas las tecnologías que consideren más convenientes y necesarias para garantizar la prestación del servicio y la capacidad requerida, sin que exista restricción respecto a marcas específicas, salvo las herramientas que ya tiene licencias la DIAN y que son referenciadas en los documentos del proceso. La DIAN es consciente que se debe asegurar la continuidad operativa, con nivles de riesgos y mitigación aceptables durante la operación y sus posibles transiciónes tecnológicas. Motivo por el cual , cada proponente podrá apoyarse en su conocimiento del mercado y en su experiencia en la operación y puesta en marcha de este tipo de servicios, siempre que se cumplan las especificaciones técnicas establecidas en el anexo del proceso. En conclusión, la DIAN reitera que el proceso no limita la elección de fabricantes o marcas, y que la valoración técnica se centrará en el cumplimiento de las condiciones y especificaciones definidas, confiando en la capacidad de los oferentes para diseñar y ejecutar una solución que asegure la continuidad operativa y la mitigación de riesgos.
	28	En calidad de fabricante TrendIA, nos permitimos manifestar nuestra preocupación frente al requisito establecido en el literal b, el cual exige que el oferente acredite su pertenencia al máximo nivel de membresía para todos los fabricantes de las tecnologías ofertadas. Desde la perspectiva del ecosistema de fabricantes y canales, esta condición resulta desproporcionada y poco alineada con la dinámica real del mercado de ciberseguridad. Los modelos de canal de los fabricantes están diseñados para especialización por líneas de producto o tecnologías, por lo que es altamente inusual que un mismo integrador ostente el nivel más alto de certificación en múltiples fabricantes simultáneamente. En consecuencia, mantener esta exigencia para todas las tecnologías genera un efecto restrictivo que limita la participación a un número muy reducido de canales, afectando la pluralidad de oferentes y reduciendo la competitividad del proceso. Adicionalmente, este tipo de requerimientos traslada implícitamente a los fabricantes la capacidad de definir qué integradores pueden participar, en función de sus programas de certificación, lo cual no necesariamente refleja la capacidad técnica, operativa o de soporte del oferente en el contexto específico del proyecto. Por lo anterior, como fabricante, consideramos más adecuado que el requisito sea ajustado bajo un criterio de proporcionalidad, permitiendo que el oferente acredite el máximo nivel de membresía al menos en una de las tecnologías principales ofertadas, mientras que para las demás soluciones se acepten mecanismos alternativos de validación, tales como niveles intermedios de certificación o cartas de respaldo del fabricante dirigidas al proyecto. Este enfoque garantiza el respaldo directo del fabricante en componentes críticos de la solución, sin limitar innecesariamente la participación de integradores calificados, promoviendo así un proceso más competitivo, transparente y alineado con las mejores prácticas del mercado. Desde una perspectiva técnica y alineada con las tendencias actuales de la industria de ciberseguridad, se considera que la entidad debería priorizar y otorgar mayor valor a aquellas propuestas que integren múltiples capacidades dentro de un mismo fabricante o plataforma unificada, en lugar de promover esquemas altamente fragmentados entre múltiples marcas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el literal b es un ítem puntuable, para el caso en específico, la Entidad da una puntuación en caso de que el futuro interesado acredite pertenecer al nivel de parner más alto en las capacidades o servicios solicitados puntuando desde el que tenga dos (2) y hasta cuatro (4) o más membresías, así las cosas el futuro interesado podrá hacerse a esta puntuación según lo comentado anteriormente, por lo tanto, no se acepta su sugerencia en el entendido que la puntuación requerida ofrece equilibrio para el proyecto.

Original firmado
CARLOS JAVIER OSORIO BELTRÁN
Gestor III - OSI

Original firmado
JAVIER EDGARDO SOTO ARGEL
Consultor Fondo DIAN

Original firmado
ÁNGELA MARÍA BUSTAMANTE RODRÍGUEZ
Especialista Líder de Adquisiciones - UCP

Original firmado
DIEGO FERNANDO PALACIOS SÁNCHEZ
Especialista de Adquisiciones - UCP