CONS	Sección	Texto de la sección comentada	Observación / Comentario	Sugerencia de Ajuste	Respuesta
1	Sección II - IAO 1.1 - DATOS DE LA LICITACIÓN	PRESTAR LOS SERVICIOS DE UN CENTRO DE OPERACIONES DE SEGURIDAD - SOC PARA EL MONITOREO Y OPERACIÓN DE LOS INSTRUMENTOS DE SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN EN LA DIAN, INCLUYENDO EL SUMINISTRO DE LAS HERRAMIENTAS REQUERIDAS BAJO LOS LINEAMIENTOS Y SEGUIMIENTO EFECTUADO POR LA OFICINA DE SEGURIDAD DE LA INFORMACIÓN DE LA DIAN.	El objeto del contrato mezcla en un solo párrafo dos cosas distintas: el suministro de herramientas tecnológicas (hardware y software) y la prestación del servicio de operación del SOC. Esto genera confusión porque cada componente tiene plazos, pagos y garantías diferentes y al estar todo en un mismo enunciado es difícil saber qué obligaciones corresponden a cada parte.	Redactar el objeto de forma que se diferencien claramente los dos componentes (a) suministro de bienes tecnológicos y (b) servicios de operación y monitoreo SOC. Esto facilita la supervisión del contrato y la aplicación de sanciones cuando corresponda.	La Dirección de Impuestos y Aduanas Nacionales - DIAN precisa al observante que, el objeto contractual es acorde a lo requerido por la Entidad, donde se solicitan servicios de SOC apalancados con las herramientas tecnologicas necesarias, por lo tanto, no se acepta su sugerencia.
2	Sección VIII - CGC 34	El plazo de ejecución del contrato será de 36 meses o hasta cumplir el tiempo objetivo que será máximo el 30 de octubre de 2028, a partir del perfeccionamiento y legalización del contrato.	El documento establece al mismo tiempo dos plazos que no coinciden. Si el contrato se firma en mayo de 2026, los 36 meses llegarían hasta mayo de 2029, pero la fecha límite fijada es octubre de 2028, es decir, hay una diferencia de aproximadamente 7 meses entre ambas medidas. No queda claro cuál de los dos plazos aplica en caso de conflicto y esto también afecta los plazos de entrega de las herramientas.	Solicitamos amablemente planificar el plazo bajo un solo criterio pues consideramos que no se fija una duración en meses o se fija una fecha de terminación, pero no los dos al mismo tiempo. Si se mantienen ambos, debe indicarse expresamente cuál prevalece.	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.
3	10. FORMA DE PAGO	Nota: El valor máximo a pagar por estas capacidades será de hasta el 38% del valor del contrato (...) Nota: El valor máximo a pagar por estas capacidades será de hasta el 39% del valor del contrato.	La forma de pago está dividida en bloques, pero la suma de los dos bloques principales (38% + 39% = 77%) no llega al 100% del valor total del contrato. El 23% restante no está asignado expresamente a ningún concepto, por lo que no es claro cómo se pagará esa parte ni en qué momento.	Amablemente solicitamos completar la tabla de pagos de manera que la suma de todos los ítems llegue al 100% del valor del contrato (USD 13.002.825). Indicar expresamente a qué conceptos (servicios mensuales de SOC, ethical hacking, capacitaciones) corresponde el porcentaje restante.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el 23% de la forma de pago está expresado en el documento SDO páginas 124 y 125, allí se describen los detalles y los entregables para hacer el pago.
4	Sección VI - ANS Id. 01	Nota: el valor a descontar no puede ser superior al 20% del valor de la mensualidad. (ANS 01 - Cumplimiento en la fecha de entrega de cada producto final).	El límite del 20% por retrasos en la entrega de productos es alto y excede el parámetro permitido. Sin embargo, el descuento se calcula en salarios mínimos (SMMLV), no en porcentaje del contrato, lo que dificulta verificar si ese tope del 20% se respeta en la práctica sin conocer el valor exacto de cada hito.	Solicitamos de manera respetuosa que se disminuya el porcentaje de las ANS al 10%. Además, agregar en la tabla del ANS 01 el valor aproximado en pesos o dólares que representa el 10% del hito correspondiente o indicar que el descuento en SMMLV nunca podrá superar ese porcentaje del valor del hito. Esto facilita el control y evita discusiones al momento de aplicar el descuento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN precisa al observante que, en la Sección VI. Requisitos de los Bienes y Servicios Conexos, numeral 8. ANS (SLA) están definidas las condiciones de aplicación de los ANS frente a los valores por mes y frente al valor tal del contrato.
5	Sección VI - ANS Id. 03	Nota: el valor a descontar no puede ser superior al 10% del valor de la mensualidad. (ANS 03 - Cumplimiento en tiempo de solución de incidentes).	El tope del 10% mensual para este indicador es razonable y está dentro del parámetro permitido. El problema es que el documento no aclara si los descuentos del ANS 01 y el ANS 03 se suman entre sí en un mismo mes. Si se acumulan podrían superar el tope global del 10% del contrato que está fijado más adelante en el mismo documento.	Agradecemos incluir una regla clara que establezca que la suma de todos los descuentos por ANS en un mismo mes no puede superar un tope mensual determinado y que en ningún caso la acumulación total puede superar el 10% del valor total del contrato.	La Dirección de Impuestos y Aduanas Nacionales - DIAN precisa al observante que, en la Sección VI. Requisitos de los Bienes y Servicios Conexos, numeral 8. ANS (SLA) están definidas las condiciones de aplicación de los ANS frente a los valores por mes y frente al valor tal del contrato.
6	2. Estrategia de implementación (40 puntos)	FIRST, Certificación que acredite vinculación directa y activa con FIRST (Forum Incident Response and Security Teams) como mínimo doce (12) meses de antigüedad.	3. Observación – Certificación FIRST Asunto: Solicitud de ajuste de la antigüedad de la certificación FIRST. El pliego establece como requisito la presentación de: *"Certificación que acredite vinculación directa y activa con FIRST (Forum of Incident Response and Security Teams), como mínimo doce (12) meses de antigüedad".* Solicitud de Modificación Respetuosamente solicitamos modificar el requisito de antigüedad en FIRST, estableciendo como condición: "Certificación que acredite vinculación directa y activa con FIRST (Forum of Incident Response and Security Teams), con una antigüedad mínima de cinco (5) años". Justificación Técnica y Estratégica El presente proceso tiene por objeto la prestación integral de un Centro de Operaciones de Seguridad (SOC) para la DIAN, entidad que administra información tributaria, aduanera y fiscal estratégica del Estado colombiano. En consecuencia, el nivel de criticidad del servicio exige un SOC con altos estándares de madurez operativa y experiencia comprobada en gestión de incidentes. La afiliación a FIRST no solo acredita reconocimiento internacional, sino que implica: • Participación activa en redes globales de respuesta a incidentes. • Acceso a inteligencia colaborativa de amenazas. • Cumplimiento de estándares técnicos y de gobernanza. • Validación entre pares (peer validation). No obstante, una antigüedad mínima de doce (12) meses resulta insuficiente para demostrar: • Madurez real de los procesos de respuesta a incidentes. • Integración efectiva en comunidades internacionales de ciberseguridad. • Trayectoria consolidada en gestión de eventos complejos. • Experiencia sostenida en cooperación internacional. Una membresía de cinco (5) años permite evidenciar: • Continuidad institucional en la operación del CSIRT/SOC. • Sostenibilidad en el cumplimiento de estándares internacionales. • Evolución y mejora continua de los procesos. • Experiencia acumulada frente a distintos ciclos de amenazas globales. Coherencia con los Criterios de Evaluación Técnica	Solicitud Final Respetuosamente solicitamos modificar el requisito de antigüedad en FIRST, estableciendo un mínimo de cinco (5) años de vinculación directa y activa, con el fin de garantizar: • Mayor madurez operativa del SOC. • Coherencia con la evaluación técnica. • Mitigación efectiva de riesgos. • Selección de un proveedor alineado con la criticidad institucional de la DIAN.	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, y se encuentra con una antigüedad de doce (12) meses lo que es amplio y suficiente a consideración de la Entidad, por lo tanto, no se acepta su sugerencia.
7	(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	4. Acreditación de Experiencia: Estado de Ejecución de los Contratos Objeto de la observación Se solicita respetuosamente a la entidad contratante que modifique el requisito de experiencia 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.
8	Sección VI	A partir de la terminación de las fechas mencionadas, el proponente deberá iniciar la implementación de las nuevas soluciones (SIEM, Protección de bases de datos e Inteligencia de amenazas) y entregar la respectiva puesta en operación de estas soluciones, las cuales quedarán bajo su gestión, monitoreo y administración hasta octubre de 2028, recordando que el derecho de uso y licenciamiento de estas plataformas es por tres (3) años, según la siguiente relación	Solicitamos a la DIAN considerar que para no tener perdidas de correlación de eventos, la nueva soluciones sea implementada 2 meses antes de la finalización del licenciamiento de la actual herramienta.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el futuro proveedor de SOC con antelación y planeación deberá realizar la implementación de los nuevos servicio de firewall de bases de datos, SIEM e inteligencia de amenazas, teniendo en cuenta las fechas de terminación de los servicios del anteriores, para así no impactar en la operación del servicio en mención y dar continuidad ininterrumpida a la operación .
9	Sección VI	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.	Teniendo en cuenta que los conceptos de NDR (Network Detection and Response) e Inteligencia de Amenazas (Threat Intelligence) corresponden a capacidades relacionadas, pero no necesariamente equivalentes, agradecemos a la entidad precisar el alcance exacto de la necesidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, las características del servicio en mención están claramente detalladas en el anexo técnico así como su respectivo alcance.
10	15.1 Sección VI	La transferencia de conocimiento y la documentación entregada deben contemplar, además de lo técnico, los lineamientos de operación, las obligaciones del proveedor y las políticas de protección de activos de información conforme a la clasificación vigente en la DIAN.	Agradecemos a la DIAN indicarnos la cantidad de personas a las que se les impartirá la trasferencia de conocimiento y si el la entidad suministrar la logistica para la misma o por el contrario el proponente debe contemplar la logistica.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, las características como cantidad y publico objetivo de la transferencia de conocimiento se encuentran descritas en el ítem 15.1 del anexo técnico.
11	Sección VI	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.	Agradecemos a la DIAN nos indique si este tiempo de implementación es aplicable para las soluciones que tienen vencimiento de licenciamiento en 2027.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, los tiempos también serían aplicables para las soluciones con vencimientos diferentes (SIEM, FIREWALL DE BASES DE DATOS e Inteligencia de amenazas), en el entendido que el proveedor de SOC deberá prever los tiempos amplios y suficientes para la implementación de estas soluciones antes de la fecha de vencimiento de los servicios actuales.
12	12.59	Deberá proveer los canales de comunicaciones que requiera en un esquema redundante entre las multinubes y los sitios on premises de la DIAN y el sitio del SOC donde se presten los servicios.	Agradecemos a la DIAN indicar si es correcto el entendimiento que el proponente debe contemplar los canales de comunicación (Internet) para interconectar el SOC con la entidad y sus nubes.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el canal de comunicación (internet) para interconectar el SOC con la Entidad y sus nubes deberá ser provisto por el proveedor del SOC, para lo cual el ítem en mención será ajustado y publicado mediante adenda los próximos días, quedando de la siguiente manera: 12.59 Prestar el servicio desde un centro de operaciones de seguridad (SOC) ubicado en la ciudad de Bogotá D.C. (Colombia), cuyo canal de comunicación con la infraestructura de la Dian deberá ser provisto por el futuro proveedor de los servicios de SOC.
13	Sección VI	Deberá proveer los canales de comunicaciones que requiera en un esquema redundante entre las multinubes y los sitios on premises de la DIAN y el sitio del SOC donde se presten los servicios.	Agradecemos a la entidad indicarnos si actualmente cuenta con una conectividad entre la DIAN y las Nubes de AWS y AZURE? (VPN S2S, Express Routing, etc.)		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, actualmente la Entidad cuenta con los canales para la conexión entre DIAN y las nubes.
14	Sección VI	Entregar todos los componentes tecnológicos (físicos y lógicos) para la operación del SOC incluidas las licencias a perpetuidad a nombre de la DIAN implementadas y configuradas durante el proyecto y que sean susceptibles de ello, con las mismas capacidades de operación del SOC en el momento de la devolución del servicio con soporte actualizado por mínimo un año.	Agradecemos a la entidad aclarar el alcance de la expresión "licencias a perpetuidad", indicando específicamente a qué componentes tecnológicos, herramientas, plataformas o módulos del SOC aplica dicha condición.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, la expresión licenciamiento a perpetuidad refiere a los casos donde aplique, es claro que, si el futuro proveedor de SOC entrega este tipo de licenciamiento, al momento de finalizar los servicios, estos deben quedar a nombre de la Entidad.
15	Sección VI	El diseño de la estrategia de presentación del servicio SOC, podrá incluir servicios tipo SaaS, PaaS, IaaS, XaaS. En el caso de on-premises, el proponente deberá proveer el hardware requerido, considerando	Agradecemos a la entidad indicar en caso de implementarse el SIEM en nube y/o premisas si pueden suministrar los colectores tanto en premisas y nubes en donde se encuentran activos a integrar. Por cada 250 Activos se debe contemplar un colector de las siguientes características 8vcpu 16 ram 480 GB SSD		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, todos los elementos necesarios para implementar y prestar los servicios requeridos por la Entidad deberán ser provistos por el futuro proveedor de SOC.
16	2.4	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.	Agradecemos a la entidad dar un alcance a este requerimiento, modificando la palabra "mínimo" a la palabra "hasta".		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los requerimientos solicitados son mínimos, y es el alcance que se debe cumplir, si el futuro proveedor estima conveniente entregar más de esa cantidad lo puede hacer sin acarrear costo alguno para la Entidad, por lo tanto, no se acepta su sugerencia.
17	2.5	Debe tener la capacidad de manejar como mínimo 25000 EPS o unidad de medida equivalente o superior.	Agradecemos a la entidad dar un alcance a este requerimiento, modificando la palabra "mínimo" a la palabra "hasta".		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los requerimientos solicitados son mínimos, y es el alcance que se debe cumplir, si el futuro proveedor estima conveniente entregar más de esa cantidad lo puede hacer sin acarrear costo alguno para la Entidad, por lo tanto, no se acepta su sugerencia.
18	2.27	Sistema incorporado de ticketing o integrarse al sistema de ticketing de la entidad (Aranda)	Agradecemos a la entidad indicar si la plataforma siem debe enviar directamente las notificaciones a ARANDA o se puede utilizar el SOAR para enviar los alertamientos del siem al soar y este despliegue a ARANDA.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento es claro en el sentido de solicitar integración la plataforma de la Entidad (Aranda).
19	2.30	Integración con cualquier sitio web externo para la búsqueda de direcciones IP.	Agradecemos a la entidad dar un alcance a este requerimiento, ya que si la web externa no tiene un api o tenga un api de pago no podrá integrarse.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento es claro en el sentido de solicitar Integración con cualquier sitio web externo para la búsqueda de direcciones IP.
20	2.25	Búsqueda de eventos en real - sin necesidad de indexación	Agradecemos a la entidad re formular esta pregunta ya que todo siem indexa primero el evento para después mostrarlo		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem 2.25 fue ajustado mediante adenda.
21	2.30	Soporte de Apache Kafka para la integración con informes mejorados de análisis, por ejemplo, PowerBI, ELK, Tableau y Hadoop.	Agradecemos a la entidad aclarar si la solución SIEM debe tener un modulo de apache kafka para la integración con PowerBI, ELK, Tableau y Hadoop ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la solución SIEM debe soportar Apache Kafka para la integración con informes mejorados de análisis.
22	3.71	La solución debe contar con conectores ya desarrollados para integración con las siguientes plataformas con las que cuenta la entidad: Firewall de Nueva generación, Sandbox, plataforma de logs y reportes (SIEM)	Agradecemos a la entidad indicar con que marca de sandbox cuentan.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se tienen dos SANDBOX, uno del fabricante TrendAI y otro de Bitdefender.
23	Sección III	2. Estrategia de implementación (40 puntos) Los oferentes deberán presentar como parte de la oferta técnica un documento que contenga el plan de seguimiento y monitoreo mediante las capacidades y servicios adquiridos, a los controles tecnológicos de la norma ISO 27001:2022, detallando las etapas, tiempos y acciones necesarias, con un desglose de actividades, especificando las fases para el seguimiento a los controles, los hitos clave y las dependencias entre tareas, de manera que se pueda monitorear cada uno de estos controles, teniendo en cuenta como mínimo los siguientes aspectos:	Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que lo requerido en este punto es que se haga una alineación entre las soluciones y servicios solicitados en el RFP y los controles técnicos de la ISO 27001:2022 que se cumplen con estas soluciones.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, Los oferentes deberán presentar como parte de la oferta técnica un documento que contenga el plan de seguimiento y monitoreo mediante las capacidades y servicios adquiridos, a los controles tecnológicos de la norma ISO 27001:2022, detallando las etapas, tiempos y acciones necesarias, con un desglose de actividades, especificando las fases para el seguimiento a los controles, los hitos clave y las dependencias entre tareas, de manera que se pueda monitorear cada uno de estos controles.
24	14.1 - 14.2	2. 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:	Agradecemos a la entidad confirmar la cantidad de capacitaciones requeridas durante la ejecución de proyecto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las capacitaciones se encuentran descritas en los ítems 14.1 y 14.2 del anexo técnico.
25	Sección IV	Cumplimiento en tiempo de contención ó solución de incidentes	Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que aunque el SOC tiene alcance al Monitoreo, detección y acciones de respuesta en los incidentes, La resolución de los mismos puede darse por parte de los Equipos internos de la DIAN o sus terceros. En este sentido es importante que la DIAN considere que el tiempo total de resolución de un incidente se vera afectado por tiempos de terceros (ajenos al Oferente) y que estos deberán ser descontados del tiempo total de resolución de la incidencia.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, su entendimiento es correcto, en el sentido de que los tiempos de terceros serán descontados del tiempo total de resolución de la incidencia.
26	Sección VI	El proponente deberá tener como referencia un modelo tipo "llave en mano", tomando como base fija el modelo presentado, las capacidades y servicios requeridos de la infraestructura de seguridad de la información descritas en el numeral 3.1 y 3.2.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: ¿el alcance "llave en mano" incluye el suministro, implementación y operación de una plataforma ITSM (herramienta de ticketing y gestión de incidentes) como parte integral del contrato, o la DIAN dispone de una plataforma ITSM existente a la cual el proponente deberá integrarse sin costo adicional?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, su entendimiento es correcto, en el sentido de que la DIAN dispone de una plataforma ITSM existente a la cual el proponente deberá integrarse sin costo adicional para la Entidad.
27	Sección VI	El proponente deberá considerar dentro de su propuesta económica todos los valores asociados al desarrollo del proyecto incluyendo los derivados de herramientas, desarrollos e integraciones con sistemas ya existentes o similares, personal, infraestructura, recursos ofimáticos y administrativos, entre otros.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: ¿la plataforma de gestión del conocimiento del SOC debe ser suministrada por el proponente como parte del modelo "llave en mano", o la DIAN dispone de una plataforma existente para este fin?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, para la plataforma de gestión del conocimiento, el futuro operador del SOC deberá utilizar la suya.
28	Sección VI	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 operacional.	Agradecemos a la entidad relacionar las especificaciones técnicas mínimas que debe cumplir el recinto físico del SOC en cuanto a: superficie mínima en metros cuadrados, capacidad eléctrica instalada (KVA), redundancia de conectividad a Internet (número de ISPs y ancho de banda mínimo), sistema de control de acceso físico, nivel de climatización requerido (temperatura y humedad)		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características mínimas que debe cumplir el recinto físico del SOC están descritas en el ítem 12 del anexo técnico.
29	Equipo Mínimo de Trabajo	La DIAN será responsable de proporcionar lo siguiente para esta modalidad: Accesos Remotos: facilitará los accesos remotos seguros a los entornos de trabajo definidos. Espacios Físicos y Servicios de TI: se facilitarán los espacios físicos adecuados con acceso a telefonía, red, internet. El proponente será responsable de proveer a su personal con los equipos de cómputo y recursos necesarios.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: ¿cuál es la proporción del equipo mínimo que deberá laborar de manera presencial en las instalaciones de la DIAN versus en el recinto SOC del proponente? ¿Existen perfiles específicos del equipo mínimo de la Tabla 6 que la DIAN requiere que operen obligatoriamente en sus instalaciones físicas?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, como mínimo se requiere que un Especialista de Respuesta a Incidentes (IR) deberá asistir de manera presencial a la Entidad, tal como se indica en la composición del Equipo Mínimo de Trabajo solicitado por la Entidad.
30	Sección VI	El valor máximo a pagar por las capacidades de las Fases 1 y 2 (ítems 2,4,5,7,8,10,14) será de hasta el 38% del valor del contrato. Cada ítem: 1 pago al recibo a satisfacción de los entregables de esta capacidad.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento, ¿cada uno de los siete ítems del Bloque A (ítems 2, 4, 5, 7, 8, 10, 14) genera un pago independiente en el momento en que ese ítem específico es recibido a satisfacción, o los siete ítems se pagan en un único desembolso consolidado al finalizar la totalidad de la Fase 1+2?.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el valor máximo a pagar por estas capacidades será de hasta el 38% del valor del contrato al termino de la implementación en los cuatro (4) meses otorgados para tal fin, siempre y cuando se cumpla la premisa de que los servicios deberán estar operativos.
31	Sección VI	Ítem 1 – SIEM Correlacionador de Eventos. Fecha de entrega: septiembre de 2027. 1 pago al recibo a satisfacción de los entregables de esta capacidad.	Solicitamos amablemente a la entidad confirmar nuestro entendimiento: ¿la operación de IBM QRadar desde el inicio del contrato hasta agosto de 2027 queda remunerada exclusivamente a través del Ítem 11 (Monitoreo y Operación SOC mensual), o existe algún reconocimiento económico adicional específico por la operación de las herramientas IBM durante el período de transición?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, su entendimiento es correcto, la operación del SIEM IBM QRADAR es un rubro que esta incluido en el ítem 11 (Monitoreo y Operación SOC mensual) por lo tanto, el futuro oferente debe tenerlo en cuenta en sus cálculos de la oferta a presentar.
32	6	Ítem 6 – NDR: Fecha de entrega enero de 2028. Ítem 3 – Herramienta de protección de bases de datos: Fecha de entrega enero de 2028. 1 pago al recibo a satisfacción de los entregables de cada capacidad.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: el Ítem 12 (Garantía y Soporte técnico de 3 años) que hace parte del Bloque B (39%), ¿se paga en una única vez al finalizar la implementación de los tres ítems del bloque (sept-2027 y ene-2028), o genera pagos anuales durante los tres años de vigencia de la garantía? Agradecemos a la entidad precisar la fecha estimada de pago del Ítem 12.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, para el ítem en cuestión y los servicios a entregar en fechas especificas (2027 y 2028) el pago de garantía y soporte técnico de tres (3) años se haría al momento de la puesta en operación de dichos servicios.
33	Sección VII	El plazo de ejecución del contrato será de 36 meses o hasta cumplir el tiempo objetivo que será máximo el 30 de octubre de 2028. Ítem 11 – Pagos mensuales hasta el agotamiento de los recursos.	Agradecemos a la entidad relacionar la información de cuántas mensualidades del Ítem 11 serán reconocidas económicamente durante la vigencia del contrato, considerando tanto el escenario de 36 meses completos como el escenario de terminación anticipada al 30 de octubre de 2028.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, para el ítem en cuestión que son de tracto sucesivo sus pagos irían hasta octubre 30 de 2028, recordando 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.
34	Sección VI	Desde el inicio del contrato y hasta las fechas mencionadas, el proponente deberá realizar la operación, administración y gestión de las soluciones con las que cuenta actualmente la entidad: IBM QRadar e IBM Guardium.	Solicitamos amablemente a la entidad confirmar nuestro entendimiento: ¿el Ítem 11 (Servicios de Monitoreo y Operación SOC mensual) comienza a generar pagos desde el Día 1 del inicio del contrato, incluyendo el período de la Fase 1+2 (primeros cuatro meses de implementación), toda vez que desde ese Día 1 el proponente está prestando efectivamente el servicio de operación de IBM QRadar e IBM Guardium?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, su entendimiento es correcto, desde el Día 1 del inicio del contrato se generan pagos para el futuro contratista del SOC que está prestando efectivamente el servicio de operación de IBM QRadar e IBM Guardium, siempre y cuando ya haya recibido dichas plataformas a satisfacción y se encuentre administrándolas y operándolas según lo requerido por la Entidad.

Información Pública

35	Sección VI	Desde el inicio del contrato [...] el proponente deberá realizar la operación, administración y gestión de las soluciones con las que cuenta actualmente la entidad IBM QRadar e IBM GUARDIUM. Lo anterior incluye la monitorización, análisis, generación de informes y soporte técnico.	Agradecemos a la entidad compartir la información técnica de IBM QRadar actualmente operativo en la DIAN, incluyendo: versión del producto , número aproximado de fuentes de log (log sources) activas y conectadas, número de reglas de correlación personalizadas configuradas, número de casos de uso (use cases) activos, y las integraciones existentes con otras herramientas de seguridad de la DIAN.		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
36	Sección VI	Un firewall de bases de datos IBM GUARDIUM contratado hasta diciembre 31 [de 2027]. Desde el inicio del contrato, el proponente deberá realizar la operación, administración y gestión de [...] IBM GUARDIUM.	Agradecemos a la entidad compartir la información técnica del IBM Guardium actualmente operativo, incluyendo: versión del producto Guardium, número de agentes S-TAP instalados y en qué servidores de base de datos, motores de base de datos que cubre actualmente (Oracle, SQL Server u otros), políticas de auditoría activas y modo de despliegue (gateway, S-TAP local, o combinado).		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.
37	Sección VI	Con anterioridad al vencimiento del licenciamiento de las soluciones en las fechas señaladas, el proponente deberá proveer herramientas que permitirán dar continuidad a la vigilancia y el monitoreo que tengan las mismas o superiores capacidades.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: ¿contempla la DIAN un período de operación en paralelo entre la plataforma IBM saliente y la nueva plataforma del proponente antes del corte definitivo?. En caso afirmativo, agradecemos a la entidad indicar la duración esperada de ese período de operación en paralelo para el SIEM (previamente a septiembre 2027) y para la protección de bases de datos (previamente a enero 2028).		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se contempla un período de operación en paralelo, el futuro operador de soc debe generar las estrategias adecuadas y necesarias para implementar las nuevas herramientas SIEM y protección de bases de datos y que garanticen la continuidad ininterrumpida de los respectivos servicios.
38	Sección VI	La solución de Inteligencia de Amenazas contratada hasta diciembre 31 de 2027 es administrada y operada por la entidad hasta el 31 de diciembre de 2027.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: ¿cuál es el mecanismo previsto para que el equipo SOC del proponente consuma los datos e indicadores de la solución de Inteligencia de Amenazas que opera la DIAN hasta diciembre 2027? Agradecemos a la entidad relacionar la información del fabricante y versión de dicha solución, así como los formatos y APIs disponibles para su integración con las herramientas del proponente.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la solución que maneja la Entidad es TREND VISION ONE y debe ser integrada como fuente al monitoreo del futuro Centro de Operaciones de Seguridad - SOC
39	2.5	SIEM – Correlacionador de Eventos. Unidad de medida: EPS o unidad de medida equivalente similar o superior. Mínimo: 25.000.	Agradecemos a la entidad compartir la información del reporte histórico de tasa de EPS procesados por IBM QRadar durante los últimos doce (12) meses, indicando la tasa promedio diaria y la tasa de pico máxima sostenida durante una hora, desagregada por tipo de fuente de log (firewalls CheckPoint, endpoints, servidores Windows/Linux, servidores Azure, conectores AWS y bases de datos Oracle/SQL).		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el histórico de EPS ha sufrido cambios drásticos debido al ajuste de falsos positivos, como consecuencia, la información histórica no refleja la realidad del comportamiento esperado.
40	Sección VI	SIEM – Correlacionador de Eventos. Mínimo: 25.000 EPS. [Catálogo Azure: 379 máquinas virtuales, 452 cuentas de almacenamiento, 128 grupos de seguridad de red, entre otros activos cloud.]	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: ¿los 25.000 EPS mínimos incluyen los eventos generados por los activos en Azure y AWS, o aplican exclusivamente a los activos on-premise del Sitio1 y Sitio2? En caso de que los eventos cloud estén excluidos, solicitamos amablemente a la entidad relacionar la información del volumen estimado de EPS provenientes de Azure y AWS.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los 25000 EPS mínimos requeridos incluyen los eventos generados en los activos en Azure y AWS.
41	Sección VI	La DIAN cuenta con sus sistemas de información y servicios tecnológicos en la multinube (nube primaria - Azure y nube secundaria – AWS) y on premises en dos centros de cómputo sitio1 y sitio2	Solicitamos amablemente a la entidad confirmar si la arquitectura de despliegue del nuevo SIEM debe incluir colectores dedicados on-premise en Sitio1 y Sitio2 (appliance físico o VM), o si acepta una arquitectura de colección mixta donde los eventos on-premise se reenvían vía syslog/agente y los eventos cloud vía APIs nativas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, si para dar cumplimiento con lo requerido para el SIEM y cualquier otro servicio solicitado por la Entidad, el proveedor del SOC requiere instalar colectores o dispositivos lo podrá hacer siempre y cuando cumpla con lo solicitado por la DIAN.
42	Sección VI	La solución debe basarse en un sistema de seguridad que reciba todo el tráfico de la red desde uno o varios switches, lo analice e identifique las amenazas o incidentes que están ocurriendo en la red. La herramienta debe soportar el modo de implementación: Port mirror (SPAN PORT).	Agradecemos a la entidad compartir la información del diagrama lógico de red de los Sitio1 y Sitio2, indicando los switches de core/distribución que tienen puertos SPAN disponibles para la instalación de sensores NDR.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la información solicitada es de carácter reservado, por lo tanto, no se acepta su petición.
43	Sección VI	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.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: ¿el requerimiento de retención de seis (6) meses en el appliance sin conexión a la nube aplica únicamente para los datos de tráfico on-premise (Sitio1 y Sitio2), permitiendo que los datos de tráfico cloud (Azure y AWS) sean analizados y almacenados en la nube del fabricante NDR, o el requerimiento aplica también para los datos de tráfico provenientes de los entornos cloud?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el requerimiento es bien claro en el sentido que solicita: 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.
44	Sección VI	Monitoreo a la Gestión de Vulnerabilidades. Unidad de medida: Activos de información. Mínimo: 18.000.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento sobre la definición de "activo de información" para efectos del licenciamiento de la herramienta de gestión de vulnerabilidades: ¿se refiere a una dirección IP única, a un dispositivo físico o virtual, o a un nombre de host/FQDN?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la cantidad mínima requerida es 25000 activos.
45	Sección VI	Monitoreo a la Gestión de Vulnerabilidades. Mínimo: 18.000. [Tabla 1 – Total activos: 24.284, incluyendo 379 VMs Azure y activos AWS.]	Agradecemos a la entidad relacionar la información del criterio de priorización que define cuáles activos del inventario total (24.284) están incluidos en los 18.000 a licenciar para gestión de vulnerabilidades. Específicamente, solicitamos confirmar si los activos en Azure (379 VMs + otros recursos) y AWS están incluidos o excluidos de los 18.000, dado que los activos cloud también presentan vulnerabilidades que requieren gestión continua.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la cantidad mínima requerida es de 25000 activos a licenciar, se aclara que dentro de esa cantidad están incluidos los activos de AZURE.
46	Sección VI	Solución de análisis de código estático y dinámico para aplicaciones. Unidad de medida: Aplicaciones. Mínimo: 50.	Solicitamos amablemente a la entidad aclarar si el modelo de licenciamiento preferido para la solución SAST/DAST es por número de aplicaciones escaneadas , o si la entidad acepta modelos alternativos como por número de desarrolladores, por repositorio de código o por proyecto de desarrollo.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la cantidad mínima a licenciar es de 50 aplicaciones.
47	9	Protección de marca. Unidad de medida: Activos públicos. Mínimo: 260.	Solicitamos amablemente a la entidad confirmar si los 260 activos públicos para protección de marca son los mismos 260 aplicaciones web del inventario de la Tabla 1, o si corresponden a una categoría diferente que incluye dominios, subdominios y perfiles en redes sociales institucionales adicionales a las aplicaciones web. Adicionalmente, agradecemos a la entidad relacionar el listado de dominios y subdominios oficiales de la DIAN.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la cantidad mínima a licenciar es de 260 aplicaciones web y son las mismas referidas en la tabla 1.
48	Sección VI	Equipo Mínimo de Trabajo: Gerente de Proyecto 1. [Nota 1]: Cada uno de los perfiles se detalla en el Anexo Técnico en la hoja "Equipo mínimo de trabajo". [Numeral 9, Obligación 5]: El proponente deberá manejar la gestión del contrato bajo una metodología de Gestión de Proyectos como los lineamientos dados por el Project Management Institute (PMI) o PRINCE2, entre otros.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: para el perfil de Gerente de Proyecto, ¿la entidad acepta como equivalente a la certificación PMP del PMI una Especialización o Maestría o Diplomado en Gerencia de Proyectos de una universidad acreditada por el Ministerio de Educación de Colombia o por un organismo internacional de acreditación?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta equivalencia a la certificación PMP, lo mínimo requerido para el perfil en mención se encuentra descrito en el respectivo ítem de equipo mínimo de trabajo.
49	Sección VI	Equipo Mínimo de Trabajo: Gerente de Proyecto 1. [Numeral 9, Obligación 5]: El proponente deberá manejar la gestión del contrato bajo metodologías PMI o PRINCE2, entre otros.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: ¿la entidad acepta certificaciones complementarias de gestión de proyectos en ciberseguridad como CISM (Certified Information Security Manager) de ISACA, o una certificación de gestión de proyectos ágiles, como requisito adicional o alternativo al PMP para el perfil de Gerente de Proyecto?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta equivalencias a las certificaciones solicitadas
50	Sección VI	Equipo Mínimo de Trabajo: Líder/Coordinador SOC 1. [Nota 1]: Cada uno de los perfiles se detalla en el Anexo Técnico.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: para el perfil de Líder/Coordinador SOC, ¿la entidad acepta como equivalente a una certificación tipo CISSP o CISM una Especialización en Seguridad Informática, Ciberseguridad o Seguridad de la Información		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta equivalencias a las certificaciones solicitadas
51	Sección VI	Equipo Mínimo de Trabajo: Líder/Coordinador SOC 1. [Sección III Criterio b]: El oferente deberá acreditar su pertenencia a la más alta membresía por parte de los fabricantes de los productos ofrecidos.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: para efectos del criterio de evaluación de nivel de partner con los fabricantes (Sección III, criterio b), ¿se exige que los miembros del equipo mínimo de trabajo del SOC cuenten con certificaciones técnicas específicas de los fabricantes , o el nivel de partnership se acredita únicamente con la certificación de la empresa como tal ante el fabricante?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el criterio puntuable de la sección III en este caso literal b, puntúa al futuro proveedor de SOC cuando este rankeado en la más alta membresía frente al fabricante del servicio ofrecido y de acuerdo a la cantidad de membresías acreditadas, no tiene nada que ver con el equipo mínimo de trabajo que es un requerimiento mínimo donde se solicitan para determinados perfiles certificaciones de conocimientos de los servicios ofrecidos emitidas por los fabricantes.
52	Sección VI	Equipo Mínimo de Trabajo: Threat Hunter / Analista de Ciberinteligencia 1. [Nota 1]: Cada uno de los perfiles se detalla en el Anexo Técnico.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: para el perfil de Threat Hunter / Analista de Ciberinteligencia, ¿la entidad acepta como certificaciones válidas y equivalentes la siguiente?: Certified Ethical Hacker (CEH)		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta equivalencias a las certificaciones solicitadas.
53	Sección VI	Threat Hunter / Analista de Ciberinteligencia 1. [Anexo Técnico NDR]: Los procesos de Threat Hunting deberán indicar las fases del ciberataque en lo que se hayan visto las anomalías detectadas. El proceso deberá poder correlacionar anomalías detectadas dentro de la misma plataforma de IA e identificar si pertenecen o no a un ataque más complejo.	Agradecemos a la entidad relacionar la información sobre si la entidad acepta como alternativa a una certificación formal de threat hunting la experiencia documentada y verificable en la ejecución de ejercicios de threat hunting en entornos productivos durante los últimos años.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta equivalencias a las certificaciones solicitadas.
54	Sección VI	Equipo Mínimo de Trabajo: Especialista de Respuesta a Incidentes (IR) 1. [Nota 1]: Cada uno de los perfiles se detalla en el Anexo Técnico.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: para el perfil de Especialista de Respuesta a Incidentes (IR), ¿la entidad acepta como certificaciones válidas las siguientes?: EC-Council Computer Hacking Forensic Investigator (C|HFI), Certified Digital Forensics Examiner (CDFE) de Mile2, experiencia documentada en respuesta a incidentes bajo estándares ISO/IEC 27035.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta equivalencias a las certificaciones solicitadas.
55	Sección VI	Equipo Mínimo de Trabajo: Especialista de Respuesta a Incidentes (IR) 1. [Sección VI, Num. 3.2]: Las actividades de Ethical Hacking deberán contar con consentimiento y autorización formal de la OSI.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: para los ejercicios de Ethical Hacking (ítem 9), ¿la entidad exige que el profesional que lidere dichos ejercicios cuente con una certificación específica de pentesting como CEH (EC-Council), LPT Master (EC-Council), u otra certificación de penetración activa?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta equivalencias a las certificaciones solicitadas.
56	Sección VI	Equipo Mínimo de Trabajo: Un (01) Analista SOC Nivel III 1.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: para el perfil de Analista SOC Nivel III, ¿la entidad acepta como certificaciones equivalentes las certificaciones avanzadas de las plataformas de las tecnológica ofertada como demostración de competencia técnica suficiente para este nivel?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta equivalencias a las certificaciones solicitadas.
57	Sección VI	Caza de amenazas (Ítem 5). Solución SAST/DAST (Ítem 7). Protección de marca (Ítem 8). [Anexo NDR]: Los procesos de Threat Hunting deberán realizarse manuales basados en TTPs MITRE de manera recurrente, identificando qué anomalías detectadas por la plataforma hacen parte de las técnicas buscadas.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: ¿los servicios de gestión de superficie de ataque externa son responsabilidad del perfil Threat Hunter / Analista de Ciberinteligencia del equipo mínimo, o la entidad contempla un perfil adicional especializado en ASM? ¿se aceptan certificaciones de experiencia documentada en la gestión de superficie de ataque?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se contemplan perfiles adicionales a los requeridos, si el futuro proveedor del SOC contempla adicionar perfiles o recurso humano lo puede hacer siempre y cuando no represente costos adicionales para la Entidad, así mismo, se aclara que no se aceptan equivalencias en las certificaciones solicitadas.
58	Sección VI	ANS Ítem 03 – Cumplimiento en tiempo de contención o solución de incidentes. INC = ((TRS-TM) * FC). Incidentes críticos (prioridad 1): 1 hora / 8 horas. Incidentes mayores (prioridad 2): 4 horas / 16 horas. Incidentes menores (prioridad 3): 8 horas / 48 horas.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: ¿desde qué evento específico comienza el cómputo del Tiempo Máximo en el ANS 03? ¿Desde la generación automática de la alerta por el SIEM/SOAR, desde la apertura del ticket en el sistema de gestión de incidentes por el Analista L1, desde la clasificación y tipificación formal del incidente por el analista, o desde la notificación oficial al supervisor?.		La Dirección de Impuestos y Aduanas Nacionales - DIAN precisa al observante que el ANS es claro y se refiere a incidente, es decir desde que el evento se tipifica formalmente como incidente
59	Sección VI	ANS Ítem 01 – Cumplimiento en la fecha de entrega de cada producto final definido en los planes de trabajo de los proyectos. D = Número de días de retraso. Nota: el valor a descontar no puede ser superior al 20% del valor de la mensualidad.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: el ANS 01 (cumplimiento de fechas de entrega), ¿aplica por ítem de capacidad de forma independiente, por ejemplo: un retraso en la implementación del SIEM no afecta el ANS del Ítem 11 de operación mensual?		La Dirección de Impuestos y Aduanas Nacionales - DIAN precisa al observante que en la Sección VI. Requisitos de los Bienes y Servicios Conexos, numeral 8. ANS (SLA) define las condiciones de aplicación de los ANS frente a los valores por mes y frente al valor tal del contrato.
60	10	Ítem 9 – Ethical hacking. Entregables: Informes de resultado de ejercicios de Ethical Hacking realizados. Hasta 6 pagos. Cada pago corresponde al valor unitario ofertado para cada ejercicio.	Agradecemos a la entidad relacionar la información del alcance mínimo que debe contemplar cada ejercicio de Ethical Hacking, incluyendo: tipo de prueba por ejercicio , número aproximado de sistemas / IPs / URLs en alcance por ejercicio,, profundidad del análisis y duración estimada en días hábiles por ejercicio.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se contemplan perfiles adicionales a los requeridos, si el futuro proveedor del SOC contempla adicionar perfiles o recurso humano lo puede hacer siempre y cuando no represente costos adicionales para la Entidad, así mismo, se aclara que no se aceptan equivalencias en las certificaciones solicitadas.
61	Sección VI	Las actividades de Ethical Hacking deberán contar con consentimiento y autorización formal de la OSI, respetando los principios de legalidad, finalidad y minimización del riesgo sobre activos. El resultado de estas pruebas deberá estar documentado con rigor probatorio y en formatos auditables.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: ¿el tiempo de coordinación pre-ejercicio para obtener las autorizaciones formales y definir el scope de cada ejercicio de Ethical Hacking se computará dentro del plazo del entregable del Ítem 9, o es un tiempo previo al inicio del ejercicio que no genera penalización por el ANS 01 de cumplimiento de fechas?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, es un tiempo previo al inicio del ejercicio que no genera penalización por el ANS 01.
62	Sección VI	Se deberán realizar cinco (5) capacitaciones para la obtención de los certificados: CISSP, CISM, ECES, CEH, CCNA. Las capacitaciones serán dictadas para cinco (5) ingenieros cada una. Cada capacitación deberá contar con sus respectivos vouchers para la certificación.	Solicitamos amablemente a la entidad confirmar nuestro entendimiento: ¿el proponente debe suministrar tanto el curso de preparación como el voucher de examen de certificación para cada uno de los 25 participantes? ¿o el requerimiento del literal 1 del numeral 7.1 se limita únicamente al curso de preparación, y los vouchers de examen son responsabilidad de la DIAN?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el proponente debe suministrar tanto el curso de preparación como el voucher de examen de certificación para cada uno de los 25 participantes
63	Sección VI	Realizar y entregar el plan de trabajo detallado para la devolución del servicio, por lo menos cuatro (4) meses antes de su finalización.	Solicitamos amablemente a la entidad aclarar nuestro entendimiento: ¿el período de cuatro (4) meses de devolución del servicio será remunerado bajo el Ítem 11 (Monitoreo y Operación mensual) de forma normal, o la DIAN contempla un esquema de remuneración diferenciado para este período de transición dado que el equipo del proponente estará simultáneamente operando el SOC y transfiriendo el conocimiento?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el período de cuatro (4) meses de devolución del servicio será remunerado bajo el Ítem 11 (Monitoreo y Operación mensual) de forma normal.
64	Sección VI	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	Se le solicita amablemente aclarar el requerimiento si hace referencia a que la herramienta o el servicio debe realizar creación y gestión de casos, ya que se menciona "herramienta/servicio" y debido al fin funcionar se sugiere que elpliego mencione "herramienta o servicio".		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, es herramienta o servicio para este ítem.
65	Sección VI	Incluir capacidades de análisis de percepción para evaluar cómo se percibe la marca en línea y detectar cualquier tendencia negativa o potencial crisis de reputación.	Se le solicita amablemente a la entidad aclarar si "la herramienta o servicio" debe "Incluir capacidades de análisis de percepción para evaluar cómo se percibe la marca en línea y detectar cualquier tendencia negativa o potencial crisis de reputación", para lo cual se recomienda hacer énfasis en el requerimiento, que sea para "la herramienta o servicio".		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, es herramienta o servicio para este ítem.
66	Sección VI	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).	Se solicita que el pliego permita, de manera explícita, modalidades de licenciamiento alternativas al conteo de activos, incluyendo el licenciamiento basado en capacidad de análisis o throughput de tráfico (Sniffer Throughput). Esto debido a que varios fabricantes líderes en soluciones NDR del mercado no utilizan como métrica de licenciamiento el número de endpoints o activos monitoreados, sino la capacidad de inspección de tráfico en la red.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se permiten diferentes formas de licenciar siempre y cuando se cubran la cantidad de activos solicitados, en este caso 25000.
67	Sección VI	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.	Se solicita que el pliego permita la participación de soluciones NDR cuya arquitectura contemple sensores en las premisas (appliance o VM) encargados de la captura y retención local de datos, pero que, para procesos avanzados de análisis, correlación, gestión centralizada y actualización continua de inteligencia de amenazas, se pueda hacer uso de componentes en la nube, y no de forma restrictiva como lo menciona el proceso. Desde el punto de vista técnico, las arquitecturas modernas de NDR basadas en machine learning, behavioral analysis y técnicas de threat hunting requieren grandes capacidades de cómputo, data lakes para analizar múltiples terabytes de metadatos y acceso continuo a fuentes globales de inteligencia de amenazas. Esto es posible únicamente cuando el sistema combina: - Captura y almacenamiento local a nivel de sensor - Procesamiento avanzado en la nube para análisis, correlación y detección de comportamiento Exigir que toda la analítica se realice exclusivamente en el appliance físico puede limitar la capacidad de detección, impedir el uso de modelos de inteligencia global, restringir la escalabilidad e, incluso, excluir tecnologías de última generación cuya eficacia depende del procesamiento en la nube. La condición solicitada en el pliego (consulta local sin conexión a la nube) se cumple plenamente mediante la retención local del tráfico o de los metadatos capturados, sin que eso deba impedir que la solución utilice la nube para: - Correlación multi tenant - Análisis basado en inteligencia global - Aprendizaje automático avanzado - Gestión centralizada - Actualización de indicadores de compromiso (IoC) - Ejecución de detecciones emergentes		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad.
68	Sección VI	El proponente deberá entregar un servicio con licenciamiento total de la solución para 17727 dispositivos por (3) años.	Se le solicita amablemente a la entidad que, adicional al licenciamiento por activo, el pliego incluya también la opción de licenciamiento por capacidad (throughput), permitiendo así la participación de soluciones que utilizan este modelo nativamente, siempre que cumplan con los requisitos funcionales del NDR.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el licenciamiento solicitado es para 25000 dispositivos por tres (3) años, licenciamiento que se puede cubrir de acuerdo a las diferentes formas que tienen los fabricantes para licenciar siempre y cuando se cumplan con las características técnicas y cantidades solicitadas por la Entidad.
69	7.19	El servicio debe basarse en un sistema de seguridad que reciba todo el tráfico de la red desde uno o varios switches, lo analice e identifique las amenazas o incidentes que están ocurriendo en la red	Teniendo en cuenta la premisa de obtención de información a través de una herramienta NDR que "reciba todo el tráfico de la red desde uno o varios switches, lo analice e identifique las amenazas o incidentes que están ocurriendo en la red", se le solicita amablemente a la entidad que, adicional al licenciamiento por activo, el pliego incluya también la opción de licenciamiento por capacidad (throughput) de tráfico que debe recibir de los switches de red, permitiendo así la participación de soluciones que utilizan este modelo nativamente y no el de cantidad de End Points o activos de red.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el licenciamiento solicitado es para 25000 dispositivos por tres (3) años, licenciamiento que se puede cubrir de acuerdo a las diferentes formas que tienen los fabricantes para licenciar siempre y cuando se cumplan con las características técnicas y cantidades solicitadas por la Entidad.
70	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	Se le solicita amablemente a la entidad reemplazar el siguiente requerimiento "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" por "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 primar el funcionamiento basado en función del comportamiento, donde no se permitan las tecnologías que hacen uso exclusivo de reglas y / o firmas", teniendo en cuenta que en algunos escenarios se pueden complementar las funciones comportamentales con reglas y / o firmas que son alimentadas del centro de investigaciones del fabricante.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem 7.26 fue ajustado mediante adenda.
71	7.27	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.	Se le solicita amablemente a la entidad reemplazar el siguiente requerimiento "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." por "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 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, transferencia de datos, destinos y resúmen de conexiones.", debido a que la forma como se solicita puede restringir la participación a una marca específica de soluciones NDR y limitando la participación de marcas líderes en el mercado.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
72	7.28	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.	Se le solicita amablemente a la entidad reemplazar el siguiente requerimiento "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." por "La solución debe ser OPEN API O API RESTFULL , que admita integraciones con otros elementos de seguridad", debido a que los formatos explícitos solicitados restringen la participación a una marca específica de soluciones NDR y limitan la participación de marcas líderes en el mercado que brindan integraciones OPEN API O API RESTFULL.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
73	8.2	En el ciclo de desarrollo las herramientas del proponente deben utilizar SASE (Secure Access Services Edge), buscando seguridad en dispositivos móviles, Internet de la cosas y migración de aplicaciones on-premise hacia Cloud.	Se le solcita a la entidad profundizar en este requerimiento, para que sea entendible si debe ser de la misma marca de la solución de análisis de código estático y dinámico de aplicaciones, para cuántos usuarios debe suministrase el licenciamiento SASE y demás elementos que lleven a dar claridad del requerimiento y poder incluir dentro de la arquitectura y servicios, los elementos adecuados de satisfagan la necesidad de la entidad.		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.
74	8.24	Debe soportar lenguajes como: Java, JavaScript, Python, Php, Ruby, C++, C, C#, otros.	Se le solicita amablemente a la entidad reemplazar el requerimiento "Debe soportar lenguajes como: Java, JavaScript, Python, Php, Ruby, C++, C, C#, otros." por "Debe soportar lenguajes como: Java, JavaScript, Python, Php, Ruby, C++, C, C# (.Net), otros."		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
75	8.31	Debe permitir integración nativa con las principales plataformas de CI/CD tales como: GitHub Actions, GitLab, Jenkins, Travis, Azure DevOps, Bamboo, CircleCI	Se le solicita amablemente a la entidad reemplazar el requerimiento "Debe permitir integración nativa con las principales plataformas de CI/CD tales como: GitHub Actions, GitLab, Jenkins, Travis, Azure DevOps, Bamboo, CircleCI" por "Debe permitir integración nativa con las principales plataformas de CI/CD tales como: GitHub Actions, GitLab, Jenkins, Azure DevOps, y otros", para no limitar la participación de soluciones lídeberes en el mercado.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
76	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf		Al revisar los documentos de la Solicitud de Ofertas, se evidencia que no se encuentra definido un cronograma detallado que indique de manera clara y expresa las fechas asociadas a las distintas etapas del proceso, tales como: Plazo máximo para presentación de observaciones y solicitudes de aclaración. Fecha límite para la publicación de respuestas a observaciones. Fecha prevista para la expedición de adendas. Fechas de evaluación, apertura de ofertas económicas y adjudicación. Inicio estimado de la ejecución contractual. Respetuosamente se solicita al Contratante publicar un cronograma detallado y consolidado del proceso, en el que se indiquen las fechas clave y los hitos de cada una de las etapas previstas, con el fin de brindar claridad y previsibilidad a los oferentes interesados.		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.
77	Sección III. Criterios de Evaluación y Calificación	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.	Solicitamos a la entidad confirmar cúal es fabricante en el cual debera entregarse el TAM, teniendo en cuenta que la solucion a ofertar contempla varios productos y fabricantes segun el requerimiento del Anexo Tecnico (ítem 1.1)		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el literal c es un ítem puntuable, para el caso en especifico, 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. Acorde a lo anterior también se aclara que para dicha puntuación, el futuro interesado podrá escoger acorde a los fabricantes entregados según las capacidades y servicios implementados, cual de estos cumple con la condición TAM y entregar dicha acreditación, ya que la Entidad no menciona ni discrimina nombre alguno de fabricante o capacidad en específico.
78	Sección III. Criterios de Evaluación y Calificación	c. Incluye servicios TAM (Thecnical account manager) (ítems 2 al 9 del anexo técnico).	Solicitamos a la entidad aclarar como se realizará el esquema de ponderación de los puntos asociados a este ítem, debido a que NO todos los fabricantes poseen el esquema de TAM (Thecnical account manager) y no poseen las capacidades requeridas en el esquema de ponderación. Agradecemos a la entidad confirmar si existe algún fabricante especifico segun el requerimiento del Anexo Tecnico (ítem 1.1)		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el literal c es un ítem puntuable, para el caso en especifico, 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. Acorde a lo anterior también se aclara que para dicha puntuación, el futuro interesado podrá escoger acorde a los fabricantes entregados según las capacidades y servicios implementados, cual de estos cumple con la condición TAM y entregar dicha acreditación, ya que la Entidad no menciona ni discrimina nombre alguno de fabricante.

79	Sección III. Criterios de Evaluación y Calificación	Sesiones Aclaración	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.
80	Sección I. Instrucciones a los Oferentes (IAO)	10. Idioma de la Oferta	Agradecemos profundamente a la entidad modificar lo solicitado, para facilitar el proceso de documentación técnica. En este sentido, solicitamos respetuosamente que, de ser aplicable, se autorice la entrega de especificaciones, fichas técnicas y/o catálogos preferiblemente en idioma inglés, sin necesidad de traducción. Dado que los fabricantes y distribuidores internacionales generan y mantienen esta documentación principalmente en inglés, permitir su presentación en dicho idioma facilitaría al equipo técnico el acceso directo a las fuentes primarias de información, asegurando una comprensión más precisa y completa de las características y funcionalidades de los productos o servicios.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las fichas técnicas, catálogos o cualquier datasheet que permita sustentar lo ofrecido se podrá entregar en inglés, siempre y cuando se señale o resalte en dichos documentos la evidencia de cumplimiento.
81	Sección III. Criterios de Evaluación y Calificación	Sesión de Aclaraciones	Con fundamento en el cronograma publicado, se solicita a la entidad confirmar si, dentro de la Fase 3 correspondiente a la operación del SOC, las herramientas QRadar y Guardium deberán encontrarse en operación desde el inicio de dicha fase, durante un periodo de veintitrés (23) meses.		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 con el respectivo equipo mínimo de trabajo 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.
82	5.3.2	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). Las licencias podrán ser reasignadas entre activos, sin generar costos adicionales para la Entidad, los tiempos para la reasignación de licencias serán acordados en su momento con el futuro CONTRATISTA, normalmente estos tiempos oscilan entre uno y quince días dependiendo de la cantidad y el grado de complejidad de la actividad.	Se solicita amablemente a la entidad confirmar cual es el estimado de crecimiento anual de cada uno de los activos en el alcance para su estimación en la oferta		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el estimado de crecimiento ya se encuentra contenido en la cantidad de 25000 y es del 20%.
83	5.4.22	La solución ofertada deberá estar en la capacidad de cubrir más de 82.000 CVEs IDs y 30.000 Bugtraq IDs, con una baja tasa de falsos positivos.	El ítem establece un umbral de cobertura de más de 82.000 CVE IDs y 30.000 Bugtraq IDs. Sin embargoy teniendo en cuenta el alto volumen actual de vulnerabiliad y técnicas de ataque, se reqomienda incrementar en un 30% esta metrica solicitada de CVEs, quedando de la siguiente manera: - CVEs 106.000 - Bugtraq IDs 30.000 De tal forma la técnologia cubrira las necesidades actuales del mercado en temas de visión de riesgos y amenazas. Dicha información deberá ser validada por medio de documentación pública.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
84	5.9.9	Debe incluir la calificación de vulnerabilidad de acuerdo con el estándar aceptado por la industria, es decir, el Sistema de calificación de vulnerabilidad común Versión 4 (CVSS 4).	El ítem exige el uso del Sistema de Calificación de Vulnerabilidades versión 4 (CVSS 4). CVSS v4 fue publicado por el FIRST en noviembre de 2023 e introduce cambios significativos respecto a CVSS v3, incluyendo nuevas métricas de suplemento (Safety, Automatable, Recovery, Value Density, Vulnerability Response Effort, Provider Urgency). No todas las plataformas del mercado han implementado CVSS v4 de forma nativa en sus reportes y dashboards. Exigir CVSS v4 sin verificar soporte real puede generar incumplimientos durante la ejecución del contrato.	Se solicita mantener la exigencia de CVSS v4 en el Ítem 5.9.9 y adicionalmente requerir que el oferente confirme en su propuesta técnica: (a) Que la plataforma presentada soporta nativamente CVSS v3 y CVSS v4 en reportes, dashboards y en el sistema de priorización de vulnerabilidades; y (b) Si la plataforma utiliza un sistema de puntuación propietario complementario, indique cómo funciona y de que manera se presenta junto con la calificación CVSS v4 en la consola de gestión.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
85	Seccion V	Se deberá entregar de forma trimestral un informe de la gestión de vulnerabilidades en el cual se refleje: - Las recomendaciones de mejores prácticas de manejo y atención de las vulnerabilidades críticas identificadas por la solución. - Estado general de los activos y FQDN monitoreados. - Avance en la resolución de hallazgos. - Informe de las auditorías realizadas. - Puntos de atención.	Se recomienda a la entidad modificar este requerimiento para que se puedan tener informes acorde a cada capacidad de las tecnologías solicitadas. Por lo cual recomendamos quede de la siguiente forma	Se deberá entregar de forma trimestral un informe de la gestión de riesgos en el cual se refleje: - Reporte de gestión de vulnerabilidades donde se refleje cantidad de dispositivos evaluados, brechas identificadas y priorización - Reporte de gestión de vulnerabilidades en aplicaciones web y mapeo de brechas de seguridad asociadas al OWASP10 - Reporte de hallazgos en recursos de nube publica (Vulnerabilidades, Malas practicas de configuración, Indentidades con privilegios exedidos y Postura de Seguridad) - Reporte de brechas de seguridad asociadas a identidades del directorio activo - Reporte de salud de superficie expuesta a internte. - Reporte de analisis de rutas de ataque, el cual incluya los componentes evaluados por cada una de las técnologías solicitadas. - Reporte Gerencial de Exposición	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia, sin embargo, se aclara que son requerimientos mínimos por lo tanto el futuro proveedor de SOC podrá entregar otras características siempre y cuando se cumpla con lo solicitado por la Entidad.
86	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 amablemente a la entidad aclarar si la herramienta solicitada debe estar en la capacidad de desplegar de manera automatica los parches de remediación de las vulnerabilidades detectadas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem mismo indica: 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.
87	5.3.2	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). Las licencias podrán ser reasignadas entre activos, sin generar costos adicionales para la Entidad, los tiempos para la reasignación de licencias serán acordados en su momento con el futuro CONTRATISTA, normalmente estos tiempos oscilan entre uno y quince días dependiendo de la cantidad y el grado de complejidad de la actividad.	Es de nuestro entendimiento que la entidad requiere capacidades de licenciamiento que puedan ser aprovicionadas o reaprovicionadas en cada una de las tecnologías requeridas, sin que lo mismo represente costos adicionales. Agradecemos confirmar si es correcto nuestro entendimiento.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el mismo ítem responde a su consulta, de acuerdo a lo siguiente: Las licencias podrán ser reasignadas entre activos, sin generar costos adicionales para la Entidad, los tiempos para la reasignación de licencias serán acordados en su momento con el futuro CONTRATISTA, normalmente estos tiempos oscilan entre uno y quince días dependiendo de la cantidad y el grado de complejidad de la actividad.
88	5.4.2	La solución ofertada deberá proveer una visibilidad completa sobre toda la superficie de ataque, sobre un único portal que proporcione una vista unificada.	Es de nuestro entendimiento que la entidad validara la información de las caracteristicas requeridas para cada una de las tecnologías incluidas en el proceso con información pública del fabricante. Agradecemos confirmar si es correcto nuesto entendimiento.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en todos los ítems que se encuentran del anexo técnico se hará verificación, en el caso especifico de la hoja de nombre Anexo Técnico items verificables, la comprobación se hará frente a datasheet del fabricante o cualquier otro documento que se allegue del fabricante para argumentar cumplimiento.
89	Seccion V	Nuevo	Solicitamos amablemente a la entidad aclarar si requiere que la tecnologia de gestion dee vulnreabilidades unifique el riesgo prove e la consola de protección de endpoint		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, su inquietud no se entiende, por lo tanto, no es posible dar una respuesta acertada.
90	5.3.2	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). Las licencias podrán ser reasignadas entre activos, sin generar costos adicionales para la Entidad, los tiempos para la reasignación de licencias serán acordados en su momento con el futuro CONTRATISTA, normalmente estos tiempos oscilan entre uno y quince días dependiendo de la cantidad y el grado de complejidad de la actividad.	Se solicita amablemente a la entidad confirmar cual es el estimado de crecimiento anual de cada uno de los activos en el alcance para su estimación en la oferta		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el estimado de crecimiento ya se encuentra contenido en la cantidad de 25000 y es del 20%.
91	5.4.22	La solución ofertada deberá estar en la capacidad de cubrir más de 82.000 CVEs IDs y 30.000 Bugtraq IDs, con una baja tasa de falsos positivos.	El ítem establece un umbral de cobertura de más de 82.000 CVE IDs y 30.000 Bugtraq IDs. Sin embargoy teniendo en cuenta el alto volumen actual de vulnerabiliad y técnicas de ataque, se reqomienda incrementar en un 30% esta metrica solicitada de CVEs, quedando de la siguiente manera: - CVEs 106.000 - Bugtraq IDs 30.000 De tal forma la técnologia cubrira las necesidades actuales del mercado en temas de visión de riesgos y amenazas. Dicha información deberá ser validada por medio de documentación pública.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
92	5.9.9	Debe incluir la calificación de vulnerabilidad de acuerdo con el estándar aceptado por la industria, es decir, el Sistema de calificación de vulnerabilidad común Versión 4 (CVSS 4).	El ítem exige el uso del Sistema de Calificación de Vulnerabilidades versión 4 (CVSS 4). CVSS v4 fue publicado por el FIRST en noviembre de 2023 e introduce cambios significativos respecto a CVSS v3, incluyendo nuevas métricas de suplemento (Safety, Automatable, Recovery, Value Density, Vulnerability Response Effort, Provider Urgency). No todas las plataformas del mercado han implementado CVSS v4 de forma nativa en sus reportes y dashboards. Exigir CVSS v4 sin verificar soporte real puede generar incumplimientos durante la ejecución del contrato.	Se solicita mantener la exigencia de CVSS v4 en el Ítem 5.9.9 y adicionalmente requerir que el oferente confirme en su propuesta técnica: (a) Que la plataforma presentada soporta nativamente CVSS v3 y CVSS v4 en reportes, dashboards y en el sistema de priorización de vulnerabilidades; y (b) Si la plataforma utiliza un sistema de puntuación propietario complementario, indique cómo funciona y de que manera se presenta junto con la calificación CVSS v4 en la consola de gestión.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
93	13.16	Se deberá entregar de forma trimestral un informe de la gestión de vulnerabilidades en el cual se refleje: - Las recomendaciones de mejores prácticas de manejo y atención de las vulnerabilidades críticas identificadas por la solución. - Estado general de los activos y FQDN monitoreados. - Avance en la resolución de hallazgos. - Informe de las auditorías realizadas. - Puntos de atención.	Se recomienda a la entidad modificar este requerimiento para que se puedan tener informes acorde a cada capacidad de las tecnologías solicitadas. Por lo cual recomendamos quede de la siguiente forma	Se deberá entregar de forma trimestral un informe de la gestión de riesgos en el cual se refleje: - Reporte de gestión de vulnerabilidades donde se refleje cantidad de dispositivos evaluados, brechas identificadas y priorización - Reporte de gestión de vulnerabilidades en aplicaciones web y mapeo de brechas de seguridad asociadas al OWASP10 - Reporte de hallazgos en recursos de nube publica (Vulnerabilidades, Malas practicas de configuración, Indentidades con privilegios exedidos y Postura de Seguridad) - Reporte de brechas de seguridad asociadas a identidades del directorio activo - Reporte de salud de superficie expuesta a internte. - Reporte de analisis de rutas de ataque, el cual incluya los componentes evaluados por cada una de las técnologías solicitadas. - Reporte Gerencial de Exposición	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
94	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 amablemente a la entidad aclarar si la herramienta solicitada debe estar en la capacidad de desplegar de manera automatica los parches de remediación de las vulnerabilidades detectadas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el mismo ítem refiere la respuesta a su consulta: 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.
95	5.3.2	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). Las licencias podrán ser reasignadas entre activos, sin generar costos adicionales para la Entidad, los tiempos para la reasignación de licencias serán acordados en su momento con el futuro CONTRATISTA, normalmente estos tiempos oscilan entre uno y quince días dependiendo de la cantidad y el grado de complejidad de la actividad.	Es de nuestro entendimiento que la entidad requiere capacidades de licenciamiento que puedan ser aprovicionadas o reaprovicionadas en cada una de las tecnologías requeridas, sin que lo mismo represente costos adicionales. Agradecemos confirmar si es correcto nuestro entendimiento.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el mismo ítem responde a su consulta, de acuerdo a lo siguiente: Las licencias podrán ser reasignadas entre activos, sin generar costos adicionales para la Entidad, los tiempos para la reasignación de licencias serán acordados en su momento con el futuro CONTRATISTA, normalmente estos tiempos oscilan entre uno y quince días dependiendo de la cantidad y el grado de complejidad de la actividad.
96	5.4.2	La solución ofertada deberá proveer una visibilidad completa sobre toda la superficie de ataque, sobre un único portal que proporcione una vista unificada.	Es de nuestro entendimiento que la entidad validara la información de las caracteristicas requeridas para cada una de las tecnologías incluidas en el proceso con información pública del fabricante. Agradecemos confirmar si es correcto nuesto entendimiento.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en todos los ítems que se encuentran del anexo técnico se hará verificación, en el caso especifico de la hoja de nombre Anexo Técnico items verificables, la comprobación se hará frente a datasheet del fabricante o cualquier otro documento que se allegue del fabricante para argumentar cumplimiento.
97	Seccion V	Nuevo	Solicitamos amablemente a la entidad aclarar si requiere que la tecnologia de gestion dee vulnreabilidades unifique el riesgo prove e la consola de protección de endpoint		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
98	9.4	La herramienta/servicio debe rastrear y monitorear continuamente la presencia en línea de la marca en sitios web, redes sociales, foros, blogs y otros espacios digitales relevantes para identificar cualquier uso no autorizado o infracción de la marca.	Al ser una tecnologia de proteccion de marca en DeepWeb y DarkWeb No deberia hacer referencia a redes sociales y ambientes de facil acceso. Al contrario la tecnologia deberia ir enfocada a la identificacion del monitoreo de la marca y el dominio DIAN.GOV.CO en los entornos donde se encuentran los ciberdelincuentes. Un ciberdelincuente no estara programando sus ataques desde una red social ya que entendemos no es el objeto de esta tecnologia. Por lo que se recomienda modificar	La herramienta/servicio debe rastrear y monitorear continuamente la presencia de DATOS, ARCHIVOS, CLAVES, SECRETOS de la DIAN y que se esten comercializando en los entornos de CIBERDELINCUENTES tales como , foros, blogs y ambitnos de intercambio en DEEPWEB Y DARKWEB Y otros espacios digitales relevantes para identificar cualquier uso no autorizado o exposicion de la informacion de la entidad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
99	9.5	La herramienta/servicio debe identificar automáticamente posibles infracciones de marca, como el uso no autorizado del logotipo, el nombre de la marca.	Entendemos que esta tecnologia es para proteger a la DIAN de ataques a gran escala, tal como el ocurrido donde se filtraron miles de registros de ciudadanos. Por lo que solicitamos modificar el numeral	La herramienta/servicio debe identificar automáticamente y basado en Inteligencia Artificial posibles suplantaciones de dominio, exfiltracion de datos y relevacion de informacion confidencial, los cuales tengan asociado usuarios de la DIAN o el Dominio DIAN. Debera estar potenciado con IA para lograr una deteccion dinamica rapida y anticiparse a los ciberataques.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
100	9.3	Se debe licenciar como mínimo para 260 activos públicos o equivalente o similar de acuerdo con la tecnologia ofrecida.	Se solicita a la entidad modificar este numeral, ya que el unico fabricante que usa esta metodologia de licenciamiento es FORTINET.	Se debe licenciar como minimo 100 dominios y Subdominios asociados a la DIAN	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento realizado acepta equivalencia en la forma de licenciar, cuando enuncia "Se debe licenciar como mínimo para 260 activos públicos o equivalente o similar de acuerdo con la tecnología ofrecida", por lo tanto, el futuro interesado puede dimensionar su oferta con base en el fabricante que represente siempre y cuando se cumpla con lo solicitado en el respectivo ítem.
101	9.3	Se debe licenciar como mínimo para 260 activos públicos o equivalente o similar de acuerdo con la tecnologia ofrecida.	Se solicita a la entidad aclarar si requieren monitorear usuarios de alto valor en la red para validar si tienen compromisos en DEEPWEB y DARKWEB o exposicion de sus datos o contraseñas. De ser asi solicitamos aclarar cuantos usuarios requieren		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad.
102	9.11	Incluir capacidades de análisis de percepción para evaluar cómo se percibe la marca en línea y detectar cualquier tendencia negativa o potencial crisis de reputación.	Se solicita a la entidad modificar este requerimiento, dado que la tecnologia al ser un monitoreo de DEEPWEB y DARKWEB no tiene sentido que tenga esta capacidad; en la deepweb o darkweb no hay tendencias de reputacion dado que son entornos de CIBERDELINCUENTES en donde se programan ataques informaticos.	incluir capacidades de análisis en mas de 8000 fuentes de DARKWEB Y DEEPWEB entre foros, discusiones, entornos de intercambio de datos esto con el fin de identificar potenciales ataques informaticos o fugas realizadas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad.
103	9.4	La herramienta/servicio debe rastrear y monitorear continuamente la presencia en línea de la marca en sitios web, redes sociales, foros, blogs y otros espacios digitales relevantes para identificar cualquier uso no autorizado o infracción de la marca.	Todas las herramientas del mercado se basan en uso de Inteligencia Artificial para la busqueda y modelado de datos exfiltrados. Esta tendencia marcara la pauta en los diferentes fabricantes en los proximos años. La entidad busca que el fabricante tenga esta capacidad? Se recomienda incluirla	La herramienta debera basarse en IA para la busqueda automatizada de datos e inforamcion exfitlrada, contando con tecnicas que permitan un monitoreo en tiempo real o programado.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
104	SECCION 9	Takedowns	Se solicita a la entidad tener en cuenta que la tecnologia cuente con el desarrollo y cumplimiento del takedowns, donde este solo se cobre una vez sea efectivo y la teconologia entregue los soportes que evidencieal cumplmiento efectivo del takedowns	La solución tecnológica debe integrar una capacidad nativa de mitigación y respuesta ante incidentes de marca que opere bajo un modelo de transferencia de riesgo y pago por resultados.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
105	10.1	Ethical Hacking	Se solicita que la capacidad de Ethical Hacking no dependa exclusivamente de ejecuciones manuales periódicas, sino que sea provista a través de una tecnología de seguridad ofensiva autónoma.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
106	Sección III — Criterios de Evaluación y Calificación	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.	La exigencia simultánea de experiencia acreditada en el sector financiero y en el sector gubernamental, combinada con el requisito de un contrato SOC superior a USD 1.000.000, configura una barrera de entrada que restringe artificialmente el universo de oferentes elegibles. Esta combinación de tres condiciones concurrentes puede favorecer al proveedor actual o a un grupo muy reducido de firmas con trayectoria específica en ambos sectores, en detrimento de empresas especializadas en ciberseguridad con amplia experiencia en uno de los dos sectores. La exigencia simultánea de los dos sectores puede resultar excluyente para empresas que atienden exclusivamente el sector público o exclusivamente el sector financiero, sin que ello implique menor idoneidad técnica para ejecutar este contrato. Esta configuración puede limitar la competencia efectiva del proceso, en contravía de los principios del BID.	Se solicita amablemente a la Entidad modificar el requisito de experiencia sectorial para que el oferente pueda acreditar experiencia en al menos uno (1) de los dos sectores indicados (financiero o gubernamental), en lugar de exigirlos de manera simultánea. Esta modificación amplía la base de competidores calificados sin reducir las garantías técnicas del proceso, en concordancia con los principios de pluralidad y competencia efectiva del BID.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
107	Sección III — Criterios de Evaluación y Calificación	c. Certificaciones vigentes del oferente como: ISO 27001:2022. ISO 22301:2019 o superior. Certificación que acredite vinculación directa y activa con FIRST (Forum Incident Response and Security Teams). (como mínimo doce (12) meses de antigüedad.). Otras certificaciones internacionales y reconocidas de SOC relevantes para el proyecto. | No tiene o solo presenta una | Presenta dos certificaciones | Presenta 3 certificaciones | Presenta 4 o más certificaciones | 0 | 5 | 10 | 20. NOTA 2: Las certificaciones allegadas deberán mantenerse vigentes durante el tiempo de operación de los servicios del SOC.	El pliego establece que las certificaciones del oferente deben estar vigentes y mantenerse durante la operación del SOC, pero no precisa si dichas certificaciones deben estar vigentes en la fecha de presentación de la oferta o si es admisible acreditarlas al inicio del contrato mediante un plan de obtención con cronograma verificable. Esta ambigüedad afecta a las cuatro (4) certificaciones del criterio c: ISO 27001:2022, ISO 22301:2019, membresía FIRST con mínimo doce (12) meses de antigüedad, y otras certificaciones SOC reconocidas. Sin una definición clara del momento de acreditación, los oferentes no pueden determinar con certeza si su situación actual les permite obtener puntaje en este factor, y el evaluador queda con discrecionalidad para interpretar el requisito de forma diferente entre propuestas.	Se solicita amablemente a la Entidad precisar si las certificaciones del criterio c del Rubro 2 deben estar vigentes en la fecha de presentación de la oferta, o si el oferente puede acreditarlas mediante un plan de obtención con cronograma y fecha máxima de cumplimiento al inicio del contrato. En el segundo caso, se sugiere establecer la fecha límite máxima de acreditación y el mecanismo de verificación durante la ejecución del contrato.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las certificaciones solicitadas deben estar vigentes.
108	7.3 - 7.18	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)." Ítem 7.18: "El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 17727 dispositivos por (3) años." Formulario Lista de Precios, Ítem 6 (NDR): Unidad de medida: IPs. Mínimo: 18.000.	El pliego presenta tres (3) cifras distintas para el licenciamiento mínimo de la solución NDR (Detección y Respuesta en Red) en tres documentos diferentes del mismo proceso: 25.000 activos en el ítem 7.3 del Anexo Técnico, 17.727 dispositivos en el ítem 7.18 del mismo Anexo, y 18.000 IPs en el Formulario de Lista de Precios. Estas cifras son materialmente diferentes entre sí y generan incertidumbre significativa sobre el alcance real del licenciamiento que el oferente debe costear y comprometer contractualmente. La diferencia entre 17.727 y 25.000 representa un incremento del 41%, con impacto directo y sustancial en el valor de la oferta económica y en el dimensionamiento técnico de la solución.	Se solicita amablemente a la Entidad definir mediante adenda la cantidad unificada y definitiva de dispositivos, activos o IPs que debe cubrir el licenciamiento mínimo de la solución NDR, asegurando coherencia entre el Anexo Técnico y el Formulario de Lista de Precios, e indicando la metodología de conteo utilizada para determinar dicha cifra.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la cantidad de dispositivos es 25000, el ítem quedó ajustado mediante adenda.
109	5.3.2	Ítem 5.3.2: "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). Las licencias podrán ser reasignadas entre activos, sin generar costos adicionales para la Entidad." Formulario Lista de Precios, Ítem 4 (Gestión de Vulnerabilidades): Unidad de medida: Activos de información. Mínimo: 18.000.	El Anexo Técnico (ítem 5.3.2) establece un licenciamiento mínimo de 25.000 activos para la solución de Gestión de Vulnerabilidades, mientras que el Formulario de Lista de Precios (ítem 4) fija el mínimo en 18.000 activos de información. La diferencia de 7.000 activos entre ambos documentos del mismo proceso representa una variación del 39% que impacta directamente el dimensionamiento técnico y el valor de la oferta económica. Esta inconsistencia no permite a los oferentes determinar con certeza cuál es el alcance real del licenciamiento a cotizar, ni cuál documento tiene precedencia en caso de controversia durante la ejecución del contrato.	Se solicita amablemente a la Entidad confirmar mediante adenda la cantidad definitiva de activos que debe cubrir el licenciamiento mínimo de la solución de Gestión de Vulnerabilidades, unificando la cifra entre el Anexo Técnico y el Formulario de Lista de Precios. Adicionalmente, se solicita precisar la distribución de activos por categoría (equipos de usuario final, infraestructura de red, servidores físicos y virtuales, cargas en nube pública, aplicaciones web e identidades en Directorio Activo) para que los oferentes puedan dimensionar correctamente su propuesta técnica y económica.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la cantidad de dispositivos es de 25000 activos, para lo cual se modifica la cantidad expresada en el Formulario Lista de Precios, cambio que se verá reflejado en la adenda a publicar en los próximos días, quedando de la siguiente manera:
110	12.55	Ítem 12.55: "El monitoreo, administración, gestión, configuración, optimización, operación, actualizaciones y demás actividades propias del SOC de todas las capacidades y servicios entregados, deberá ser prestado por el futuro CONSULTOR en horario 7x24x365 durante toda la duración del contrato que es de tres (3) años." Formulario Lista de Precios, Nota 6: "Los servicios de monitoreo y operación del SOC van hasta octubre de 2028 y debe contemplar todas y cada una de las capacidades y servicios requeridos en este proyecto."	El Anexo Técnico (ítem 12.55) establece que los servicios de monitoreo SOC se prestan durante toda la vigencia del contrato, que es de tres (3) años. Sin embargo, la Nota 6 del Formulario de Lista de Precios acota esos servicios hasta octubre de 2028, lo que equivale aproximadamente a treinta (30) meses desde un inicio estimado en 2026. Esta diferencia de seis (6) meses tiene un impacto directo en el dimensionamiento del servicio, en el número de analistas requeridos y en el valor total de la oferta económica. Los oferentes no pueden determinar con certeza si deben cotizar 30 o 36 meses de operación del SOC, lo que puede generar propuestas económicas no comparables entre sí.	Se solicita amablemente a la Entidad confirmar la fecha exacta de inicio y terminación de los servicios de monitoreo y operación del SOC, y garantizar que dicha fecha sea coherente con la duración del contrato establecida en la Solicitud de Ofertas y con el cronograma real del proceso de selección.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, la operación será hasta octubre 31 de 2028, el ítem será ajustado y se publicará mediante adenda en los próximos días, quedando de la siguiente manera: 12.55: El monitoreo, administración, gestión, configuración, optimización, operación, actualizaciones y demás actividades propias del SOC de todas las capacidades y servicios entregados, deberá ser prestado por el futuro CONSULTOR en horario 7x24x365 durante toda la duración del monitoreo y operación que será hasta el 31 de octubre de 2028.
111	5.3.2	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). Las licencias podrán ser reasignadas entre activos, sin generar costos adicionales para la Entidad, los tiempos para la reasignación de licencias serán acordados en su momento con el futuro CONTRATISTA, normalmente estos tiempos oscilan entre uno y quince días dependiendo de la cantidad y el grado de complejidad de la actividad.	Para efectos de dimensionamiento y proyección de la oferta, agradecemos que la Entidad indique la tasa de crecimiento anual estimada para cada categoría de activos contemplada en el alcance del proyecto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el estimado de crecimiento ya se encuentra contenido en la cantidad de 25000 y es del 20%.

ITEM	DESCRIPCIÓN	ESPECIFIQUE MARCA	ESPECIFIQUE REFERENCIA Y/O MODELO	UNIDAD DE MEDIDA	MINIMO	CANTIDAD	VALOR UNITARIO ANTES DE IVA	IVA	VALOR UNITARIO INCLUIDO IVA	VALOR TOTAL PROPUESTA ANTES DE IVA	VALOR TOTAL PROPUESTA
4	Monitoreo a la Gestión de Vulnerabilidades (Ver características en el ítem 5 del anexo).			Activos de información	25000			N/A			

112	5.4.22	La solución ofertada deberá estar en la capacidad de cubrir más de 82.000 CVEs IDs y 30.000 Bugtraq IDs, con una baja tasa de falsos positivos.	El requerimiento actual fija el umbral mínimo en 82.000 CVE IDs y 30.000 Bugtraq IDs. No obstante, dado el ritmo acelerado con el que se publican nuevas vulnerabilidades en el panorama actual de amenazas, se considera pertinente elevar dicho umbral en un 35%, lo que resultaría en: - CVEs: 110.000 Este ajuste permitirá que la plataforma seleccionada ofrezca una cobertura acorde a las exigencias del mercado en materia de visibilidad de riesgos.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
113	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.	A fin de precisar el alcance técnico de la solución requerida, solicitamos que la Entidad aclare si la plataforma de gestión de vulnerabilidades debe contar con capacidades nativas de despliegue automatizado de parches de remediación sobre los activos identificados.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem mismo indica: 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.
114	5.4.2	La solución ofertada deberá proveer una visibilidad completa sobre toda la superficie de ataque, sobre un único portal que proporcione una vista unificada.	Entendemos que la Entidad llevará a cabo la validación de las capacidades técnicas de cada solución ofertada con base en información pública disponible del fabricante. Agradecemos confirmar si esta es la metodología de verificación prevista.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en todos los ítems que se encuentran del anexo técnico se hará verificación, en el caso especifico de la hoja de nombre Anexo Técnico ítems verificables, la comprobación se hará frente a datasheet del fabricante o cualquier otro documento que se allegue del fabricante para argumentar cumplimiento.
115	Seccion V	Nuevo	Se solicita a la Entidad precisar si dentro del alcance del presente proceso se contempla que la plataforma de gestión de vulnerabilidades consolide e integre el riesgo proveniente de la consola de protección de endpoints.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los requerimientos mínimos se encuentran claramente detallados en el anexo de características técnicas, por lo tanto, se invita a su respectiva revisión.
116	4.7	Contar con facilidades o herramientas analíticas para la conducción de análisis forense cuando sea reportado algún incidente.	Solicitamos a la entidad confirmar que dentro del requerimiento de "Herramienta de proteccion de bases de datos" cuando se hace referencia a ""herramientas de analíticas para la conducción de análisis forense cuando sea reportado algún incidente" hace referencia a que se solicita que la solucion no sea unicamente un firewall de bases de datos, sino que incluya una herramienta dedicada de analitica de comportamiento en bases de datos proactivo que detecte anomalias de forma automatica usando algoritos de analisis de comportamiento y deteccion de anomalias mas alla de ataques.	Disponer de una herramienta dedicada de analitica de comportamiento en bases de datos proactivo que detecte anomalias de forma automatica usando algoritos de analisis de comportamiento y deteccion de anomalias mas alla de ataques.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem refiere a que el servicio o capacidad de protección de bases de datos debe poseer o contar con funcionalidades o herramientas para la conducción de análisis forense, por lo tanto, no se acepta su sugerencia.
117	4.54.9	La solución deberá ser capaz de poder desplegarse en nubes públicas como Amazon Web Services o Microsoft Azure	Solicitamos a la entidad confirmar que la herramienta debera estar licenciada y lista para integrar a su servicio bases de datos actuales o a futuro en modelos PaaS o en nubes IaaS con el objetivo de cubrir procesos de actualizacion y adopcion de bases de datos de alta capacidad como big data.	La herramienta debera estar licenciada y lista para integrar a su servicio bases de datos actuales o a futuro en modelos PaaS o en nubes IaaS (AWS y Azure) con el objetivo de cubrir procesos de actualizacion y adopcion de bases de datos de alta capacidad como big data.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la característica referida hace mención a que el servicio deberá ser capaz de desplegarse en nubes públicas, por lo tanto, no se acepta su sugerencia.
118	4.4	La solución entregada deberá ser implementada, configurada y puesta en marcha para monitorear todas las bases de datos de la Entidad, de acuerdo con el inventario de bases de datos que se encuentra en este archivo en la hoja "Inventario Infraestructura IT".	Solicitamos a la entidad confirmar que la herramienta se debe licenciar por servidores de bases de datos sin limites de cores o transaccionalidad.	La solución entregada deberá ser implementada, configurada y puesta en marcha para monitorear todas las bases de datos de la Entidad, de acuerdo con el inventario de bases de datos que se encuentra en este archivo en la hoja "Inventario Infraestructura IT". Así mismo, la herramienta se debe licenciar por servidores de bases de datos sin limites de cores o transaccionalidad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem es bien claro en cuanto a que, se deberá licenciar para las cantidades solicitadas por la Entidad.
119	18.2	"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"	Cada fabricantes cuenta con un programas de canales, dicho programa generalmente arranca en una clasificaciòn llamada registrado, es decir, el fabricante ya tiene visibilidad de ese canal de distribuciòn y lo autoriza para ofrecer sus productos y servicios. Pero hasta aquì, dicho canal registrado no tiene ningùn compromiso en ventas o en cantidad de ingenieros certificados. Una vez el canal empieza a generar ventas y a certificar a su personal tanto comercial como tecnicamente, el fabricante incluye a ese canal en su programa de membresìas, es decir, la fàbrica le indica la cuota al partner (en ventas y en ingenieros cerfificados) y de acuerdo a su cumplimiento y extracumplimiento le da el nombre de una membresía y generalmente de acuerdo a la fàbrica son 3 niveles (por ejemplo bronce, plata y oro, siendo oro el màs alto, pero en cada marca se llaman de manera distinta), es decir un canal que tiene una membresìa con una fàbrica tiene experiencia en venta de sus productos y/o servicios màs està cumpliendo una cuota indicada por el fabricante de acuerdo a su plan de mercadeo. Ahora, contar con una membresía también permite que el canal de distribuciòn cuente con beneficios (descuentos, acceso a informaciòn tècnica, participaciòn en eventos), porque de alguna manera el fabricante reconoce el esfuerzo y la inversiòn por preparar su personal y por hacer eventos que permitan posicionar la marca, sin emgargo, puede pasar que un canal haya tenido la màxima membresìa en una fàbrica pero si no hizo las ventas de acuerdo a la cuota del periodo planteado pierde la membresìa y puede llegar inclusive solo a "registrado". En los ùltimos años hemos visto como los proyectos de gobierno que es el principal comprador del pais, no ejecuta sus procesos, porque hya muchos cambios en las entidades, los ingenieros que llegan no estàn nombrados y los que llegan en encargo no se atreven a sacar los procesos y hemos visto como se ha movido de forma abrupta las membresìas en los ùltimos años, es decir, hemos visto como canales tradicionales de una marca dejaron de tener sus ventas, pero tambièn vimos como canales recièn creados crecieron exponencialmente con alguna marca con alguna marca. Por lo anteriormente expuesto insistimos a la entidad que permitan que en el anexo técnico requieran "la carta de distribuidor autorizado emitida por el fabricant" por cada marca de cada "CAPACIDAD" ofrecida, y no que exijan una membresìa de ningùn tipo para participar, toda vez que esto obligarìa a los oferentes a hacer uniones temporales o APCAS de acuerdo al nùmero de marcas que ofrezca en su solucion o en el peor de los casos que solo oferte un proponente.	"Certificación emitida por el repressentante legal del fabricante o quien estè aurorizado para hacerla, difiriga a la entidad e indicando el número del proceso, donde cerifique que el proponente es canal autorizado para vender sus productos y servicios"	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 expertícia 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.
120	18.2	"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"	Que un oferente no pertenezca a una de las tres màximas membresìas de cada fabricante es una medida restrictiva de participaciòn, aun cuando se consideren crear APCAS, porque entre otras, los fabricantes incluyen en sus programas de membresìas a los canales que se comprometen con su marca y no con su competencia. Dificilmente encontrarán que un APCA tenga las 3 máximas membresìas de todas las solcuiones incluidas en la oferta. ESte proceso incluye 8 "CAPACIDADES" cuales se relacionan a continuaciòn: 1.SIEM - Correlacionador de Eventos 2. SOAR - Orquestación, automatización y respuesta de seguridad) 3. Herramienta de protección de bases de datos. 4. Monitoreo a la Gestión de Vulnerabilidades. 5. Caza de amenazas. 6. NDR - Detección y respuesta en red e Inteligencia de amenazas 7. Solución de análisis de código estático y dinámico para aplicaciones 8. Protección de marca Supongamos que todo el anexo tècnico para estas 8 capaciades se cubren con cinco (5) marcas y solo en una marca de ellas el oferente tiene una membresìa, y en las otras cuatro (4) solo es registrado del fabricante. Asì estarìa habilitado el oferente?	"Certificación emitida por el repressentante legal del fabricante o quien estè aurorizado para hacerla, difiriga a la entidad e indicando el número del proceso, donde cerifique que el proponente es canal autorizado para vender sus productos y servicios"	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 sugerencia.
121	18.2	"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 a la entidad permitir que como requisito habilitante solo se requiera la carta de distribuidor autorizado emitida por el fabricante, la cual debe contener el número del proceso y dirigido a la entidad, un fabricante no se va a exponer a entregar esta certificación a un partner no apto para este proceso.. Ahora bien, si de algo sirve, para que la medida no quede restrictiva, pidan una de las tres maximas membresias para al menos el 50% de las capacidades, es decir, 4.	"Certificación emitida por el repressentante legal del fabricante o quien estè aurorizado para hacerla, difiriga a la entidad e indicando el número del proceso, donde cerifique que el proponente es canal autorizado para vender sus productos y servicios" y al menos una de ellas debe pertenecer a una de las tres maximas membresias del programa de membresias de las capacidades ofertadas"	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 sugerencia.
122	18.2	"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"	A manera de ejemplo con el ànimo de ilustrar la observaciòn, invitamos a la entidad a ingresar al siguiente link: https://www.tenable.com/partners/channel-partner-program ro membresìas Bronze (es como indicar registrado) ; mientras que Sylver, Gold y Platimun se entiende como los 3 nivles màs altos. Al dia de hoy, los canales Bronze que son los mismos registrados no aparecen en el portal de Tenable, pero Tenable fcaciòn de distriuidor autorizado, en nuestro caso particular, no aparecemos en el portal de Tenable porque estamos en categoria Bronze aunque en el año 2024 fuimos Platinum.	"Certificación emitida por el repressentante legal del fabricante o quien estè aurorizado para hacerla, difiriga a la entidad e indicando el número del proceso, donde cerifique que el proponente es canal autorizado para vender sus productos y servicios" y al menos una de ellas debe pertenecer a una de las tres maximas membresias del programa de membresias de las capacidades ofertadas"	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 sugerencia.
123	410-Solicitud-de-Oferta-VSD-SdO-SOC		que TRM se debe utilizar para convertir los 6 millones de USD que solicitan en la parte de experiencia, será la misma que indica en la página 58, IAO 32.1 : "La fecha de las tasas de cambio es: Una (1) semana antes de la fecha límite definida para la presentación de		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la TRM referida es para la presentación de las ofertas y para verificar las certificaciones de experiencia aportadas se tomará la TRM de las fechas de los contratos presentados.
124	410-Solicitud-de-Oferta-VSD-SdO-SOC		r si en el criterio de ponderación se calificará de acuerdo con las capacidades expresadas en la ficha técnica o por fabricantes de las soluciones a ofertar. Es decir, las capacidades solicitadas por la entidad son las siguientes: protección de Bases de Datos 5Especificaciones Técnicas Gestión y Monitoreo de Vulnerabilidades. 6Especificaciones Técnicas Caza de Amenazas 7Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas 8Especificaciones Técnicas Solución de análisis de código estático y dinámico para aplicaciones 9Especificaciones Técnicas Protección de Marca (Deep&Dark Web) Si nosotros como proponente presentamos la misma fabrica para cubrir múltiples capacidades se podrán cubrir varias capacidades descritas o estas deben ser de fabricas independientes.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, no existe restricción alguna por parte de la Entidad para los casos en que un fabricante cumpla con varias capacidades o servicios requeridos, siempre y cuando cumpla con los requerimientos mínimos para cada una de estas.
125	2.7		Se solicita amablemente a la entidad ajustar el requerimiento relacionado con la retención de información de la herramienta SIEM (correlacionador de eventos), en el sentido de precisar que la retención exigida de doce (12) meses en línea y doce (12) meses fuera de línea pueda ser soportada mediante el uso de almacenamiento externo. En este contexto, se requiere que dicho almacenamiento externo sea suministrado como parte integral de la solución por el oferente, garantizando el cumplimiento de los tiempos de retención establecidos. Lo anterior se fundamenta en que la solución contempla la correlación de aproximadamente 2.500 dispositivos, lo cual incrementa significativamente el volumen de logs a gestionar y almacenar, haciendo necesario contar con capacidades adicionales de almacenamiento que aseguren la operación eficiente y el cumplimiento del requerimiento de retención.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
126	2.27		Se solicita amablemente a la entidad ajustar la redacción del requerimiento relacionado con la integración con sistemas de ticketing externos,se recomienda eliminar la mención explícita de "Aranda" dentro del listado de herramientas de ticketing, ya que mas adelante se menciona que la solución de SIEM se debe integrar con dicha herramienta . Adicionalmente, frente al requerimiento de integración con el sistema de ticketing de la entidad (actualmente Aranda), se propone precisar que dicha integración puede realizarse mediante mecanismos estándar de interoperabilidad, tales como el consumo de APIs, la implementación de flujos de trabajo (workflows) o el uso de herramientas de automatización tipo SOAR, sin que esto implique una dependencia directa o nativa con una plataforma específica.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la integración solicitada en este punto se puede hacer con APIs o con herramientas tipo SOAR o con cualquier otro método siempre y cuando se cumpla con lo requerido por la Entidad.
127	2.30		Se solicita ajustar la redacción del requerimiento relacionado con la integración con sistemas de mesa de ayuda (help desk). En particular, se recomienda que no se limite la integración a una única herramienta específica, sino que se contemplen de manera opcional soluciones ampliamente utilizadas en el mercado, tales como ServiceNow, Aranda o Remedy, entre otras equivalentes. Asimismo, se sugiere precisar que la integración bidireccional requerida puede llevarse a cabo mediante el consumo y desarrollo de APIs, o alternativamente a través del uso de soluciones de automatización tipo SOAR, garantizando así flexibilidad en la implementación y compatibilidad con diferentes entornos tecnológicos.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la integración solicitada en este punto se puede hacer con APIs o con herramientas tipo SOAR o con cualquier otro método siempre y cuando se cumpla con lo requerido por la Entidad.
128	8.20		Se solicita amablemente a la entidad ampliar y detallar este requerimiento, con el fin de clarificar si la solución debe corresponder a la misma marca de la herramienta de análisis estático y dinámico de código de aplicaciones. Asimismo, es necesario especificar el número de usuarios para los cuales se requiere el licenciamiento SASE, junto con cualquier otro aspecto relevante que permita comprender completamente la necesidad. Esto facilitará la correcta inclusión de los componentes y servicios adecuados dentro de la arquitectura propuesta, garantizando el cumplimiento de los objetivos de la entidad.		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.
129	8.24	Debe soportar lenguajes como: Java, JavaScript, Python, Php, Ruby, C++, C, C#, otros.	Se solicita amablemente a la entidad ajustar el requerimiento, de modo que donde actualmente se indica: "Debe soportar lenguajes como: Java, JavaScript, Python, PHP, Ruby, C++, C, C#, otros.", se reemplace por: "Debe soportar lenguajes como: Java, JavaScript, Python, PHP, Ruby, C++, C, C# (.NET), otros.". La inclusión explícita de "C# (.NET)" permite precisar el alcance tecnológico requerido, considerando que el lenguaje C# se utiliza comúnmente dentro del ecosistema .NET. Esta aclaración evita ambigüedades en la interpretación del requerimiento, asegura la compatibilidad con aplicaciones desarrolladas sobre dicha plataforma y facilita a los proponentes dimensionar adecuadamente sus soluciones técnicas conforme a las necesidades reales de la entidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem menciona la palabra otros, donde cabe cualquier otro lenguaje que no hay sido incluido en el requerimiento, por lo tanto, la solicitud de ajuste no procede.
130	8.31	Debe permitir integración nativa con las principales plataformas de CI/CD tales como: GitHub Actions, GitLab, Jenkins, Travis, Azure DevOps, Bamboo, CircleCI	Se solicita amablemente a la entidad ajustar el requerimiento, de manera que donde actualmente se establece: "Debe permitir integración nativa con las principales plataformas de CI/CD tales como: GitHub Actions, GitLab, Jenkins, Travis, Azure DevOps, Bamboo, CircleCI", se reemplace por: "Debe permitir integración nativa con las principales plataformas de CI/CD tales como: GitHub Actions, GitLab, Jenkins, Azure DevOps, y otros". Este ajuste busca evitar la restricción innecesaria, si bien pueden no integrar de forma nativa todas las plataformas inicialmente listadas, sí cuentan con capacidades equivalentes o mecanismos de integración eficientes. De esta manera, se promueve una mayor pluralidad de oferentes, se fomenta la libre competencia y se facilita la selección de alternativas tecnológicas que satisfagan adecuadamente las necesidades de la entidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem hace referencia a una plataformas en especial, pero esto no quiere decir que no este abierto a cualquier otra plataforma, se aclara que, son requerimientos mínimos, por lo tanto, se puede integrar con cualquier otra, siempre y cuando se cumpla con lo solicitado.
131	5.4.11	La solución ofertada deberá ser provista por un fabricante en el cuadrante de lideres de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	Se solicita respetuosamente quitar o modificar el requisito que exige que la solución ofertada provenga de un fabricante ubicado en el cuadrante de líderes de Gartner o Forrester en su última evaluación para tecnologías de Vulnerability Risk Management. Lo anterior, considerando que actualmente no existe una evaluación reciente y vigente publicada por ambas firmas analistas para esta categoría específica. En particular, los estudios disponibles presentan una antigüedad superior a dos (2) años o no se encuentran publicados de manera activa en una de las firmas mencionadas, lo que limita la aplicabilidad del criterio como referencia objetiva de mercado. En este sentido, mantener esta condición podría restringir la libre concurrencia y la participación de múltiples oferentes cuyas soluciones cumplen plenamente con capacidades técnicas, funcionales y de madurez ampliamente reconocidas en la industria.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
132	5.4.19	Se debe ofrecer despliegue de fabricante para las soluciones consideradas y entrenamiento gratuito en línea como parte de la oferta para los integrantes de la DIAN por parte del fabricante de la solución. Esto durante la vigencia del contrato de soporte.	Se solicita respetuosamente a la entidad ajustar el requerimiento relacionado con que el despliegue de la solución deba ser realizados exclusivamente por el fabricante. Lo anterior, considerando que dicha condición solo se está exigiendo para la tecnología de análisis de vulnerabilidades y no para los demás componentes del proyecto, generando una inconsistencia en los criterios aplicados. Adicionalmente, los partners autorizados de los fabricantes cuentan con la experiencia, certificaciones y personal técnico especializado necesarios para llevar a cabo la implementación, configuración y capacitación de este tipo de soluciones, bajo los lineamientos y buenas prácticas del fabricante. En este sentido, mantener esta exigencia de forma exclusiva puede limitar la participación de oferentes y fabricantes que operan a través de sus canales certificados, sin que ello represente una diferencia en la calidad del servicio. Por lo anterior, se recomienda permitir que el despliegue pueda ser realizados tanto por el fabricante como por sus partners o canales autorizados, debidamente certificados, garantizando así mayor pluralidad de oferentes y condiciones equitativas de participación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
133	5.11.1	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	Se solicita respetuosamente a la entidad modificar el requerimiento relacionado con la inclusión obligatoria del componente de Data Security Posture Management (DSPM) dentro de la arquitectura CNAPP. Lo anterior, considerando que este componente aún presenta un nivel de madurez y adopción no homogéneo en el mercado, a diferencia de capacidades como CSPM, CWPP o CIEM. Actualmente, la protección y gestión de datos sensibles puede ser abordada mediante funcionalidades equivalentes integradas en otros módulos o a través de soluciones complementarias. En este sentido, exigir DSPM como capacidad nativa e independiente puede limitar la participación de oferentes, sin representar necesariamente un beneficio técnico diferencial frente a otras arquitecturas que cumplen el mismo objetivo. Por lo anterior, se solicita que este componente sea opcional o que se permita su cumplimiento mediante capacidades equivalentes orientadas a la identificación y protección de datos sensibles en entornos cloud.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
134	4.54.8	La solución podrá ser desplegada dentro de ambientes virtuales VMWare como dispositivo virtual.	Se solicita amablemente a la entidad no limitar a VMWARE como unico elemento de virtualización para la instalación y despliegue de la solución de administración para las bases de datos, lo anterior, a razón que existen múltiples alternativas en el mercado global que permiten virtualizar este tipo de soluciones, tales como, Microsoft Hyper-V, KVM y/o Red Hat OpenShift Virtualization y entre otros. Estos esquemas de virtualización permiten generar la implementación del sistema de manera segura y garantizando el correcto rendimiento y capacidad para su correcto funcionamiento, a lo cual se contaría con soporte y garantía del fabricante de la virtualización contemplada.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
135	4.54.10	La solución deberá soportar el volumen de tráfico y deberá tener una latencia menor a 5ms, para no impactar el desempeño de las aplicaciones.	Se solicita amablemente a la entidad aclarar en que casos la solución debe cumplir este requerimiento, teniendo en cuenta que este requisito es restrictivo cuandos las DBs que se encuentran fuera del Datacenter principal o disitantes a donde se implemente la solución. Lo anterior teniendo en cuenta que si la DB se encuentra en un servicio de nube se dependen de tiempos de latencia ajenos a la solución (hosting de nube (localización), canales de internet, tiempos de respuesta entre aplicaciones, etc) o donde sería imposible cumplir con una transaccionabilidad de datos inferior a 5 milisegundos. Según lo argumentado la entidad debería considerar que la solución soporte el volumen de tráfico de las DBs con el máximo de rendimiento de la solución ofertada, no afectando el desempeño de las aplicaciones sin retringirlo a un limite de tiempo finito debido a que la integración se puede llevar a cabo en DBaaS, en nube u en premisas ubicadas en un datacenter distinto al principal.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
136	11.4	Todos los elementos necesarios para la implementación de cualquiera de las capacidades requeridas por la Entidad en este proyecto, debe ser provista por el futuro oferente, entendiéndose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones. Recordando que se deberá suministrar los recursos necesarios (rack, conexiones, entre otros) para la instalación y configuración de dispositivos colectores (en caso de ser necesario) en las diferentes sedes de la Entidad, ya sean físicos o virtuales.	Solicitamos amablemente a la entidad aclarar si en caso de que se requiera hacer una instalación en los datacenter de la entidad para la prestación del servicio, se dispondra del recurso para el despliegue del mismo. Lo anterior teniendo en cuenta que de acuerdo con varias de las capacidades solicitadas se requiere la implementación de sensores y/o colectores que deben instalarse dentro de la infraestructura de la entidad por lo tanto se hace indispensable que al menos la entidad proporcione recursos de rack o conexiones físicas o recursos de computo en nube para el correcto funcionamiento de las soluciones, de lo contrario no se estaría implementando de manera idonea la solución adquirida para el proyecto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en el caso de tener que instalar infraestructura en los datacenter, o las seccionales o en cualquier sitio de la Entidad, el futuro proveedor del SOC, deberá disponer de todo lo necesario para implementar los elementos que se requieran para la puesta en operación de todos los servicios requeridos.
137	11.22	Con su oferta el proponente deberá incluir datasheets o documentación pública del fabricante, para validar el respectivo cumplimiento de cada uno de los requerimientos técnicos de la herramientas, servicios y capacidades solicitados en el presente anexo técnico, para lo cual el futuro proponente deberá indicar página y señalar párrafo del respectivo catalogo donde cumpla con lo solicitado.	Solicitamos amablemente a la entidad permitir aportar los datasheet y/o documentos técnicos del fabricante para la validación de los requisitos técnicos en su idioma original, lo anterior a razón que cualquier traducción podría mal interpretar los documentos originales del fabricante ocasionando el no cumplimiento de cada uno de los requerimientos técnicos.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las fichas técnicas, catálogos o cualquier datasheet que permita sustentar lo ofrecido se podrá entregar en inglés, siempre y cuando se señale o resalte en dichos documentos la evidencia de cumplimiento.

138	12.37	El servicio debe incluir Threat Intelligence o Inteligencia Global, que permita usar un servicio mundial de amenazas identificadas.	Solicitamos amablemente a la entidad aclarar si este punto corresponde a otra capacidad que debe tener en cuenta el proponente para la prestación del servicio SOC y si esta debe estar licenciada por un fabricante incluyendo soporte y garantía por los 3 años del proyecto. De igual forma aclarar si esta capacidad debe incluirse dentro del listado de las membresías de partner o canal.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem refiere a ese monitoreo proactivo que debe tener un Centro de Operaciones de Seguridad (SOC) cuente con Threat Intelligence o Inteligencia Global significa que integra fuentes de datos externas y actualizadas a nivel mundial sobre tácticas, técnicas, procedimientos (TTPs) e indicadores de compromiso (IoC) utilizados por ciberdelincuentes. En lugar de reaccionar solo ante lo que sucede dentro de su red, el SOC se vuelve proactivo al utilizar información recolectada globalmente para anticipar y bloquear amenazas antes de que afecten a la organización.
139	15.3	Se debe ofrecer entrenamiento gratuito en línea como parte de la oferta para los integrantes del área de tecnología y la Oficina de Seguridad (OSI) de la DIAN para mínimo cincuenta (50) integrantes, por parte del fabricante de las soluciones y plataformas entregadas, durante la vigencia del contrato que es de tres (3) años, considerando por lo menos un reentrenamiento en cada año para por lo menos diez (10) ingenieros, por el tiempo que dure el contrato, en temas de administración, gestión, operación, optimización, actualización, configuración, y demás actividades propias en las capacidades y servicios entregados del SOC.	Se solicita amablemente a la entidad reconsiderar que este tipo de entrenamiento NO lo dicte directamente el fabricante de las soluciones ofertadas, a razón que sería inviable por los todos los fabricantes ofertados presentar cursos a la medida de la entidad, lo anterior teniendo en cuenta que los proponentes disponen de los ingenieros certificados en las soluciones ofertadas permitiendo garantizar y capacitar idoneamente al equipo de la DIAN en las capacidades operativas de las plataformas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la transferencia de conocimiento referido en este punto la deberá hacer el futuro proveedor de los servicios SOC o los fabricantes de las soluciones ofertadas.
140	20.2	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.	Solicitamos a la entidad aclarar si para la fecha de devolución del servicio esta se deberá licenciar por un (1) año adicional, es decir, en total 4 años de licenciamiento previo al ya suscrito licenciamiento de los 3 años contemplados en el inicio de la operación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem en mención será ajustado mediante adenda a publicar en los próximos días, quedando de la siguiente manera: 20.2 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.
141	Equipo Mínimo de Trabajo	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.	Se solicita respetuosamente a la entidad revisar el requisito de formación académica establecido para el perfil de Especialista de Respuesta a Incidentes (IR), específicamente en lo relacionado con la exigencia de posgrado en Seguridad Informática. Lo anterior, con el fin de permitir la inclusión de programas académicos equivalentes y afines, tales como ciberseguridad, seguridad de la información u otras denominaciones relacionadas, que en la práctica académica y profesional abarcan las mismas competencias y conocimientos requeridos para el desempeño del rol. En este sentido, se recomienda ajustar el requisito de la siguiente manera: "Posgrado en Seguridad Informática o áreas afines como ciberseguridad, seguridad de la información o similares." Este ajuste permitirá ampliar la participación de profesionales idóneos, sin afectar el nivel técnico requerido, y garantizará una mayor pluralidad en la conformación del equipo de trabajo.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
142	Equipo Mínimo de Trabajo	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.	Se solicita respetuosamente a la entidad revisar el requisito relacionado con las certificaciones exigidas para el perfil de Gerente de Proyecto, específicamente en lo referente a la obligatoriedad de contar simultáneamente con certificaciones PMP y Scrum Master. Lo anterior, considerando que el perfil ya contempla un posgrado en Gerencia de Proyectos, así como una experiencia profesional mínima de diez (10) años, de los cuales cinco (5) años corresponden a la gestión de proyectos de seguridad de la información, lo cual garantiza ampliamente las competencias, conocimientos y aplicación de metodologías necesarias para el adecuado desempeño del rol. Adicionalmente, en el mercado existen diversas certificaciones reconocidas que acreditan competencias en gestión de proyectos y gestión de servicios de TI, las cuales pueden ser equivalentes en función del enfoque metodológico requerido. En este sentido, se recomienda ajustar el requisito permitiendo que el profesional cuente con al menos una (1) de las siguientes certificaciones vigentes: PMP, o Scrum Master, o ITIL V3 o superior Este ajuste permitirá mayor flexibilidad en la conformación del equipo de trabajo, promoverá la pluralidad de oferentes y garantizará la participación de profesionales altamente calificados, sin afectar el nivel técnico requerido por la entidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
143	Equipo Mínimo de Trabajo	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	Se solicita respetuosamente a la entidad revisar el requisito relacionado con las certificaciones exigidas para el perfil de Gerente de Proyecto, específicamente en lo referente a la obligatoriedad de contar simultáneamente con certificaciones PMP y Scrum Master. Lo anterior, considerando que el perfil ya contempla un posgrado en Gerencia de Proyectos, así como una experiencia profesional mínima de diez (10) años, de los cuales cinco (5) años corresponden a la gestión de proyectos de seguridad de la información, lo cual garantiza ampliamente las competencias, conocimientos y aplicación de metodologías necesarias para el adecuado desempeño del rol. Adicionalmente, en el mercado existen diversas certificaciones reconocidas que acreditan competencias en gestión de proyectos y gestión de servicios de TI, las cuales pueden ser equivalentes en función del enfoque metodológico requerido. En este sentido, se recomienda ajustar el requisito permitiendo que el profesional cuente con al menos una (1) de las siguientes certificaciones vigentes: PMP, o Scrum Master, o ITIL V3 o superior Este ajuste permitirá mayor flexibilidad en la conformación del equipo de trabajo, promoverá la pluralidad de oferentes y garantizará la participación de profesionales altamente calificados, sin afectar el nivel técnico requerido por la entidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
144	Equipo Mínimo de Trabajo	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) 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	Se solicita respetuosamente a la entidad considerar la inclusión, dentro del requisito de posgrado, del título de Especialización en Seguridad de la Información o Ciberseguridad, dado que el objeto del presente proceso corresponde a la prestación de servicios de un SOC (Security Operations Center), donde este tipo de formación resulta altamente pertinente y directamente alineada con las funciones del perfil requerido. Adicionalmente, se recomienda incluir dentro del apartado de certificaciones opcionales las certificaciones Certified Ethical Hacker (CEH) y/o Cyber Threat Intelligence Analyst (CTIA), las cuales guardan relación directa con las competencias de un perfil de Threat Hunter / Analista de Ciberinteligencia, fortaleciendo así la idoneidad técnica de los candidatos y ampliando el espectro de certificaciones relevantes para el rol. Esta inclusión permitiría una mayor correspondencia entre los requisitos del perfil y las buenas prácticas actuales en operaciones de seguridad, sin afectar los estándares de exigencia establecidos por la entidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
145	Equipo Mínimo de Trabajo	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) 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	Se solicita amablemente a la Entidad aclarar el alcance del requisito de experiencia relacionado con "tres (3) años con participación en proyectos de seguridad de la información, plan de recuperación de desastres o continuidad de negocio", en el sentido de precisar si dichos tres (3) años deben entenderse como experiencia acumulada en cualquiera de estos tipos de proyectos de manera indistinta (seguridad de la información o plan de recuperación de desastres o continuidad de negocio), o si, por el contrario, se requiere experiencia específica en cada uno de ellos. Adicionalmente, se solicita confirmar si dentro de la experiencia exigida se contemplan como válidos los proyectos relacionados con la operación o servicios de Centros de Operaciones de Seguridad (SOC).		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, deben entenderse como experiencia acumulada en cualquiera de estos tipos de proyectos de manera indistinta (seguridad de la información o plan de recuperación de desastres o continuidad de negocio).
146	Equipo Mínimo de Trabajo	QA / Analista de Calidad SOC. Ingeniería industrial , de sistemas o, telemática o, electrónica o, telecomunicaciones. Postgrado en Gerencia de proyectos Certificaciones vigentes: • ISO 9001 Mínimo tres (3) 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	Se solicita respetuosamente a la entidad revisar y considerar la eliminación del perfil de QA / Analista de Calidad SOC dentro de los requerimientos del proceso. Lo anterior, teniendo en cuenta que las funciones asociadas a este perfil no se evidencian como directamente alineadas con el objeto principal del proceso, el cual está orientado a la implementación y operación de servicios de ciberseguridad y gestión de vulnerabilidades. Adicionalmente, el proyecto ya contempla un perfil de Gerente de Proyecto que, por su formación académica, certificaciones y experiencia, cumple con los estándares necesarios para garantizar la adecuada gestión, seguimiento y control de calidad del servicio, incluyendo la aplicación de buenas prácticas, metodologías y cumplimiento de entregables. En este sentido, mantener este perfil adicional podría generar redundancia en las funciones, así como un posible sobredimensionamiento del equipo requerido, sin aportar un valor diferencial claro frente a los objetivos del proyecto. Por lo anterior, se recomienda eliminar este perfil		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
147	Equipo Mínimo de Trabajo	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.	Se solicita respetuosamente a la entidad revisar el requisito de formación académica establecido para el perfil de Analista SOC Nivel III, específicamente en lo relacionado con la exigencia de posgrado en seguridad informática. Lo anterior, con el fin de permitir la inclusión de programas académicos equivalentes y afines, tales como seguridad de la información o ciberseguridad, los cuales abarcan competencias técnicas y conceptuales alineadas con las funciones requeridas para este perfil. En este sentido, se recomienda ajustar el requisito de la siguiente manera: "Postgrado en seguridad informática o en áreas afines como seguridad de la información o ciberseguridad." Este ajuste permitirá ampliar la participación de profesionales idóneos, sin afectar el nivel técnico requerido, garantizando así una mayor pluralidad de oferentes y alineación con la oferta académica actual.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
148	Solicitud de Oferta VSD - sdo SOC Pagina 62	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.	Se solicita amablemente a la entidad ajustar el requerimiento anterior, incorporando los servicios de un TAM (Technical Account Manager) o sus equivalentes, teniendo en cuenta que algunos fabricantes ofrecen este tipo de acompañamiento bajo diferentes denominaciones. Lo anterior, con el fin de evitar que el uso exclusivo del término TAM resulte restrictivo.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el literal c es un ítem puntuable, para el caso en especifico, 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. Acorde a lo anterior también se aclara que para dicha puntuación, el futuro interesado podrá escoger acorde a los fabricantes entregados según las capacidades y servicios implementados, cual de estos cumple con la condición TAM y entregar dicha acreditación, ya que la Entidad no menciona ni discrimina nombre alguno de fabricante o capacidad en específico.
149	Solicitud de Oferta VSD - sdo SOC Pagina 62	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.	Se solicita amablemente a la entidad ajustar el requerimiento establecido en la "Solicitud de Oferta VSD - SDO SOC", con el fin de alinearlo con lo dispuesto en el Anexo Técnico del Proyecto SOC DIAN (Anexo Técnico Administrativo). Lo anterior, considerando que en el Anexo Técnico se establece que el oferente deberá contar con certificación del fabricante por solución, plataforma, servicios y dispositivos, acreditando que se encuentra en alguno de los tres niveles de membresía más altos. Este criterio permite una mayor pluralidad de oferentes en el proceso.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el literal b del documento solicitud de oferta - SDO, es un ítem puntuable, no es obligatorio, el interesado podrá optar a dichos puntajes presentando las certificaciones solicitadas, se diferencia del ítem 18.2 del anexo técnico, por lo tanto, no se acepta su sugerencia.
150	Anexo Técnico Proyecto SOC DIAN (Anexo técnico Administrativos) Item 18.2	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.	En ese sentido, se solicita respetuosamente mantener el requerimiento conforme a lo indicado en el Anexo Técnico, teniendo en cuenta que esta condición ya ha sido previamente considerada en el proceso y resulta menos restrictiva, promoviendo así la participación de un mayor número de oferentes.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el literal b del documento solicitud de oferta - SDO, es un ítem puntuable, no es obligatorio, el interesado podrá optar a dichos puntajes presentando las certificaciones solicitadas, se diferencia del ítem 18.2 del anexo técnico, por lo tanto, no se acepta su sugerencia.
151	Sección VI. Requisitos de los Bienes y Servicios Conexos	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.	Dada la criticidad de los activos de la DIAN, se requiere que el SOC sea una unidad operativa autónoma y demostrable en Bogotá.	Precisar que el SOC debe ser una locación física propia del oferente en Bogotá, con carácter visitable y demostrable previo a la adjudicación.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el servicio de SOC solicitado deberá estar ubicado en la ciudad de Bogotá, y es un requerimiento de obligatorio cumplimiento.
152	Sección VI. Requisitos de los Bienes y Servicios Conexos	Deberá diseñar todos los procesos y procedimientos de gobierno y operativos (Modelo de operación) del SOC considerando la legislación, normativa de seguridad digital en Colombia, buenas prácticas y referencias de arquitecturas seguras, como son las del Gartner, NIST (National Institute of Standards and Technology) y las del CMMI (Capability Maturity Model Integration).	El texto solicita "considerar" el modelo CMMI para el diseño, pero no establece un mecanismo para verificar que el oferente posee la capacidad instalada y la experiencia certificada en dicho modelo.	Precisar que el oferente debe acreditar que sus procesos operativos de SOC están certificados por un tercero independiente con alcance específico en SOC. No se aceptarán autoevaluaciones ni declaraciones juramentadas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento es claro en cuanto a lo requerido, por ende, no se considera necesario agregar su sugerencia.
153	8.5	Dentro de los servicios del SOC se debe administrar y configurar los componentes de una solución de análisis de vulnerabilidades para Código fuente con módulos como son SCA, SCC, WEB Inspect, Runtime y sensores cuando sea requerido, y escalar a DIGIT y/o fabricas los eventos presentados para su solución.	El texto menciona WEB Inspect el cual es un nombre comercial del fabricante Fortify	Se sugiere modificar a Herramienta de análisis dinámico (DAST)	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, el ítem será ajustado y se publicará mediante adenda en los próximos días, quedando de la siguiente manera: 8.5 Dentro de los servicios del SOC se debe administrar y configurar los componentes de una solución de análisis de vulnerabilidades para Código fuente con módulos como son SCA, SCC, Runtime y sensores entre otros cuando sea requerido, y escalar a la Dirección de Gestión de Innovación y Tecnología de la DIAN, y/o fabricas los eventos presentados para su solución.
154	1.3	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.	Obligar a cotizar a futuro sin indexación fuerza al proponente a incluir un "colchón de riesgo" que encarece artificialmente la oferta.	Desvincular la compra de 2028 del precio global fijo. Definir un presupuesto máximo referencial sujeto a actualización de mercado en el año de ejecución.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor de SOC deberá tener en cuenta todo lo requerido para dimensionar su oferta, en este caso el poder presentar precios de servicios que se implementarán a futuro como los mencionados para este ítem, por lo tanto, no se acepta su sugerencia.
155	9	N/A	Eficacia en la Reducción del Fraude. Una alerta sin una acción de mitigación inmediata no reduce el riesgo para el contribuyente. El SOC debe garantizar el desmonte de sitios fraudulentos para proteger el recaudo.	Incluir como requisito obligatorio el servicio de Takedown gestionado y garantizado (24/7) con KPIs de éxito en la eliminación de activos fraudulentos.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
156	9	N/A	La inteligencia aislada genera silos de información. Para prevenir el fraude, los indicadores de compromiso (IoC) deben integrarse sin intervención humana a los controles perimetrales.	Vincular técnicamente la plataforma de inteligencia con el SOAR, garantizando la orquestación de bloqueos automáticos en el perímetro ante indicadores de compromiso (IoC).	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, todos los servicios y capacidades adquiridas deberán poderse automatizar con el servicio SOAR requerido por la Entidad, siempre y cuando sean susceptibles a ello.
157	9	N/A	Al ser la DIAN un nodo de recaudo, la omisión de monitoreo sobre activos financieros expuestos facilita el fraude transaccional masivo contra el Estado.	Ampliar el objeto técnico para incluir obligatoriamente el monitoreo y detección de activos financieros (BINs de tarjetas y datos de pago) vinculados a la pasarela de la entidad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
158	Anexo técnico: Especificaciones Técnicas Protección de Marca (Deep&Dark Web)	N/A	Las campañas de "Fake News" suplantando a la DIAN destruyen la confianza del contribuyente y son el vector principal de los ataques de fraude actuales.	Tipificar y penalizar la incapacidad del sistema para detectar y reportar campañas coordinadas de desinformación y bots dirigidos a la suplantación institucional.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
159	Anexo técnico: Especificaciones Técnicas Protección de Marca (Deep&Dark Web)	N/A	El objeto del contrato debe basarse en resultados tangibles. Los informes no reducen el fraude; la mitigación de riesgos sí lo hace.	Sustituir los indicadores de cantidad por indicadores de impacto: Tiempo Medio de Respuesta (MTTR) y porcentaje de reducción de superficie de ataque digital verificable.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
160	5.4.11	La solución ofertada deberá ser provista por un fabricante en el cuadrante de lideres de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	Con el objetivo de garantizar la pluralidad de oferentes y la neutralidad tecnológica, solicitamos ampliar los criterios de reconocimiento de fabricantes. Sugerimos que se acepten soluciones calificadas en los niveles más altos de reportes especializados (v.gr. Forrester, Gartner, IDC o SC Awards). Cabe destacar que el mercado ha evolucionado hacia plataformas de 'Exposure Assessment', donde fabricantes líderes han demostrado superioridad técnica en reportes de 2025, asegurando que la DIAN acceda a herramientas con visión de riesgo integral y no solo de escaneo pasivo.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
161	8.4	Dentro del servicio del SOC el CONTRATISTA debe realizar análisis de vulnerabilidades y análisis automático y manual del código fuente de las aplicaciones de la entidad cada vez que se requiera validar La aplicación de las prácticas de SDLC sobre los desarrollos de la DIAN de acuerdo con el procedimiento de desarrollo seguro vigente referenciado por DIGIT (Dirección de Gestión de Información y Tecnología) de la DIAN.	Tanto para la revisión de resultados como para el desarrollo de ejercicios manuales, es necesario contar con herramientas open source que permitan diversificar y confirmar resultados.	El contratista debe proveer herramientas licenciadas y soportadas por el fabricante para el desarrollo de ejercicios de análisis de vulnerabilidades a nivel del codigo, adicionalmente, podrá soportar sus ejercicios e investigaciones en herramientas propias, las cuales podrán ser open source dado que hacen parte de su know how.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
162	8.6	Debe dar soporte a las fábricas de desarrollo y pruebas en el proceso de Desarrollo Seguro.	Existen herramientas que permiten el seguimiento a nivel del ciclo de vida del desarrollo seguro, y lo que hacen es informar de malas practicas a nivel de desarrollo. Ahora bien, el acompañamiento y soporte a una casa de desarrollo, será un trabajo similar a otra casa de desarrollo que haga un trabajo de auditoria y seguimiento, lo cual es propio de desarrolladores, más no de equipos de seguridad.	La herramienta debe soportar proteger el código desde el desarrollo identificando vulnerabilidades en las fases CI/CD y proporcionando sugerencias de remediación. Se debe definir el numero de desarrolladores de la DIAN que serán incluidos en esta estrategia.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
163	10	El alcance de los ejercicios de ethical hacking no se limita únicamente a los activos críticos de la entidad sino también a los que hacen parte del anexo de inventarios de éste proyecto. Aunque se priorizarán activos de relevancia en cada ejercicio, la selección de activos incluirá aquellos que la DIAN considere esenciales para evaluar la postura de seguridad de la infraestructura tecnológica en general. La determinación específica de los activos a incluir se hará en la fase de planeación de cada ejercicio, en conjunto con el contratista, de acuerdo con las necesidades de seguridad identificadas (como mínimo cien (100) activos).	Es necesario definir el numero y tipo de activos a considerar o al menos indicar que estos serán definidos en conjunto con el contratista, de mutuo acuerdo. Si bien ya se dice que minimo son 100, cuanto es el maximo, y que tipo de activos se verán, bases de Datos, servidores, dispositivos de red, aplicaciones. Esto es necesario para poder definir el esfuerzo a considerar.	El alcance de los ejercicios de ethical hacking no se limita únicamente a los activos críticos de la entidad sino también a los que hacen parte del anexo de inventarios de éste proyecto. Aunque se priorizarán activos de relevancia en cada ejercicio, la selección de activos incluirá aquellos que la DIAN considere esenciales para evaluar la postura de seguridad de la infraestructura tecnológica en general. La determinación específica de los activos a incluir se hará en la fase de planeación de cada ejercicio, en conjunto con el contratista, de acuerdo con las necesidades de seguridad identificadas (como mínimo cien (100) activos). De estos activos, el 90% corresponderan a activos de red o servidores, y el 10% a aplicaciones.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas para este requerimiento se encuentran claramente definidas así como su alcance y cantidades en el ítem 10 del anexo técnico.
164	10.5	Se deberán establecer protocolos claros para la comunicación durante el proyecto, incluyendo puntos de contacto, actualizaciones regulares y manejo de hallazgos críticos.	Por favor aclarar la espectativa de lo solicitado, si se requiere que cada que se desarrolle un ejercicio de ethical hacking en cualquiera de sus fases, al evidenciar o al tener hallazgos criticos, se deben comunicar para que sean remediados.	Se deberán establecer protocolos claros para la comunicación durante el proyecto, incluyendo puntos de contacto, actualizaciones regulares y manejo de hallazgos críticos. Dicha comunicación oportuna busca que los equipos de administración y seguridad tomen medidas oportunidad en la mitigación del riesgo	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem es claro en cuanto a que, se debe manejar y establecer protocolos claros al evidenciar o al tener hallazgos críticos, se deben comunicar para que sean remediados

165	10.6	Se deberá preparar un plan de respuesta a incidentes en caso de que se descubran vulnerabilidades graves.	En ejercicios ofensivos, se tienen hallazgos más no incidentes, los incidentes deben ser manejados por los equipos de CSIRT	Se deberá entregar de manera oportuna recomendaciones de remediación en caso de que se descubran vulnerabilidades graves. El proveedor deberá manifestar y entregar las recomendaciones de remediación para los hallazgos críticos antes de la entrega del informe final	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el requerimiento refiere a entregar un plan de respuesta en caso de descubrir vulnerabilidades graves en el entendido en que el futuro proveedor del SOC actuaría como apoyo en la resolución más no como actor principal, las actividades de remediación que implique infraestructura de la Entidad serán realizadas directamente por personal de la Entidad.
166	410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	Todos los elementos necesarios para la implementación de cualquiera de las capacidades requeridas por la Entidad en este proyecto, debe ser provista por el futuro oferente, entendiéndose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones. Recordando que se deberá suministrar los recursos necesarios (rack, conexiones, entre otros) para la instalación y configuración de dispositivos colectores (en caso de ser necesario) en las diferentes sedes de la Entidad, ya sean físicos o virtuales.	Se requiere mayor claridad respecto al alcance de la responsabilidad del proveedor, considerando que algunas soluciones operan sobre equipos físicos que demandan condiciones específicas de instalación, tales como disponibilidad de espacio en rack o cuartos de equipos con condiciones adecuadas de refrigeración y suministro eléctrico. Asimismo, existen soluciones de tipo virtual que dependen de la provisión de máquinas virtuales integradas o conectadas a la infraestructura de la DIAN. Estas diferencias implican consideraciones técnicas que deben ser definidas con precisión por la entidad.	e sugiere solicitar a la entidad mayor claridad sobre las capacidades actuales de infraestructura disponibles para los despliegues requeridos. Adicionalmente, se recomienda contemplar la realización de una visita técnica en el marco del proceso, con el fin de dimensionar adecuadamente las condiciones y necesidades del requerimiento objeto de contratación.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el requerimiento refiere a que el futuro proveedor del SOC deberá entregar e implementar todos los elementos necesarios en caso de que aplique y que deban ser instalados en las sedes de la Entidad.
167	12.81	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.	La definición de planes de remediación no debe estar de parte del proveedor, ya que la aplicación de este no depende del proveedor sino de los equipos internos de la entidad, lo que si se hace es generar las recomendaciones de remediación, acompañamiento y aclaraciones necesarias. Igualmente, centrarse solo en vulnerabilidades criticas para lograr una sinergia y dinamica de trabajo que pueda	Se deberá prestar el servicio de acompañamiento, asesoramiento, generación de recomendaciones de remediación entre otros para la solución de las vulnerabilidades críticas 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.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
168	13.2	Las actualizaciones de software, firmware y parches/fixes de toda la plataforma y dispositivos entregados, deben ser realizadas periódicamente en forma integrada y considerando todos los componentes. Una vez el fabricante o fabricantes de los dispositivos entregados, libera las nuevas versiones. De común acuerdo la Entidad programará dichas actividades para que el CONSULTOR proceda a realizarlas y probarlas. Por lo tanto, su periodicidad depende exclusivamente de la liberación de las actualizaciones de los fabricantes y deberá hacerse por los tres (3)años del soporte y garantía.	Las actualizaciones a nivel de Firmware o parchado, debe comprometerse a nivel de buen funcionamiento o fallas de seguridad, no solo a liberaciones por parte del fabricante.	Las actualizaciones de software, firmware y parches/fixes de toda la plataforma y dispositivos entregados, deben ser realizadas periódicamente en forma integrada y considerando todos los componentes. Una vez el fabricante o fabricantes de los dispositivos entregados, libera las nuevas versiones. De común acuerdo la Entidad programará dichas actividades para que el CONSULTOR proceda a realizarlas y probarlas. La periodicidad dependerá de las recomendaciones del fabricante a nivel de buen funcionamiento o de seguridad, por tanto, no toda actualización o liberación implica si o si la aplicación.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
169	5.4.11	La solución ofertada deberá ser provista por un fabricante en el cuadrante de lideres de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management)	Se solicita muy amablemente a la entidad ajutar este item para adicionar que la solución debe estar reconocida como Leader o Strong Performer en The Forrester Wave™: Vulnerability Risk Management, en su edición vigente, esto para permitir la pluralidad de fabricantes ya que en este momento solo esta cumpliendo el fabricante Tenable.	La solución ofertada deberá ser provista por un fabricante en el cuadrante de lideres de Gartner o lider o Strong Performer en Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su solicitud.
170	13.15	Tiempos de Atención Se detallan los tiempos de atención requeridos por la Entidad para la atención de incidentes de seguridad u operación, este tiempo se define como el transcurrido entre el registro del incidente y el inicio de la atención de este por parte de un asesor de soporte y servicio Prioridad Crítica: Situación que se presenta y genera pérdida total del servicio en el ambiente de producción por indisponibilidad de todas las componentes críticas del mismo. La afectación genera un impacto catastrófico para el negocio. Prioridad Alta: Situación que se presenta y genera impacto mayor para el negocio sobre el servicio por indisponibilidad de algunas componentes críticas del mismo. Prioridad Media: Situación que se presenta y genera un impacto moderado para el negocio por degradación de algunas componentes del servicio. Prioridad Baja: Situación que se presenta pero que no genera afectación del servicio. Se trata de un evento que no impide en forma alguna la operación y el impacto para el negocio es menor.	Se deben definir los tiempos	Tiempos de Atención Se detallan los tiempos de atención requeridos por la Entidad para la atención de incidentes de seguridad u operación, este tiempo se define como el transcurrido entre el registro del incidente y el inicio de la atención de este por parte de un asesor de soporte y servicio Prioridad Crítica: Situación que se presenta y genera pérdida total del servicio en el ambiente de producción por indisponibilidad de todas las componentes críticas del mismo. La afectación genera un impacto catastrófico para el negocio. Prioridad Alta: Situación que se presenta y genera impacto mayor para el negocio sobre el servicio por indisponibilidad de algunas componentes críticas del mismo. Prioridad Media: Situación que se presenta y genera un impacto moderado para el negocio por degradación de algunas componentes del servicio. Prioridad Baja: Situación que se presenta pero que no genera afectación del servicio. Se trata de un evento que no impide en forma alguna la operación y el impacto para el negocio es menor. Acuerdos de Nivel de Servicio Tiempo de Respuesta Tiempo de Resolución > 4 horas ≤ 3 días ≤ 3 horas ≤ 2 días ≤ 2 horas ≤ 8 horas ≤ 1 hora ≤ 4 horas En los casos que se requiera escalamientos al fabricante, los tiempos se modificarán y sumaran los aplicados por el soporte del fabricante	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los tiempos están definidos en el ítem 19.2.7.
171	13.17	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.	Limitarlo a las más criticas, además de aclarar que las remediación debe ser responsabilidad del equipo de infraestructura del cliente, salvo los eventos que correspondan a las herramientas del presente contrato	Para la plataforma de gestión de vulnerabilidades, se debe tener el servicio de análisis y recomendaciones de 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 realizar el apoyo, soporte y acompañamiento durante la remediación de todas las vulnerabilidades críticas encontradas en la prestación del servicio y la ejecución del contrato.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, en el entendido que el ítem en mención hace referencia apoyo al área técnica de la Entidad - DGIT, por lo tanto, no se acepta su sugerencia.
172	18.2	Una certificación emitida directamente de los fabricantes de las soluciones ofertadas donde se evidencie que los equipos suministrados no se encuentran en fin de venta y contaran con soporte por mínimo 5 años, estas cartas deben ser dirigidas a la Entidad.	Solicitarla tambien para que sea directa a este proceso	El oferente deberá presentar certificación expedida directamente por los fabricantes de las soluciones ofertadas, en la cual se acredite que los equipos suministrados no se encuentran en estado de fin de venta (End of Sale - EOS) y que contarán con soporte técnico por un término mínimo de cinco (5) años. Las certificaciones deberán estar dirigidas a la Entidad e indicar de manera expresa el proceso de contratación al cual se presentan. Así mismo, para las tecnologías de CNAPP, SOAR, SIEM y Deceptor, el oferente deberá acreditar que cuenta con mínimo cinco (5) especializaciones, certificaciones o competencias vigentes emitidas por el fabricante correspondiente, las cuales deberán estar relacionadas directamente con la implementación, administración o soporte de dichas tecnologías.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
173	5.9.22	La solución ofertada deberá incluir la posibilidad de programar ventanas de escaneo.	Si nuestro entendimiento es correcto, la solución ofertada deberá permitir la programación de ventanas de escaneo y proporcionar una visión centralizada de los activos y exposiciones de seguridad. Al respecto, se solicita respetuosamente a la Entidad aclarar si dentro del alcance de este requerimiento se contempla que dicha visión centralizada incluya la consolidación e integración de información proveniente de múltiples fuentes de escaneo y evaluación, tanto internas como externas, permitiendo una gestión unificada, contextualizada y orientada al riesgo. En caso de no ser un requisito obligatorio, se sugiere confirmar si este tipo de capacidades podrán ser presentadas por los oferentes como un elemento adicional dentro de la solución propuesta, considerando que su incorporación contribuye a mejorar la visibilidad integral del entorno, optimizar la priorización de vulnerabilidades y fortalecer la toma de decisiones en materia de ciberseguridad.	"La solución ofertada deberá permitir la programación de ventanas de escaneo y proporcionar una visión centralizada y consolidada de los activos y exposiciones de seguridad, integrando información proveniente de múltiples fuentes de escaneo y evaluación, tanto internas como externas, con el fin de facilitar una gestión unificada, contextualizada y basada en riesgo."	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
174	5.10.22	La solución ofertada deberá contar con la capacidad de gestionar los hallazgos, donde se puedan observar todas las vulnerabilidades descubiertas en la infraestructura	La herramienta se complementaria para aumentar su performance una vez El mecanismo de optimización permita una reducción significativa del tiempo de ejecución de los escaneos, manteniendo una cobertura completa de seguridad mediante procesos de perfilado inicial y planes de detección dinámicos basados en el historial y características de la aplicación evaluada.	"La solución ofertada deberá contar con la capacidad de gestionar los hallazgos, permitiendo la visualización de las vulnerabilidades identificadas en la infraestructura. Adicionalmente, la solución podrá incorporar mecanismos de optimización de escaneos que permitan reducir los tiempos de ejecución, manteniendo una cobertura completa de seguridad mediante procesos de perfilado inicial y planes de detección dinámicos basados en el historial y características de los activos o aplicaciones evaluadas."	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
175	6.5.6	Debe escanear automáticamente la red haciendo uso de técnicas de escaneo pasivo y sugerir los elementos de decepción que se deben desplegar.	La modificación propuesta busca garantizar la neutralidad tecnológica y la pluralidad de oferentes, evitando restringir el requisito a un único mecanismo específico como el escaneo pasivo automático. Se amplía el alcance a capacidades equivalentes de descubrimiento y análisis del entorno, ya sea de forma automática, asistida o basada en mejores prácticas, manteniendo el objetivo funcional sin afectar la efectividad de la solución y reduciendo el riesgo de direccionamiento del proceso.	La solución debe contar con capacidades de descubrimiento de red, análisis del entorno o mecanismos de identificación de activos que permitan sugerir, facilitar o apoyar la definición de estrategias de despliegue de elementos de decepción, ya sea de forma automática, asistida o basada en mejores prácticas del fabricante	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
176	Sección III. Criterios de Evaluación y Calificación	c. Incluye servicios TAM (Thecnical account manager) (ítems 2 al 9 del anexo técnico). con el mismo contexto	Muy bueno (5): en 5 o más de las capacidades.	Se solicita a la Entidad aclarar el alcance del criterio "incluye servicios TAM (Technical Account Manager) (ítems 2 al 9 del anexo técnico)", en el entendido de si el puntaje se otorga cuando el oferente incluye este servicio para varias de las capacidades requeridas, independientemente de si estas son cubiertas por un mismo fabricante. Bajo este entendimiento, se considera que el puntaje debería asignarse de manera acumulativa por las capacidades que incluyan el servicio TAM, sin limitarse a la diversidad de fabricantes. Se solicita confirmar si esta interpretación es correcta.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, que el puntaje puede asignarse de manera acumulativa por las capacidades que incluyan el servicio TAM, sin limitarse a la diversidad de fabricantes. Recordando que el literal c es un ítem puntuable, para el caso en especifico, 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. Acorde a lo anterior también se aclara que para dicha puntuación, el futuro interesado podrá escoger acorde a los fabricantes entregados según las capacidades y servicios implementados, cual de estos cumple con la condición TAM y entregar dicha acreditación, ya que la Entidad no menciona ni discrimina nombre alguno de fabricante.
177	Sección III (numeral ii)	(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:	Con relación al requisito de experiencia y capacidad técnica general, sugerimos analizar la conveniencia de no admitir contratos en ejecución como mecanismo de acreditación de experiencia, aun cuando presenten un porcentaje de avance mínimo. Lo anterior, considerando que la aceptación de contratos no terminados puede generar incertidumbre en la verificación objetiva de la experiencia, en la medida en que: El alcance definitivo del contrato aún no se encuentra completamente ejecutado; Existe riesgo de modificaciones, suspensiones o terminaciones anticipadas; y No es posible verificar con certeza la totalidad de las actividades desarrolladas ni los resultados finales obtenidos. En ese sentido, estimamos que limitar la acreditación de la experiencia a contratos debidamente terminados permitiría fortalecer los principios de selección objetiva, verificabilidad y comparabilidad, así como reducir eventuales controversias durante la etapa de evaluación. Agradecemos nos indiquen si la Entidad estaría dispuesta a ajustar el requisito en ese sentido o, en su defecto, a establecer reglas más estrictas de verificación que mitiguen los riesgos asociados a la aceptación de contratos en ejecución.	(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:	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
178	Sección III (numeral ii)	Presentar máximo seis (6) contratos. La sumatoria de los contratos debe ser mínimo de seis (6) millones de dólares.	Sobre el requisito del valor de la experiencia, les pedimos confirmar los siguientes puntos - ¿Cómo se calculará la TRM para verificar el cumplimiento del monto mínimo de seis (6) millones de dólares, y cuál será la fecha de referencia que se tomará para dicho cálculo? - ¿Cuál será el criterio para la conversión de los contratos pactados en monedas diferentes al dólar, en particular en pesos colombianos (COP) y euros (EUR)?	Contratos terminados o iniciados (mínimo 40% de ejecución) dentro de los últimos siete (7) años	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la TRM que se tomará será la de finalización de cada contrato, y para los contratos en ejecución se tomará la actual de acuerdo al porcentaje de avance de ejecución, así mismo, se indica que serán los mismos criterios para conversión si estos se encuentran en otras monedas.
179	Sección III (numeral ii)	Presentar máximo seis (6) contratos. La sumatoria de los contratos debe ser mínimo de seis (6) millones de dólares.	Agradecemos se nos aclare cómo debe interpretarse el alcance del requisito, en particular si los hasta seis (6) contratos que pueden presentarse deben acreditar en su conjunto las tres (3) actividades señaladas, o si, por el contrario, cada contrato debe cumplir individualmente con una o varias de dichas actividades.		La Dirección de Impuestos y Aduanas Nacionales (DIAN) informa al observante que se debe cumplir con un máximo de seis (6) contratos, los cuales en cada uno deben incluir al menos una de las tres (3) actividades señaladas.
180	Sección VI (numeral 6.1)	El equipo mínimo de trabajo presentado por el contratista no deberá ser modificado durante el desarrollo del proyecto no obstante, lo anterior, si por causas excepcionales no atribuibles al CONTRATISTA es necesario realizar alguna modificación, se deberá tener en cuenta lo siguiente:	Consideramos que los cambios en el equipo de trabajo no necesariamente deban obedecer a causas excepcionales no imputables al Contratista. En ese sentido y dado la autonomía que tiene el CONTRATISTA respecto a su organización administrativa, solicitamos se permitan cambios en el equipo mínimo cuando lo determine necesario el CONTRATISTA, siempre que éste garantice el cumplimiento del proceso de reemplazo culpa con las condiciones técnicas mínimas previstas en esta invitación.	El equipo mínimo de trabajo presentado por el contratista no deberá ser modificado durante el desarrollo del proyecto no obstante, lo anterior, si el CONTRATISTA considera necesario realizar alguna modificación, se deberá tener en cuenta lo siguiente:	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
181	Sección VI (numeral 6.1)	El profesional que lo remplace deberá tener un perfil igual o superior al del profesional que fue propuesto en la oferta presentada y el cambio será aprobado por el supervisor del contrato	Si bien entendemos que el equipo de trabajo mínimo es un elemento de la oferta del Contratista y es un pilar fundamental para la ejecución del contrato, por lo cual cualquier cambio en los perfiles mínimos deben ser aprobados por la Entidad, solicitamos se precise que el nuevo perfil deberá cumplir con iguales o mejores condiciones a las exigidas en el Anexo Técnico, sin que necesariamente acredite iguales o mejores condiciones que el perfil saliente.	El profesional que lo remplace deberá tener un perfil igual o superior al perfil exigido en el Anexo Técnico y el cambio será aprobado por el supervisor del contrato	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
182	Sección I	El oferente deberá acreditar su pertenencia a la más alta membresía por parte de las fabricantes de los productos, servicios, plataformas o ... e deberá informar los mecanismos suficientes para corroborar dicha	Si se presentar a través de una Asociación en Participación, consorcio o asociación -APCA, es viable que solo uno de los integrantes cumplan con este requerimiento?	Favor responder la Observación / Comentario.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, su entendimiento es correcto, en caso de APCA con solo uno de los integrantes que cumpla el requisito se da como válida la membresía, siempre y cuando se cumpla con lo solicitado.
183	Sección I	- 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.	Se debe demostrar los tres tipos de contrato o solo es necesario uno de ellos ?	Favor responder la Observación / Comentario.	La Dirección de Impuestos y Aduanas Nacionales (DIAN) informa al observante que se debe cumplir con un máximo de seis (6) contratos, los cuales en su conjunto deben satisfacer los tres criterios solicitados.
184	Sección VII	Para IBM QRADAR e IBM GUARDIUM, favor indicar el modelo, serial, licenciamiento, capacidad y demás características técnicas de los equipos	Para IBM QRADAR e IBM GUARDIUM, favor indicar el modelo, serial, licenciamiento, capacidad y demás características técnicas de los equipos	Compartir capacidades técnicas de los equipos IBM QRADAR e IBM GUARDIUM	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. 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.
185	Sección III	FIRST, Certificación que acredite vinculación directa y activa con FIRST (Forum Incident Response and Security Teams) como mínimo doce (12) meses de antigüedad.	En este punto se pide antigüedad de 12 meses.	Se solicita a la entidad ajustar este punto antigüedad de la certificación donde este abierto a tener la certificación y estar vinculado al FIRST.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la certificación FIRST es puntuable con una antiguedad mínimo de doce (12) meses.
186	Sección VII	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.	En este punto se solicita tener capoacidades que hace una herramientas de obervabiliodad y no de correlación de eventos.	Se solicita a la entidad ajustrar este punto con el fin de poder hacer una integración con un herramienta especlizada en obervabilidad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem fue eliminado mediante adenda.
187	Sección VII	2.13 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	En este punto se pide una solución de SIEM que este instalada on premise o en nube publica (IaaS o Paas).	Se solicita a la entidad ajustar este punto con el fin de poder brindar un servicio de SIEM SaaS.	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.
188	Sección VII	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.	En este punto se solicita tener los informes predefindos y listos para ser usuados.	Se solicita a la entidad ajustar este punto donde el SIEM este en capacidad de generar Dashboards pre construidos y workbooks, los cuales se usan como informes y cubren los controles que exige la norma.	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.
189	Sección VII	2,28 Paneles de control personalizados, como mínimo debe incluir los siguientes elementos: - Dashboards configurables en tiempo real, con desplazamiento "Slide-Show" para mostrar KPIs. - Informes y análisis exportables entre organizaciones y usuarios. - Identificación rápida los problemas críticos, por ejemplo, a través de un código de colores. - Actualización rápida mediante el cálculo en memoria, sin acceso a disco. - Dashboards especializados para servicios empresariales, infraestructura virtualizada y aplicaciones especializadas.	En este punto se pide una solución de SIEM que este instalada on premise o en nube publica (IaaS o Paas).	Se solicita a la entidad eliminar este punto "- Actualización rápida mediante el cálculo en memoria, sin acceso a disco." con el fin de poder brindar un servicio de SIEM SaaS.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.

190	Sección VII	2,33 Supervisión de disponibilidad, como minimo 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.	En este punto se solicita tener capoacidades que hace una herramientas de monitoreo de salubridad y no de correlación de eventos.	Se solicita a entidad ajustrar este punto con el fin de poder hacer una integración con un herramienta especlizada en el monitoreo de salubridad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem fue ajustado mediante adenda.
191	Sección VII	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.	Para cumplir este punto se pide una solución de SIEM que este instalada on premise o en nube publica (IaaS o Paas).	Se solicita a la entidad elimnar este punto "-Soporte de archivado de logs tanto para NFS como HDFS." con el fin de poder brindar un servicio de SIEM SaaS.	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. Por lo tanto, asegurar que se está dando prelación a un sólo fabricante es inexacto, así mismo, se indica que las características solicitadas por la Entidad obedecen a necesidades puntuales, por lo tanto, no se acepta su observación.
192	8.5	Dentro de los servicios del SOC se debe administrar y configurar los componentes de una solución de análisis de vulnerabilidades para Código fuente con módulos como son SCA, SCC, WEB Inspect, Runtime y sensores cuando sea requerido, y escalar a DIGIT y/o fabricas los eventos presentados para su solución.	Se solicita muy amablemente ajustar o eliminar el requerimiento relacionado con “runtime y sensores”, considerando que estas capacidades corresponden a soluciones de protección en tiempo de ejecución (como WAAP o RASP), orientadas a aplicaciones en producción, mientras que el alcance del presente proceso está enfocado en herramientas de análisis de código (SAST, DAST y SCA) dentro del ciclo de desarrollo (SDLC), por lo que su inclusión podría limitar la participación de soluciones especializadas sin aportar valor directo al objetivo del servicio requerido.	Dentro de los servicios del SOC se debe administrar y configurar los componentes de una solución de análisis de vulnerabilidades para Código fuente con módulos como son SCA, SCC y WEB Inspect, cuando sea requerido, y escalar a DIGIT y/o fabricas los eventos presentados para su solución.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, el ítem será ajustado y se publicará mediante adenda en los próximos días, quedando de la siguiente manera: 8.5 Dentro de los servicios del SOC se debe administrar y configurar los componentes de una solución de análisis de vulnerabilidades para Código fuente con módulos como son SCA, SCC, Runtime y sensores entre otros cuando sea requerido, y escalar a la Dirección de Gestión de Innovación y Tecnología de la DIAN, y/o fabricas los eventos presentados para su solución.
193	10.1	Se deben realizar como mínimo dos (2) ejercicios de ethical hacking por año durante la vigencia del contrato del Centro de Operaciones de Seguridad de la Entidad, para lo cual se deberá entregar el respectivo cronograma el cual debe incluir como mínimo las etapas de preparación, ejecución de pruebas, análisis y elaboración de informes. Las pruebas deben aplicar metodologías de EH COMO: OSSTMM, ISSAF, OTP (OWASP Testing Project), entre otras.	Por favor indicar si se requiere retest, lo cual es lo más recomendable	Se deben realizar como mínimo dos (2) ejercicios de ethical hacking con retest por año durante la vigencia del contrato del Centro de Operaciones de Seguridad de la Entidad, para lo cual se deberá entregar el respectivo cronograma el cual debe incluir como mínimo las etapas de preparación, ejecución de pruebas, análisis y elaboración de informes. Las pruebas deben aplicar metodologías de EH COMO: OSSTMM, ISSAF, OTP (OWASP Testing Project), entre otras.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características técnicas solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
194	10.7	Para realizar los ejercicios de Ethical Hacking se debe disponer de un equipo como mínimo de tres (3) ingenieros con conocimientos en programación, sistemas operativos y estar certificados en hacking ético.	El numero de ingenieros no garantiza el cumplimiento de metas o indicadores necesariamente, adicionalmente, este personal no sería dedicado solo a este proyecto, por lo que se sugiere que no se limite solo a 3 ingenieros, sino que sea potestad del contratista el numero de ingenieros a disponer, garantizando el liderazgo de dicho equipo y la idoneidad. O por favor aclarar si se requieren recurso dedicado a la DIAN	Para realizar los ejercicios de Ethical Hacking se debe disponer de un equipo ingenieros con conocimientos en programación, sistemas operativos y estar certificados en hacking ético.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
195	12.4	Dentro del plan de trabajo deberá especificar la metodología que utilizará para administrar, configurar, monitorear y gestionar el servicio de monitoreo objeto del presente contrato, especificando etapas, recursos, entregables, herramientas y técnicas a utilizar. Nota: La Entidad se reserva el derecho de ajustar aspectos de la metodología.	Es necesario conocer detalles de la operación actual, telemetria de incidentes reportados, solicitudes de Análisis forense, con cuanto personal opera hoy el SOC de la entidad.	Si nuestro entendimiento es correcto, el requerimiento establece que el oferente deberá definir la metodología para la administración, configuración, monitoreo y gestión del servicio SOC, incluyendo etapas, recursos, entregables, herramientas y técnicas a utilizar. Con el fin de estructurar una propuesta metodológica adecuada, alineada a la realidad operativa de la Entidad y a las necesidades específicas del servicio, se considera relevante contar con mayor visibilidad sobre el estado actual de operación en materia de monitoreo de seguridad. En este sentido, se solicita respetuosamente a la Entidad confirmar si actualmente cuenta con un servicio SOC en operación y, de ser así, suministrar información general que permita dimensionar el alcance del servicio, tales como: volumen de telemetría de incidentes gestionados, número de eventos o alertas procesadas, solicitudes de análisis forense atendidas, así como la capacidad operativa actual en términos de personal asignado. Esta información permitirá a los oferentes diseñar una metodología más precisa, eficiente y ajustada a las condiciones reales de la Entidad, optimizando la asignación de recursos, la definición de niveles de servicio y la adecuada transición o implementación del servicio requerido.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, en la actualidad la Entidad no tiene un servicio de SOC en operación, por tanto, no es posible entregar información acerca de la operación del mismo, adicionalmente, el plan de trabajo es justamente para identificar el acercamiento metodológico a la implementación y sus ajustes a través del tiempo, de forma que pueda ser evaluada su pertinencia, adaptabilidad, estructura y resultados esperados.
196	12.7	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	Estos son procesos con los que hoy ya cuenta la entidad y se requiere una auditoria de cumplimiento? Por favor aclarar la espectativa porque esto es más labores de administración y operación, no de seguridad.	Se sugiere manejar esto como labores de auditoria que se darán 2 veces al año, más no como actividades de monitoreo continuo, ya que dependen más de que los controles sean configurades y se mantenga, esto se evidencia más en una auditoría	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud, puesto que corresponden a acciones de verificación no de auditoría.
197	19.4.4	Reportar incidentes de seguridad a los entes externos: En caso de presentarse un incidente de seguridad de la información es el único autorizado para reportarlos de ser necesario. Se pueden reportar incidentes de seguridad de la información a través de los siguientes canales: - ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), reportar al correo electrónico: contacto@colcert.gov.co o al Teléfono: (+571) 2959897. - CSIRT Gobierno reportar al correo csirtgob@mintic.gov.co - Centro cibernético Policial reportar en la siguiente ruta: https://caivirtual.policia.gov.co/	Existe un riesgo reputacional asociado al reporte de los incidentes por lo que es clave que si bien, el oferente que detecta, reporte a la DIAN, sea la DIAN quien apruebe que se comunique y se reporten los incidentes.	Reportar incidentes de seguridad a los entes externos: En caso de presentarse un incidente de seguridad de la información la DIAN es el único autorizado para reportarlos o delegar que se reporten de ser necesario. Se pueden reportar incidentes de seguridad de la información a través de los siguientes canales: - ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), reportar al correo electrónico: contacto@colcert.gov.co o al Teléfono: (+571) 2959897. - CSIRT Gobierno reportar al correo csirtgob@mintic.gov.co - Centro cibernético Policial reportar en la siguiente ruta: https://caivirtual.policia.gov.co/	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud. puesto que, es deber de la Entidad informar los incidentes de acuerdo con el Decreto 338 de 2022.
198	5.10.23	La solución ofertada deberá permitir la priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación que denote la urgencia de atención a una vulnerabilidad	A su vez la solucion debera utilizar técnicas de inteligencia artificial para analizar el perfil de la aplicación y optimizar automáticamente el conjunto de detecciones a ejecutar, priorizando aquellas relevantes para el contexto específico de la aplicación, sin omitir detecciones previamente identificadas como aplicables.	Si nuestro entendimiento es correcto, la solución ofertada deberá permitir la priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación, que denote la urgencia de atención de cada vulnerabilidad. En línea con las mejores prácticas actuales en gestión de vulnerabilidades y con el fin de fortalecer el alcance técnico del proceso, se sugiere a la entidad considerar que dicha priorización pueda apoyarse en capacidades avanzadas de análisis, tales como el uso de técnicas de inteligencia artificial o analítica avanzada, que permitan optimizar de manera automática la identificación y priorización de vulnerabilidades en función del contexto del activo o aplicación. Lo anterior, teniendo en cuenta que este tipo de capacidades contribuyen significativamente a mejorar la precisión en la toma de decisiones, reducir tiempos de respuesta y enfocar los esfuerzos de remediación sobre los riesgos más relevantes, por lo cual se consideran elementos altamente recomendables dentro de soluciones modernas de gestión de vulnerabilidades.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud. Adicionalmente, no hay propuesta de cambio del texto de la sección.
199	5.4.11	El fabricante de la solución deberá poner a disposición acceso a una API que permita crear conectores, importar/exportar datos y automatizar procesos	Se recomienda a la entidad que a su vez deberá incorporar capacidades de optimización inteligente de escaneos de vulnerabilidades mediante el uso de AI scan optimization, con el objetivo de reducir tiempos de escaneo, optimizar el consumo de recursos y mantener una cobertura integral y efectiva de detección de vulnerabilidades en aplicaciones web y APIs.	Si nuestro entendimiento es correcto, el fabricante de la solución deberá poner a disposición acceso a una API que permita crear conectores, importar/exportar datos y automatizar procesos. En línea con las mejores prácticas actuales en gestión de vulnerabilidades y con el fin de fortalecer el alcance técnico del proceso, se sugiere a la entidad considerar que la solución incorpore capacidades avanzadas de optimización inteligente de escaneos, tales como el uso de técnicas de inteligencia artificial (AI Scan Optimization), orientadas a reducir tiempos de escaneo, optimizar el consumo de recursos y mantener una cobertura integral y efectiva en la detección de vulnerabilidades en aplicaciones web y APIs. Lo anterior, teniendo en cuenta que este tipo de capacidades permiten mejorar la eficiencia operativa del servicio, optimizar el desempeño de la herramienta en entornos de alta demanda y asegurar una evaluación continua y contextualizada de la superficie de ataque, por lo cual se consideran elementos altamente recomendables dentro de soluciones modernas de gestión de vulnerabilidades.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud. puesto que no hay propuesta de cambio del texto de la sección.
200	5.4.11	La solución ofertada deberá ser provista por un fabricante en el cuadrante de lideres de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	Solicitamos respetuosamente a la entidad considerar un ajuste al requerimiento, con el fin de ampliar y clarificar los criterios de validación de la tecnología propuesta, garantizando así la pluralidad de oferentes y la selección objetiva dentro del proceso. El criterio actualmente definido, al limitar el reconocimiento exclusivamente a cuadrantes específicos de determinados analistas, puede restringir la participación de soluciones que, si bien cuentan con capacidades técnicas equivalentes o superiores en gestión de vulnerabilidades y riesgo, son evaluadas bajo otros marcos de análisis igualmente reconocidos en la industria. En este sentido, mantener una única referencia de validación podría generar una limitación innecesaria del mercado, afectando la competitividad del proceso y la posibilidad de que la entidad acceda a alternativas tecnológicas robustas, innovadoras y alineadas con las mejores prácticas actuales en ciberseguridad.	“La solución propuesta debe estar reconocida en evaluaciones recientes de analistas de la industria en gestión de vulnerabilidades y riesgo, tales como The Forrester Wave™, IDC MarketScape, GigaOm Radar, SC Awards Europe, Gartner u otros informes equivalentes y ampliamente reconocidos en el mercado, en su versión más reciente.”	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
201	5.4.15	Debe incluir una capacidad integrada de exploración activa y pasiva, incluyendo análisis continuo por medio de análisis de tráfico desde un puerto espejo o similar.	Si nuestro entendimiento es correcto, la solución ofertada deberá incluir una capacidad integrada de exploración activa y pasiva, contemplando análisis continuo de tráfico mediante mecanismos como puertos espejo o similares. **Con el fin de fortalecer el alcance técnico del requerimiento** y alinearlo con prácticas modernas de visibilidad de red, se sugiere a la entidad considerar la incorporación de capacidades avanzadas de monitoreo pasivo, orientadas a optimizar el descubrimiento continuo de activos y reducir dependencias operativas en la infraestructura de red. En particular, este tipo de capacidades permiten mejorar la cobertura de detección en entornos dinámicos, minimizar impactos en la red y facilitar una visibilidad más distribuida y escalable, lo cual resulta clave en arquitecturas híbridas y de alta complejidad.	“La solución deberá incluir capacidades de monitoreo pasivo mediante sensores no intrusivos que permitan el análisis de tráfico de red en tiempo real para el descubrimiento continuo de activos. Deberá soportar el análisis de tráfico replicado mediante mecanismos como SPAN, RSPAN, ERSPAN o equivalentes, sin generar impacto en la operación de la red. Adicionalmente, deberá permitir el uso de agentes ligeros como sensores pasivos distribuidos, reduciendo la dependencia exclusiva de configuraciones de puertos espejo tradicionales. Los activos detectados deberán integrarse automáticamente en un inventario centralizado, garantizando su visibilidad y gestión dentro de la plataforma.”	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
202	5.4.16	La solución ofertada deberá poder ejecutar descubrimiento de activos y vulnerabilidades a través de: - Monitoreo pasivo mediante el análisis de red a través de un puerto espejo para el descubrimiento de activos, incluyendo el descubrimiento pasivo de objetivos utilizando IPv6. - Sensores activos para el descubrimiento de activos y análisis de vulnerabilidades incluyendo el uso de IPv6. Estos sensores se pueden desplegar en forma de escáneres o agentes.	Si nuestro entendimiento es correcto, la solución ofertada deberá poder ejecutar el descubrimiento de activos y vulnerabilidades mediante monitoreo pasivo a través de análisis de red (por ejemplo, mediante puerto espejo) y sensores activos desplegados como escáneres o agentes, incluyendo soporte para entornos IPv6. Con el fin de fortalecer el alcance técnico del requerimiento y alinearlo con capacidades modernas de descubrimiento continuo, se sugiere a la entidad considerar la inclusión de funcionalidades adicionales de monitoreo pasivo avanzado, que permitan optimizar la visibilidad de activos en entornos dinámicos y distribuidos. En este sentido, este tipo de capacidades permiten ampliar la cobertura de descubrimiento, mejorar la eficiencia operativa y reducir dependencias de configuraciones específicas de red, constituyéndose como un valor agregado relevante dentro de soluciones actuales de gestión de vulnerabilidades.	“La solución ofertada deberá poder ejecutar el descubrimiento de activos y vulnerabilidades a través de: Monitoreo pasivo mediante el análisis de red a través de un puerto espejo o mecanismos equivalentes para el descubrimiento de activos, incluyendo el descubrimiento pasivo de objetivos utilizando IPv6. Sensores activos para el descubrimiento de activos y análisis de vulnerabilidades, incluyendo el uso de IPv6, los cuales podrán desplegarse en forma de escáneres o agentes. **Adicionalmente, la solución deberá:** Permitir, a través de agentes ligeros, el descubrimiento pasivo de activos no gestionados dentro de los entornos monitoreados, integrándolos automáticamente en un inventario centralizado. Contar con sensores pasivos no intrusivos que permitan el análisis continuo del tráfico de red, minimizando la dependencia exclusiva de configuraciones de puertos espejo o mecanismos de reenvío de tráfico. Soportar capacidades de descubrimiento y gestión de activos en entornos IPv6, incluyendo su identificación, seguimiento e integración dentro del inventario de la solución.”	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud. El oferente podrá exceder la expectativa sin que esto implique puntuación extra.
203	5.4.19	Se debe ofrecer despliegue de fabricante para las soluciones consideradas y entrenamiento gratuito en línea como parte de la oferta para los integrantes de la DIAN por parte del fabricante de la solución. Esto durante la vigencia del contrato de soporte.	El requerimiento limita la prestación de servicios de despliegue y entrenamiento exclusivamente al fabricante TENABLE, cuando en el mercado estos servicios frecuentemente son brindados por partners autorizados, manteniendo los mismos estándares de calidad y respaldo.	“El oferente deberá garantizar el despliegue, implementación y capacitación de la solución durante la vigencia del contrato. Estos servicios podrán ser prestados directamente por el fabricante o a través de partners autorizados y certificados, garantizando en todo momento el respaldo oficial del fabricante".	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
204	5.9.8	Detección, Análisis y Evaluación de Vulnerabilidades	Luego de un análisis técnico detallado del alcance definido en el ítem 5.9 (desde el 5.9.1 hasta el 5.9.8), el cual se enfoca en capacidades de detección, análisis y evaluación de vulnerabilidades, se evidencia una oportunidad de fortalecimiento del requerimiento, con el fin de alinear el proceso con las mejores prácticas actuales en gestión de exposición y reducción efectiva del riesgo cibernético. En este sentido, respetuosamente sugerimos a la entidad complementar el alcance incorporando capacidades avanzadas que permitan no solo identificar vulnerabilidades, sino también optimizar su priorización, validación, mitigación y trazabilidad a lo largo de todo su ciclo de vida. Estas capacidades resultan altamente relevantes para cerrar brechas de seguridad, mejorar la eficiencia operativa, reducir tiempos de respuesta y fortalecer la toma de decisiones basada en riesgo, especialmente en entornos complejos y de alta criticidad como los de la Entidad. **La inclusión de estos elementos no limita la participación de oferentes**, sino que permite elevar el estándar técnico del proceso, garantizando la adopción de soluciones modernas, integrales y alineadas con enfoques actuales de gestión de vulnerabilidades basadas en riesgo y exposición.	Como resultado de un análisis técnico detallado del alcance definido en el ítem 5.9 (desde el 5.9.1 hasta el 5.9.8), respetuosamente se sugiere a la entidad considerar la incorporación de buenas prácticas técnicas adicionales que actualmente no se encuentran explícitamente contempladas, y que son ampliamente adoptadas en soluciones modernas de gestión de vulnerabilidades. **1. Evaluación de confiabilidad de parches basada en analítica avanzada:** La solución deberá proporcionar capacidades de análisis que permitan estimar la confiabilidad de los parches antes de su despliegue, considerando múltiples fuentes de información y actualizando dinámicamente dicha evaluación durante su ciclo de vida, con el fin de reducir riesgos operativos asociados a su implementación. **2. Gestión de mitigaciones compensatorias:** La solución deberá permitir, ante escenarios donde el parcheo no sea viable o represente riesgos, recomendar e implementar medidas compensatorias que reduzcan la superficie de ataque, manteniendo trazabilidad entre vulnerabilidad, mitigación y estado final. **3. Aplicación de controles mitigatorios desde el agente:** La solución deberá contar con la capacidad de recomendar y aplicar medidas mitigatorias directamente desde el mismo agente utilizado para la detección de vulnerabilidades, sin afectar la operación normal de los sistemas. **4. Gestión de riesgo sin dependencia exclusiva de parcheo:** La solución deberá permitir implementar medidas de mitigación cuando la aplicación de parches represente un riesgo operativo elevado, asegurando continuidad del servicio. **5. Trazabilidad integral de vulnerabilidades:** La solución deberá reflejar en sus reportes el estado completo de cada vulnerabilidad, incluyendo su detección, mitigación, aceptación o cierre, conforme a las políticas definidas por la Entidad. **6. Documentación detallada de mitigaciones:** Para cada vulnerabilidad tratada, la solución deberá permitir registrar el tipo de mitigación aplicada, así como la descripción de la acción ejecutada. **7. Recalculo del riesgo post-mitigación:** La solución deberá actualizar dinámicamente el nivel de riesgo de las vulnerabilidades, permitiendo diferenciar entre riesgo inicial y riesgo residual posterior a la mitigación. **8. Aislamiento controlado de dispositivos:** La solución deberá permitir el aislamiento automático de activos basado en condiciones de riesgo, así como la reversión controlada de dichas acciones una vez mitigada la condición que las originó. **9. Confirmación activa de vulnerabilidades:** La solución deberá incorporar capacidades de validación que permitan identificar vulnerabilidades efectivamente explotables, priorizando aquellas de mayor impacto. **10. Validación segura mediante técnicas controladas:** La solución deberá ejecutar procesos de validación utilizando métodos seguros que no afecten la disponibilidad ni operación de los sistemas. **Priorización basada en explotabilidad real:** Las vulnerabilidades confirmadas como explotables deberán reflejar un mayor nivel de riesgo, integrándose con los flujos de gestión para priorizar su remediación de forma inmediata.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
205	5.9.8	Debe proporcionar integración con los sistemas de administración de parches: Microsoft WSUS / SCCM, entre otros, esto como herramienta adicional para la auditoria de actualización.	el ítem 5.9.8, al permitir la auditoría, evaluación y seguimiento del estado de actualizaciones y parches de forma nativa, sin requerir integraciones adicionales con herramientas como Microsoft WSUS o SCCM.	la solución deberá permitir la auditoría, evaluación y seguimiento del estado de actualizaciones y parches, contando con capacidades nativas para la gestión de cumplimiento, tales como inventario de activos, identificación de actualizaciones faltantes, detección de vulnerabilidades y generación de evidencia auditable. Adicionalmente, deberá proporcionar integración con sistemas de administración de parches como Microsoft WSUS, SCCM, entre otros, los cuales podrán utilizarse como herramientas complementarias para la auditoría de actualizaciones y/o mecanismos de despliegue. Esta aproximación busca garantizar visibilidad, control y eficiencia en los procesos de gestión de parches, reduciendo dependencias y facilitando su aplicación en entornos diversos.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.

206	Equipo Minimo de trabajo	Un (01) Analista SOC Nivel II	Se solicita a la entidad validar y ajustar el perfil requerido para el Analista SOC Nivel III, toda vez que actualmente se enfoca principalmente en la experiencia general. Se considera necesario que dicho perfil no solo contemple experiencia, sino que además incorpore formación académica de posgrado (especialización o maestría) en Seguridad de la Información o áreas afines, en concordancia con el nivel de responsabilidad, complejidad técnica y toma de decisiones propias de este rol.	Sugerencia de ajuste (perfil propuesto) Un (01) Analista SOC Nivel III Profesional en Ingeniería de Sistemas o, Telemática o, Electrónica o, Telecomunicaciones o áreas afines, con experiencia mínima de cinco (5) años contados a partir de la expedición de la Tarjeta Profesional. Para su verificación deberá presentar, conforme a lo dispuesto en la Ley 842 de 2002 y la Ley 51 de 1986, los siguientes documentos: Cédula de ciudadanía. Tarjeta profesional. Título de posgrado en Seguridad de la Información, Ciberseguridad o áreas afines (especialización o maestría). Adicionalmente, deberá cumplir con los siguientes requisitos: Acreditar al menos tres (3) certificaciones técnicas vigentes de nivel profesional o superior, emitidas por fabricantes de soluciones de seguridad, orientadas a dominios como: gestión de eventos e información de seguridad (SIEM), orquestación y automatización de respuesta (SOAR), análisis y correlación avanzada de eventos, seguridad perimetral de nueva generación, análisis de tráfico de red (NDR) y protección de infraestructuras críticas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
207	Pagina 63	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.	Se solicita a la entidad fortalecer el perfil requerido para el rol de Gerente de Proyecto, teniendo en cuenta que las responsabilidades asociadas a la gestión de proyectos de seguridad de la información, continuidad del negocio y recuperación ante desastres demandan un alto nivel de especialización técnica, metodológica y de gobierno de TI. En este sentido, se recomienda complementar los requisitos actuales mediante la inclusión de certificaciones adicionales que respalden conocimientos en marcos de referencia, gestión de servicios, auditoría, gobierno de TI, continuidad del negocio y ciberseguridad, garantizando así la idoneidad del profesional para liderar iniciativas de alta criticidad.	Propuesta de redaccion para el perfil en asunto: **Un (01) Gerente de Proyecto** Profesional en Ingeniería de Sistemas o, Telemática o, Electrónica o, Telecomunicaciones o áreas afines. Título de posgrado en Gerencia de Proyectos y/o seguridad de la informacion. Certificaciones obligatorias vigentes: PMP (Project Management Professional). El profesional deberá contar con al menos cinco (5) certificaciones vigentes, adicionales a las obligatorias, seleccionadas de la siguiente lista: Certificación en Sistema de Gestión de Continuidad del Negocio ISO 22301:2012 o superior. Certificación vigente en ITIL Foundation v3 o superior. Certificación vigente en ITIL Managing Professional. Certificación en IPv6 básico emitida por LACNIC o entidad equivalente. Certificación de Auditor Líder ISO 27001:2022. Certificación COBIT (en cualquiera de sus niveles vigentes). Certificación CISM (Certified Information Security Manager). Certificación SFPC (Scrum Foundation Professional Certificate). Certificación CISA (Certified Information Systems Auditor). Experiencia: 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 informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
208	9.11	Incluir capacidades de análisis de percepción para evaluar cómo se percibe la marca en línea y detectar cualquier tendencia negativa o potencial crisis de reputación.	El ajuste propuesto permite alinear el requerimiento con el alcance real de las soluciones de protección de marca y riesgo digital, evitando interpretaciones hacia herramientas de analítica de marketing o reputación comercial. De esta forma, se enfoca la capacidad de análisis de percepción en la identificación de amenazas de seguridad, como campañas de suplantación, fraude o uso indebido de la marca, asegurando coherencia con los objetivos del proceso y permitiendo la participación de plataformas especializadas como Axur, sin ampliar innecesariamente el alcance funcional ni generar restricciones técnicas para los oferentes.	Incluir capacidades de análisis de percepción de marca orientadas a la identificación de riesgos reputacionales y de seguridad digital, que permitan detectar tendencias negativas, campañas de suplantación o posibles crisis asociadas al uso indebido de la marca.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
209	Equipo Mínimo de Trabajo	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.	Se propone el presente ajuste como una mejora orientada a fortalecer el perfil del Analista SOC Nivel II, incorporando mayores niveles de especialización académica y técnica, así como un esquema de certificaciones más robusto y alineado con las tecnologías actualmente involucradas en los servicios de ciberseguridad. Esta optimización permite garantizar que el recurso cuente con competencias más integrales en múltiples dominios (SIEM, SOAR, NDR, gestión de vulnerabilidades y superficie de ataque), incrementando la capacidad de análisis, respuesta y operación frente a escenarios de amenazas cada vez más complejos, sin modificar el alcance funcional del perfil requerido.	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 - Postgrado en Seguridad de la Información. -El oferente deberá contar con al menos dos (2) certificaciones vigentes emitidas directamente por el fabricante de las soluciones ofertadas, que acrediten al personal propuesto como profesional, especialista o arquitecto en seguridad de redes, o en su equivalente técnico, de acuerdo con la estructura de certificaciones vigente del fabricante. Las certificaciones deberán corresponder a las tecnologías o dominios involucrados en las soluciones presentadas, tales como SIEM o SOAR o Caza de Amenazas, NDR o Protección de Marca. - Contar con al menos cuatro (4) certificaciones vigentes emitidas por el fabricante de la solución de Gestión de la Superficie de Ataque o de Gestión de Vulnerabilidades, que acrediten al personal propuesto como profesional, especialista o ingeniero con competencias en implementación, administración y operación de dichas plataformas. Las certificaciones deberán corresponder a la línea tecnológica del fabricante, tales como las asociadas a seguridad en la nube, gestión de vulnerabilidades, seguridad OT o administración de la superficie de ataque, según aplique a la solución ofertada. - Certificaciones de experiencia mínima de tres (2) años en implementación y/o soporte y/o administración de soluciones de seguridad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
210	VACIO	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.	Se propone el presente ajuste como una mejora orientada a fortalecer el perfil del Especialista de Respuesta a Incidentes, incorporando un esquema de certificaciones más robusto que garantice competencias tanto en gestión de servicios como en sistemas de gestión de seguridad de la información, alineados con estándares internacionales. Adicionalmente, la adopción de un modelo de prestación del servicio principalmente remoto con disponibilidad para atención en sitio cuando se requiera, permite optimizar la eficiencia operativa, asegurar una respuesta oportuna ante incidentes y facilitar la asignación de recursos altamente especializados, sin afectar la calidad ni el alcance del servicio requerido por la Entidad.	Especialista de Respuesta a Incidentes (IR) Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Seguridad Informática Debera contar con al menos Dos (2) Certificaciones vigentes: • ITIL V3 o superior. • ISO IEC 27001 2013 Auditor Interno • ISO IEC 27001 2013 Auditor Interno • ISO IEC 27001 2013 Auditor Interno 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 prestará sus servicios de manera remota, contando con los conocimientos necesarios y suficientes en las plataformas, servicios y capacidades entregadas e implementadas. Deberá garantizar disponibilidad para la atención y acompañamiento frente a las remediaciones de vulnerabilidades identificadas en el monitoreo y demás actividades contempladas en el presente anexo técnico. Así mismo, deberá presentarse en sitio en la sede principal de la DIAN en Bogotá o en la Sede del Ministerio de Hacienda, cuando la Entidad lo requiera, para brindar soporte, asesoramiento o atención de situaciones que demanden presencia física.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
211	14.2	"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. NOTA 2. Se debe suministrar al menos 2 vouchers de certificación por capacitación."	Estos cursos requieren de conocimiento previo de los participantes El proceso de certificación del funcionario no esta supeditado a que apruebe el exámen de certificación.	"El CONTRATISTA deberá diseñar e implementar un programa de capacitación orientado a la apropiación de competencias en seguridad de la información, alineado al nivel de conocimiento de los participantes y a los objetivos definidos por la Entidad. Las capacitaciones deberán ser oficiales y permitir a los funcionarios adquirir los conocimientos necesarios para optar por certificaciones en estándares internacionales de seguridad informática. Se deberá contemplar la entrega de vouchers de certificación conforme a lo establecido por la Entidad; sin embargo, la obtención de la certificación estará sujeta a la aprobación del examen por parte de cada participante, siendo responsabilidad individual del mismo. El CONTRATISTA deberá garantizar el acompañamiento académico, material de estudio y preparación necesaria para la presentación de los exámenes de certificación."	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
212	19.1.5	Realizar el análisis Forense para incidentes críticos, y determinar el origen y el vector de inicio del incidente.	Por favor compartir que telemetría se tiene actualmente de este servicio, cuantos requerimeintos de estos son solicitados en el mes y en el año.	"La Entidad deberá proporcionar información de referencia sobre la operación actual relacionada con la gestión de incidentes críticos y análisis forense, incluyendo, cuando esté disponible, datos de telemetría, volumen estimado de requerimientos mensuales y anuales, con el fin de permitir una adecuada estructuración del servicio por parte de los oferentes."	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la información presentada en el proyecto es amplia y suficiente para el dimensionamiento del respectivo ofrecimiento.
213	6.4.17	Debe tener la capacidad de definir una lista de Ips legítimas de la red para que no generen alertas cuando interactúen con los señuelos.	La modificación propuesta busca garantizar la neutralidad tecnológica y evitar restricciones a un único enfoque de implementación, ya que el manejo de excepciones no siempre se realiza mediante listas explícitas de IPs en todas las soluciones del mercado. Al ampliar el requisito a mecanismos de exclusión, supresión o afinamiento de alertas, se asegura el mismo objetivo funcional evitar falsos positivos sobre activos legítimos permitiendo diferentes enfoques técnicos equivalentes, manteniendo el nivel de control requerido y reduciendo el riesgo de direccionamiento del proceso.	La solución debe permitir la exclusión, supresión o ajuste de alertas sobre activos o direcciones IP legítimas mediante mecanismos de afinamiento, listas de exclusión, perfiles de comportamiento o funcionalidades equivalentes	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
214	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.	Se evidencia que el requerimiento exige explícitamente el uso de modelos matemáticos probabilísticos lo cual limita la participación de soluciones basadas en tecnologías modernas como Machine Learning que no necesariamente exponen este enfoque de forma explícita, Hay un fabricante que explícitamente maneja este alcance DARKTRACE, agradecemos se reconsidere el requerimeinto.	"La herramienta deberá utilizar técnicas avanzadas de análisis para la detección de comportamientos anómalos en la red, tales como modelos matemáticos probabilísticos, Machine Learning (supervisado y/o no supervisado), modelos estadísticos o algoritmos de inteligencia artificial, que permitan analizar y correlacionar múltiples dimensiones de información de manera eficiente."	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
215	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).	Se observa que el requerimiento combina capacidades propias de múltiples categorías tecnológicas (NDR, CASB, CNAPP y XDR), Hay un fabricante que explícitamente maneja este alcance DARKTRACE, lo cual puede restringir la participación de soluciones especializadas en análisis de tráfico de red limitando la pluralidad de oferentes.	Agradecemos a la entidad nos informe si nuestro entendimeinto es correcto y la solución debe proporcionar visibilidad completa del tráfico de red en entornos IT, OT e IoT, y permitir integración con otras soluciones para ampliar visibilidad en entornos cloud, SaaS y arquitecturas modernas", dejando estas últimas capacidades como opcionales dado que su implementación depende de arquitecturas complementarias	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
216	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.	Se solicita ajustar el requerimiento teniendo en cuenta que la definición de un periodo fijo de retención en el appliance no se alinea con modelos actuales donde la retención depende de variables como el volumen de tráfico, la capacidad de almacenamiento y la arquitectura de la solución.	La solución deberá permitir la consulta, almacenamiento y gestión de los datos capturados, con capacidades de retención acordes a las necesidades de la entidad. Los mecanismos de retención podrán implementarse mediante almacenamiento local, escalable o integrado con plataformas complementarias, en este caso, se contempla la plataforma SIEM la cual podra realizar la ingesta y retención de logs.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
217	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.	Si nuestro entendimiento es correcto, el requerimiento establece que la solución debe realizar captura de paquetes en tiempo real, así como permitir un análisis exhaustivo de los mismos directamente en su interfaz o mediante herramientas externas como Wireshark. Al respecto, **se solicita respetuosamente a la Entidad** aclarar el alcance esperado de esta funcionalidad dentro de una **plataforma de Network Detection and Response (NDR)**, teniendo en cuenta que este tipo de soluciones, bajo las mejores prácticas del mercado, se enfocan principalmente en el análisis de metadatos de red, detección de comportamientos anómalos, análisis de tráfico mediante técnicas avanzadas (como inspección profunda, análisis de protocolos y correlación de eventos), y no necesariamente en la inspección forense completa de paquetes dentro de la misma herramienta, lo cual corresponde a soluciones especializadas. En este sentido, las plataformas NDR modernas suelen ofrecer capacidades de captura selectiva de tráfico, generación de evidencias y exportación en formatos estándar (como PCAP), permitiendo su análisis detallado en herramientas externas especializadas cuando se requiere un análisis forense profundo. Por lo anterior, se sugiere a la Entidad precisar si el alcance del requerimiento está orientado a: **Capacidades de detección, análisis y correlación de tráfico propias de una solución NDR, o Funcionalidades avanzadas de análisis forense de paquetes, propias de herramientas especializadas.** Esta aclaración permitirá a los oferentes alinear adecuadamente sus propuestas y garantizar la correspondencia entre el alcance funcional solicitado y las capacidades propias de cada tipo de solución.	"La solución deberá permitir la captura de tráfico de red y la generación de evidencias para el análisis de incidentes en tiempo real. Asimismo, deberá permitir la exportación de tráfico en formatos estándar (como PCAP o equivalentes) para su análisis en herramientas externas especializadas. Adicionalmente, la solución deberá contar con capacidades de análisis dentro de la plataforma, orientadas a la visualización de flujos, inspección de protocolos, análisis de comportamiento y correlación de eventos, propias de soluciones NDR."	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
218	7.16	La solución debe permitir la personalización y adaptación del aprendizaje automático a condiciones y características específicas de la red.	Se observa que el requerimiento implica la modificación directa de modelos de inteligencia artificial lo cual no es una práctica estándar en soluciones comerciales, En este sentido se propone la siguiente redacción aplicable: **"La solución deberá permitir el ajuste y afinamiento de los modelos de detección mediante configuración,** de tal forma que las capacidades propias de las herramienta propuesta del fabricante cumpla con el requerimiento no se cierre a una sola tecnologia del fabricante DARKTRACE.	La solución deberá permitir el ajuste y afinamiento de los modelos de detección mediante configuración, retroalimentación del usuario y establecimiento de líneas base adaptativas	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
219	7.18	El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 17727 dispositivos por (3) años.	Si nuestro entendimiento es correcto, el requerimiento establece que el servicio debe contemplar licenciamiento total de la solución para 17.727 dispositivos por un periodo de tres (3) años. Al respecto, se solicita respetuosamente a la Entidad aclarar si este esquema corresponde a un modelo de referencia para dimensionamiento del servicio o si constituye un requisito obligatorio en términos de modelo de licenciamiento. Lo anterior, teniendo en cuenta que en el mercado existen diferentes esquemas de licenciamiento (por dispositivo, por capacidad, por volumen de datos, entre otros), los cuales permiten cubrir de manera equivalente o superior el alcance funcional requerido, garantizando la protección integral del entorno durante el periodo contratado. En este sentido, la aclaración permitirá a los oferentes estructurar propuestas acordes al modelo más eficiente y adecuado, sin afectar el cumplimiento de los requerimientos técnicos ni la cobertura del servicio solicitado.	"El CONTRATISTA deberá garantizar el licenciamiento total de la solución durante el periodo contratado, asegurando la cobertura del entorno requerido por la Entidad, independientemente del modelo de licenciamiento propuesto, siempre que se garantice el cumplimiento funcional y operativo del servicio."	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 ajusta el ítem mediante adenda, quedando de la siguiente manera: 7.18 El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 25000 dispositivos por (3) años.
220	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	Si nuestro entendimiento es correcto, el requerimiento establece que, posterior al período de aprendizaje inicial, la solución debe proporcionar de manera automática un seguimiento de auditoría completo de todos los dispositivos en el entorno, incluyendo atributos como tipo de dispositivo, nombre de host, dirección MAC y registros de primera y última detección. Al respecto, se solicita respetuosamente a la Entidad aclarar el alcance esperado de estas capacidades, teniendo en cuenta que funcionalidades como la identificación detallada de dispositivos, correlación de información y trazabilidad completa pueden depender de la integración con fuentes externas, tales como servicios de identidad, directorio activo, CMDB, SIEM u otras plataformas complementarias. En este sentido, se solicita confirmar si la expectativa de la Entidad contempla que dichas capacidades sean provistas de manera nativa por la solución o mediante esquemas de integración dentro de la arquitectura del servicio.	"Después del período de aprendizaje inicial, la solución deberá proporcionar capacidades de auditoría y visibilidad de los dispositivos en la red, incluyendo información como tipo de dispositivo, nombre de host (cuando esté disponible), dirección MAC y registros de primera y última detección, ya sea de manera nativa o mediante integración con fuentes de información complementarias dentro de la arquitectura del servicio."	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
221	7.21	El servicio debe basarse en el análisis de comportamiento y correlación inteligente pudiendo detectar: - Toda conectividad inusual en la red. - Todas las actividades anómalas en la red. - Ser capaz de hacer un seguimiento detallado del dispositivo, indicando incluso su historial de dirección IP, uso del protocolo DHCP, etc. - Tener la capacidad de hacer un seguimiento detallado del usuario indicando incluso todos los nombres de host asociados a unas determinadas credenciales. - Identificar un volumen de conexiones significativamente inusual. - Identificar el nivel de rareza de un dispositivo en la red, así como el nivel de rareza de un acceso a un sitio externo	**Si nuestro entendimiento es correcto,** el requerimiento establece que el servicio debe basarse en capacidades de análisis de comportamiento y correlación inteligente para la detección de eventos de seguridad. Al respecto, se solicita respetuosamente a la **Entidad confirmar** si el alcance de este enunciado corresponde a capacidades de análisis de comportamiento a nivel de red y dispositivos, propias de soluciones NDR, y no necesariamente a funcionalidades completas de análisis de comportamiento de usuarios (UEBA), las cuales corresponden a otro tipo de soluciones especializadas. Lo anterior, teniendo en cuenta que la inclusión implícita de capacidades avanzadas de análisis de comportamiento de usuarios dentro de una solución NDR puede corresponder a arquitecturas específicas del mercado, **como las implementadas por plataformas tipo Darktrace,** lo cual podría limitar la pluralidad de oferentes al no corresponder con el alcance funcional estándar de este tipo de tecnologías. En este sentido, se entiende que la solución podría complementar su capacidad de análisis mediante la integración con fuentes de identidad u otras herramientas externas, con el fin de enriquecer el contexto de usuario cuando sea requerido, sin que esto implique la obligatoriedad de incorporar funcionalidades completas de tipo UEBA dentro de la misma plataforma. La presente aclaración busca alinear el requerimiento con el alcance funcional propio de **soluciones NDR**, promoviendo la pluralidad de oferentes y evitando interpretaciones que puedan direccionar el proceso hacia arquitecturas específicas.	"La solución deberá analizar el comportamiento a nivel de red y dispositivos, pudiendo integrar información de fuentes de identidad u otras herramientas externas para enriquecer el análisis de usuarios, sin que sea obligatoria la incorporación de funcionalidades completas de tipo UEBA dentro de la misma plataforma."	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
222	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 cada ejercicio de Treath Hunting propuesto. "	Si nuestro entendimiento es correcto, el requerimiento establece que la solución debe contar con capacidades de investigación autónoma de incidentes basadas en inteligencia artificial, incluyendo ejecución sin intervención humana, correlación avanzada y generación de reportes con contexto técnico, alineados a marcos como Cyber Kill Chain y MITRE ATT&CK. Al respecto, se solicita respetuosamente a la Entidad confirmar el alcance esperado de esta funcionalidad, teniendo en cuenta que el nivel de investigación completamente autónoma descrito corresponde, en la práctica, a capacidades propias de arquitecturas avanzadas que integran múltiples componentes (por ejemplo, XDR, SOAR o servicios SOC), y no necesariamente a una única herramienta de manera aislada. En este sentido, las soluciones modernas incorporan capacidades de análisis automatizado apoyadas en técnicas de ciencia de datos, tales como inteligencia artificial, Machine Learning y analítica avanzada, que permiten realizar procesos de correlación, priorización e investigación asistida de incidentes, generando contexto técnico y reportes ejecutivos. Sin embargo, las capacidades de investigación completamente autónoma, correlación extendida y enriquecimiento profundo del análisis suelen lograrse mediante la integración con otras herramientas o servicios especializados dentro de una arquitectura de seguridad más amplia. Por lo anterior, se sugiere a la Entidad validar si el requerimiento está orientado a capacidades de investigación automatizada soportadas en analítica avanzada y ciencia de datos, o si se espera que dichas funcionalidades sean provistas de manera integral mediante esquemas de integración dentro de la solución propuesta. La presente aclaración permitirá a los oferentes alinear sus propuestas con el alcance real esperado, promoviendo la pluralidad de oferentes y asegurando coherencia entre las capacidades solicitadas y las arquitecturas tecnológicas disponibles en el mercado.	"La solución deberá contar con capacidades de investigación automatizada de incidentes, apoyadas en técnicas de analítica avanzada, inteligencia artificial o Machine Learning, que permitan la correlación de eventos, generación de contexto técnico y elaboración de reportes con resumen ejecutivo. Las funcionalidades de investigación autónoma avanzada, correlación extendida, enriquecimiento del análisis y mapeo a marcos como Cyber Kill Chain y MITRE ATT&CK podrán ser implementadas de manera integral mediante la solución propuesta o a través de la integración con otras herramientas o servicios especializados dentro de la arquitectura de seguridad."	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.

223	7.24	Debe poder realizar investigaciones autónomas basadas en inteligencia artificial, sea por demanda a través de la interfaz gráfica y/o a través de la integración vía API, esta investigación debe incluso poder realizarse sin intervención humana y generar un reporte donde se evidencia al menos un resumen ejecutivo del incidente, las alertas que fueron investigadas que hacen parte de incidente e información técnica de cada uno de los eventos identificados, asociándolos a la fase del Cyber Kill Chain y a una posible TTP de framework ATT&CK Mitre.	Solicita el cliente considerar replantear el requerimiento dado que el nivel de investigación autónoma solicitado corresponde a capacidades propias de soluciones XDR/SOAR o servicios SOC avanzados las cuales en la práctica se implementan mediante arquitecturas integradas.	“La solución deberá contar con capacidades de investigación automatizada de incidentes, apoyadas en técnicas de ciencia de datos, tales como inteligencia artificial, Machine Learning o analítica avanzada, que permitan la correlación de eventos, generación de contexto técnico y elaboración de reportes con resumen ejecutivo del incidente. Las funcionalidades de investigación autónoma avanzada, correlación extendida, enriquecimiento del análisis y mapeo a marcos como Cyber Kill Chain y MITRE ATT&CK podrán ser implementadas de manera integral dentro de la solución o mediante integración con otras herramientas o servicios especializados dentro de la arquitectura de seguridad.”	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
224	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 "	Requerimos la validación del requerimiento teniendo en cuenta que restringir el uso de tecnologías basadas en firmas limita la participación de soluciones que emplean enfoques híbridos los cuales son considerados buenas prácticas en ciberseguridad al mejorar la precisión y reducir falsos positivos.	La solución deberá contar con un enfoque basado en análisis de comportamiento mediante inteligencia artificial, capaz de adaptarse dinámicamente al entorno. De manera opcional, podrá complementar estas capacidades con otros mecanismos de detección como inteligencia de amenazas, análisis estático o firmas con el fin de mejorar la precisión.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem 7.26 será ajustado, se ajusta mediante adenda quedando de la siguiente manera: 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.
225	7.27	"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."	Se observa que el requerimiento exige capacidades de generación de lenguaje natural propias de soluciones de inteligencia artificial generativa como la propuesta del fabricante DARKTRACE, lo cual no es estándar en plataformas NDR	La solución deberá generar reportes técnicos estructurados con cronología de eventos, contexto del incidente y detalles relevantes, dejando como opcional la generación automática de narrativa basada en procesamiento de lenguaje natural	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
226	7.30	La tecnología debe ser auto-configurable, es decir, debe tener capacidad de adaptarse de forma automática a los cambios del entorno en tiempo real.	Se observa que el requerimiento plantea que la solución sea completamente autónoma lo cual no es viable en entornos empresariales donde se requiere control y gobierno de la herramienta.	La solución deberá contar con capacidades de autoaprendizaje y adaptación dinámica con mínima intervención administrativa manteniendo la posibilidad de configuración por parte del usuario.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
227	7.32	La solución debe tener la capacidad de modelar el comportamiento normal a nivel de usuario, dispositivos y red y a partir de estos identificar de forma autónoma las anomalías que corresponden a brechas de seguridad.	Con base en el requerimiento incluye modelado completo de comportamiento de usuarios lo cual corresponde a soluciones UEBA y no exclusivamente NDR	La solución deberá modelar el comportamiento a nivel de red y dispositivos, permitiendo integración con otras soluciones para ampliar el análisis de usuarios, dejando como opcional esta última capacidad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
228	18.2	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.	Si nuestro entendimiento es correcto, el requerimiento establece que el oferente debe contar con certificación de fabricante en alguno de los tres niveles de membresía más altos para las soluciones, plataformas, servicios y dispositivos ofertados. Al respecto, se solicita respetuosamente a la Entidad considerar el alcance de este requisito, teniendo en cuenta que el proyecto integra múltiples fabricantes con diferentes modelos de canal, esquemas de certificación y estructuras de membresía, los cuales no son homogéneos entre sí. En particular, existen fabricantes que no manejan niveles escalonados de membresía (por ejemplo, Gold, Platinum, Elite), sino esquemas de habilitación basados en figuras como partner autorizado o distribuidor autorizado, obtenidos mediante procesos de selección, certificación y cumplimiento técnico. En este sentido, se solicita a la Entidad aclarar: A. ¿Cómo se evaluará el cumplimiento de este requisito para aquellos fabricantes que no cuentan con esquemas de niveles de membresía, sino con modelos de autorización directa (partner autorizado o distribuidor autorizado)? B. Si es posible considerar como válido que el oferente acredite su relación con el fabricante mediante la figura de distribuidor autorizado en Colombia, cuando aplique, garantizando el respaldo técnico y comercial correspondiente. Adicionalmente, es importante resaltar que en el documento “410 Solicitud de Ofertas de Bienes”, página 64, Sección III – Criterios de Evaluación y Calificación, numeral B (Nivel de partner más alto en las capacidades ofertadas), este aspecto ya es evaluado como criterio ponderable, otorgando puntaje diferencial a quienes acrediten niveles superiores de membresía. Por lo anterior, se sugiere revisar la condición actual como requisito habilitante, dado que podría generar una restricción innecesaria a la pluralidad de oferentes, considerando que el mismo criterio ya es objeto de evaluación dentro del proceso.	"El oferente deberá acreditar relación directa con los fabricantes de las soluciones ofertadas, mediante certificaciones vigentes que demuestren su capacidad técnica y comercial, tales como partner autorizado, distribuidor autorizado u otros esquemas equivalentes definidos por cada fabricante. En los casos en que el fabricante cuente con niveles de membresía, se podrá acreditar el nivel correspondiente. Para fabricantes que no manejan esquemas de niveles, se aceptarán certificaciones de autorización oficial. El nivel de partner o membresía más alto será considerado como criterio de evaluación ponderable, conforme a lo establecido en la Sección III del proceso.”	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
229	7.18	Se debe licenciar como mínimo para 25000 activos que incluyen (15000 pc´s, más 2727 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web). El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 17727 dispositivos por (3) años.	Se solicita a la Entidad aclarar la cantidad exacta de ítems que deben ser licenciados, dado que en el numeral 7.3 se establece un total de 25.000 unidades, mientras que en el numeral 7.8 se indica una cantidad de 17.727. Esta inconsistencia impide realizar un dimensionamiento adecuado y afecta el diseño técnico de la solución.	Se debe licenciar como mínimo para 25000 activos, actualmente se incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web). y se proyecta un crecimiento del 40% mas o menos El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 17727 dispositivos por (3) años.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la cantidad de dispositivos es 25000, el ítem en mención se modifica mediante adenda, quedando de la siguiente manera. 7.18 El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 25000 dispositivos por (3) años.
230	4.7	Contar con facilidades o herramientas analíticas para la conducción de análisis forense cuando sea reportado algún incidente.	Tanto en los ejercicios de Análisis forense como de ethical hacking entre otros, se utilizan una variedad importante de herramientas que hacen parte no necesariamente de herramientas dedicadas al cliente en particular, sino de utilitarias usadas por el ingeniero o perito forense. Muchas de estas herramientas son o se desarrollan sobre software Open Source	Se hace necesario que se considere una alcaratoria indicando que, a nivel de las herramientas que hagan parte del desarrollo de las actividades propias del contratista, como análisis forense, Ethical hacking entre otras, estas podrán ser open source. En todo caso, el contratista es responsable del buen uso de los datos e información de seguridad y reputacional de la DIAN.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
231	12.1	Presentar Plan de trabajo y cronograma de trabajo dentro de los cinco (5) días calendario siguientes a la suscripción del acta de inicio, para aprobación del supervisor y realizar los ajustes a que haya lugar.	Dado el tamaño de la solución y el servicio a proveer, 5 días se hacen muy poco tiempo para poder trabajar en conjunto con el equipo de la DIAN en la definición del plan de trabajo y un cronograma aterrizado.	Presentar Plan de trabajo y cronograma de trabajo de alto nivel dentro de los diez (10) días calendario siguientes a la suscripción del acta de inicio, para aprobación del supervisor y realizar los ajustes a que haya lugar.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
232	1.3	La Entidad requiere de servicios de monitoreo de un SOC, el cual será realizado con las plataformas, soluciones y servicios adquiridos, así también con las plataformas y servicios prestados por parte del oferente. Se aclara que toda la infraestructura tecnológica de la Entidad cuenta con soporte y garantía por parte de los fabricantes con vigencias entre 2026 y 2028.	Se evidencia que la entidad cuenta con herramientas de seguridad, por ejemplo Qradar hasta el 2027, como se desea trabajar entre las nuevas soluciones a ofertar, se debe mantener lo que esta hasta la futura vigencia de la nueva solución, o deben convivir ambas soluciones? Quien administra las soluciones actuales?	No se sugiere modificación, ya que depende de validar lo que tiene la entidad y como desea mantenerlo	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.
233	4.7		Solicitamos a la entidad confirmar que dentro del requerimiento de "Herramienta de proteccion de bases de datos" cuando se hace referencia a ""herramientas de analíticas para la conducción de análisis forense cuando sea reportado algún incidente" hace referencia a que se solicita que la solucion no sea unicamente un firewall de bases de datos, sino que incluya una herramienta dedicada de analitica de comportamiento en bases de datos proactivo que detecte anomalias de forma automatica usando algoritos de analisis de comportamiento y deteccion de anomalias mas alla de ataques.	La solución no se debe limitar a funcionalidades de firewall de bases de datos; adicionalmente, deberá incluir capacidades avanzadas de analítica de comportamiento sobre bases de datos, que permitan la detección proactiva y automática de anomalías mediante el uso de algoritmos de análisis de comportamiento, más allá de la identificación de ataques conocidos.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
234	4		Solicitamos a la entidad confirmar que la herramienta debera estar licenciada y lista para integrar a su servicio bases de datos actuales o a futuro en modelos PaaS o en nubes IaaS con el objetivo de cubrir procesos de actualizacion y adopcion de bases de datos de alta capacidad como big data.	La solución debera estar licenciada y lista para integrar a su servicio bases de datos actuales o a futuro en modelos PaaS o en nubes IaaS con el objetivo de cubrir procesos de actualizacion y adopcion de bases de datos de alta capacidad como big data	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados están claramente definidos en el anexo técnico por lo tanto no se acepta su solicitud.
235	10.9	Para los ejercicios de ethical hacking se debe tener en cuenta la conformación de equipos de blue team, red team y purple team, acorde a las siguientes caracteristicas: 1. Evaluar la postura de seguridad de la organización Simular ataques reales (Red Team) y medir la capacidad de detección y respuesta (Blue Team). Identificar vulnerabilidades técnicas, operativas y procedimentales en los sistemas y procesos del SOC. 2. Fortalecer las capacidades defensivas del SOC Permitir al Blue Team mejorar sus habilidades en detección, análisis, contención y recuperación ante incidentes. Validar la efectividad de herramientas como SIEM, SOAR, EDR, NDR, y CMDB en escenarios reales. 3. Promover la colaboración entre equipos ofensivos y defensivos El Purple Team actúa como facilitador entre Red y Blue Team, asegurando que los ejercicios generen aprendizaje mutuo. Documentar tácticas ofensivas y respuestas defensivas para mejorar playbooks, alertas y procesos. 4. Generar métricas de desempeño y mejora continua Medir tiempos del ciclo COS (identificación, confirmación, contención, erradicación y recuperación). Establecer indicadores clave (KPIs) para evaluar la madurez del SOC y definir planes de mejora. 5. Validar la integración tecnológica y operativa Comprobar que los sistemas del SOC están correctamente integrados y que los flujos de información funcionan como se espera. Evaluar la capacidad de automatización, orquestación y respuesta ante amenazas complejas. 6. Asegurar la preparación ante amenazas avanzadas Simular ataques persistentes avanzados (APT), movimientos laterales, exfiltración de datos, y otros escenarios críticos. Preparar al equipo para responder ante incidentes reales con mayor eficacia y rapidez	Es necesario aclarar estos equipos quienes los conforman, personal de la entidad, o el contratista debe proveer el personal para conformarlos en la entidad. En los ejercicios de etehical hacking no se definen por defectos ejercicios de red team o table top, por lo que es necesario aclarar cuantos ejercicios de este tipo se desean al año.	Ademas de los ejercicios de ethical hacking, se debe realizar un ejercicio de red team que pretende tener una medida de efectividad o respuesta de los equipos de seguridad de la DIAN, acorde a las siguientes caracteristicas: 1. Evaluar la postura de seguridad de la organización 2. Fortalecer las capacidades defensivas del SOC 3. Promover la colaboración entre equipos de seguridad, operaciones y CSIRT 4. Generar métricas de desempeño para mejora continua Medir tiempos del ciclo COS (identificación, confirmación, contención, erradicación y recuperación). Establecer indicadores clave (KPIs) para evaluar la madurez del SOC y definir planes de mejora. 5. Validar la integración tecnológica y operativa Evaluar la capacidad de automatización, orquestación y respuesta ante amenazas complejas. 6. Asegurar la preparación ante amenazas avanzadas Simular ataques persistentes avanzados (APT), movimientos laterales, exfiltración de datos, y otros escenarios críticos. Preparar al equipo para responder ante incidentes reales con mayor eficacia y rapidez.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos enunciados y sus actividades estarán a cargo del futuro proveedor del SOC.
236	11.12	Todo el cableado eléctrico, lógico, patchs cords, conectores, patch panels y demás elementos y accesorios necesarios para la instalación deben ser provistos para la prestación de los servicios. Se debe entender que es un contrato llave en mano, donde todos los componentes de las soluciones deben estar a cargo del contratista.	Estas son condiciones fisicas que normalmente debe proveer la entidad, en caso de que sea mandatorio, sería necesario definir las locaciones donde se intalarán las soluciones y validar mediante visitas de Site Survey las condiciones para dar respuesta, se sugiere dejar este punto de lado de la entidad, y solo solicitar que el proveedor garantice proveer sus equipos y licencias necesarios para la prestación del servicio	No se hace sugerencia de como escribirlo, ya que depende de validar las capacidades con las que cuenta la DIAN para entregar o no algunas capacidades	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados están claramente definidos en el anexo técnico por lo tanto no se acepta su solicitud.
237	12.2	Los servicios de monitoreo, correlación, administración, gestión, automatización y los demás que hagan parte del centro de operaciones de seguridad - SOC, deberán hacerse sobre toda la infraestructura tecnológica (appliance, plataformas, pc´s, endpoints, aplicaciones, bases de datos, servidores, entre otros) estipulada en el archivo de inventarios que hace parte de este anexo técnico, y hasta copar las capacidades de licenciamiento solicitadas en este proyecto, con una disponibilidad de 7x24x365,	No se evidencia en el inventario detalle de PCs o Endpoints, solo se ve que se habla del Antivirus, es necesario que se aclare, si se requiere un monitoreo sopre los PCs o Endpoint, si este se puede hacer desde las consolas de EPP o EDR o si necesariamente se requiere propiamente en el dispositivo y sea necesario un agente adicional en ellos	Los servicios de monitoreo, correlación, administración, gestión, automatización y los demás que hagan parte del centro de operaciones de seguridad - SOC, deberán hacerse sobre toda la infraestructura tecnológica (appliance, plataformas, aplicaciones, bases de datos, servidores, entre otros) estipulada en el archivo de inventarios que hace parte de este anexo técnico, y hasta copar las capacidades de licenciamiento solicitadas en este proyecto, con una disponibilidad de 7x24x365,	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario de la infraestructura tecnológico de la Entidad se encuentra detallada en el documento 410-Solicitud-de-Oferta-VSD-SdO-SOC.
238	12.24	Proporcionar durante el período de la operación de los servicios un esquema de escalamiento interno a la herramienta.	A que herramienta se refiere, por favor aclarar y detallar el alcance		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem 12.24 se ajusta en el anexo técnico, cambio que se hará mediante adenda, quedando de la siguiente manera: 12.24 Proporcionar durante el período de la operación de los servicios un esquema de escalamiento para los requerimientos que se lleguen a presentar.
239	12.46	El SOC debe estar protegido al menos con tres anillos de seguridad física. Indicar cuantos anillos de seguridad utilizan para la protección física, describa cada uno de ellos, y quien provee el servicio de protección (Propio, condominio, administración, etc).		El SOC debe contar con sistemas de seguridad física como biometricos, cctv, apertura remota y controlada de puertas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
240	12.57	Las evidencias que sean recopiladas por el servicio de monitoreo SOC son propiedad de la Entidad y podrán ser solicitadas en cualquier momento para atención de requerimientos legales.	La entidad debe disponer de los repositorios para el almacenamiento de su información y los respectivos procesos de custodia	Las evidencias que sean recopiladas por el servicio de monitoreo SOC son propiedad de la Entidad, La entidad dispondrá de repositorios para el almacenamiento y custodia de esta información.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
241	12.71	La Entidad podrá solicitar los informes que considere pertinentes, en la medida en que se vayan integrando nuevas herramientas.	No es claro si se refiere solo a herramientas contempladas en este proyecto o hace referencia a futuras adquicisones	La Entidad podrá solicitar los informes que considere pertinentes, en la medida en que se operen y entiendan las herramientas provistas e implementadas por el oferente del presente proceso	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el requerimiento refiere únicamente a los servicios o capacidades entregadas por el futuro proveedor para el SOC.
242	13.4	Se deberá atender y resolver cualquier problema técnico de las capacidades, soluciones y servicios, en un esquema de atención 7x24X365 (telefónico, e-mail, acceso remoto o presencial en caso de que la DIAN así lo requiera, este soporte deberá ser suministrado por personal especializado en las plataformas entregadas. La atención se debe prestar dentro de las dos (2) horas siguientes al reporte de incidente, la solución en un tiempo máximo de ocho (8) horas calendario. En el caso específico que se requiera de soporte de tercer nivel (fabricante), toda estas labores y demás labores propias del soporte y garantía serán gestionadas por el contratista, quien deberá escalar, gestionar y realizar todos los procedimientos que el fabricante solicite, en cuyo caso se establece un tiempo máximo de dos (2) días calendario para la solución definitiva.	No es posible comprometer soluciones, si tiempos de atención y respuesta, se debe definir un ANS con distintos niveles de atención o prioridad	Se deberá atender cualquier problema técnico de las capacidades, soluciones y servicios, en un esquema de atención 7x24X365 (telefónico, e-mail, acceso remoto o presencial en caso de que la DIAN así lo requiera, este soporte deberá ser suministrado por personal especializado en las plataformas entregadas. La atención se debe prestar bajo un esquema definido a continuación: Prioridad de la solicitud Impacto Urgencia Bajo Afecta a un solo usuario o tiene un impacto mínimo en un servicio no critico Puede programarse para ser resuelto en un plazo más amplio sin un impacto significativo. Medio Afecta a un grupo de usuarios o a un servicio importante, pero se trabaja bajo un proceso de contingencia viable que disminuye la afectación Debe resolverse en un plazo razonable para evitar un impacto moderado. Alto Afecta a un departamento o a un servicio crítico, causando una interrupción significativa. Requiere atención rápida para evitar una interrupción mayor o una escalada del problema. Critico Afecta a toda la organización o a un servicio esencial que detiene completamente las operaciones del negocio. Demanda atención inmediata para prevenir pérdidas críticas o restaurar servicios esenciales lo antes posible. Acuerdos de Nivel de Servicio Tiempo de Respuesta Tiempo de Resolución > 4 horas ≤ 3 días ≤ 3 horas ≤ 2 días ≤ 2 horas ≤ 8 horas ≤ 1 hora ≤ 4 horas En los casos que se requiera escalamientos al fabricante, los tiempos se modificarán y sumaran los aplicados por el soporte del fabricante	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
243	13.7	Realizar visitas de seguimiento técnico para mantenimiento preventivo a la plataformas, soluciones y servicios ofertados e implementados, de manera cuatrimestral, durante el tiempo de garantía, soporte y la duración del presente proceso contractual, para lo cual se deberá realizar y documentar entre otras, las siguientes actividades como parte del mantenimiento, previa coordinación con el supervisor del contrato en desarrollo: Revisar, diagnosticar y afinar todas las plataformas y dispositivos entregados, así como el desempeño de sus capacidades.	Sugerencia, dejarlo semestral para permitir un tiempo de estabilización y operación	Realizar visitas de seguimiento técnico para mantenimiento preventivo a la plataformas, soluciones y servicios ofertados e implementados, de manera semestral, durante el tiempo de garantía, soporte y la duración del presente proceso contractual, para lo cual se deberá realizar y documentar entre otras, las siguientes actividades como parte del mantenimiento, previa coordinación con el supervisor del contrato en desarrollo: Revisar, diagnosticar y afinar todas las plataformas y dispositivos entregados, así como el desempeño de sus capacidades.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
244	14.1	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.	Estos cursos requieren de conocimiento previo de los participantes El proceso de certificación del funcionario no esta supeditado a que apruebe el exámen de certificación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
245	6.5.10	La solución debe soportar el marco de referencia MITRE para Sistemas de Control Industrial (MITRE ICS).	La modificación propuesta busca asegurar la neutralidad tecnológica y una mayor participación de oferentes, evitando limitar el requisito a la adopción explícita de un único marco específico como MITRE ICS. En su lugar, se amplía a marcos reconocidos como MITRE ATT&CK y/o enfoques equivalentes, garantizando que la solución mantenga capacidades sólidas para la identificación, clasificación y análisis de tácticas y técnicas de ataque en entornos IT y OT, sin afectar el nivel técnico exigido y reduciendo el riesgo de direccionamiento del proceso.	La solución debe alinearse o ser compatible con marcos de referencia reconocidos para la detección de amenazas en entornos IT y OT, tales como MITRE ATT&CK y/o MITRE para sistemas de control industrial (ICS), o proporcionar capacidades equivalentes para la identificación, clasificación y análisis de tácticas y técnicas de ataque.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
246	18.2	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.	El requerimiento exige certificación del fabricante indicando pertenencia a alguno de los tres niveles más altos de membresía. Sin embargo, considerando que el proyecto integra múltiples fabricantes con distintos modelos de canal, esta condición puede resultar restrictiva para aquellos casos en los que no existen niveles escalonados o donde la figura aplicable es la de distribuidor autorizado en Colombia, aun contando con capacidades técnicas y de implementación. Adicionalmente, en el documento 410 – Sección III. Criterios de Evaluación y Calificación (pág. 57), ya se contempla como criterio ponderable la acreditación del nivel de partner más alto por ítem, por lo que mantener esta condición como requisito puede limitar la pluralidad de oferentes.	"El oferente deberá acreditar relación con el fabricante mediante certificación vigente que demuestre su capacidad técnica y de implementación, tales como partner autorizado, distribuidor autorizado en Colombia u otros esquemas equivalentes definidos por el fabricante. Cuando existan niveles de membresía, estos serán considerados dentro de los criterios de evaluación ponderables establecidos por la Entidad.”	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
247	6.4.1	Debe permitir la creación de trampas de alta interacción, con capacidad de clonar activos existentes.	Al ser un requerimiento específico de deception limita totalmente la participación de tecnologías de inteligencia de amenazas. **Creación de trampas (traps)** se encuetra enfocado exclusivamente en tecnología FortiDeceptor	El anexo técnico prioriza capacidades específicas de deception, como la creación de múltiples capas de señuelos, emulación de servicios y captura de interacción del atacante. Esto orienta la evaluación hacia soluciones diseñadas bajo un modelo ‘assume breach’, como FortiDeceptor, y puede limitar la participación de tecnologías igualmente válidas que abordan el problema desde la prevención y la inteligencia de amenazas. **Sugerencia:** Aceptar incluir soluciones de inteligencia de amenazas, que garanticen la reducción de la superficie de ataque, limitando C2 y aplicando IOC en tiempo real.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible su ajuste de acuerdo a su solicitud.
248	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.	Solcitamos incluir como parte del requerimiento una modificación.	La solución debe soportar escalabilidad en entornos segmentados (VLANs), garantizando cobertura y visibilidad de amenazas acorde a la infraestructura de la entidad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
249	6.4.3	El licenciamiento de la solución debe ser como mínimo ciento veinte (120) vlans.	Solcitamos incluir como parte del requerimiento una modificación.	El modelo de licenciamiento debe cubrir la totalidad de la infraestructura monitoreada, independientemente de su segmentación	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.

250	6.4.4	Debe permitir la creación de trampas activas con un flujo de tráfico de red falso entre las trampas implementadas para confundir y desviar a los atacantes que monitorean el tráfico, asegurando que interactúen con las trampas implementadas.	Al ser un requerimiento específico de deception limita totalmente la participación de tecnologías de inteligencia de amenazas. **Creación de trampas (traps)** se encuetra enfocado exclusivamente en tecnología FortiDeceptor	El anexo técnico prioriza capacidades específicas de deception, como la creación de múltiples capas de señuelos, emulación de servicios y captura de interacción del atacante. Esto orienta la evaluación hacia soluciones diseñadas bajo un modelo 'assume breach', como FortiDeceptor, y puede limitar la participación de tecnologías igualmente válidas que abordan el problema desde la prevención y la inteligencia de amenazas. **Sugerencia:** Aceptar incluir soluciones de inteligencia de amenazas, que garanticen la reducción de la superficie de ataque, limitando C2 y aplicando IOC en tiempo real. La solución debe permitir identificar y/o interrumpir la actividad maliciosa en tiempo real. La solución debe permitir la identificación proactiva de amenazas mediante técnicas de detección, engaño o prevención	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
251	6.4.10	Debe estar en capacidad de hacer detección de reconocimientos de red que usen ping (ICMP)	Se plantea desde una perspectiva de interacción con señuelos, esto denota un enfoque específico de **Deception** en lugar de enfocarse en prevención del ataque.	La solución debe permitir la identificación proactiva de amenazas mediante técnicas de detección, engaño o prevención	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
252	6.4.11	Debe contar con señuelos que simulen conectores a base de datos que usen ODBC	Esta se considera una función nativa de **FortiDeceptor**, lo que claramente demuestra un sesgo técnico que limita la participación de mas oferentes. Simulación de servicios (SMB, RDP, DB, etc.) Engagement del atacante	La solución debe permitir identificar accesos no autorizados a servicios mediante mecanismos de detección, simulación o análisis de comportamiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
253	6.4.12	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.	Solcitamos incluir como parte del requerimiento una modificación.	La solución debe integrarse con el NGFW y proporcionar visibilidad centralizada de eventos, amenazas y activos	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
254	6.4.14	Debe permitir el despliegue de señuelos en activos reales para que dirijan al atacante a la solución de Decepción de amenazas.	Estas es arquitectura de Deception completa, limitando y sesgando tecnicamente a Fortideceptor limitando la participación a soluciones proactivas de inteligencia de amenazas en tiempo real. En qué se justifica: - Despliegue de decoys en activos - Emulación de activos IT - Emulación de servicios/protocolos - Lista de activos críticos protegidos mediante señuelos - Mapa visual de decoys Esto es considerado una arquitectura completa de **Deceptor** basado en el alcance y ficha técnica de Fortideceptro	La solución debe permitir proteger activos mediante mecanismos activos o pasivos de detección y/o prevención.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
255	6.4.15	Debe tener la capacidad de emular activos del tipo Gateway de VPN SSL.	La emulación de activos IT y host reales es una característica CORE de Deception, limitando la capacidad de participación de oferentes con capacidades frente a inteligencia de amenazas.	La solución debe permitir visibilidad sobre activos y servicios, ya sea mediante emulación, monitoreo o inteligencia de amenazas	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
256	6.4.16	Debe tener la capacidad de emular activos con servicios SAMBA, SMB, SSH y HTTP/S habilitados.	La emulación de servicios y protocolos es una característica enfocada al core de Deception muy específico de plataformas como FortiDeceptor.	La solución debe permitir visibilidad sobre activos y servicios, ya sea mediante emulación, monitoreo o inteligencia de amenazas	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
257	6.4.17	Debe tener la capacidad de definir una lista de Ips legítimas de la red para que no generen alertas cuando interactúen con los señuelos.	Este es un requerimiento de protección basado en engaño, lo que no se enmarca en prevencion ni inteligencia de amenazas.	La solución debe permitir definir y proteger activos críticos mediante controles de seguridad avanzados.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
258	6.4.18	Debe permitir visualizar en un mapa los señuelos desplegados o visualizar con características similares o superiores en las tecnologías ofrecidas.	**Visualización centrada en señuelos** **UI típica de deception**	La solución debe ofrecer visualización centralizada de eventos de seguridad, activos y amenazas	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos solicitados en este proyecto obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
259	6.5.2	Debe tener al menos 4 capas de decepción (o tecnologia similar o superior), con la capacidad de crear como minimo 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).	Este es un requerimiento **específico** enfocado a FortiDeceptor alineado con la arquitectura exacta que describe el fabricante: - Decoys - Lures - Tokens - Network Deception	La solución debe implementar múltiples capas de protección (detección, prevención, inteligencia, respuesta) o tecnologías equivalentes o superiores	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento no está orientado a una marca o fabricante específico, sino a capacidades funcionales mínimas de tecnología de decepción, o tecnología similar o superior, necesarias para fortalecer la detección temprana de actividades maliciosas en la infraestructura tecnológica de la Entidad. La sugerencia propuesta modifica el alcance técnico requerido, al sustituir capacidades específicas de decepción por controles generales de protección. Por lo anterior, no se acepta la solicitud.
260	6.5.6	Los tokens falsos creados no deben ser visibles para los usuarios de la entidad, únicamente para el atacante.	Los honeytokens son requerimientos específicos de arquitecturas de Deception y excluyen soluciones de respuesta a incidentes proactivas y no reactivas.	La solución debe detectar accesos indebidos mediante técnicas avanzadas como análisis de comportamiento, inteligencia o mecanismos equivalentes.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento corresponde a una capacidad funcional asociada a la detección de accesos indebidos mediante recursos señuelo o mecanismos equivalentes, sin que ello limite la participación a una marca o fabricante específico. La sugerencia propuesta modifica el alcance técnico requerido, al reemplazar una funcionalidad específica de detección basada en tokens falsos por capacidades generales de análisis de comportamiento o inteligencia. Por lo anterior, no se acepta la solicitud.
261	6.5.7	Debe tener la capacidad de emular activos con servicios SAMBA, SMB, SSH y HTTP/S habilitados.	Solcitamos incluir como parte del requerimiento una modificación.	La solución debe analizar la red mediante técnicas activas o pasivas para identificar riesgos y amenazas	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos, toda vez que responde a las necesidades técnicas identificadas por la Entidad para la prestación del servicio. El oferente podrá presentar tecnologías equivalentes o superiores, siempre que cumplan con las capacidades solicitadas en los documentos del proceso. Por lo anterior, no se acepta la solicitud.
262	6.5.8	La solución debe poder crear señuelos para ambientes OT (Tecnología Operacional) y para redes SCADA (PLC, HMI, Sensores IoT, entre otros).	Al solicitarse Decoys para IT y OT (SCADA, PLC, IoT) se esta limitando demasiado la participación de oferentes.	La solución debe cubrir entornos IT y OT mediante capacidades de detección, monitoreo o protección.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos, toda vez que responde a las necesidades técnicas identificadas por la Entidad para la prestación del servicio. El oferente podrá presentar tecnologías equivalentes o superiores, siempre que cumplan con las capacidades solicitadas en los documentos del proceso. Por lo anterior, no se acepta la solicitud.
263	6.5.9	La solución, al desplegar un señuelo, debe permitir una interacción completa sobre el mismo. Esto con el fin de evitar que el atacante detecte que se trata de un señuelo.	Las características de señuelos por entorno, son una caracterísitica específica de FortiDeceptor.	La solución debe permitir adaptación a las características del entorno.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos, en atención a las necesidades técnicas definidas para la operación del servicio requerido. El oferente podrá presentar tecnologías equivalentes o superiores, siempre que permitan cumplir con las capacidades funcionales solicitadas en los documentos del proceso. Por lo anterior, no se acepta la solicitud.
264	6.5.11	La solución debe ofrecer diferentes tipos de señuelos para desplegar y adicionalmente, debe permitir la creación de señuelos personalizados.	Las características de señuelos por entorno, son una caracterísitica específica de FortiDeceptor. **Este es un requerimiento altamente específico.**	La solución debe cubrir múltiples vectores de ataque (credenciales, red, aplicaciones, endpoints)	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos, toda vez que la disponibilidad de diferentes tipos de señuelos y la posibilidad de personalización hacen parte de las capacidades técnicas requeridas por la Entidad. El oferente podrá presentar tecnologías equivalentes o superiores que acrediten el cumplimiento de lo solicitado. Por lo anterior, no se acepta la solicitud.
265	6.5.15	Debe estar en la capacidad de crear señuelos falsos de los tipos presentes en la DIAN:	Honey Credential se considera un requerimiento altamente específico enfocado exclusivamente en soluciones como FortiDeceptor.	La solución debe detectar uso indebido de credenciales mediante técnicas avanzadas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos, considerando que la capacidad solicitada hace parte de las funcionalidades definidas por la Entidad para la detección de uso indebido de credenciales. El oferente podrá presentar tecnologías equivalentes o superiores, siempre que cumplan con lo solicitado en los documentos del proceso. Por lo anterior, no se acepta la solicitud.
266	2.6	Debe ofrecer una representación visual tipo mapa que muestre en tiempo real los ataques o señuelos que han sido tocados por el atacante.	Solcitamos incluir como parte del requerimiento una modificación.	La solución debe ofrecer visualización en tiempo real de ataques y eventos de seguridad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos, toda vez que la representación visual solicitada hace parte de las capacidades requeridas para facilitar el monitoreo, análisis y seguimiento de los eventos asociados a la solución. Por lo anterior, no se acepta la solicitud.
267	2.6	Debe realizar analítica en tiempo real.	Solcitamos incluir como parte del requerimiento una modificación.	Debe realizar analítica en tiempo real, Detección proactiva, incluso sobre tráfico cifrado	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos en los documentos del proceso. La inclusión de capacidades adicionales podrá ser considerada por el oferente dentro de su propuesta, siempre que no sustituya ni limite el cumplimiento de las condiciones mínimas exigidas por la Entidad. Por lo anterior, no se acepta la solicitud.
268	2.25	SIEM debe realizar analítica en tiempo real	Detección proactiva, incluso sobre tráfico cifrado	SIEM debe realizar analítica en tiempo real aplicando millones de indicadores en tiempo real	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos en los documentos del proceso. Las capacidades adicionales que el oferente considere pertinentes podrán ser incluidas en su propuesta, siempre que no modifiquen el alcance ni las condiciones mínimas requeridas por la Entidad. Por lo anterior, no se acepta la solicitud.
269	2.27	Búsqueda, patrones complejos, informes personalizables	Reducción de falsos positivos y evidencia auditable	Búsqueda, patrones complejos, informes personalizables, generando reportes verificables, trazabilidad y listas dinámicas	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos. Los informes, trazabilidad y evidencias que se generen deberán atender las condiciones definidas en los documentos del proceso y las necesidades operativas de la Entidad. Por lo anterior, no se acepta la solicitud.
270	2.29	Framework de notificación, integración con ticketing	Escalamiento ágil y reducción de carga operativa	Framework de notificación, integración con ticketing, integración vía API con SOAR/SIEM y debe generar reportes automáticos	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos, incluyendo las capacidades de notificación e integración previstas en los documentos del proceso. Las integraciones adicionales podrán ser propuestas por el oferente, siempre que no sustituyan las condiciones mínimas solicitadas. Por lo anterior, no se acepta la solicitud.
271	4.3	API para integrar feeds de amenazas	Inteligencia viva, actualizada continuamente	API para integrar feeds de amenazas com más de 200 fuentes globales (STIX/TAXII, OSINT, CTI feeds)	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos. Las fuentes, mecanismos e integraciones de inteligencia de amenazas deberán cumplir con lo solicitado en los documentos del proceso, sin que resulte procedente incorporar cantidades o condiciones adicionales no previstas inicialmente. Por lo anterior, no se acepta la solicitud.
272	6.3	Autoaprendizaje con mínima intervención	Construcción de listas blancas sin riesgo operativo	Autoaprendizaje con mínima intervención en modo pasivo (monitor-only)	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos en los documentos del proceso. El oferente podrá incluir funcionalidades adicionales o modos de operación que fortalezcan la prestación del servicio, siempre que se cumpla con las condiciones mínimas requeridas por la Entidad. Por lo anterior, no se acepta la solicitud.
273	7.4	Herramienta para interceptar ataques ocultos	Threat hunting automatizado y reducción de ventana de exposición	Herramienta para interceptar ataques ocultos correlacionando indicadores globales y anomalías	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos, de acuerdo con las capacidades técnicas definidas para la identificación e interceptación de ataques ocultos. Las capacidades adicionales de correlación o análisis podrán ser presentadas por el oferente como parte de su solución, siempre que no modifiquen el alcance mínimo requerido. Por lo anterior, no se acepta la solicitud.
274	12.31	Monitoreo de red con inteligencia artificial	IA aplicada a threat intelligence, detección temprana	Monitoreo de red con inteligencia artificial con un motor de correlación que incluya millones de indicadores	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos. La solución deberá cumplir con las capacidades de monitoreo de red con inteligencia artificial solicitadas en los documentos del proceso, sin que resulte procedente incorporar condiciones adicionales asociadas a cantidades mínimas de indicadores. Por lo anterior, no se acepta la solicitud.
275	12.37	Informes extraordinarios SOC 7x24	Boletines con contexto global y trazabilidad	Informes extraordinarios SOC 7x24 con actualización de indicadores en tiempo real	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos. Los informes extraordinarios deberán generarse conforme a las condiciones, oportunidad y alcance definidos en los documentos del proceso. Las capacidades adicionales podrán ser ofrecidas sin modificar los mínimos exigidos. Por lo anterior, no se acepta la solicitud.
276	19.1	SOC debe incluir inteligencia mundial	Cobertura global y actualización continua	SOC debe incluir inteligencia mundial integrando un mínimo de 200 feeds globales	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos. La inteligencia mundial requerida deberá atender las condiciones previstas en los documentos del proceso, sin que resulte procedente incorporar cantidades mínimas específicas de fuentes globales no definidas inicialmente. Por lo anterior, no se acepta la solicitud.
277	19.2	Evaluación de eventos, análisis forense	Proactividad superior a IDS/IPS tradicionales	Evaluación de eventos, análisis forense incluyendo Inspección SSL/TLS y evidencia verificable	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos. Las capacidades de evaluación de eventos y análisis forense deberán cumplirse conforme a lo definido en los documentos del proceso. Las funcionalidades adicionales podrán ser incluidas por el oferente, siempre que no sustituyan ni condicionen los mínimos requeridos. Por lo anterior, no se acepta la solicitud.
278	19.4	Canalizar alertas, registrar incidentes en SOAR	Optimiza tiempos de respuesta y priorización	Canalizar alertas, registrar incidentes en SOAR realizando filtrado previo con el fin de reducir alertas de manera medible y cuantificable.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos, incluyendo la canalización de alertas y el registro de incidentes en la herramienta correspondiente. Las capacidades adicionales de filtrado, priorización o reducción de alertas podrán ser propuestas por el oferente, siempre que no modifiquen el alcance mínimo requerido. Por lo anterior, no se acepta la solicitud.
279	Financiera	Interoperabilidad con CSIRT, COLCERT, Policía, Fiscalía	Cumplimiento BID y estándares internacionales	Interoperabilidad con CSIRT, COLCERT, Policía, Fiscalía con evidencia auditable compartible con entes externos	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos. La interoperabilidad y articulación con las entidades competentes deberá desarrollarse conforme al alcance, canales y condiciones definidos por la Entidad en los documentos del proceso y en el marco normativo aplicable. Por lo anterior, no se acepta la solicitud.
280	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.	Al ser un requerimiento para un proveedor Intrernacional, por favor eliminar el requerimiento de una facilidad fisica en el pais.	Como proveedor Internacional, contamos con infraestructura fisica desplegada en varios paises y con una capacidad de atencion global 7x24	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos, toda vez que responde a las necesidades de continuidad operativa, seguridad física y lógica, coordinación del servicio y atención oportuna requeridas por la Entidad. Se precisa que el requerimiento está asociado a la operación del SOC en la ciudad de Bogotá, sin que ello implique que el centro de datos que soporte dicha operación deba encontrarse en la misma ubicación. Por lo anterior, no se acepta la solicitud.
281	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, licencias, suscripciones, 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 XXX. 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 XXX 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.	Se solicita a la entidad permitir que el SOC no esté restringido a una ubicación geográfica específica, aceptando un modelo distribuido con redundancia geográfica, siempre que se garantice el cumplimiento de los SLA, la disponibilidad, la continuidad del servicio y la adopción de estándares como ISO 27001 e ISO 22301. Este esquema proporciona mayor resiliencia operativa, elimina puntos únicos de falla y mantiene capacidades completas de monitoreo, gestión y respuesta a incidentes, pudiendo complementarse con presencia local cuando sea requerido.	Se debe contar con un Centro de Operaciones de Seguridad (SOC), el cual podrá estar ubicado en territorio nacional o internacional, siempre que garantice las condiciones adecuadas para la continuidad operativa, la seguridad física y lógica, y el cumplimiento de las mejores prácticas del sector. El SOC deberá disponer de toda la infraestructura necesaria para la instalación y operación de los productos, capacidades, plataformas, licencias, suscripciones, soluciones y servicios requeridos para dar cumplimiento a lo solicitado en el anexo técnico, permitiendo la ejecución integral de las actividades encomendadas por la XXX. Se aceptarán esquemas de operación distribuidos, incluyendo modelos de SOC principal y sitios de respaldo (redundancia geográfica), siempre que se garantice la alta disponibilidad del servicio, la continuidad del negocio y la ausencia de puntos únicos de falla. El CONTRATISTA será responsable de la gestión integral del servicio, incluyendo monitoreo, administración, optimización, actualización, acompañamiento, soporte y garantía, cubriendo toda la infraestructura tecnológica de la Entidad. Para tal efecto, deberá contar con la capacidad de detectar, analizar, escalar, informar, acompañar y soportar la resolución de incidentes durante la vigencia del contrato. Adicionalmente, el SOC deberá contar con certificaciones vigentes en estándares internacionales de seguridad de la información y continuidad del negocio, tales como ISO 27001 e ISO 22301, o equivalentes. En caso de requerirse interacción en sitio, el CONTRATISTA deberá garantizar disponibilidad de personal o capacidades locales en la ciudad de Bogotá, sin que esto implique la obligatoriedad de ubicar el SOC principal en dicha ciudad. Los activos y demás características se encuentran detallados en el apartado de inventarios, y las especificaciones de cada una de las soluciones, plataformas, capacidades, servicios, soporte y garantía corresponden a lo establecido en el presente anexo técnico, siendo de obligatorio cumplimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos, toda vez que responde a las necesidades de continuidad operativa, seguridad física y lógica, coordinación del servicio y atención oportuna requeridas por la Entidad. Se precisa que el requerimiento está asociado a la operación del SOC en la ciudad de Bogotá, sin que ello implique que el centro de datos que soporte dicha operación deba encontrarse necesariamente en la misma ubicación. Por lo anterior, no se acepta la solicitud.
282	2.22	Supervisión de rendimiento, como minimo 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.	Se solicita a la entidad permitir que el cumplimiento del requisito de informes de cumplimiento normativo no se limite exclusivamente a la disponibilidad de todos los marcos regulatorios listados en modalidad “out-of-the-box”, sino que también se acepten soluciones que: Dispongan de informes predefinidos para estándares ampliamente adoptados (ej. PCI-DSS, HIPAA, CIS Controls), y Cuenten con capacidades avanzadas de parametrización, personalización y automatización de reportes, que permitan construir y adaptar informes para otros marcos regulatorios (ISO, SOX, NERC, FISMA, GLBA, entre otros), a partir de la telemetría recolectada por la plataforma. Lo anterior, considerando que los modelos modernos de XDR/SIEM priorizan la flexibilidad y adaptabilidad normativa, permitiendo cubrir múltiples estándares sin depender exclusivamente de plantillas rígidas preconfiguradas. Esto debido a que la exigencia de funcionalidades consolidadas en una única plataforma podría corresponder a arquitecturas propias de fabricantes específicos, limitando la pluralidad de oferentes que implementan enfoques modulares ampliamente adoptados en entornos empresariales.	El sistema deberá contar con informes de cumplimiento normativo, los cuales podrán ser predefinidos (out-of-the-box) y/o configurables, que soporten necesidades de auditoría y cumplimiento para marcos como PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13 y SANS Critical Controls. Se aceptarán soluciones que dispongan de un conjunto base de reportes preconfigurados y que, adicionalmente, permitan la parametrización, personalización y automatización de informes, de tal forma que se puedan adaptar a diferentes estándares y marcos regulatorios a partir de la información recolectada por la plataforma.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el texto señalado corresponde a capacidades de supervisión de rendimiento y no a informes de cumplimiento normativo. En todo caso, los requerimientos asociados a informes, auditoría y cumplimiento deberán atenderse conforme a lo establecido en los documentos del proceso. Por lo anterior, no se acepta la solicitud.
283	2.22	Supervisión de rendimiento, como minimo 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.	Se solicita a la entidad aclarar que el requisito de supervisión de rendimiento podrá cumplirse mediante soluciones que integren capacidades nativas y/o integraciones con herramientas especializadas, siempre que en conjunto permitan: Monitoreo de métricas de sistema (CPU, memoria, disco, red). Recolección de información mediante protocolos estándar (SNMP, WMI, PowerShell, APIs). Visibilidad sobre entornos virtualizados (VMware, Hyper-V) a nivel de host y máquinas virtuales. Integración con servicios críticos como Active Directory y aplicaciones empresariales. Extensibilidad mediante métricas personalizadas o parsers configurables. Se entiende que, en arquitecturas modernas, el monitoreo de rendimiento profundo de aplicaciones (APM) puede realizarse mediante integraciones complementarias, sin que esto afecte la capacidad integral de supervisión requerida para el SOC. La exigencia actual podría estar alineada a soluciones específicas del mercado que integran estas capacidades de forma monolítica, restringiendo la participación de oferentes que utilizan arquitecturas desacopladas pero igualmente robustas.	El sistema deberá contar con informes de cumplimiento normativo, los cuales podrán ser predefinidos (out-of-the-box) y/o configurables, que soporten necesidades de auditoría y cumplimiento para marcos como PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13 y SANS Critical Controls. Se aceptarán soluciones que dispongan de un conjunto base de reportes preconfigurados y que, adicionalmente, permitan la parametrización, personalización y automatización de informes, de tal forma que se puedan adaptar a diferentes estándares y marcos regulatorios a partir de la información recolectada por la plataforma.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento podrá ser cumplido mediante capacidades nativas y/o integraciones provistas, implementadas, operadas y soportadas por el contratista, siempre que en conjunto se cumplan las funcionalidades mínimas solicitadas en los documentos del proceso. Lo anterior no modifica el alcance ni las obligaciones previstas para la prestación integral del servicio.
284	2.23	Supervisión del cambio de configuraciones en tiempo real, como minimo debe incluir los siguientes elementos: - Recopilar archivos de configuración de red, almacenados en un repositorio versionado. - Recopilar las versiones de software instaladas, almacenadas en un repositorio versionado. - Detección automatizada de cambios en la configuración de la red y el software instalado. - Detección automatizada de cambios de archivos y carpetas - Windows y Linux - quién y qué. - Detección automatizada de cambios desde un archivo de configuración. - Posibilidad de detección automatizada de cambios en el registro de Windows a través de agente.	Se solicita a la entidad permitir que el requisito de supervisión de cambios de configuración sea cumplido mediante plataformas que: Realicen detección, correlación y trazabilidad de cambios en tiempo real (archivos, configuraciones, registro, software instalado), incluyendo información de quién, qué y cuándo. Mantengan históricos de eventos y capacidades de auditoría sobre los cambios detectados. Sin que sea obligatorio que la solución funcione como un sistema de Network Configuration Management (NCM) con repositorio versionado de archivos de configuración. En caso de requerirse capacidades de versionamiento de configuraciones (backups y control de versiones), estas podrán ser cubiertas mediante integración con herramientas especializadas, manteniendo el enfoque del SOC en detección, monitoreo y respuesta a incidentes. Esto considerando que la definición actual de tecnologías específicas puede evidenciar un sesgo hacia determinados fabricantes, en lugar de centrarse en los principios de integridad, trazabilidad y disponibilidad de la información.	a solución deberá permitir la supervisión de rendimiento de la infraestructura tecnológica, incluyendo métricas de sistema, estado de servicios y aplicaciones, y visibilidad sobre entornos virtualizados. Se aceptarán soluciones que integren capacidades nativas y/o integraciones con herramientas externas, siempre que en conjunto permitan: Monitoreo de métricas de sistema (CPU, memoria, almacenamiento, red). Recolección de información mediante protocolos estándar (SNMP, WMI, PowerShell, APIs u otros). Supervisión de entornos virtualizados (VMware, Hyper-V) a nivel de host y máquinas virtuales. Integración con servicios como Active Directory y aplicaciones empresariales. Incorporación de métricas personalizadas. Las capacidades de monitoreo avanzado de aplicaciones (APM) podrán ser cubiertas mediante integración con herramientas especializadas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento se mantiene en los términos establecidos, incluyendo las capacidades de trazabilidad, detección de cambios y repositorio versionado previstas en los documentos del proceso. El oferente podrá apoyarse en capacidades nativas o integradas, siempre que cumpla integralmente con las funcionalidades solicitadas. Por lo anterior, no se acepta la solicitud.

285	2.26	Recolección de logs escalable y flexible, como minimo debe incluir los siguientes elementos: - Soporte inmediato para una amplia variedad de sistemas de seguridad y APIs de proveedores - tanto locales como en la nube. - Los agentes de Windows proporcionarán una colección de eventos altamente escalable y rica, los cambios de software instalados y la supervisión de cambios en el registro. - Protección de la integridad de los logs almacenados en la plataforma utilizando SHA-256. - Capacidad para modificar los analizadores directamente desde la interfaz gráfica de usuario y aplicarlos en el sistema en ejecución sin pérdida de tiempo de inactividad y de evento. - Creación de nuevos analizadores (plantillas XML) a través del entorno de desarrollo integrado y capacidad para compartir a través de la función de exportación / importación. - Recopilación segura y fiable de eventos para usuarios y dispositivos ubicados en cualquier lugar.	¿La entidad permite que el requisito de recolección de logs sea cumplido mediante mecanismos equivalentes a los explícitamente indicados, tales como cifrado en tránsito y en reposo, firmas digitales o funciones hash distintas a SHA-256, así como el uso de frameworks de parsing configurables diferentes a plantillas XML, siempre que se garantice la integridad, trazabilidad, disponibilidad y flexibilidad en la gestión de logs? La exigencia de mecanismos específicos podría limitar la participación de soluciones que, aunque cumplen funcionalmente, no siguen exactamente la misma implementación tecnológica de un fabricante particular.	La solución deberá contar con capacidades de recolección de logs escalable y flexible, soportando múltiples fuentes de información tanto en entornos locales como en la nube. Como mínimo, deberá incluir: Soporte para la integración con una amplia variedad de sistemas de seguridad y APIs de proveedores. Recolección de eventos mediante agentes (incluyendo Windows), que permitan obtener información de eventos del sistema, cambios de software instalado y monitoreo de cambios en el registro. Mecanismos de protección de la integridad y confidencialidad de los logs, tales como cifrado en tránsito y en reposo, firmas digitales, funciones hash o mecanismos equivalentes. Capacidad para modificar y desplegar analizadores de logs de manera dinámica desde la interfaz de usuario, sin afectar la continuidad del servicio. Capacidad para crear y gestionar analizadores de logs mediante herramientas configurables, sin que sea obligatorio el uso de un esquema específico basado en plantillas XML, siempre que se permita su reutilización y portabilidad. Recolección segura y confiable de eventos para usuarios y dispositivos ubicados en cualquier localización. Se aceptarán soluciones que implementen mecanismos equivalentes a los solicitados, siempre que garanticen la integridad, disponibilidad y trazabilidad de la información recolectada.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la solución deberá cumplir con las capacidades mínimas de recolección, protección de integridad, trazabilidad, flexibilidad y disponibilidad de logs establecidas en los documentos del proceso. Podrán presentarse mecanismos equivalentes o superiores, siempre que no disminuyan el nivel de seguridad requerido y permitan verificar la integridad, confidencialidad, disponibilidad y trazabilidad de la información recolectada.
286	2.33	Supervisión de disponibilidad, como minimo 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 acepta que el requisito de supervisión de disponibilidad, incluyendo los modelos de Synthetic Transaction Monitoring, pueda ser cumplido mediante una combinación de capacidades nativas y/o integraciones con herramientas especializadas o scripts, siempre que se garantice la medición de disponibilidad, detección de fallas y cálculo de SLA de los servicios?	La solución deberá contar con capacidades de supervisión de disponibilidad de la infraestructura tecnológica y los servicios, permitiendo identificar cambios de estado, degradación y afectación en la operación. Como mínimo, deberá incluir: Monitoreo de estado de dispositivos y servicios mediante protocolos estándar (Ping, SNMP, WMI, APIs u otros mecanismos equivalentes), incluyendo visibilidad sobre interfaces, procesos, servicios y eventos de red. Capacidad de identificar cambios de estado en componentes de red, sistemas y servicios, incluyendo eventos asociados a enrutamiento, interfaces y almacenamiento, ya sea de forma directa o mediante integración con fuentes de datos. Monitoreo de hardware y variables del entorno, ya sea de forma nativa o mediante integración con herramientas externas o sensores. Definición y gestión de ventanas de mantenimiento mediante calendarios configurables. Medición y visualización de indicadores de disponibilidad y cumplimiento de SLA, incluyendo configuraciones de horarios hábiles y no hábiles. Para la evaluación de disponibilidad de servicios, se aceptarán soluciones que implementen: Monitoreo basado en eventos, tráfico o telemetría, y/o Pruebas activas tipo Synthetic Transaction Monitoring, ya sea de forma nativa o mediante integración con herramientas especializadas. Se aceptarán esquemas que combinen capacidades nativas e integraciones, siempre que se garantice la visibilidad, medición y gestión integral de la disponibilidad de los servicios.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem en mención será retirado mediante adenda.
287	3.28	El administrador del sistema debe tener la capacidad de administrar el campo de comentarios y los archivos adjuntos agregando, editando o eliminando comentarios y mensajes	¿La entidad acepta que, por razones de integridad, auditoría y cadena de custodia, los comentarios y evidencias registrados en la gestión de incidentes sean inmutables, y que cualquier ajuste se realice mediante la adición de nuevos registros o versiones, en lugar de la edición o eliminación directa de la información? Esto debido a que permitir edición directa puede responder a modelos de herramientas específicas, mientras que las mejores prácticas internacionales priorizan la trazabilidad y la cadena de custodia.	El sistema deberá permitir la gestión de comentarios y archivos adjuntos dentro del proceso de atención de incidentes, garantizando la trazabilidad, integridad y auditoría de la información registrada. Como mínimo, deberá permitir: La adición de comentarios y adjuntos como evidencia dentro de los casos o incidentes. La gestión de la información registrada mediante mecanismos que permitan su actualización o corrección, ya sea mediante edición controlada o mediante la generación de nuevos registros asociados. La conservación del historial completo de cambios sobre comentarios y evidencias, asegurando trazabilidad de quién, qué y cuándo se realizaron modificaciones. La protección de la integridad de la información mediante mecanismos de inmutabilidad, control de versiones o auditoría. No será obligatorio permitir la eliminación o modificación directa de registros previamente almacenados, siempre que la solución garantice controles de auditoría, trazabilidad y cumplimiento de cadena de custodia.	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 sugerencia.
288	3.38	Permitir agregar y eliminar archivos y pruebas directamente desde o hacia los tickets.	¿La entidad acepta que la gestión de archivos y evidencias se realice de forma centralizada dentro de la plataforma de seguridad (SOC/XDR), y que su asociación con sistemas de ticketing se lleve a cabo mediante integraciones (APIs, conectores o Webhooks), sin que sea obligatorio permitir la edición o eliminación directa de archivos desde el ticket en tiempo real? La exigencia de funcionalidades específicas dentro del sistema de tickets podría estar alineada a herramientas particulares, limitando esquemas de integración ampliamente utilizados en arquitecturas modernas.	La solución deberá permitir la gestión de archivos y evidencias asociadas a incidentes de seguridad, garantizando su trazabilidad, integridad y disponibilidad para análisis y respuesta. Como mínimo, deberá permitir: La adición y gestión de archivos, evidencias digitales e indicadores (IOCs) dentro del contexto del incidente o caso. La asociación de evidencias a tickets o sistemas externos de gestión mediante mecanismos de integración. La sincronización de información relevante del incidente, incluyendo evidencias, contexto y estado, con herramientas de ticketing mediante conectores, APIs o Webhooks. La posibilidad de consultar, transferir o referenciar evidencias desde los sistemas de ticketing integrados. La eliminación o gestión directa de archivos dentro del sistema de ticketing externo no será obligatoria, siempre que la solución garantice la gestión centralizada de evidencias y su integración con dichos sistemas.	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 sugerencia.
289	3.45	Ciertos campos deben ser visibles y / u obligatorios bajo condiciones específicas (ejemplo: las notas de cierre deben ser visibles y obligatorias solo cuando el estado de alerta está configurado como cerrado).	¿La entidad acepta que la validación de campos obligatorios o visibles bajo condiciones específicas pueda ser implementada mediante integración con plataformas ITSM o de gestión de tickets, y no necesariamente de forma nativa en la herramienta XDR, siempre que se garantice el control del flujo de atención y el cumplimiento de las políticas de cierre de incidentes? Esto con el fin de evitar dependencias sobre funcionalidades nativas de fabricantes específicos y permitir la interoperabilidad entre herramientas líderes del mercado.	La solución deberá permitir la gestión del ciclo de vida de alertas e incidentes, incluyendo la definición de estados y el registro de información asociada a cada fase del proceso. Como mínimo, deberá permitir: La gestión de estados de incidentes (por ejemplo: Abierto, En Progreso, Resuelto, Cerrado). El registro de información relevante mediante comentarios, notas o campos asociados al caso. La aplicación de reglas de validación sobre la información requerida para el cierre o avance de los incidentes. Las reglas de visibilidad u obligatoriedad de campos bajo condiciones específicas (por ejemplo, notas de cierre obligatorias al cerrar un incidente) podrán ser implementadas: De forma nativa en la plataforma, y/o Mediante integración con herramientas externas de gestión de tickets o ITSM (ej. ServiceNow, Jira, Remedy), siempre que se garantice la validación de la información y la consistencia del flujo de atención de incidentes.	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 sugerencia.
290	3.56	El sistema debe proporcionar un generador gráfico de playbook visual de arrastrar y soltar.	¿La entidad acepta que la construcción de playbooks de automatización se realice mediante interfaces gráficas no-code o low-code basadas en formularios o asistentes guiados, sin requerir obligatoriamente un diseñador tipo drag-and-drop en formato canvas, siempre que se garantice la orquestación de acciones, la automatización de respuestas y la facilidad de configuración? Esto con el fin de evitar dependencias sobre funcionalidades nativas de fabricantes específicos y permitir la interoperabilidad entre herramientas líderes del mercado.	La solución deberá permitir la creación, gestión y ejecución de playbooks de respuesta automatizada para la atención de incidentes de seguridad. Como mínimo, deberá incluir: Definición de flujos de trabajo basados en eventos, alertas o condiciones configurables. Capacidad de orquestar acciones automáticas y/o manuales, incluyendo integraciones con herramientas externas. Interfaz gráfica que permita la construcción y gestión de playbooks sin necesidad de desarrollo de código (no-code o low-code). Disponibilidad de acciones predefinidas y capacidad de integración mediante APIs, conectores o Webhooks. La construcción de playbooks podrá realizarse mediante interfaces gráficas basadas en formularios, asistentes guiados o diseñadores visuales, sin que sea obligatorio el uso de un modelo específico de arrastrar y soltar tipo canvas, siempre que se garantice la facilidad de configuración, mantenimiento y ejecución de los flujos de automatización.	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 sugerencia.
291	3.57	El sistema debe proporcionar un generador gráfico de playbook visual de arrastrar y soltar. "La plataforma Stellar Cyber permite la creación de flujos de trabajo de respuesta automatizada (playbooks) desde la interfaz gráfica web, orientados a la orquestación de acciones de seguridad ante eventos o condiciones específicas.	¿La entidad acepta que la construcción de playbooks de automatización se realice mediante interfaces gráficas no-code o low-code basadas en formularios o asistentes guiados, sin requerir obligatoriamente un diseñador tipo drag-and-drop en formato canvas, siempre que se garantice la orquestación de acciones, la automatización de respuestas y la facilidad de configuración? Esto con el fin de evitar dependencias sobre funcionalidades nativas de fabricantes específicos y permitir la interoperabilidad entre herramientas líderes del mercado.	La solución deberá permitir la creación, gestión y ejecución de playbooks de respuesta automatizada para la atención de incidentes de seguridad. Como mínimo, deberá incluir: Definición de flujos de trabajo basados en eventos, alertas o condiciones configurables. Capacidad de orquestar acciones automáticas y/o manuales, incluyendo integraciones con herramientas externas. Interfaz gráfica que permita la construcción y gestión de playbooks sin necesidad de desarrollo de código (no-code o low-code). Disponibilidad de acciones predefinidas y capacidad de integración mediante APIs, conectores o Webhooks. La construcción de playbooks podrá realizarse mediante interfaces gráficas basadas en formularios, asistentes guiados o diseñadores visuales, sin que sea obligatorio el uso de un modelo específico de arrastrar y soltar tipo canvas, siempre que se garantice la facilidad de configuración, mantenimiento y ejecución de los flujos de automatización.	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 sugerencia.
292	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	¿La entidad acepta que la detección de amenazas se realice mediante un enfoque híbrido que combine técnicas de machine learning, reglas de correlación, firmas e inteligencia de amenazas, en lugar de limitarse exclusivamente a modelos basados en comportamiento sin uso de reglas o firmas, considerando que este enfoque es el adoptado por las plataformas XDR/SIEM de nivel empresarial? Esto con el fin de evitar dependencias sobre funcionalidades nativas de fabricantes específicos y permitir la interoperabilidad entre herramientas líderes del mercado.	La solución deberá contar con capacidades avanzadas de analítica de seguridad basadas en inteligencia artificial y/o machine learning, que permitan el aprendizaje del comportamiento del entorno y la detección de anomalías. Como mínimo, deberá cumplir con: Capacidad de establecer líneas base de comportamiento dinámicas y adaptativas del entorno. Identificación de desviaciones respecto al comportamiento normal mediante técnicas de analítica avanzada. Capacidad de aprendizaje continuo que permita ajustar los modelos ante cambios en la infraestructura o patrones de uso. La solución podrá operar mediante un enfoque híbrido que combine: Modelos de Machine Learning (supervisado y/o no supervisado), Reglas de correlación, Firmas, e Inteligencia de amenazas (Threat Intelligence), siempre que en conjunto permitan mejorar la capacidad de detección, reducir falsos positivos y cubrir tanto amenazas conocidas como desconocidas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem 7.26 será ajustado, para evitar equívocos 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.
293	Pagina 64	a. Modelo operacional de servicios SOC (Documento Integral).	Se solicita a la entidad precisar y objetivar los criterios de evaluación asociados al “Modelo Operacional de Servicios SOC (Documento Integral)”, toda vez que la redacción actual presenta un alto grado de subjetividad, lo que puede generar interpretaciones dispares entre los evaluadores y los oferentes. En particular, se recomienda definir de manera más granular los parámetros de calificación para cada nivel de puntaje (1, 4, 8, 12), estableciendo criterios verificables y medibles, tales como: nivel de detalle esperado, componentes mínimos del modelo de gobierno, alcance específico de las capacidades SOC requeridas, definición de entregables, y lineamientos claros para la identificación de “aspectos diferenciadores” y “valores agregados”. Lo anterior con el fin de garantizar transparencia, trazabilidad y equidad en el proceso de evaluación, permitiendo a los oferentes estructurar sus propuestas de forma alineada a expectativas objetivas y comparables.	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los criterios mínimos para este documento, están claramente detallados en la página 55 sección III del documento "410-Solicitud-de-Oferta-VSD-SdO-SOC", que a la letra menciona: a. Como parte de la oferta técnica los oferentes deberán presentar un documento que incluya el modelo operacional de servicios SOC que propone utilizar para prestar los servicios y desarrollar las actividades descritas en la sección VI del documento y el anexo de características técnicas mínimas, conforme a las siguientes consideraciones: • Deberá contemplar la descripción del enfoque que será utilizado para alcanzar los objetivos del proyecto. Debe incluir el esquema de gobernanza, así como la descripción de las metodologías a utilizar, considerando expresamente la adopción del Modelo de operación para la gestión y ejecución del proyecto. • Deberá incluir la descripción de las herramientas que soportarán la gestión del proyecto, y las herramientas que permitan acelerar la productividad y la implementación y operación del SOC. • Deberá detallar los mecanismos, procedimientos y componentes que utilizará para asegurar la calidad de los servicios, y la operación y ejecución de los mismos, así como la forma de facilitar la verificación de estos por parte de la DIAN. Todo lo anterior, en concordancia con los lineamientos y requerimientos del servicio establecidos en la sección VI de este documento y el anexo de características técnicas, el cual es de obligatorio cumplimiento.
294	Pagina 64	c. Incluye servicios TAM (Thecnical account manager) (ítems 2 al 9 del anexo técnico).	Se solicita a la entidad aclarar y objetivar los criterios de evaluación relacionados con la inclusión del servicio de TAM, considerando que actualmente la asignación de puntaje basada en el número de capacidades cubiertas no define claramente el alcance ni las responsabilidades del servicio. Se recomienda detallar: El alcance mínimo esperado del servicio TAM (dedicación, funciones, nivel de especialización). Si el TAM debe ser dedicado o compartido. Los entregables esperados (reportes, seguimiento, planes de mejora, etc.). Cómo se valida la cobertura del servicio sobre cada capacidad evaluada. Esto permitirá evitar interpretaciones subjetivas y asegurar comparabilidad entre propuestas.	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los criterios mínimos para este documento, están claramente detallados en la página 55 sección III del documento "410-Solicitud-de-Oferta-VSD-SdO-SOC", que a la letra menciona: 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
295	Pagina 64	d. Metodología para el cálculo de ROSI (Retorno a la inversión en seguridad de la Información).	Se solicita a la entidad precisar los criterios de evaluación asociados a la “Metodología para el cálculo de ROSI”, dado que conceptos como “precisión en la estimación de riesgos”, “costos relevantes” y “facilidad de uso y comunicación” pueden ser interpretados de manera subjetiva. Se recomienda definir de forma explícita: Los componentes mínimos que debe incluir la metodología (identificación de activos, amenazas, vulnerabilidades, impacto, probabilidad, etc.). Los criterios para determinar la “precisión” en la estimación de riesgos. Qué se considera dentro de “todos los costos relevantes”. Los entregables mínimos esperados. Parámetros objetivos para evaluar la “facilidad de uso y comunicación” (ej. dashboards, reportes ejecutivos, visualizaciones, etc.). Esto permitirá una evaluación más transparente, medible y alineada entre oferentes.	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los criterios mínimos para este documento, están claramente detallados en la página 56 sección III del documento "410-Solicitud-de-Oferta-VSD-SdO-SOC", que a la letra menciona: d. El interesado deberá generar una metodología que permita calcular el retorno a la inversión en seguridad de la información (ROSI) que contenga como mínimo los siguientes criterios: o Identificar los riesgos. o Estimar la Tasa Anual de Ocurrencia (ARO) de cada riesgo. o Calcular la Expectativa Anual de Pérdidas (ALE). o Estimar la reducción de ALE o Calcular el beneficio. o Aplicar la fórmula de ROSI.

296	Pagina 64	e. Estrategia de Monitoreo y Ciberseguridad.	Se solicita a la entidad detallar y objetivar los criterios de evaluación para la "Estrategia de Monitoreo y Ciberseguridad", ya que actualmente incluye elementos cualitativos que pueden generar subjetividad en la asignación de puntajes. Se recomienda especificar: Qué políticas nacionales y marcos normativos deben considerarse (ej. ISO, NIST, regulaciones locales, etc.). Los indicadores de desempeño mínimos requeridos (KPIs/KRIs específicos). La forma en que deben presentarse los escenarios de ciberataques (ej. casos de uso, simulaciones, threat modeling, etc.). Qué se considerará como "aspectos diferenciadores" y "valores agregados". Lo anterior con el fin de garantizar criterios de evaluación claros, comparables y verificables.	N/A	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los criterios mínimos para este documento, están claramente detallados en la página 56 sección III del documento "410-Solicitud-de-Oferta-VSD-SdO-SOC", que a la letra menciona: e. Dentro de la oferta técnica el futuro oferente deberá diseñar y entregar documento con la estrategia de monitoreo de ciberseguridad, acorde con los siguientes criterios: • Fortalecimiento de la Gestión de monitoreo: o Estrategia general del monitoreo o Objetivos del Monitoreo o Roles y responsabilidades o Herramientas de monitoreo o Indicadores y métricas o Integración con la gestión de incidentes o Auditoría y mejora continua • Fortalecimiento de la Gestión de Incidentes: o Propuesta procedimiento de gestión de incidentes o Roles y responsabilidades (equipos de gestión y respuesta) o Herramientas de gestión o Proceso (Preparación, detección, contención, erradicación, recuperación, lecciones aprendidas) o Clasificación y escalamiento o Registro y mejora continua
297	1.1	NOTA 2: Todos los elementos adquiridos y entregados, producto del presente proceso contractual serán de propiedad de la DIAN, para los casos donde aplique.	Se solicita a la entidad definir de manera expresa y clara, en que casos aplica y no aplica que los elementos adquiridos serán de propiedad de la DIAN. La ausencia de esta definición vulnera los principios de igualdad y transparencia, al dejar a la interpretación de cada oferente la determinación de los activos a considerar, lo cual afecta la selección objetiva del proceso.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el requerimiento menciona "para los casos donde aplique", refiere al licenciamiento a perpetuidad donde al momento de finalizar los servicios, este debe quedar a nombre de la Entidad o a aquellos elementos que sean instalados en los datacenter de la Entidad o que sean necesarios para continuar con el derecho a uso de los diferentes servicios.
298	1.3	NOTA 5: El SIEM debe ser cotizado a tres (3) años, y su implementación se hará a partir de septiembre 1 de 2027 con licenciamiento soporte, garantía y derecho a uso sería hasta septiembre de 2030, El futuro contratista deberá, recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 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 SIEM solicitado en las capacidades requeridas por la DIAN.	Conforme a las prácticas comerciales vigentes del mercado y a las políticas de los fabricantes de tecnología SIEM, no es posible cotizar de manera vinculante precios, condiciones comerciales o licenciamiento específicos para periodos futuros cuya vigencia inicia con varios años de antelación. En consecuencia, el valor económico presentado para el nuevo SIEM corresponde a una estimación referencial, y esta sujeto a cambio según el mercado lo exija y la cual será ajustada y formalizada al momento de la implementación efectiva en 2027, sin que ello afecte el alcance funcional, las capacidades técnicas requeridas ni la continuidad del servicio SOC.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el oferente deberá estructurar su propuesta económica conforme a las condiciones, vigencias y alcances definidos en los documentos del proceso. Los valores ofertados deben considerar el licenciamiento, soporte, garantía y derecho de uso requeridos para el periodo señalado. Por lo anterior, no se acepta la solicitud.
299	Seccion VI 3.1	NOTA 5: El SIEM debe ser cotizado a tres (3) años, y su implementación se hará a partir de septiembre 1 de 2027 con licenciamiento soporte, garantía y derecho a uso sería hasta septiembre de 2030, El futuro contratista deberá, recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 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 SIEM solicitado en las capacidades requeridas por la DIAN.	Confirmar el tiempo de transición estimada para la fase de transición al SIEM nuevo propuesto por el Ofertente. Cuanto tiempo tendrá que operar los dos SIEM en paralelo.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se contempla un período de operación en paralelo, el futuro operador de soc debe generar las estrategias adecuadas y necesarias para implementar las nuevas herramientas SIEM y protección de bases de datos y que garanticen la continuidad ininterrumpida de los respectivos servicios.
300	Seccion VI 3.1	NOTA 7: La protección de bases de datos (Firewall de bases de datos) debe ser cotizado 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 el 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.	Conforme a las prácticas comerciales vigentes del mercado y a las políticas de los fabricantes de tecnología firewall de bases de datos, no es posible cotizar de manera vinculante precios, condiciones comerciales o licenciamiento específicos para periodos futuros cuya vigencia inicia con varios años de antelación. En consecuencia, el valor económico presentado para el nuevo firewall de bases de datos corresponde a una estimación referencial, y esta sujeto a cambio según el mercado lo exija y la cual será ajustada y formalizada al momento de la implementación efectiva en 2027, sin que ello afecte el alcance funcional, las capacidades técnicas requeridas ni la continuidad del servicio SOC		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el oferente deberá estructurar su propuesta económica conforme a las condiciones, vigencias y alcances definidos en los documentos del proceso. Los valores ofertados deben considerar el licenciamiento, soporte, garantía y derecho de uso requeridos para el periodo señalado, y sus precios deberán mantenerse por ser una propuesta económica.
301	Seccion VI 3.1	NOTA 8: Inteligencia de Amenazas (NDR) debe ser cotizado 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.	Conforme a las prácticas comerciales vigentes del mercado y a las políticas de los fabricantes de tecnología Inteligencia de Amenazas (NDR), no es posible cotizar de manera vinculante precios, condiciones comerciales o licenciamiento específicos para periodos futuros cuya vigencia inicia con varios años de antelación. En consecuencia, el valor económico presentado para el nuevo Inteligencia de Amenazas (NDR) corresponde a una estimación referencial, y esta sujeto a cambio según el mercado lo exija y la cual será ajustada y formalizada al momento de la implementación efectiva en 2027, sin que ello afecte el alcance funcional, las capacidades técnicas requeridas ni la continuidad del servicio SOC.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el oferente deberá estructurar su propuesta económica conforme a las condiciones, vigencias y alcances definidos en los documentos del proceso. Los valores ofertados deben considerar el licenciamiento, soporte, garantía y derecho de uso requeridos para el periodo señalado, y sus precios deberán mantenerse por ser una propuesta económica.
302	Seccion VI 3.1	NOTA 6: Los servicios de monitoreo y operación del SOC van hasta octubre de 2028 y debe contemplar todas y cada una de las capacidades y servicios requeridos en este proyecto.	Se solicita aclarar la coherencia temporal entre la vigencia indicada para los servicios de monitoreo y operación del SOC hasta octubre de 2028, y el requerimiento de otros componentes y servicios con duración de tres (3) años, tales como garantía y soporte técnico, entre otros ítems listados. Unos componentes mas allá de los 3 años hasta el 2030. La ausencia de esta definición vulnera los principios de igualdad y transparencia, al dejar a la interpretación de cada oferente la determinación de los activos a considerar, lo cual afecta la selección objetiva del proceso.		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.
303	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	Se solicita a la entidad confirmar si se requiere hacer migracion de los datos de su actual solucion ORION a la que el proveedor ofrecerá con el fin de alimentar la herramienta con Logs históricos. En caso de que la respuesta a la regunta anterior sea SI, favor precisar en donde se encuentran reposando dichos datos, si se garantizará el acceso a ellos para ejecutar el proceso de migración por parte del oferente y confirmar la herramienta actual sobre la cual se hace correlacion de eventos y almacenamiento de dichos logs, ubicación, capacidad en Gigas (GB) y si se permite acceso por internet.		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.
304	2.14	Se deberá realizar la correlación, monitoreo y casos de uso sobre la plataforma suministrada a la entidad, de tal forma que todo el know how y parametrizaciones queden para la entidad. Para la fase de implementación se deberán desarrollar y ejecutar 20 casos de uso, de manera, posterior durante la operación los que sean requeridos por la DIAN.	Se solicita a la entidad confirmar si se requiere hacer migracion de casos de uso implementados en su actual solucion SIEM IBM y ORION a la que el proveedor ofrecerá. En caso de que la respuesta a la regunta anterior sea SI, favor precisar los casos de uso tanto de SIEM como del NOC.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el contratista deberá desarrollar y ejecutar los casos de uso requeridos en los documentos del proceso, incluyendo los veinte (20) casos de uso previstos para la fase de implementación y los adicionales que sean requeridos durante la operación. No se establece como obligación general la migración automática de casos de uso existentes; sin embargo, la DIAN podrá suministrar la información necesaria para su análisis y parametrización durante la fase correspondiente.
305	2.17	Se debe realizar la integración y monitoreo de los dispositivos y activos tecnológicos que conforman la infraestructura tecnológica de la entidad (Revisar hoja en este archivo "Inventario Infraestructura IT")	Solicitamos compartir el documento asosiado a la hoja en este archivo "Inventario Infraestructura IT"		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.
306	2.20	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 .	Confirmar si la entidad espera que el oferente despliegue una herramienta de escaneo de vulnerabilidades y la capa de servicio para la gestión de las mismas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el proyecto contempla capacidades asociadas a la identificación, monitoreo y gestión de vulnerabilidades conforme a lo definido en los documentos del proceso. El oferente deberá incluir las herramientas, licenciamiento, implementación, operación y capa de servicio necesarias para cumplir integralmente con dicho alcance.
307	2.27	Notificación y Gestión de Incidentes - Framework de notificación de incidentes basado en políticas. - Posibilidad de activar una secuencia de comandos de corrección cuando se produce un incidente específico. - Integración basada en API a sistemas externos de ticketing - Aranda, ServiceNow, Salesforce, ConnectWise, Remedy y Jira. - Sistema incorporado de ticketing o integrarse al sistema de ticketing de la Entidad (Aranda).	Se solicita aclarar con respecto al Sistema ITSM oficial del servicio, cuál será el sistema de ticketing que actuará como repositorio oficial para el registro, gestión, seguimiento, cierre y auditoría de incidentes de seguridad (por ejemplo, Aranda u otro), y si dicho sistema será suministrado por la DIAN o por el proveedor.		La Dirección de Impuestos y Aduanas Nacionales - DIAN, informa al observante que, el ítem es claro en cuanto a que menciona lo siguiente respondiendo su inquietud: Sistema incorporado de ticketing o integrarse al sistema de ticketing de la Entidad (Aranda).
308	2.27	Notificación y Gestión de Incidentes - Framework de notificación de incidentes basado en políticas. - Posibilidad de activar una secuencia de comandos de corrección cuando se produce un incidente específico. - Integración basada en API a sistemas externos de ticketing - Aranda, ServiceNow, Salesforce, ConnectWise, Remedy y Jira. - Sistema incorporado de ticketing o integrarse al sistema de ticketing de la Entidad (Aranda).	Confirmar si el futuro contratista deberá suministrar, licenciar e implementar un sistema de ticketing propio, o si deberá integrarse exclusivamente al ITSM institucional de la DIAN.		La Dirección de Impuestos y Aduanas Nacionales - DIAN, informa al observante que, el ítem es claro en cuanto a que menciona lo siguiente respondiendo su inquietud: Sistema incorporado de ticketing o integrarse al sistema de ticketing de la Entidad (Aranda).
309	2.27	Notificación y Gestión de Incidentes - Framework de notificación de incidentes basado en políticas. - Posibilidad de activar una secuencia de comandos de corrección cuando se produce un incidente específico. - Integración basada en API a sistemas externos de ticketing - Aranda, ServiceNow, Salesforce, ConnectWise, Remedy y Jira. - Sistema incorporado de ticketing o integrarse al sistema de ticketing de la Entidad (Aranda).	Aclarar si la integración requerida es unidireccional o bidireccional (creación, actualización automática de estados, cierre, adjuntos, evidencias y comentarios), así como el nivel de detalle esperado para la documentación de incidentes, SLA/ANS y actividades de respuesta.		La Dirección de Impuestos y Aduanas Nacionales - DIAN, informa al observante que, el ítem es claro en cuanto a que menciona lo siguiente respondiendo su inquietud: Sistema incorporado de ticketing o integrarse al sistema de ticketing de la Entidad (Aranda).
310	2.35	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.	Con respecto a requerimiento "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" Debido a que mensionan que no deberán conllevar consumo asociado ni de licencia de dispositivos ni de EPS, solicitamos aclarar cual es la unidad de medida y cantidad requerido por la DIAN para este licenciamiento UEBA.		La Dirección de Impuestos y Aduanas Nacionales - DIAN, informa al observante que, las cantidades para cada servicio están expresamente definidas en el anexo técnico.
311	1.4	1.4. Descripción de la arquitectura TI actual de los ecosistemas en la DIAN - Tipo Infraestructura	Se solicita a la entidad definir y listar de manera expresa, clara y precisa el nombre, la referencia y la ubicación de los activos críticos que deben ser integrados en la solución referentes a Tipo Infraestructura, toda vez que en el presente numeral no se identifica con claridad cuáles activos son de carácter obligatorio. La ausencia de esta definición vulnera los principios de igualdad y transparencia, al dejar a la interpretación de cada oferente la determinación de los activos a considerar, lo cual afecta la selección objetiva del proceso. En consecuencia, resulta necesario que la entidad suministre esta información de forma uniforme y previa, con el fin de que todos los proponentes presenten sus ofertas bajo las mismas condiciones técnicas y de información, garantizando la igualdad de trato, la pluralidad de oferentes y la comparabilidad objetiva de las propuestas.		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.
312	1.4	1.4. Descripción de la arquitectura TI actual de los ecosistemas en la DIAN - Infraestructura Seguridad informática	Se solicita a la entidad definir y listar de manera expresa, clara y precisa el nombre, la referencia y la ubicación de los activos críticos que deben ser integrados en la solución referentes a Infraestructura Seguridad informática, toda vez que en el presente numeral no se identifica con claridad cuáles activos son de carácter obligatorio. La ausencia de esta definición vulnera los principios de igualdad y transparencia, al dejar a la interpretación de cada oferente la determinación de los activos a considerar, lo cual afecta la selección objetiva del proceso. En consecuencia, resulta necesario que la entidad suministre esta información de forma uniforme y previa, con el fin de que todos los proponentes presenten sus ofertas bajo las mismas condiciones técnicas y de información, garantizando la igualdad de trato, la pluralidad de oferentes y la comparabilidad objetiva de las propuestas.		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.
313	1.4	1.4. Descripción de la arquitectura TI actual de los ecosistemas en la DIAN - Infraestructura comunicaciones	Se solicita a la entidad definir y listar de manera expresa, clara y precisa el nombre, la referencia y la ubicación de los activos críticos que deben ser integrados en la solución referentes aInfraestructura comunicaciones , toda vez que en el presente numeral no se identifica con claridad cuáles activos son de carácter obligatorio. La ausencia de esta definición vulnera los principios de igualdad y transparencia, al dejar a la interpretación de cada oferente la determinación de los activos a considerar, lo cual afecta la selección objetiva del proceso. En consecuencia, resulta necesario que la entidad suministre esta información de forma uniforme y previa, con el fin de que todos los proponentes presenten sus ofertas bajo las mismas condiciones técnicas y de información, garantizando la igualdad de trato, la pluralidad de oferentes y la comparabilidad objetiva de las propuestas.		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.
314	1.4	1.4. Descripción de la arquitectura TI actual de los ecosistemas en la DIAN - Bases de Datos Oracle	Se solicita a la entidad definir y listar de manera expresa, clara y precisa el nombre, la referencia y la ubicación de los activos críticos que deben ser integrados en la solución referentes a Bases de Datos Oracle , toda vez que en el presente numeral no se identifica con claridad cuáles activos son de carácter obligatorio. La ausencia de esta definición vulnera los principios de igualdad y transparencia, al dejar a la interpretación de cada oferente la determinación de los activos a considerar, lo cual afecta la selección objetiva del proceso. En consecuencia, resulta necesario que la entidad suministre esta información de forma uniforme y previa, con el fin de que todos los proponentes presenten sus ofertas bajo las mismas condiciones técnicas y de información, garantizando la igualdad de trato, la pluralidad de oferentes y la comparabilidad objetiva de las propuestas.		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.
315	Administrativa	1.4. Descripción de la arquitectura TI actual de los ecosistemas en la DIAN - Bases de Datos SQL	Se solicita a la entidad definir y listar de manera expresa, clara y precisa el nombre, la referencia y la ubicación de los activos críticos que deben ser integrados en la solución referentes a Bases de Datos SQL, toda vez que en el presente numeral no se identifica con claridad cuáles activos son de carácter obligatorio. La ausencia de esta definición vulnera los principios de igualdad y transparencia, al dejar a la interpretación de cada oferente la determinación de los activos a considerar, lo cual afecta la selección objetiva del proceso. En consecuencia, resulta necesario que la entidad suministre esta información de forma uniforme y previa, con el fin de que todos los proponentes presenten sus ofertas bajo las mismas condiciones técnicas y de información, garantizando la igualdad de trato, la pluralidad de oferentes y la comparabilidad objetiva de las propuestas.		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.
316	Seccion III 3.1	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.	DIAN espera un TAM por tecnología. Se solicita a la entidad definir de manera expresa y clara, en que casos aplica y no aplicael servicio de TAM referente a las tecnologías y servicios adquiridos serán de propiedad de la DIAN. La ausencia de esta definición vulnera los principios de igualdad y transparencia		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los criterios mínimos para este documento, están claramente detallados en la página 55 sección III del documento "410-Solicitud-de-Oferta-VSD-SdO-SOC", que a la letra menciona: 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.
317	Seccion III 3.1	d. El interesado deberá generar una metodología que permita calcular el retorno a la inversión en seguridad de la información (ROSI) que contenga como mínimo los siguientes criterios:	Se considera necesario precisar que el ROSI constituye un indicador estimativo y prospectivo, basado en supuestos de riesgo, probabilidad e impacto, los cuales pueden variar en el tiempo y dependen de múltiples factores internos y externos a la operación del proveedor. En este sentido, se solicita confirmar que el requerimiento se entiende como la obligación de definir, documentar y aplicar una metodología de análisis económico del riesgo, y no como un compromiso de generación, garantía o cumplimiento de un valor específico de ROSI, dado que dicho resultado no puede ser asegurado de forma objetiva ni contractual.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el interesado deberá generar una metodología que permita calcular el retorno a la inversión en seguridad de la información (ROSI) que contenga como mínimo los siguientes criterios: o Identificar los riesgos. o Estimar la Tasa Anual de Ocurrencia (ARO) de cada riesgo. o Calcular la Expectativa Anual de Pérdidas (ALE). o Estimar la reducción de ALE o Calcular el beneficio. o Aplicar la fórmula de ROSI. Así mismo, se indica que no es un compromiso de generación, garantía o cumplimiento de un valor específico de ROSI.
318	Seccion III , 1	d. El interesado deberá generar una metodología que permita calcular el retorno a la inversión en seguridad de la información (ROSI) que contenga como mínimo los siguientes criterios:	Se entiende que La metodología propuesta permitirá apoyar la toma de decisiones, priorización de controles y análisis costo-beneficio de las inversiones en seguridad, sin que ello implique garantía de ocurrencia, no ocurrencia o impacto económico de incidentes futuros. Es correcto nuestro entendimiento?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que su entendimiento es correcto. La metodología ROSI deberá apoyar la toma de decisiones, la priorización de controles y el análisis costo-beneficio de inversiones en seguridad, sin que ello implique garantía sobre la ocurrencia, no ocurrencia o impacto económico de incidentes futuros.
319	Seccion III , 2	El plan tiene como objetivo definir la forma en que el oferente llevará a cabo la puesta en marcha del SOC, etallando las etapas, tiempos y acciones necesarias hasta alcanzar su pleno funcionamiento. Este plan deberá ermitir evaluar el proceso de implementación, asegurando que el SOC esté completamente operativo en los plazos establecidos1 y cumpla con los estándares de calidad exigidos.	Se considera necesario aclarar que, dado que la implementación de las plataformas tecnológicas del SOC se realizará en una fecha futura (SIEM, SOAR, NDR, DAM), el plan de implementación deberá entenderse como un marco metodológico y orientativo, basado en las condiciones actuales conocidas del entorno, y sujeto a ajustes razonables derivados de cambios en la infraestructura, arquitectura, inventario de activos, tecnologías, regulaciones o necesidades del negocio que puedan presentarse antes del inicio efectivo de la implementación. En este sentido, se solicita confirmar que el plan de implementación podrá contemplar supuestos explícitos, así como mecanismos de ajuste, refinamiento y validación durante la fase inicial del proyecto, sin que modificaciones derivadas de cambios en el entorno tecnológico del cliente sean consideradas incumplimientos atribuibles al proveedor.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem en mención es muy claro en cuanto a lo solicitado para el plan de implementación que a la letra menciona lo siguiente: a. Como parte de la oferta técnica los oferentes deberán presentar un documento que contenga el Plan general de implementación del proyecto requerido por la DIAN (señalada en la sección VI de este documento), conforme al siguiente alcance: • El plan tiene como objetivo definir la forma en que el oferente llevará a cabo la puesta en marcha del SOC, detallando las etapas, tiempos y acciones necesarias hasta alcanzar su pleno funcionamiento. Este plan deberá permitir evaluar el proceso de implementación, asegurando que el SOC esté completamente operativo en los plazos establecidos y cumpla con los estándares de calidad exigidos. • El plan deberá incluir un desglose de actividades, especificando las fases de implementación, los hitos clave y las dependencias entre tareas, de manera que se pueda monitorear el avance y la disponibilidad progresiva del servicio. También deberá contemplar la organización del equipo de trabajo, describiendo los roles, responsabilidades y la asignación de recursos en función de los requerimientos del servicio. En este plan, se deberá asegurar que el oferente deberá garantizar que sus mecanismos internos de gestión, supervisión y control estén alineados con lo requerido por la DIAN dentro de sus especificaciones, asegurando una transición progresiva y efectiva hacia su operación estable.
320	Seccion VI, 1.2	La DIAN, como resultado del programa "Apoyo a la Modernización de la DIAN", espera que la arquitectura objetivo de tecnología sea una multinube, conformada por múltiples proveedores como Azure y AWS que soportan la operación de multiples aplicaciones CORE de la DIAN.	Se considera necesario aclarar que el dimensionamiento técnico de las plataformas, soluciones y componentes del SOC será realizado por el proveedor con base en la información disponible a la fecha, el contenido del presente documento y los supuestos técnicos explícitos definidos durante la etapa de planeación, entendiendo que la arquitectura, los volúmenes de información, los patrones de uso, las integraciones y los parámetros operativos pueden evolucionar en el tiempo por decisiones propias de la DIAN. En este sentido, se solicita confirmar que los cambios futuros en la arquitectura, configuración, proveedores de nube, topología o parámetros técnicos que sean introducidos por la DIAN y que difieran de las condiciones consideradas para el dimensionamiento inicial, no serán imputables al proveedor, ni darán lugar a responsabilidades por impactos en desempeño, cobertura o funcionamiento de las soluciones originalmente dimensionadas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el dimensionamiento deberá realizarse con base en la información suministrada en los documentos del proceso, las condiciones técnicas conocidas y los supuestos que el oferente estime necesarios declarar en su propuesta. En todo caso, la solución deberá contemplar criterios de escalabilidad, adaptabilidad e integración con la arquitectura objetivo de la Entidad. Los cambios posteriores se gestionarán conforme a los mecanismos contractuales y de control que resulten aplicables.
321	Seccion VI 3.5	5. Tecnología: Las premisas principales son:	Se considera necesario aclarar que los costos derivados de la injerencia directa en las nubes públicas, inherentes a su operación y administración, tales como —sin limitarse a— consumo de servicios de cómputo, almacenamiento, redes, tráfico saliente, APIs, logs nativos, servicios gestionados, licenciamiento propio del proveedor cloud, cuentas, suscripciones o cargos por uso (pay-as-you-go), deberán ser asumidos directamente por la DIAN, en su calidad de propietaria y administradora de dichos entornos cloud.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la infraestructura de nube se tomará como fuente para el SOC, y así poder realizar el monitoreo y seguimiento requerido por la DIAN, en ningún momento se solicita que le proveedor del SOC administre la infraestructura de la Entidad.
322	Seccion VI 1.5	Así las cosas, la DIAN ha adoptado internamente modelos de trabajo colaborativos como el desarrollo por células ágiles, promoviendo así la implementación de prácticas de integración y entrega continua (CI/CD), y la utilización de herramientas bajo enfoque DevSecOps. En consecuencia, el SOC deberá estar en capacidad de interactuar, proteger y monitorear entornos dinámicos, automatizados y distribuidos, asegurando el cumplimiento de los requisitos jurídicos y operativos en todo el ciclo de vida de los activos de información.	Se considera necesario que la Entidad aclare de manera clara, expresa y detallada el modelo esperado de interacción entre el SOC y los entornos DevSecOps, con el fin de evitar ambigüedades técnicas, operativas y contractuales. En particular, se solicita precisar, como mínimo, los siguientes aspectos: Alcance de la intervención del SOC dentro de los flujos CI/CD (por ejemplo, monitoreo, visibilidad, detección, control, aprobación, bloqueo o generación de alertas). Que herramientas espera del SOC asociadas a este requerimiento. Momentos del ciclo de vida en los cuales el SOC debe intervenir (desarrollo, integración, pruebas, despliegue, operación). Responsabilidades específicas entre los equipos DevOps/DevSecOps de la DIAN y el proveedor del SOC, incluyendo límites de actuación y toma de decisiones. Herramientas, plataformas y pipelines sobre los cuales se espera la integración del SOC, así como los mecanismos técnicos permitidos (APIs, agentes, webhooks, escaneo, monitoreo pasivo, entre otros). Nivel de automatización esperado, incluyendo si el SOC está autorizado a ejecutar acciones automáticas que impacten pipelines, despliegues o ambientes productivos. Responsabilidad sobre fallos, bloqueos o impactos operativos derivados de controles de seguridad integrados al flujo DevSecOps.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la interacción del SOC con entornos DevSecOps estará orientada al monitoreo, visibilidad, detección, generación de alertas, análisis y acompañamiento en la gestión de riesgos de seguridad durante el ciclo de vida de los activos de información. Cualquier acción automatizada que pueda impactar pipelines, despliegues o ambientes productivos deberá estar previamente definida, autorizada y coordinada con la Entidad.

323	Seccion VI 3.2	Licenciamiento: El licenciamiento por tres años debe incluir todas las funcionalidades necesarias para la operación y gestión completa de las herramientas (SIEM, Protección de bases de datos e Inteligencia de amenazas) durante todo el periodo especificado.	Se considera necesario que la Entidad aclare de manera expresa y detallada el licenciamiento por tres años debe incluir todas las funcionalidades necesarias para la operación y gestión completa de las herramientas. Con el fin de ofrecer el licenciamiento adecuado acorde a las necesidades y requerimientos de la DIAN		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el licenciamiento por tres años deberá incluir todas las funcionalidades, módulos, capacidades, soporte, garantía y derechos de uso necesarios para la operación y gestión completa de las herramientas requeridas, conforme al alcance y cantidades definidas en los documentos del proceso.
324	SDO 3.3 pagina 107	Pruebas: Actividades de puesta a punto, compatibilidad, manejo de errores e inconvenientes. Las pruebas funcionales y de seguridad deberán realizarse con entornos controlados y bajo procedimientos formalizados que aseguren la integridad de la información y el no uso indebido de datos personales o activos sujetos a reserva. El proveedor deberá entregar actas de validación, bitácoras técnicas y legales, y evidencias digitales bajo cadena de custodia, que permitan verificar el cumplimiento de estándares de ciberseguridad, normatividad y obligaciones contractuales.	Se considera necesario que la Entidad aclare de manera expresa y detallada las Actividades de puesta a punto, compatibilidad, manejo de errores e inconvenientes. La evitar ambiguedades en la entrega de cada solución. Listar las prubas solicitadas para cada tecnología solicitada.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, todas las características y requerimientos de la Entidad para el proyecto SOC están claramente definidas en el documento anexo técnico, así como todas las actividades a realizar.
325	Seccion VI 4.1	8. Todo el licenciamiento o servicios tipo SaaS, PaaS, IaaS, XaaS que se activen, deberán estar a nombre de la DIAN, conectarse de forma nativa y/o personalizada inicialmente con la infraestructura tecnológica que se encuentra en el inventario sin perjuicio a futuro de conexiones a nuevas soluciones y datos de la DIAN, limitado hasta las cantidades indicadas en el anexo de características técnicas mínimas requeridas.	Se considera necesario que la Entidad aclare de manera detallada si requiere que el licenciamiento relacionado al servicio tipo SaaS, PaaS, IaaS, XaaS que se activen para lograr ofrecer, Monitoreo a la Gestión de Vulnerabilidades, Solución de análisis de código estático y dinámico para aplicaciones, Protección de Marca y cacería de amenazas, tambien deberán estar a nombre de la DIAN. Por Faovr aclarar y listar las que si requiere y deberán estar a nombre de la DIAN		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, si para la entrega de los servicios o requerimientos de la Entidad el futuro proveedor contempla licenciamiento a perpetuidad el mismo quedará a nombre de la DIAN una vez terminen los servicios prestados, así como cualquier otro dispositivo que sea instalado en los centros de datos de la Entidad.
326	Seccion VI 3.4	9. 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.	Se considera necesario que la Entidad aclare de manera detallada la cantidad de casos de uso de monitoreo a nivel de SIEM que el proveedor debe configurar en todo el contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, para la fase de implementación, deberán desarrollarse y ejecutarse veinte (20) casos de uso, conforme a lo establecido en los documentos del proceso. Durante la operación, el contratista deberá desarrollar los casos de uso adicionales que sean requeridos por la DIAN, de acuerdo con las necesidades del servicio y la priorización definida por la Entidad.
327	Seccion VI 3.4	9. 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.	Se considera necesario que la Entidad aclare de manera detallada la cantidad de casos de uso de monitoreo a nivel de SOAR que el proveedor debe configurar en todo el contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los casos de uso, playbooks o automatizaciones asociadas a SOAR deberán definirse e implementarse conforme al modelo de operación, los casos de uso priorizados, las capacidades de la solución y las necesidades que establezca la Entidad durante la implementación y operación del servicio.
328	Seccion VI 4.1	10. Deberá proveer los canales de comunicaciones que requiera en un esquema redundante entre las multinubes y los sitios on premises de la DIAN y el sitio del SOC donde se presten los servicios	Se considera necesario que la Entidad confirme si en cada una de las nubes públicas y privada cuenta con firewalls que permitan configurar VPN Site to Site, con el fin de enviar la información de seguridad al SOC en caso de ser necesario.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la Entidad cuenta con infraestructura de seguridad y conectividad que permite habilitar mecanismos seguros de comunicación, incluyendo esquemas tipo VPN Site to Site cuando técnica y operativamente resulte aplicable. No obstante, el contratista deberá proveer los canales de comunicación que requiera para la prestación del servicio, en esquema redundante, conforme a lo establecido en los documentos del proceso. Los detalles técnicos de conectividad, integración, configuración y seguridad serán definidos durante la fase de implementación, de acuerdo con la arquitectura autorizada por la Entidad y los controles de seguridad aplicables.
329	Pág 112 Sección VI 410-Solicitud-de-Oferta-VSD-SdO-SOC	14. Todas las herramientas que se incluyan en el diseño de la estrategia de presentación del servicio SOC deberán contar con un análisis de confianza del ciclo de vida de la tecnología.	Se considera necesario que la Entidad aclare y amplie la expectativa de este requerimiento. No es claro lo que se requiere, y puede considerarse como ambigüedad en el contrato		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento implica mencionar: * Qué garantías de continuidad, seguridad, soporte técnico y actualizaciones ofrece el fabricante o proveedor. * Si existen riesgos asociados (por ejemplo, productos ya descontinuados o sin soporte), entre otros.
330	Pág 112 Sección VI 410-Solicitud-de-Oferta-VSD-SdO-SOC	3. Deberá realizar las integraciones necesarias entre los servicios y capacidades de SOC adquiridas y las herramientas o sistemas informáticos externos que se requieran.	Se considera necesario que la Entidad aclare y liste las herramientas o sistemas informáticos externos que se requieran con el fin de evitar ambiguedades.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las herramientas o sistemas mencionados se refieren a la infraestructura tecnológica descrita en las tablas de inventario que se encuentran detalladas en el mismo documento.
331	Pág 112 Sección VI 410-Solicitud-de-Oferta-VSD-SdO-SOC	5. Deberá realizar las pruebas para verificar la adecuada funcionalidad y en caso de no lograrlo, deberá realizar los ajustes y probar nuevamente hasta que sean exitosas.	Se considera necesario que la Entidad aclare y liste las pruebas requeridas para verificar la adecuada funcionalidad con el fin de evitar ambiguedades.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la actividad en mención hace parte de la fase de implementación y se refiere a las diferentes pruebas que deberá hacer el futuro proveedor para poner en operación los servicios o capacidades solicitadas.
332	Pág 113 Sección VI 410-Solicitud-de-Oferta-VSD-SdO-SOC	12. Deberá incluir en la operación, el servicio de auditorías de código sobre las aplicaciones de la DIAN.	Por favor confirmar la cantidad de aplicaciones y lineas de codigo por cada una de ellas. Adicionalmente, la periodicidad requerida		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la cantidad de aplicaciones son 50 y las características de este servicio están detalladas en el anexo técnico.
333	Pág 114 Sección VI 410-Solicitud-de-Oferta-VSD-SdO-SOC	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.	Se entiende que el proveedor no cierra las vulnerabilidades. Sin embargo, si acompaña y asesora a la DIAN en el proceso de cierre. Es correcto neustro entendimiento.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, su entendimiento es correcto, el proveedor del SOC realiza acompañamiento, apoyo, soporte, recomendaciones, entre otros para lograr que los administradores de la infraestructura tecnológica de la DIAN realicen el pertinente cierre de vulnerabilidades.
334	Pág 116 Sección VI 410-Solicitud-de-Oferta-VSD-SdO-SOC	• Se deberá presentar en un término no superior a diez (10) días hábiles a la manifestación de solicitud de cambio, la hoja de vida del candidato que cumpla el perfil requerido debidamente soportado, para que la interventoría adelante la evaluación y aprobación escrita correspondiente.	Se solicita ampliar el término a veinte (20) días habiles		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
335	Pág 120 Sección VI 410-Solicitud-de-Oferta-VSD-SdO-SOC	Cumplimiento en tiempo de contencion ó solución de incidentes	Teniendo en cuenta que 7. La gestión de las infraestructuras de seguridad informática tales como firewall, IPS, DDoS, antivirus, VPN, WAF, etc, estará a cargo de la DIAN a través de DGIT. Ssolicitamos modificar el ANS por: Cumplimiento en tiempo de contencion.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
336	Pág 122 Sección VI 410-Solicitud-de-Oferta-VSD-SdO-SOC	22) El CONTRATISTA deberá considerar dentro de su propuesta económica todos los valores asociados al desarrollo del proyecto incluyendo los derivados de herramientas, desarrollos e integraciones con sistemas ya existentes o similares, personal, infraestructura, recursos ofimáticos y administrativos, entre otros.	Se considera indispensable señalar que la correcta estructuración de una propuesta económica integral, coherente y responsable depende directamente de la disponibilidad, claridad y completitud de la información técnica y funcional suministrada por la DIAN, particularmente aquella relacionada con: inventarios definitivos, arquitecturas objetivo, sistemas existentes, modelos de integración, flujos de operación, responsabilidades y alcances esperados. En este sentido, se solicita que la DIAN entregue y confirme de manera clara, expresa y no ambigua la totalidad de la información solicitada por los oferentes a través de las preguntas formuladas en el proceso, dado que la ausencia, ambigüedad o indeterminación de dicha información impide estimar con precisión los costos asociados a desarrollos, integraciones y demás componentes exigidos, y podría dar lugar a diferencias de interpretación en consecuencia desviaciones en costos del proyecto o ejecución del contrato, llevando al no cumplimiento de este punto		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la información con el detalle en especifico de la infraestructura tecnológica de la Entidad se encuentra detallada en los documentos del proyecto, la cual se considera amplia y suficiente para que los diferentes interesados puedan confeccionar sus ofertas.
337	Pág 122 Sección VI 410-Solicitud-de-Oferta-VSD-SdO-SOC	10. Forma de pago Capacidades de la fase 1 y 2 Capacidades de la 1 a la 13 Entregables Hito de pago	Se solicita que la Entidad defina de manera clara, expresa y verificable, para cada componente solicitado, fase, capacidad o componente del proyecto, los entregables específicos, medibles y auditables que deberán cumplirse como condición para el recibo a satisfacción y la habilitación del pago correspondiente. En particular, se solicita precisar, como mínimo, para cada hito de pago: Entregables concretos (documentos, configuraciones, plataformas operativas, reportes, evidencias técnicas, actas, entre otros). Criterios objetivos de aceptación, que permitan verificar de manera inequívoca el cumplimiento del entregable (funcionalidad, cobertura, disponibilidad, calidad, evidencias). Responsable del proceso de validación y aceptación por parte de la DIAN. Mecanismo formal de aprobación, incluyendo acta de aceptación o documento equivalente.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el detalle y la información de los pagos se encuentra claramente definida en los ítems de pago del documento SDO, así mismo, que cada uno de los servicios o capacidades entregadas se pagará a su puesta en operación junto con el respectivo informe del detalle de dicha implementación.
338	Pág 160 Sección VI 410-Solicitud-de-Oferta-VSD-SdO-SOC	CGC 16.1 La forma y condiciones de pago al Contratista en virtud del Contrato serán las siguientes:	Se solicita que la Entidad defina de manera clara, expresa y verificable, para cada componente solicitado, fase, capacidad o componente del proyecto, los entregables específicos, medibles y auditables que deberán cumplirse como condición para el recibo a satisfacción y la habilitación del pago correspondiente. En particular, se solicita precisar, como mínimo, para cada hito de pago: Entregables concretos (documentos, configuraciones, plataformas operativas, reportes, evidencias técnicas, actas, entre otros). Criterios objetivos de aceptación, que permitan verificar de manera inequívoca el cumplimiento del entregable (funcionalidad, cobertura, disponibilidad, calidad, evidencias). Responsable del proceso de validación y aceptación por parte de la DIAN. Mecanismo formal de aprobación, incluyendo acta de aceptación o documento equivalente.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el detalle y la información de los pagos se encuentra claramente definida en los ítems de pago del documento SDO, así mismo, que cada uno de los servicios o capacidades entregadas se pagará a su puesta en operación junto con el respectivo informe del detalle de dicha implementación.
339	4.4	La solución entregada deberá ser implementada, configurada y puesta en marcha para monitorear todas las bases de datos de la Entidad, de acuerdo con el inventario de bases de datos que se encuentra en este archivo en la hoja "Inventario Infraestructura IT".	Solicitamos a la entidad aclarar si para la solucion de proteccion de bases de datos se requiere despliegues en alta disponibilidad		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el futuro proveedor del SOC deberá entregar todos y cada uno de los servicios requeridos por la Entidad, así como también brindar los diferentes esquemas de disponibilidad para brindar servicios en esquemas de 7x24x365.
340	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.	Solicitamos a la entidad confirmar la periodicidad de las pruebas en cada una de las 50 aplicaciones		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se realizan bajo demanda o cada vez que la Entidad las requiera.
341	9.3	Se debe licenciar como mínimo para 260 activos públicos o equivalente o similar de acuerdo con la tecnología ofrecida.	Solicitamos a la entidad compartir cada uno de las marcas asociadas a la DIAN que requiere que el proveedor monitoree		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el servicio solicitado debe licenciarse para 260 activos públicos.
342	2.4	Número de dispositivos (2467), métricas de rendimiento basadas en EPS (25.000 EPS)	Se solicita aclarar que los valores establecidos como referencia para el dimensionamiento del SIEM, tales como número de dispositivos (2467), métricas de rendimiento basadas en EPS (25.000 EPS) u otras unidades de medida, deben entenderse como parámetros referenciales y no restrictivos, permitiendo la participación de tecnologías SIEM que utilicen modelos alternativos de licenciamiento y dimensionamiento (por ejemplo, por volumen de datos, nodos de cómputo, capacidad de procesamiento o métricas equivalentes), siempre que se garantice un desempeño igual o superior al requerido.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y cantidades solicitadas son mínimas, así mismo, el mismo ítem acepta equivalencia siempre y cuando se cumpla con lo requerido por la Entidad.
343	2.30 - 2.8	CMDB	Se solicita eliminar el requerimiento de CMDB ya que no implica la obligación de que la solución SIEM cuente con una CMDB propietaria.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
344	2.21	PCI, HIPAA, SOX, NERC, FISMA, GLBA, US GPG, SANS	Se solicita aclarar que la exigencia de informes de cumplimiento "out-of-the-box" deberá interpretarse como la capacidad de generar reportes alineados a marcos de control reconocidos, y no como la obligación de contar con plantillas predefinidas específicas, siempre que la solución permita su construcción y personalización para el marco regulatorio aplicable a la DIAN.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
345	3.30	Incorpore gestión de casos, dashboards, IOC store, RCA, PIA, SLA multinivel, kill chain, análisis gráfico, etc.	Se solicita aclarar que los requerimientos funcionales descritos para la plataforma SOAR podrán ser satisfechos de manera nativa o mediante integraciones plenamente soportadas, siempre que la experiencia de operación, correlación, automatización y gestión de incidentes sea integrada y transparente para el analista, evitando interpretaciones que restrinjan la evaluación únicamente a soluciones monolíticas específicas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
346	3.52	La solución debe tener al menos 300 playbooks preconfigurados	Se solicita aclarar que el número mínimo de playbooks preconfigurados debe entenderse como un indicador referencial de madurez, y no como un criterio restrictivo, permitiendo la participación de soluciones que ofrezcan playbooks equivalentes o superiores en cobertura funcional, priorizando la capacidad de desarrollo, adaptación y personalización de playbooks orientados a los casos de uso reales de la DIAN, independientemente del conteo nominal.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y cantidades solicitadas son mínimas, por lo tanto, el futuro proveedor podrá entregar más o mayor número al solicitado.
347	3.70	La solución debe incluir al menos 300 conectores	Se solicita aclarar que el número de conectores preexistentes debe entenderse como referencial, y no como un requisito restrictivo, permitiendo la participación de soluciones SOAR que ofrezcan capacidades equivalentes o superiores de integración mediante APIs, SDKs y desarrollo de conectores personalizados, siempre que se garantice la interoperabilidad con los sistemas actuales y futuros de la DIAN, sin dependencia de un marketplace propietario.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y cantidades solicitadas son mínimas, por lo tanto, el futuro proveedor podrá entregar más o mayor número al solicitado.
348	3.14-3.58	HTML / JSON / JS Python SVN / GIT-like	Se solicita aclarar que la referencia a tecnologías específicas como HTML, JSON, JavaScript o Python deberá entenderse como ejemplo referencial, permitiendo el uso de lenguajes, frameworks o entornos equivalentes o superiores, siempre que se garantice la capacidad de automatización, personalización, auditoría y extensibilidad requerida.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y cantidades solicitadas son mínimas, por lo tanto, el futuro proveedor podrá entregar más o mayor número al solicitado, siempre y cuando se cumpla con lo solicitado.
349	3.33	RCA PIA Gestión completa del ciclo de vida SLA multinivel Kill Chain mapping	Se solicita aclarar que las capacidades avanzadas de gestión de incidentes podrán integrarse o interoperar con plataformas ITSM existentes, siempre que el SOAR permita la orquestación, automatización y trazabilidad de los incidentes de seguridad, evitando interpretaciones que exijan funcionalidades propias de plataformas ITSM completas como condición excluyente.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, su entendimiento es correcto.
350	4.8	La solución no deberá requerir agentes, pero deberá tener la opción en caso de ser necesario	Se solicita aclarar que el requerimiento de operación sin agentes deberá considerarse como preferencial, y no como una restricción excluyente, permitiendo el uso de agentes livianos, sensores o mecanismos equivalentes cuando sean necesarios por razones técnicas, de cifrado, entornos cloud o bases de datos gestionadas, siempre que no se afecte el desempeño ni la transparencia de las aplicaciones.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
351	4.54.10	Latencia menor a 5 ms en todo escenario	Se solicita aclarar que los parámetros de latencia y desempeño deberán evaluarse en condiciones comparables y reales de operación, considerando topología, cifrado, volumen de tráfico y arquitectura del entorno, evitando interpretaciones absolutas que favorezcan arquitecturas específicas y permitiendo soluciones que cumplan con niveles de desempeño adecuados sin afectar la disponibilidad y operación de las bases de datos.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
352	4.39	Nativo. DB2 z/OS, IMS, Netezza, Exadata, Teradata, SAP HANA, etc.	Se solicita aclarar que el listado de plataformas de bases de datos debe entenderse como referencial y no restrictivo, permitiendo soluciones que ofrezcan cobertura parcial o progresiva, priorizando aquellas bases de datos efectivamente utilizadas por la DIAN, y habilitando integraciones futuras conforme evolucione el inventario tecnológico de la Entidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
353	7.26	No se permitan tecnologías que hacen uso de reglas y/o firmas	Se solicita aclarar que el uso de inteligencia artificial y aprendizaje automático deberá entenderse como enfoque principal, permitiendo modelos de detección híbridos que combinen análisis de comportamiento, firmas, heurísticas y reglas adaptativas, siempre que se garantice una capacidad efectiva de detección de amenazas avanzadas, reducción de falsos positivos y mejora continua del contexto de seguridad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem 7.26 será ajustado, para evitar equívocos 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.
354	7.27	Narrativa en lenguaje natural Resumen automático de incidentes por IA	Se solicita aclarar que la generación de reportes narrativos automáticos deberá considerarse como una capacidad avanzada deseable, permitiendo soluciones que ofrezcan reportes estructurados con información técnica completa y contextual, aun cuando la narrativa ejecutiva sea generada de manera asistida por analistas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
355	1.3	Administración Operación de Pltaformas	Se considera necesario que la DIAN aclare de manera expresa y detallada el modelo de responsabilidad aplicable una vez finalizada la etapa de implementación, en particular respecto a si las plataformas y soluciones entregadas de: NDR - Detección y respuesta en red e Inteligencia de amenazas Postura de Seguridad infraestructura Cloud Consola de Administración de la Plataforma de Monitoreo de Bases de Datos Especificaciones Técnicas herramienta de protección de Bases de Datos Serán entregadas formalmente a la DIAN, quedando bajo su responsabilidad la administración, operación, soporte, mantenimiento y evolución de las mismas, o Permanecerán bajo la administración, soporte y operación del oferente, como parte de un servicio gestionado durante la vigencia contractual, o Se adoptará un modelo híbrido, en el cual determinadas funciones (por ejemplo, operación N1/N2/N3, administración de plataforma, soporte técnico, ajustes de configuración, actualización de versiones, atención de incidentes, entre otros) serán compartidas entre la DIAN y el proveedor. Así mismo, se solicita que la Entidad indique de forma clara: El punto de corte formal entre implementación y operación. Las responsabilidades específicas de cada parte durante la etapa de operación del SOC. Si la transferencia de conocimiento y documentación implica o no la transferencia total de la operación de las plataformas. El alcance del soporte técnico y mantenimiento posterior a la implementación, en caso de que la operación sea asumida parcial o totalmente por la DIAN.		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.
356	N/A	Cronograma	Solicitamos amplair la fecha de entrega de las ofertas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, de acuerdo con la Adenda No. 1, la fecha para la presentación de las ofertas quedó así: La fecha límite para presentar las ofertas es: Fecha: 9 de junio de 2026 Hora: hasta las 10:00 am (hora legal colombiana)
357	10.2 - 10.4	El alcance de los ejercicios de ethical hacking no se limita únicamente a los activos críticos de la entidad sino también a los que hacen parte del anexo de inventarios de éste proyecto. Aunque se priorizarán activos de relevancia en cada ejercicio, la selección de activos incluirá aquellos que la DIAN considere esenciales para evaluar la postura de seguridad de la infraestructura tecnológica en general. La determinación específica de los activos a incluir se hará en la fase de planeación de cada ejercicio, en conjunto con el contratista, de acuerdo con las necesidades de seguridad identificadas (como mínimo cien (100) activos).	Se solicita establecer el invertario final rqeuerido por la DIAN para hacer los ejercicios de Ethical Hacking, ya que la ausencia de esta definición vulnera los principios de igualdad y transparencia, al dejar a la interpretación de cada oferente la determinación de los activos a considerar, lo cual afecta la selección objetiva del proceso. Y adicionalmente encarece el proyecto por ambiguedades.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem en mención detalla que la cantidad mínima requerida para los ejercicios de ethical hacking es de 100 activos.
358	10	Los ejercicios a realizar deben ser de caja gris.	Se solicita confirmar si la entidad comparte roles y usuarioa para cada prueba. Confirmar cantidad de usuarios o roles a evaluar por cada aplicación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la descripción de las características requeridas para este servicio están claramente definidas en el ítem 10 del anexo técnico.
359	10.7	Para realizar los ejercicios de Ethical Hacking se debe disponer de un equipo como mínimo de tres (3) ingenieros con conocimientos en programación, sistemas operativos y estar certificados en hacking ético.	Se solicita a la DIAN, listar claramente los requerimientos de los tres ingenieros para ejecución de Ethical Hacking, en hoja de vida, certificaciones, experiencia y otros. Ya que la ausencia de esta definición vulnera los principios de igualdad y transparencia, al dejar a la interpretación de cada oferente la determinación de los activos a considerar, lo cual afecta la selección objetiva del proceso. Y adicionalmente encarece el proyecto por ambiguedades.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la descripción de las características requeridas para este servicio están claramente definidas en el ítem 10.7 del anexo técnico, donde se describen los conocimientos mínimos de los profesionales para atender estas actividades y claramente se describe que tienen que estar certificados en hacking ético.
360	10.9	1. Evaluar la postura de seguridad de la organización Simular ataques reales (Red Team) y medir la capacidad de detección y respuesta (Blue Team). Identificar vulnerabilidades técnicas, operativas y procedimentales en los sistemas y procesos del SOC.	Se solicita aclarar el alcance esperado de la evaluación de seguridad. Toda vez que los escenarios pueden ser tan complejos o simples como la DIAN lo requiera. Lo anterior se solicita ya que la ausencia de esta definición vulnera los principios de igualdad y transparencia, al dejar a la interpretación de cada oferente la determinación de los activos a considerar, lo cual afecta la selección objetiva del proceso. Y adicionalmente encarece el proyecto por ambiguedades.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la descripción de las características requeridas para este servicio están claramente definidas en el ítem 10.9 del anexo técnico, donde se describen las actividades mínimas a realizar.
361	10.9	2. Fortalecer las capacidades defensivas del SOC Permitir al Blue Team mejorar sus habilidades en detección, análisis, contención y recuperación ante incidentes. Validar la efectividad de herramientas como SIEM, SOAR, EDR, NDR, y CMDB en escenarios reales.	Se solicita aclarar el alcance esperado de la evaluación de seguridad. Toda vez que los escenarios pueden ser tan complejos o simples como la DIAN lo requiera. Lo anterior se solicita ya que la ausencia de esta definición vulnera los principios de igualdad y transparencia, al dejar a la interpretación de cada oferente la determinación de los activos a considerar, lo cual afecta la selección objetiva del proceso. Y adicionalmente encarece el proyecto por ambiguedades.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la descripción de las características requeridas para este servicio están claramente definidas en el ítem 10.9 del anexo técnico, donde se describen las actividades mínimas a realizar.
362	11.1	El CONSULTOR deberá realizar el diseño integral, la Instalación, Implementación, configuración y puesta en marcha de todas las soluciones ofertadas, así como los equipos ofertados tanto físicos como virtuales con personal profesional e idóneo para realizar las labores pertinentes.	Se solicita a la entidad aclarar y definir de manera expresa cual es la expectativa de personal profesional e idóneo. Esto asegura este requerimiento y permite al oferente cumplir correctamente este requerimiento,		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el personal referido aquí es el mínimo solicitado, y sus perfiles se encuentran detallados en la hoja Equipo Mínimo de Trabajo del archivo anexo técnico.
363	11.7	Se deberá garantizar soporte y garantía para las plataformas ofertadas en un esquema 7 x 24 x 365 por tres (3) años.	Se solicita que la Entidad aclare de manera expresa, detallada y no ambigua el modelo de servicio esperado, con el fin de asegurar homogeneidad en el dimensionamiento de recursos, igualdad en la estructuración económica y comparabilidad objetiva entre las propuestas. En particular, se solicita precisar si el esquema requerido corresponde a alguno de los siguientes modelos, u otro definido formalmente por la DIAN: Malla operativa 7x24 dedicada, garantizando la disponibilidad permanente de personal asignado para cada plataforma o tecnología (por ejemplo, SIEM, SOAR, NDR, entre otras). Modelo 5x8 con disponibilidad 7x24, donde la atención fuera del horario hábil se cubra bajo esquemas de guardia, turnos pasivos o escalamiento bajo demanda. Modelo híbrido, combinando recursos dedicados en horario extendido con esquemas de soporte especializado bajo activación. Así mismo, se solicita aclarar: Si la exigencia de cobertura 7x24 implica presencia continua de personal activo o únicamente capacidad de atención y respuesta garantizada. Si el modelo aplica por plataforma, por servicio o de forma transversal a toda la solución SOC. Los niveles de atención esperados (N1, N2, N3) y su relación con el esquema horario definido. La presente observación tiene carácter estrictamente aclaratorio y tiene como finalidad evitar interpretaciones disímiles del alcance del servicio, garantizar condiciones equitativas de dimensionamiento técnico y económico entre oferentes, y asegurar la correcta evaluación de las propuestas por parte de la DIAN.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el modelo de atención es 7x24x365 con el personal requerido como equipo mínimo de trabajo, se requiere atención en sitio con uno de los perfiles solicitados allí en horario de 5x8.
364	11.9	Todos los elementos necesarios para la implementación de cualquiera de las capacidades requeridas por la Entidad en este proyecto, debe ser provista por el futuro oferente, entendiéndose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones. Recordando que se deberá suministrar los recursos necesarios (rack/s, conexiones, entre otros) para la instalación y configuración de dispositivos colectores (en caso de ser necesario) en las diferentes sedes de la Entidad, ya sean físicos o virtuales. De acuerdo con la arquitectura y topología diseñada, y que sea aprobada por la supervisión del contrato en concordancia con las mejores prácticas recomendadas por el fabricante).	Se solicita aclaración detallada de parte de la entidad de lo que requiere a nivel de recursos como (rack/s, conexiones, entre otros) para la instalación y configuración de dispositivos colectores (en caso de ser necesario) en las diferentes sedes de la Entidad, ya sean físicos o virtuales. Es imprescindible esta imformación para lograr un servicio llave en mano, de lo contrario, el proveedor no puede garantizar la totalidad de recursos necesarios para llevar a cabo el proyecto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el detalle dado en el ítem es amplio y suficiente para que los interesados puedan dimensionar su oferta, y su aplicación depende del mismo proveedor de como realizaría su implementación.

365	11.12	Todo el cableado eléctrico, lógico, patchs cords, conectores, patch panels y demás elementos y accesorios necesarios para la instalación deben ser provistos para la prestación de los servicios. Se debe entender que es un contrato llave en mano, donde todos los componentes de las soluciones deben estar a cargo del contratista.	Se solicita aclaración detallada de parte de la entidad de lo que requiere a nivel de recursos como todo el cableado eléctrico, lógico, patchs cords, conectores, patch panels y demás elementos y accesorios necesarios para la instalación Es imprescindible esta imformación para lograr un servicio llave en mano, de lo contrario, el proveedor no puede garantizar la totalidad de recursos necesarios para llevar a cabo el proyecto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el detalle dado en el ítem es amplio y suficiente para que los interesados puedan dimensionar su oferta, y su aplicación depende del mismo proveedor de como realizaría su implementación.
366	12.6	Dispositivos Adicionales: La Entidad solicitará incluir la cantidad de dispositivos adicionales que requiera hasta ocupar todo el licenciamiento de la herramientas y servicios adquiridos (SIEM, SOAR, NDR, Gestión de Vulnerabilidades, protección de bases de datos, entre otras).	Se solicita aclarar cuales son las herramientas y/o licenciamientos cuando la entidad menciona el término "entre otras"		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, "entre otras" se refiere a los demás servicios solicitados para el proyecto SOC, hasta copar la cantidad mínima requerida de activos, de licenciamiento, de dispositivos, etc.
367	12.8	Se deberá realizar la integración de la herramienta GRC de NOVASEC propiedad de la DIAN con la plataforma SOAR, cuya función sea alimentar los riesgos de los controles tecnológicos de la ISO 270001 de modo tal que ante cualquier cambio en las herramientas que soportan estos controles sea informado al sistema GRC.	Se solicita aclarar la fecha de fin de soporte de la herramienta GRC de NOVASEC propiedad de la DIAN		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la herramienta GRC de la Entidad cuenta con el soporte amplio y suficiente y lo tendrá en el momento de realizar la integración.
368	19.2.7	Se debe gestionar y canalizar las alertas a los diferentes grupos de interés y partes interesadas. Definir los casos de uso (eventos externos), sobre posibles ataques de ciberseguridad que se lleguen a presentar, estos casos de uso se deberán realizar entre el contratista y la DIAN. Definir los casos de uso (eventos internos), generados por los usuarios al interior de la DIAN. ANS Tiempo máximo para solución definitiva.	Se solicita eliminar el ANS de Tiempo máximo para solución definitiva, ya que la solución definitiva de un incidente no solo depende del proveedor, sino y en mas relevancia de la DIAN. Esta dependencia imposibilita el cumplimiento de este ANS.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
369	7.3	Licenciamiento para 25.000 activos que incluyen PCs, infraestructura y aplicaciones web	Agradecemos confirmar si dentro de los 25.000 activos se incluyen dispositivos OT/IoT y su nivel de criticidad	Aclarar el alcance exacto de los activos a monitorear (IT, OT, IoT)	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, dentro los activos está incluida toda la infraestructura tecnológica de la Entidad
370	7.3	Licenciamiento NDR para hasta 25.000 activos	Agradecemos precisar si el número de activos NDR es fijo o podrá incrementarse durante la vigencia sin ajuste contractual	Establecer si existe crecimiento esperado o límite máximo contractual de activos NDR	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la cantidad mínima requerida es de 25000 activos, no "hasta"
371	Equipo Mínimo de Trabajo	Se define equipo mínimo para operación SOC 7x24x365.	Agradecemos indicar si el equipo mínimo definido debe ser 100% dedicado a la DIAN o puede operar bajo modelo compartido, dado el impacto económico directo.	Aclarar explícitamente el modelo de dedicación del equipo SOC.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el equipo mínimo de trabajo solicitado es con dedicación del 100% al proyecto SOC de la DIAN, no es compartido.
372	1.2	SOC ubicado físicamente en Bogotá.	Agradecemos confirmar si el SOC físico debe ser exclusivo para la DIAN o compartido con otros clientes del contratista.	Precisar si se exige exclusividad física del SOC para la Entidad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, no se exige exclusividad física del SOC para la Entidad.
373	10	Se requieren seis (6) ejercicios de Ethical Hacking.	Agradecemos detallar el alcance de cada ejercicio (red interna, externa, aplicaciones, nube), dado que el esfuerzo varía significativamente según el tipo de prueba.	Definir alcance técnico detallado por cada ejercicio de Ethical Hacking, asi como numero de IPs a realizar pruebas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características de este servicio están claramente detalladas en el ítem 10 del anexo técnico.
374	9.3	Cobertura de hasta 260 aplicaciones web	Agradecemos confirmar si se incluyen APIs, microservicios, autenticación avanzada y aplicaciones críticas de alta disponibilidad	Detallar tipología de aplicaciones incluidas en el alcance DAST/SAST	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la cobertura es como mínimo para 260 aplicaciones web
375	19	Se establecen tiempos de atención y resolución de incidentes.	Agradecemos confirmar si los SLA aplican de forma homogénea a todos los activos o diferenciados según criticidad del activo o servicio.	Definir esquema de SLA por niveles de criticidad para una aplicación proporcional del servicio.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
376	N/A	Penalidades por incumplimiento de ANS.	Agradecemos aclarar si las penalidades aplican de forma acumulativa entre diferentes servicios o de manera individual.	Especificar el mecanismo de aplicación de penalidades para evitar interpretaciones ambiguas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los mecanismos y penalidades están descritos en el documento "410-Solicitud-de-Oferta-VSD-SdO-SOC" página 119. ítem 8. ANS.
377	N/A	Se entiende el contrato como llave en mano.	Agradecemos confirmar que los alcances están limitados estrictamente a lo descrito en el pliego y anexos, y que no se considerarán obligaciones implícitas no documentadas.	Incluir cláusula de delimitación de alcance basada exclusivamente en lo definido en el pliego.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los requerimientos, obligaciones y demás detalle del proyecto SOC están en los documentos publicados.
378	Equipo Mínimo de Trabajo	Se especifica un equipo mínimo con perfiles altamente especializados.	Agradecemos a la Entidad confirmar si para los roles definidos se aceptan perfiles equivalentes, que acrediten experiencia y competencias técnicas demostrables, aun cuando no cuenten con certificaciones o denominaciones idénticas.	Permitir equivalencia de perfiles basada en experiencia comprobada y competencias técnicas, manteniendo el cumplimiento funcional del rol.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
379	Equipo Mínimo de Trabajo	Se definen roles separados para monitoreo, análisis, hunting y respuesta.	Agradecemos confirmar si algunos de los roles descritos pueden ser cubiertos bajo un modelo de roles escalonados, donde un mismo recurso cuente con competencias para asumir más de una función según la fase del servicio.	Permitir un modelo de roles escalonados o multifuncionales, garantizando cumplimiento de SLA y continuidad del servicio.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
380	Equipo Mínimo de Trabajo	Se exigen perfiles especializados por nivel (N1, N2, N3).	Agradecemos confirmar si los niveles de analistas SOC pueden definirse con base en responsabilidades operativas y experiencia práctica, y no exclusivamente por certificaciones formales.	Autorizar clasificación de analistas SOC por funciones y experiencia, aceptando certificaciones equivalentes o experiencia demostrada.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
381	Equipo Mínimo de Trabajo	Se exige un perfil dedicado de Threat Hunter.	Agradecemos confirmar si la función de Threat Hunting puede ser desempeñada por perfiles de Analista SOC Senior / N3, con experiencia comprobada, cuando la demanda operativa así lo permita.	Permitir que las funciones de Threat Hunting sean asumidas por analistas senior con competencias equivalentes.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
382	Equipo Mínimo de Trabajo	Se establece un rol especializado de respuesta a incidentes.	Agradecemos confirmar si las funciones de respuesta a incidentes pueden ser cubiertas por perfiles SOC N3 o líderes técnicos, certificados o con experiencia directa en manejo de incidentes.	Autorizar equivalencia entre perfiles de IR y SOC senior para la ejecución de estas funciones.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
383	Equipo Mínimo de Trabajo	Se exige un conjunto específico de certificaciones por rol.	Agradecemos indicar si se aceptan certificaciones equivalentes reconocidas internacionalmente o combinaciones de experiencia y certificación, bajo el principio de equivalencia técnica.	Permitir certificaciones equivalentes o experiencia demostrada como criterio válido de cumplimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
384	Equipo Mínimo de Trabajo	Se hace referencia a recursos dedicados al 100 %.	Agradecemos confirmar si la dedicación de los recursos puede gestionarse mediante un modelo de dedicación funcional, garantizando cobertura, SLA y continuidad, sin requerir exclusividad absoluta permanente.	Autorizar modelo de dedicación funcional que asegure cumplimiento del servicio sin requerir exclusividad rígida.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el equipo mínimo de trabajo solicitado es con dedicación del 100% al proyecto SOC de la DIAN, no es compartido.
385	Equipo Mínimo de Trabajo	Se exige disponibilidad continua 7x24x365.	Agradecemos confirmar si la cobertura 7x24 puede lograrse mediante esquemas de turnos rotativos y respaldo cruzado entre recursos, evitando la sobrededicación de perfiles altamente escasos.	Permitir esquemas de turnos y respaldo cruzado que garanticen la disponibilidad continua.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, tal como se describe en el anexo técnico - equipo mínimo de trabajo, se permiten los turnos y respaldo cruzado que garantizan la disponibilidad continua.
386	Equipo Mínimo de Trabajo	Se exige un rol de gobierno especializado.	Agradecemos confirmar si el rol de gobierno del SOC puede ser desempeñado por un Líder SOC o Arquitecto de Seguridad, con experiencia en gestión y gobernanza.	Aceptar perfiles de liderazgo técnico con experiencia en gobierno SOC como equivalentes funcionales.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas obedecen a necesidades puntuales de la Entidad, por lo tanto, no es posible aceptar su sugerencia.
387	15.1	Se exige transferencia de conocimiento continua.	Agradecemos confirmar si la transferencia de conocimiento puede ser realizada por el equipo técnico involucrado en la operación, y no únicamente por perfiles altamente especializados.	Permitir que la transferencia de conocimiento sea realizada por recursos operativos con experiencia comproba	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas para la transferencia de conocimiento están descritas en el ítem 15.1 y su cumplimiento puede ser con el personal que estime el operador del SOC, siempre y cuando se cumplan con las características solicitadas por la Entidad.
388		La gestión de infraestructuras de seguridad (Firewall, IPS, WAF, etc.) estará a cargo de la DIAN	Pregunta: Por favor aclarar ¿ cuál es el alcance exacto del SOC frente a las plataformas de seguridad existentes (Firewall, IPS, WAF, etc.), específicamente si el contratista tendrá acceso de solo monitoreo o también capacidades de configuración, tuning y respuesta activa (ej. bloqueo, cuarentena)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las plataformas en mención son propiedad de la DIAN, por lo tanto, su administración sólo es competencia de la Entidad.
389		Realizar integraciones necesarias con herramientas o sistemas externos	Pregunta: Por favor aclarar ¿ cuál es el inventario detallado de herramientas de seguridad y TI a integrar (SIEM, EDR, NDR, IAM, nube, etc.), incluyendo versiones, fabricantes y mecanismos de integración disponibles (API, syslog, agentes)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el detalle y demás características de la infraestructura tecnológica de la Entidad se encuentran en el documento publicado de nombre "410-Solicitud-de-Oferta-VSD-SdO-SOC"
390		Modelo tipo llave en mano con licenciamiento elástico	Pregunta: Por favor aclarar ¿ el modelo de licenciamiento esperado debe ser 100% provisto por el contratista (tipo MSSP) o coexistirá con licencias actuales de la DIAN (BYOL)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el licenciamiento solicitado así como los servicios requeridos deberán ser provistos por el futuro contratista.
391		Debe incorporar capacidades y servicios mínimos	Pregunta: Por favor aclarar ¿ existe un listado detallado y obligatorio de capacidades SOC (ej. SIEM, SOAR, UEBA, Threat Intelligence, DFIR) que deban incluirse, o queda a criterio del proponente siempre que cumpla los objetivos funcionales?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, todos los servicios y capacidades requeridas deberán monitorear y cubrir toda la infraestructura tecnológica de la Entidad, de acuerdo al inventario estipulado en los documentos publicados.
392		Herramientas actuales no cubren capacidades críticas	Pregunta: Por favor aclarar ¿ cuáles herramientas de seguridad actualmente posee la DIAN (SIEM, EDR, NDR, etc.) y cuáles deben ser reemplazadas vs integradas en el nuevo SOC?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, todos los servicios y capacidades requeridas deberán cubrir y monitorear toda la infraestructura tecnológica de la Entidad, de acuerdo al inventario estipulado en los documentos publicados.
393		Monitoreo 24/7 y correlación avanzada	Pregunta: Por favor aclarar ¿ cuál es la volumetría estimada actual (EPS, GB/día, número de eventos) que deberá soportar el SOC, incluyendo crecimiento proyectado?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la volumetría estimada actual es de 25000 EPS tal cual como se estipula en los documentos técnicos del proceso.
394		Alineado con ISO 27001, NIST, MITRE ATT&CK	Pregunta: Por favor aclarar ¿ se requiere certificación formal del SOC bajo ISO 27001 o únicamente alineación metodológica a los controles?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el criterio de certificaciones es puntuable más no obligatorio, en el entendido de que el interesado podrá hacerse acreedor a dicha puntuación, siempre y cuando entregue las debidas certificaciones solicitadas para el SOC (FIRST, ISO 27001, ISO 22301 entre otras).
395		Levantamiento de información para aspectos no incluidos	Pregunta: Por favor aclarar ¿ cuáles son los entregables mínimos esperados del diagnóstico inicial (ej. assessment de madurez SOC, gap analysis, roadmap)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, para la etapa en mención se deberá entregar el respectivo informe teniendo en cuenta como mínimo, situación actual, análisis de brechas, evaluación tecnológica, entre otras.
396		Debe permitir crecimiento futuro	Pregunta: Por favor aclarar ¿ cuál es la proyección de crecimiento esperada (usuarios, endpoints, logs, aplicaciones críticas) durante la vigencia del contrato?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los crecimientos futuros están dimensionados dentro de las cantidades solicitadas para cada uno de los servicios requeridos.
397		Implementar casos de uso y umbrales	Pregunta: Por favor aclarar ¿ la DIAN proporcionará un catálogo base de casos de uso (use cases) o se espera que el contratista los diseñe completamente desde cero?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, para los casos de uso, se tendrán que diseñar desde cero.
398		Operación bajo modelo definido	Pregunta: Por favor aclarar ¿ cuáles son los SLA/OLA esperados para monitoreo, detección, respuesta y contención de incidentes (tiempos de atención por criticidad)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los diferentes ANS están detallados en el documento publicado de nombre 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN.
399		OSI define casos de uso, escalamiento, etc.	Pregunta: Por favor aclarar ¿Exite un modelo de modelo de responsabilidad (RACI) entre la DIAN y el contratista en la gestión de incidentes (detección, análisis, respuesta y cierre)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las responsabilidades detalladas se encuentran en el documento publicado de nombre 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN, sin embargo, se aclara que el futuro contratista del SOC deberá realizar el respectivo apoyo y acompañamiento durante todo el proceso de la incidencia, desde su inicio hasta su resolución.
400		OSI coordina respuesta a incidentes	Pregunta: Por favor aclarar ¿ el contratista podrá ejecutar acciones de contención automática (SOAR) o todas las acciones deberán ser aprobadas por la DIAN?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, podrá ejecutar acciones de contención automática, sin embargo, habrán situaciones donde se requerirá de la aprobación de la Entidad.
401		Aprovisionamiento de herramientas	Pregunta: Por favor aclarar ¿ existe preferencia o restricción de fabricantes (vendor lock-in) para las soluciones de seguridad a implementar (SIEM, SOAR, EDR, etc.)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no existen restricciones, sin embargo, se aclara que se deberán cumplir todas y cada una de las características requeridas por la Entidad.
402		Entrega de logs últimos 6 meses	Pregunta: Por favor aclarar ¿ cuál es la política de retención de logs durante la operación (hot, warm, cold storage) y si existen requerimientos regulatorios específicos?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características de retención de logs y su descripción están detalladas en el documento publicado de nombre 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN.
403	si	Cadena de custodia y evidencias digitales	Pregunta: Por favor aclarar ¿ se requiere cumplimiento específico con normas forenses (ej. ISO 27037, cadena de custodia legal) para la gestión de evidencias?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el detalle de las especificaciones se encuentra en el documento publicado de nombre 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN.
404		Tiempo máximo 4 meses	Pregunta: Por favor aclarar ¿ el plazo de 4 meses incluye adquisición, licenciamiento, implementación, integración, pruebas y puesta en producción completa del SOC?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, su entendimiento es correcto, el tiempo de implementación es de cuatro (4) meses finiquitando con la puesta en producción de los servicios requeridos.
405		Incluye vulnerabilidades, forense, ciberinteligencia	Pregunta: Por favor aclarar ¿El servicio y la gestión forence son servicios obligatorios dentro del alcance o opcionales?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los servicios solicitados son de obligatorio cumplimiento, el detalle de las especificaciones se encuentra en el documento publicado de nombre 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN.
406		On-premise y multinube híbrida	Pregunta: Por favor aclarar ¿ cuáles plataformas cloud están en alcance (AWS, Azure, GCP, nube privada) y si se requiere cobertura multicloud nativa?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el detalle de la infraestructura tecnológica se encuentra especificado en el documento "410-Solicitud-de-Oferta-VSD-SdO-SOC"
407		Definir y medir indicadores	Pregunta: Por favor aclarar ¿ cuáles son los KPIs obligatorios del SOC (ej. MTTR, MTTD, tasa de falsos positivos, cobertura MITRE ATT&CK)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, dentro de los documentos solicitados el futuro contratista deberá detallar las métricas, indicadores, entre otros, para el futuro SOC.
408		Equipo especializado requerido	Pregunta: Por favor aclarar ¿ cuál es la cantidad mínima de recursos por rol (N1, N2, N3, Threat Hunter, DFIR, etc.) exigidos en dedicación total para el presente proceso actual?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el equipo mínimo de trabajo está detallado en el documento anexo técnico.
409		Cálculo de ROSI	Pregunta: Por favor aclarar ¿ existe un modelo o framework definido por la DIAN para el cálculo del ROSI o debe ser propuesto completamente por el oferente?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, debe ser propuesto por los interesados
410		Integraciones externas	Pregunta: Por favor aclarar ¿ existen restricciones de conectividad, seguridad o segmentación de red que puedan limitar la integración y deban se tenidos en cuenta por parte del SOC con sistemas críticos?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se darán todos los permisos necesarios para la implementación del SOC por parte del futuro contratista.
411		SOC continuo	Pregunta: Por favor aclarar ¿ se requiere esquema de alta disponibilidad (HA/DR) del SOC y en qué niveles (activo-activo, activo-pasivo, geográfico)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se requiere alta disponibilidad para el futuro SOC, los niveles los propondrá el futuro contratista.
412		Levantamiento de información complementario	Pregunta: Por favor aclarar ¿ el levantamiento de información incluye acceso a ambientes productivos, logs históricos y configuraciones actuales o se limitará a información documental suministrada por la DIAN?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el levantamiento de información lo hará el contratista, y se darán los permisos amplios y suficientes por parte de la Entidad para su acceso.
413		Arquitectura de seguridad de la información	Pregunta: Por favor aclarar ¿ se espera que la arquitectura SOC sea centralizada, distribuida o híbrida (on-premise + cloud), y si existe alguna restricción de ubicación de componentes críticos?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el SOC del contratista deberá estar ubicado en la ciudad de Bogotá, las otras locaciones no tienen restricción, siempre y cuando se cumpla con lo requerido por la Entidad.
414		Infraestructura on-premise y multinube híbrida	Pregunta: Por favor aclarar ¿ cuál es la distribución actual de cargas (porcentaje on-premise vs nube) y qué servicios críticos deben priorizarse en el monitoreo?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el detalle de la infraestructura tecnológica se encuentra especificado en el documento "410-Solicitud-de-Oferta-VSD-SdO-SOC"
415		Integraciones SOC	Pregunta: Por favor aclarar ¿ se cuenta con un bus de integración, SIEM actual o plataforma de orquestación existente que deba reutilizarse obligatoriamente?		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.
416		Operación continua	Pregunta: Por favor aclarar ¿ el servicio SOC requerido es completamente 7x24x365 desde el inicio o se contempla una fase de madurez progresiva mientras su implementación inicial?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los servicios del futuro SOC requeridos, deberán trabajar ininterrumpidamente por el tiempo solicitado a partir de la puesta en producción de cada uno de ellos.
417		OSI define escalamiento	Pregunta: Por favor aclarar ¿ existen matrices de escalamiento ya definidas o deben ser diseñadas por el contratista incluyendo niveles técnicos, ejecutivos y legales?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, deben ser diseñadas por los interesados
418		Contención y mitigación	Pregunta: Por favor aclarar ¿ el contratista tendrá autoridad para ejecutar acciones de contención en endpoints, red o identidad (ej. aislamiento EDR, bloqueo IP, deshabilitación de usuarios)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, únicamente se dará autorización de bloqueos, contenciones, aislamiento previa autorización de la DIAN.
419		Seguridad de la información	Pregunta: Por favor aclarar ¿ existen políticas de Zero Trust o modelo de identidad (IAM/PAM) vigente que deban integrarse al SOC?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, deben cumplirse con todas las características solicitadas en el anexo de características técnicas.
420		Entrega de logs 6 meses	Pregunta: Por favor aclarar ¿ la DIAN exige que los datos del SOC permanezcan dentro del territorio nacional (soberanía de datos) o se permite procesamiento en nube internacional?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se permiten procesamiento en nubes internacionales siempre y cuando se cumpla con lo solicitado por la Entidad.
421		Logs y eventos	Pregunta: Por favor aclarar ¿ se requiere normalización bajo algún estándar específico (CEF, LEEF, JSON, OpenTelemetry)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, deben cumplirse con todas las características solicitadas en el anexo de características técnicas.
422		Threat Intelligence	Pregunta: Por favor aclarar ¿ se espera integración con feeds de inteligencia externos (comerciales, gubernamentales, FIRST, MISP, etc.) o serán provistos por la DIAN?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, es importante y deseable que el futuro SOC cuente con integración con fuentes de inteligencia como las mencionadas, las cuales deberán ser provistas por el contratista.
423		MITRE ATT&CK	Pregunta: Por favor aclarar ¿ se requiere cobertura formal de MITRE ATT&CK (matriz de cobertura y gap analysis) como entregable del SOC?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los entregables requeridos para la presentación de ofertas están claramente detallados en el documento "410-Solicitud-de-Oferta-VSD-SdO-SOC"
424		Preparación para auditorías	Pregunta: Por favor aclarar ¿ el SOC deberá soportar auditorías regulatorias específicas (Contraloría, Procuraduría, entes internacionales) y con qué periodicidad?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el proyecto SOC puede estar supeditado a visitas, auditorías y demás revisiones que sean requeridas por parte de los entes de control, pero se indica que estas no tienen periodicidad regular.
425		ISO 27001	Pregunta: Por favor aclarar ¿ el SOC debe integrarse al SGSI existente de la DIAN o construir uno independiente para el servicio?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el proyecto SOC debe poder integrarse al SGSI de la Entidad.
426		Operación SOC	Pregunta: Por favor aclarar ¿ se requiere un sitio alterno de operación SOC (DRP) y cuál es el RTO/RPO esperado?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el servicio de SOC cuente con alta disponibilidad
427		Toda la infraestructura	Pregunta: Por favor aclarar ¿ cuál es el número total de activos (servidores, endpoints, dispositivos de red, aplicaciones) a monitorear en el alcance inicial?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las cantidades estipuladas se encuentran detalladas en los documentos hacen parte del proyecto SOC, en este caso se tiene una cantidad de 25000.
428	x	SOAR	Pregunta: Por favor aclarar ¿ el nivel de automatización esperado incluye playbooks completamente autónomos o solo semi-automatización con aprobación humana?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, de acuerdo a los requerimientos de la DIAN y a la implementación que se haga de ellos, los playbooks podrán ser completamente automatizados o semiautomatizados según lo autorizado por la Entidad.
429		Vulnerabilidades en tiempo real	Pregunta: Por favor aclarar ¿ la gestión de vulnerabilidades incluye escaneo activo, priorización, remediación o solo correlación con eventos de seguridad?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la gestión de vulnerabilidades incluyen todas las actividades requeridas por la Entidad en el anexo técnico.
430		DFIR	Pregunta: Por favor aclarar ¿ el servicio de análisis forense incluye adquisición de evidencia en sitio (on-site) o solo análisis remoto?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, según el ítem en mención se contempla análisis forense para los eventos críticos, si para ello es necesario que el proveedor este en sitio lo deberá hacer.
431		Equipo especializado	Pregunta: Por favor aclarar ¿ se requiere personal residente en sitio (on-site) o el modelo puede ser remoto (nearshore/offshore)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en el equipo mínimo de trabajo exigido se contempla un perfil que deberá estar en sitio, los demás miembros del equipo deberán prestar el servicio desde las locaciones del SOC que deberá estar en la Ciudad de Bogotá.
432		Conocimiento	Pregunta: Por favor aclarar ¿ se requiere transferencia de conocimiento formal (KT) y entrega de runbooks/playbooks como propiedad de la DIAN?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, dentro de las características y requerimientos técnicos del proyecto SOC se contempla transferencia de conocimiento, por favor verificar su detalle en el archivo anexo técnico del proyecto.
433		Tecnologías SOC	Pregunta: Por favor aclarar ¿ se requiere que las herramientas implementadas queden en propiedad de la DIAN al finalizar el contrato o bajo modelo de servicio (SaaS/MSSP)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en caso de que se entregue licenciamiento a perpetuidad dentro del servicio, el mismo debe quedar a nombre de la Dian, una vez termine el proyecto SOC.
434		Reversibilidad de información	Pregunta: Por favor aclarar ¿ cuáles son los requerimientos de reversibilidad del servicio (transferencia de datos, configuraciones, playbooks) al finalizar el contrato?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor del SOC deberá confeccionar el plan de devolución del servicio donde deberá incluir todas las actividades propias de este plan.
435		Incidentes	Pregunta: Por favor aclarar ¿ existe obligación de notificación de incidentes a entes regulatorios o judiciales y en qué tiempos?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las obligaciones referidas se encuentran detalladas en el ítem 19 del anexo técnico, favor consultarlo para ver lo pertinente.
436		Proyecto SOC	Pregunta: Por favor aclarar ¿ cómo se gestionarán los riesgos asociados a indisponibilidad de herramientas existentes durante la transición al nuevo SOC?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las herramientas actuales tienen soporte por parte del fabricante 7x24x365, en caso de sufrir alguna indisponibilidad el fabricante deberá soportar la operación de dichas herramientas.
437		OSI define reglas, roles y perfiles	Pregunta: Por favor aclarar ¿ el modelo de gestión de identidades (IAM/PAM) será provisto por la DIAN o el contratista deberá integrar o implementar controles adicionales de acceso privilegiado para la operación del SOC?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor del SOC deberá tener en cuenta todo lo necesario para llevar a feliz término la puesta en operación de los diferentes servicios, en este caso, si requiere implementar nuevos controles lo podrá hacer, siempre y cuando cuente con el aval de la Entidad y se cumplan con las características solicitadas.
438		Operar bajo modelo definido	Pregunta: Por favor aclarar ¿ se requiere la implementación de capacidades de Threat Hunting proactivo con dedicación exclusiva o será una función reactiva dentro de la operación SOC estándar?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las capacidades y servicios solicitados deben manejar posiciones proactivas anticipándose a posibles problemas.
439	12.20 - 12.68	Custodia digital y evidencia	Pregunta: Por favor aclarar ¿ existen requerimientos específicos de cifrado de datos (en tránsito y en reposo) y gestión de llaves (KMS/HSM) que deban implementarse en la solución SOC?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los requerimientos y características se encuentran en el documento anexo de características técnicas.
440		Aprovisionamiento de herramientas	Pregunta: Por favor aclarar ¿ se requiere que las plataformas del SOC cuenten con certificaciones específicas (ej. Common Criteria, FIPS 140-2/3) para cumplimiento gubernamental?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los requerimientos y características se encuentran en el documento anexo de características técnicas.
441	x	Integración con sistemas externos	Pregunta: Por favor aclarar ¿ el SOC deberá integrarse con sistemas de gestión ITSM existentes (ej. ServiceNow, Remedy) para la gestión de tickets e incidentes?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se deberá integrar con la plataforma ITSM de la Entidad
442	x	Operación SOC	Pregunta: Por favor aclarar ¿ se exige un plan formal de continuidad del servicio SOC (BCP) con pruebas periódicas y validación por parte de la DIAN?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los planes y/o documentos requeridos se encuentran claramente definidos en el documento SDO que hace parte del proyecto SOC. "410-Solicitud-de-Oferta-VSD-SdO-SOC".
443	x	Normativas	Pregunta: Por favor aclarar ¿ el servicio SOC deberá cumplir con regulaciones adicionales locales (ej. Ley de Protección de Datos Personales en Colombia - Ley 1581) y cómo se validará dicho cumplimiento?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, para el presente proyecto en lo que tiene que ver con manejo de la información, aplican las respectivas normativas de ley de protección de datos personales en Colombia, y su validación en caso de que aplique se hará por medio del manual de protección de datos personales de la Entidad y puede ser mediante diagnósticos o auditorías.
444	IOA.22.1	Elasticidad y licenciamiento	Pregunta: Por favor aclarar ¿ el modelo de elasticidad requerido implica ajuste dinámico de licencias basado en consumo (ej. EPS/GB) durante la ejecución contractual o será un dimensionamiento fijo?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los requerimientos y características se encuentran en el documento anexo de características técnicas.
445	2.13	(Ítem 2.13)	Observación: - Requisito actual: La solución debe estar en capacidad de instalarse en Azure, AWS, HyperV, VMware (en las versiones con que cuenta la entidad). - Solicitud de modificación: Se solicita amablemente a la Entidad modificar este numeral para permitir y valorar soluciones nativas de nube (SaaS) que utilicen recolectores locales o máquinas virtuales intermedias para la ingesta de datos desde la infraestructura local, sin obligar a que el motor central del SIEM se instale en una arquitectura basada en máquinas virtuales previstas por el cliente. - Justificación: Exigir la instalación del motor central en servidores locales limita el acceso a tecnologías de Inteligencia Artificial avanzadas orientadas al SOC. Una arquitectura SaaS moderna exime a la entidad de los altos costos de mantenimiento, parcheo y escalabilidad de infraestructura, permite centralizar la telemetría y proporciona el inmenso poder de cómputo necesario para ejecutar modelos de IA y automatización a escala.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los requerimientos y características del respectivo ítem admiten equivalencia, y se acepta soluciones tipo SaaS.
446	2.21	(Ítem 2.21)	Observación: - Requisito actual: 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. - Solicitud de modificación: Se solicita amablemente a la Entidad ajustar este requerimiento para eliminar la obligatoriedad de contar con plantillas predefinidas de normativas internacionales que no aplican a la jurisdicción colombiana ni al sector de la Entidad (como NERC, FISMA, GLBA o GPG13). En su lugar, sugerimos solicitar: Capacidad de generación de reportes de cumplimiento normativo y de auditoría personalizables, que incluyan plantillas nativas o paneles de control orientados a frameworks globales modernos de ciberseguridad, como MITRE ATT&CK, ISO 27000 o CIS Controls, así como capacidades avanzadas para la creación dinámica de reportes. - Justificación técnica y estratégica: Exigir de manera obligatoria plantillas predefinidas para marcos normativos como NERC (regulación eléctrica de Norteamérica), GLBA (sector financiero de EE. UU.), FISMA (agencias federales de EE. UU.) o GPG13 (gobierno del Reino Unido) restringe innecesariamente la participación de plataformas modernas de analítica de seguridad, obligando a ofertar herramientas con módulos de cumplimiento específicos orientados a un fabricante.		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.
447	2.12	(Ítems 2.12, 2.22 y 2.33)	Observación: - Requisito actual: Debe tener monitoreo de transacciones sintéticas (Ping, DNS, JDBC), estado de aplicaciones (JMX, WMI) y protocolos de enrutamiento (BGP/OSPF). - Solicitud de modificación: Se solicita amablemente a la Entidad eliminar estos requerimientos como funciones nativas del SIEM, o en su defecto, permitir que el cumplimiento de este punto se realice mediante la integración vía API con la herramienta especializada de monitoreo NOC. - Justificación: El propósito de un Centro de Operaciones de Seguridad es la detección, investigación y remediación de ciberamenazas, no el monitoreo de rendimiento y disponibilidad de TI (NOC). Exigir funcionalidades transaccionales de NOC dentro del SIEM diluye el enfoque de seguridad y descarta plataformas líderes en IA y herramientas SIEM de nueva generación. La mejor práctica de la industria es mantener las herramientas NOC (ya existentes en la DIAN) y enviar sus alertas de disponibilidad al SIEM para su correlación con eventos de seguridad.		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 equívocos en el requerimiento de la Entidad, los ítems en mención 2.12 y 2.33 serán eliminados del respectivo anexo técnico, cambio que se verá reflejado en la adenda a publicar en los próximos días.
448	2.34	(Ítem 2.34)	Observación: - Requisito actual: Soporte de archivado de logs tanto para NFS como HDFS. - Solicitud de modificación: Se solicita a la Entidad permitir que el ciclo de vida y almacenamiento a largo plazo de los logs se gestione de manera nativa en el Data Lake en nube del fabricante, o aceptar el reenvío de eventos hacia sistemas externos mediante mecanismos estándar de Event Forwarding en lugar de exigir compatibilidad directa con sistemas de archivos heredados como NFS/HDFS. - Justificación: El almacenamiento de Big Data de seguridad en sistemas locales NFS/HDFS requiere una inversión significativa en discos, mantenimiento físico y balanceo continuo por parte de la Entidad. Con un modelo de servicio SaaS, el ciclo de vida de los datos se gestiona eficientemente y de manera transparente en la nube, permitiendo esquemas flexibles de retención en caliente (hot storage) y retención en frío (cold storage) para cumplimiento normativo. Esta arquitectura garantiza escalabilidad y alta disponibilidad sin costos ocultos de hardware para la DIAN. En caso de que la Entidad requiera una copia local por políticas estrictas, se puede solicitar el uso de Event Forwarding para exportar la telemetría en bruto hacia almacenamientos externos o ecosistemas de terceros, eliminando la dependencia de tecnologías específicas de archivos en red.		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.

449	3.59	(Ítems 3.52 al 3.67)	Observación: - Requisito actual: El pliego exige detalladamente un editor visual de playbooks estructurado con soporte para bucles, condiciones lógicas, depuración visual (debugging), ejecución manual paso a paso, y una dependencia absoluta de la creación y gestión de playbooks estáticos. - Solicitud de modificación: Se solicita amablemente a la Entidad ampliar y modernizar estos numerales para aceptar y valorar plataformas que ofrezcan resolución autónoma de incidentes mediante Inteligencia Artificial Agéntica, reduciendo la dependencia exclusiva de la creación y mantenimiento manual de playbooks estáticos. - Justificación: El enfoque de un Centro de Operaciones de Seguridad moderno no debe centrarse en cuántos playbooks manuales debe construir un analista, sino en cómo la tecnología reduce la carga operativa. A diferencia del enfoque tradicional basado en reglas estáticas, los agentes de IA utilizan Modelos LLM para analizar la intención, razonar, y generar dinámicamente un plan único de múltiples pasos para investigar amenazas complejas sin intervención humana (donde se requiera o se establezca). Esto automatiza la toma de decisiones complejas, reduce drásticamente el Tiempo Medio de Resolución (MTTR) y mitiga la fatiga del analista frente a la sobrecarga de alertas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
450	3.14	(Ítem 3.59)	Observación: - Requisito actual: Se exige que la arquitectura escalable permita aumentar la capacidad de ejecución mediante la adición de nodos, instancias o licencias adicionales... sin que ello implique costos adicionales para la Entidad - Solicitud de modificación: Se solicita a la Entidad modificar el requerimiento para admitir arquitecturas nativas de nube (SaaS), donde la escalabilidad no se mide por la agregación de "nodos" o "instancias" de infraestructura, sino que es gestionada dinámicamente por el fabricante, permitiendo el uso de modelos de licenciamiento basados en unidades de cómputo para cargas masivas. - Justificación: El concepto de agregar nodos o instancias es propio de arquitecturas On-Premise heredadas que requieren mantenimiento, parcheo y gestión por parte del cliente. Las ventajas de un modelo SaaS radican en que el lago de datos centraliza toda la telemetría y proporciona un poder de cómputo unificado para IA y automatización sin que la Entidad deba administrar servidores.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem en mención acepta equivalencias dentro de lo requerido, por lo tanto, no se acepta su sugerencia.
451	7.7 7.14 7.19	(Ítem 3.14)	Observación: - Requisito actual: Proporcionar un marco de desarrollo de tableros basado en HTML / JSON / JS para crear widgets personalizados. - Solicitud de modificación: Se solicita a la Entidad eliminar el requerimiento de uso obligatorio de lenguajes de programación web (HTML/JS) de forma libre y permitir plataformas que utilicen constructores visuales nativos y lenguajes de consulta de datos propios y seguros para la creación de tableros personalizados. - Justificación: Por principios de Security by Design, algunas plataformas SaaS restringen la invección de código abierto (como HTML o JavaScript) en la interfaz gráfica para prevenir vulnerabilidades y proteger la confidencialidad de la información alojada en la nube.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem en mención acepta equivalencias dentro de lo requerido, por lo tanto, no se acepta su sugerencia.
452	7.7	(Ítems 7.7, 7.14 y 7.19)	Observación: - Requisito actual: El pliego exige que el equipo de recepción de tráfico se instale fuera de línea vía puertos pasivos o SPAN port y solicita la capacidad de realizar consultas a los datos almacenados en un hardware específico (appliance) sin conectarse a la nube, reteniendo localmente al menos 6 meses de información. - Solicitud de modificación: Se solicita amablemente a la Entidad modificar estos numerales para permitir arquitecturas nativas de nube (SaaS) que utilicen sensores locales o máquinas virtuales intermedias para la recolección del tráfico y registros locales, centralizando el almacenamiento y el procesamiento analítico en un Data Lake en la nube. - Justificación: Limitar la solución a hardware local desconectado restringe severamente el poder de cómputo necesario para procesar modelos avanzados de Inteligencia Artificial (IA). Las arquitecturas SaaS modernas centralizan toda la telemetría en un Data Lake en la nube, el cual proporciona una única fuente para la normalización de datos y la automatización a gran escala.		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.
453	7.15	(Ítem 7.15)	Observación: - Requisito actual: La solución debe realizar una captura de paquetes en tiempo real que permita un análisis exhaustivo en herramientas como Wireshark y la extracción de datos en formato completo (.pcap). - Solicitud de modificación: Se sugiere a la Entidad ampliar el requerimiento para aceptar tecnologías modernas de inspección profunda que recojan, correlacionen y analicen metadatos enriquecidos de red, en lugar de hacer obligatoria la captura y extracción masiva de paquetes crudos .pcap - Justificación: El almacenamiento y análisis manual de archivos .pcap en herramientas como Wireshark es un enfoque forense reactivo que contribuye drásticamente a la sobrecarga de datos y a la fatiga operativa de los especialistas del SOC. En lugar de forzar a un humano a leer paquetes de red crudos, la plataforma debería recoger metadatos de red, firewalls y endpoints de manera continua, normalizarlos y enriquecerlos para entregar un contexto transversal.		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.
454	7.26	(Ítem 7.26)	Observación: - Requisito actual: El documento indica que la solución debe funcionar completamente en función del comportamiento, estableciendo estrictamente que no se permitan las tecnologías que hacen uso de reglas y / o firmas - Solicitud de modificación: Se solicita a la Entidad suprimir la prohibición del uso de reglas y firmas, y en su lugar, requerir una plataforma híbrida que incluya algoritmos de Machine Learning/IA para el análisis de comportamiento, pero que además cuente con la capacidad de generar y utilizar reglas y firmas de inteligencia de amenazas en tiempo real. - Justificación: Prohibir el uso de reglas y firmas degrada la seguridad general de la organización frente a amenazas conocidas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem 7.26 será ajustado, para evitar equívocos 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.
455	7.10	(Ítem 7.10)	Observación: - Requisito actual: 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. - Solicitud de modificación: Solicitamos a la entidad suprimir este punto ya que hace referencia a una tecnología propietaria de Darktrace.		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.
456			En la medida en que el objeto de la licitación no incluye el suministro de bienes, agradecemos su confirmación respecto a que no será necesario aportar una declaración o garantía de fabricante		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en los casos donde aplique y de acuerdo a los servicios entregados, el futuro proveedor del SOC deberá certificar la garantía del fabricante
457	Sección VIII - CGC 27.1	El valor de la liquidación por daños y perjuicios será: 1% por semana. El monto máximo de la liquidación por daños y perjuicios será: 10%.	La tasa del 1% semanal equivale aproximadamente a 0,143% diario, lo que supera el parámetro de referencia que establece un máximo de 0,1% diario. Tampoco se aclara si esta sanción se suma o no a los descuentos por ANS del mismo periodo.	Requerimos a la entidad respetuosamente ajustar la tasa a máximo 0,1% diario (equivalente a 0,7% semanal) conservando el tope máximo del 10% del valor del contrato. Aclarar si esta sanción se aplica de forma independiente o en conjunto con los descuentos por ANS.	Se aclara al observante que el porcentaje establecido para la liquidación por daños y perjuicios corresponde a una condición contractual definida por la Entidad en atención a la naturaleza, criticidad y alcance de los servicios requeridos, razón por la cual no se considera procedente modificar la tasa establecida en el documento de Solicitud de Ofertas. No obstante, se precisa que la eventual aplicación de dichas penalidades se realizará observando el debido proceso, garantizando al Contratista el derecho de defensa y contradicción. En ese sentido, previo a la imposición de cualquier medida, el supervisor y/o la Entidad pondrán en conocimiento del Contratista los presuntos incumplimientos identificados, otorgándole la posibilidad de presentar las explicaciones, soportes y acciones correctivas o planes de mejora que considere pertinentes para su evaluación. Así mismo, se aclara que las penalidades por daños y perjuicios y los descuentos asociados al incumplimiento de los Acuerdos de Niveles de Servicio (ANS) obedecen a mecanismos distintos, asociados a eventos y finalidades diferentes dentro de la ejecución contractual, por lo cual podrán aplicarse de manera independiente cuando haya lugar a ello, de conformidad con las condiciones establecidas en el contrato.
458	Sección VIII / Sección VI	N/A	El documento tiene descuentos por ANS para indicadores de servicio y una liquidación de daños por retrasos (CGC 27), pero no tiene una cláusula penal general que cubra otro tipo de incumplimientos, como por ejemplo lo es el no renovar las garantías a tiempo, violar la confidencialidad o abandonar parcialmente la prestación del servicio.	Amablemente solicitamos que se incluya en las condiciones especiales del contrato una cláusula penal general que establezca una sanción económica para incumplimientos distintos a los cubiertos por los ANS y la CGC 27. El valor de esa cláusula no debería superar el 20% del valor total del contrato. De manera enfática solicitamos que nos indique la DIAN en caso de incumplimiento, cuál es el procedimiento a seguir y si la ley aplicable es el reglamento del contrato o si esta entidad se remite a alguna otra Ley.	No se acoge la solicitud. Los Acuerdos de Niveles de Servicio (ANS) y las disposiciones de las Condiciones Generales del Contrato (CGC) ya contemplan mecanismos suficientes para la gestión de riesgos, seguimiento y consecuencias por incumplimiento durante la ejecución contractual. Estos instrumentos resultan adecuados y proporcionales, por lo que no se considera necesario incorporar una cláusula penal adicional. El proceso se rige por las Políticas de Adquisiciones del BID (GN-2349-15) y por las condiciones establecidas en la Solicitud de Ofertas, que definen los procedimientos aplicables en caso de incumplimiento.
459	Sección II – IAO 19.1	N/A	En lugar de una garantía bancaria con monto en dinero, el documento exige una declaración escrita de mantenimiento de la oferta. Esto cumple con el parámetro aplicable donde la garantía de seriedad no debe superar el 10% del presupuesto. Sin embargo, si un oferente incumple esta declaración, la consecuencia no es cobrarle una suma de dinero sino inhabilitarlo por 5 años, lo que puede resultar de difícil aplicación práctica.	Solicitamos amablemente verificar que el formulario de la Declaración de Mantenimiento de la Oferta incluya de forma clara las consecuencias del incumplimiento (inhabilitación de 5 años ante el Fondo DIAN y la DIAN). Para procesos futuros de montos similares considerar si conviene exigir una garantía bancaria de entre el 1% y el 3% del presupuesto que sea más ejecutable.	No se acoge la solicitud. La Declaración de Mantenimiento de la Oferta se encuentra prevista en el documento de licitación conforme a las Políticas de Adquisiciones del BID (GN-2349-15), y su aplicación se rige por lo establecido en la IAO 19, la cual contempla las consecuencias frente a su incumplimiento. En este sentido, el mecanismo adoptado resulta válido, suficiente y acorde con el marco normativo aplicable, por lo que no se considera necesario modificar el formulario ni incorporar disposiciones adicionales. En consecuencia, se mantienen las condiciones establecidas en la Solicitud de Ofertas.
460	Sección VIII - CGC 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.	Las condiciones generales del contrato (CGC 16.3) establecen que el comprador tiene máximo 60 días para pagar después de recibir la factura, sin embargo, las condiciones especiales alargan ese plazo a 90 días antes de que se generen intereses de mora, lo que favorece al comprador en perjuicio del contratista sin que se explique la razón de ese cambio.	Respetuosamente solicitamos fijar el plazo de la CGC 16.5 a 60 días calendario, en concordancia con lo que ya establece la CGC 16.3 o explicar en el documento por qué se justifica la ampliación a 90 días.	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.
461	Sección II - IAO 22.1	Las firmas participantes deberán informar al correo adquisiciones@fondodian.gov.co que presentarán oferta dentro del proceso para que el Fondo DIAN remita un link para cada oferente interesado en el que podrán cargar las ofertas.	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.	Establecer un plazo mínimo dentro del cual el Fondo DIAN debe enviar el link de cargue al oferente que lo solicite. Por ejemplo, que el link deba ser remitido dentro de los 2 días hábiles siguientes a la solicitud y que en todo caso se envíe al menos 5 días hábiles antes del cierre del proceso.	No se acoge la solicitud. El plazo establecido en las Condiciones Especiales del Contrato para el reconocimiento de intereses de mora obedece a la necesidad de garantizar la adecuada verificación, validación y trámite interno de los pagos, en el marco de los procedimientos administrativos y financieros aplicables a la entidad. Este término no modifica la obligación de pago, sino que define el momento a partir del cual se generan intereses, y se encuentra alineado con las condiciones contractuales y prácticas aplicables en procesos financiados con recursos del BID. En consecuencia, se mantienen las condiciones establecidas en la Solicitud de Ofertas.
462	Sección VIII (CEC) - CGC 10.2	Las partes harán todo lo posible para resolver las controversias que surjan en virtud del contrato o en relación con él, en forma amistosa, de buena fe, mediante negociaciones directas informales iniciales y posteriormente agotando todas las instancias requeridas para utilizando figuras como la conciliación, la composición o la transacción y en caso de no existir solución y solo en última instancia se podrá acudir a los reglamentos de los procedimientos para los procesos de arbitraje	La cláusula obliga a agotar negociación directa, conciliación, composición y transacción antes de llegar al arbitraje pero no fija un plazo concreto para cada una de esas etapas. La CGC 10.2 establece que si en 28 días no hay acuerdo se puede notificar el arbitraje pero las demás CEC modifican ese esquema exigiendo más instancias sin decir cuánto tiempo debe durar cada una. Esto significaría que cualquiera de las partes podría alargar indefinidamente las etapas previas al arbitraje.	Solicitamos de manera respetuosa fijar en la cláusula un plazo máximo para cada etapa previa al arbitraje.	No se acoge la solicitud. Las condiciones contractuales establecen un esquema de resolución de controversias que prioriza mecanismos alternativos de solución de conflictos, en línea con buenas prácticas contractuales y con el marco aplicable. La referencia a dichas instancias no implica una dilación indefinida del proceso, en tanto su desarrollo se rige por los principios de buena fe, razonabilidad y oportunidad. Adicionalmente, la CGC prevé la posibilidad de acudir al arbitraje cuando no se alcance un acuerdo entre las partes, por lo que no se limita el acceso a dicho mecanismo.
463	Sección VI - ANS párrafo introductorio y Sección VIII (CEC) - CGC 27.1	**ANS:** Las consecuencias económicas por incumplimiento son acumulables (...) pero en ningún caso podrá superar el 10% del valor de costo del contrato. / **CGC 27.1:** El monto máximo de la liquidación por daños y perjuicios será 10%.	El documento tiene dos mecanismos de sanción económica que conviven, los descuentos por ANS (máximo 10% del contrato en total) y la liquidación de daños de la CGC 27 (máximo 10% del contrato). Ambos tienen el mismo tope individualmente pero el documento no aclara si ese 10% es un límite compartido o si cada mecanismo puede llegar al 10% de forma independiente. Esto es vital pues si fueran independientes, el proveedor podría enfrentar hasta un 20% del valor del contrato en sanciones económicas acumuladas, lo que cambiaría completamente el análisis de riesgo de la propuesta.	Definir expresamente si el 10% de los ANS y el 10% de la CGC 27 son límites independientes o si existe un tope único de sanciones económicas para ambos mecanismos combinados. Si el tope es único, indicarlo así. Si son independientes, aclarar en qué supuestos aplica cada uno para evitar doble sanción por el mismo hecho.	No se acoge la solicitud. Los mecanismos de descuentos asociados a los ANS y la liquidación de daños prevista en la CGC 27 corresponden a figuras distintas, con naturaleza, finalidad y supuestos de aplicación diferentes. Los ANS se orientan a medir y gestionar el nivel de cumplimiento del servicio durante la ejecución contractual, mientras que la CGC 27 regula la indemnización de perjuicios derivados de incumplimientos contractuales específicos. En este sentido, no se trata de mecanismos concurrentes sobre un mismo hecho, sino de instrumentos diferenciados dentro de la gestión contractual. En consecuencia, los límites establecidos para cada uno operan de manera independiente dentro de su respectivo ámbito de aplicación, sin que ello implique una doble sanción por un mismo incumplimiento.
464	Sección VII (CGC) - Cláusula 30 y Sección VI - ANS	**CGC 30.1(b):** La responsabilidad total del Proveedor frente al Comprador, ya sea contractual, de agravio o de otra índole, no podrá exceder el Precio del Contrato. / **ANS:** Las consecuencias económicas por incumplimiento [...] no podrán superar el 10% del valor de costo del contrato.	La CGC 30 limita la responsabilidad total del proveedor al valor del contrato, sin embargo, hay una tensión entre esta limitación general y la facultad del comprador de ejecutar la garantía de cumplimiento (10% del contrato), aplicar descuentos por ANS (hasta 10%) y cobrar liquidación de daños (hasta 10%), todo al mismo tiempo. Si se acumulan todos esos mecanismos sin un tope conjunto claro, el proveedor podría quedar expuesto a un valor superior al que sugiere la limitación del CGC 30, especialmente si además se inician reclamaciones por daños indirectos.	Requerimos respetuosamente a la entidad añadir una cláusula que establezca de forma expresa el tope máximo de todas las sanciones económicas combinadas (ANS + liquidación de daños + garantía de cumplimiento) para que el proveedor tenga claridad sobre su exposición total. Este tope debería ser coherente con la limitación de responsabilidad de la CGC 30 y no debería superarse aunque se activen todos los mecanismos de forma simultánea.	No se acoge la solicitud. La limitación de responsabilidad prevista en la CGC 30 establece el marco general aplicable a la responsabilidad del contratista, mientras que los mecanismos como la garantía de cumplimiento, los descuentos por ANS y la liquidación de daños corresponden a figuras contractuales con naturaleza y finalidad distintas, cada una con su propio ámbito de aplicación. En particular, la garantía de cumplimiento tiene carácter preventivo y de respaldo contractual, los ANS se orientan al seguimiento del nivel de servicio, y la liquidación de daños se aplica frente a incumplimientos contractuales específicos. Estos mecanismos no implican una superposición automática ni una acumulación indiscriminada, sino que operan conforme a las condiciones y supuestos definidos en el contrato.
465	Sección VI - ANS	ANS: Las deducciones aplicadas no eximen al CONTRATISTA de las demás consecuencias jurídicas previstas en el contrato, incluyendo la activación de garantías o la terminación anticipada por incumplimiento reiterado.	El documento permite que incluso después de aplicar descuentos por ANS, la DIAN pueda además ejecutar la garantía de cumplimiento o terminar el contrato pero no establece si para eso se requiere un proceso previo de notificación y descargos. La aplicación de sanciones sin procedimiento previo puede ser cuestionada jurídicamente, especialmente si el contratista alega que el incumplimiento fue causado por factores imputables a la DIAN (demoras en aprobaciones, restricciones de acceso, cambios en el alcance).	De manera respetuosa sugerimos agregar un procedimiento claro que deba seguirse antes de activar cualquier consecuencia grave que podría contener el siguiente esquema (1) informe técnico del supervisor con las causas del incumplimiento, (2) notificación escrita al contratista, (3) plazo para presentar descargos y pruebas de que el incumplimiento no le es imputable y (4) decisión motivada. Esto protege a ambas partes y reduce el riesgo de litigios posteriores.	No se acoge la solicitud. Las actuaciones contractuales relacionadas con la verificación de incumplimientos, la aplicación de medidas y la eventual ejecución de garantías se rigen por lo dispuesto en las condiciones del contrato, así como por los principios de debido proceso, buena fe y contradicción aplicables a la gestión contractual. En ese sentido, la supervisión del contrato implica la verificación técnica de los hechos, la comunicación al contratista y la oportunidad de presentar las aclaraciones que correspondan, dentro de los procedimientos administrativos aplicables, sin que resulte necesario incorporar un esquema adicional en el documento de licitación.
466	IAO 22.1	Link entrega oferta		Amablemente nos permitimos solicitar a la entidad aclarar si una persona jurídica realiza la solicitud para el link de entrega de oferta, este puede ser usado por un APCA o si en su defecto es el APCA quien tiene que solicitar desde un inicio el link para la entrega	El enlace se puede solicitar por alguna de las firmas que integre el APCA.
467	5.1 Criterios de Calificación (IAO 38.1)		**1.Ajuste de Requisitos Financieros** De conformidad con las Políticas de Adquisiciones del Banco Interamericano de Desarrollo (BID), que garantizan a los interesados el derecho a formular observaciones al pliego de condiciones dentro del término establecido para tal efecto, se solicita respetuosamente a la entidad contratante reconsiderar el requisito habilitante de capacidad financiera correspondiente al indicador de apalancamiento a corto plazo, actualmente fijado en un valor **menor a 0,5**, con el fin de que sea ajustado a un valor **menor a 1,0.** **Justificación:** El umbral vigente (menor a 0,5) resulta excesivamente restrictivo y, a juicio de esta parte, contraviene el deber de proporcionalidad y razonabilidad que debe orientar la fijación de requisitos habilitantes conforme a los principios de economía, eficiencia, igualdad de oportunidades y fomento de la competencia que rigen las adquisiciones financiadas con recursos del BID. Dicho indicador no refleja de manera adecuada las condiciones reales del mercado ni la dinámica financiera propia de las empresas que prestan servicios especializados en tecnología, como los asociados a la operación de un Centro de Operaciones de Seguridad (SOC). La modificación propuesta se sustenta en los siguientes aspectos: **1.Principio de proporcionalidad y razonabilidad** : De conformidad con las Políticas de Adquisiciones del BID, los requisitos de elegibilidad y calificación deben ser adecuados y proporcionales a la naturaleza y al valor del contrato. Un umbral de 0,5 exige una estructura financiera altamente conservadora que excede lo razonable frente al nivel de riesgo inherente al objeto contractual, constituyendo una carga desproporcionada que restringe de manera injustificada la participación de oferentes con plena capacidad de ejecución. Las directrices del BID han establecido consistentemente que los requisitos de calificación no deben convertirse en barreras de acceso que desnaturalicen el proceso de selección ni restrinjan indebidamente la competencia. **2.Principio de libre concurrencia y pluralidad de oferentes:** Las Políticas de Adquisiciones del BID consagran el principio de igualdad de oportunidades y el deber de la entidad ejecutora de garantizar la más amplia participación de oferentes elegibles en los procesos de contratación. El requisito actual reduce significativamente la concurrencia en el proceso, dado que pocas empresas del sector mantienen niveles de apalancamiento de corto plazo tan bajos, especialmente en actividades intensivas en operación y talento humano calificado. Esta limitación injustificada podría configurar una restricción indebida a la libre competencia, en contravía de los principios de competencia e igualdad de oportunidades que rigen los procesos de adquisición financiados con recursos del BID. **3.Condiciones objetivas del mercado sectorial:** Las Políticas de Adquisiciones del BID exigen que los requisitos de calificación financiera se establezcan con base en un análisis objetivo del mercado y del sector económico respectivo. En la industria de servicios de TI y ciberseguridad es habitual operar con esquemas de financiamiento de corto plazo vinculados a la gestión del flujo de caja operativo, sin que ello comprometa la solidez financiera ni la capacidad efectiva de ejecución contractual. Un estudio adecuado del sector habría evidenciado que la práctica comercial estándar en este tipo de servicios involucra ratios de apalancamiento superiores al umbral exigido, lo cual debe ser considerado por la entidad al momento de fijar los indicadores habilitantes. **4.Nivel de riesgo controlado y selección objetiva**: Conforme a las Políticas de Adquisiciones del BID, el proceso de selección debe fundamentarse en criterios objetivos, justos y transparentes que permitan identificar la oferta más ventajosa. Un indicador inferior a 1,0 continúa representando un grado aceptable de apalancamiento y permite identificar empresas con adecuada capacidad de respuesta financiera, sin imponer barreras de entrada desproporcionadas frente al objeto del contrato. De este modo, se preserva la finalidad del requisito habilitante —verificar la aptitud financiera del proponente— sin incurrir en restricciones que carezcan de justificación técnica o contractual. **5.Evaluación integral conforme al marco normativo:** Las buenas prácticas en adquisiciones del BID establecen que la capacidad financiera debe evaluarse de manera integral mediante el conjunto de indicadores definidos por la entidad ejecutora. El ajuste propuesto permite valorar la capacidad financiera de los oferentes de manera articulada con los demás indicadores habilitantes (liquidez, capital de trabajo, endeudamiento total), evitando que un solo requisito excesivamente estricto descalifique a proponentes técnica y financieramente idóneos. Mantener el umbral actual implicaría privilegiar un criterio aislado por encima de la valoración sistémica de la capacidad financiera, lo cual resulta contrario a la finalidad del marco de adquisiciones aplicable.	En virtud de lo expuesto, y con fundamento en los principios de economía, eficiencia, transparencia, igualdad de oportunidades y fomento de la competencia que rigen las adquisiciones financiadas con recursos del BID, se solicita a la entidad contratante acoger la presente observación y ajustar el indicador de apalancamiento a corto plazo al valor propuesto (menor a 1,0). La modificación solicitada contribuiría a garantizar un proceso de selección más competitivo, plural y ajustado a derecho, sin menoscabo de las garantías financieras necesarias para la adecuada ejecución del contrato. Se deja constancia de que la presente observación se formula dentro del término previsto para tal efecto, en ejercicio legítimo del derecho de participación en el proceso de adquisición, y con el ánimo de contribuir al mejoramiento del pliego de condiciones en beneficio de los fines del proyecto financiado por el BID.	En atención a la observación. no se acepta la solicitud, el indicador se mantiene debido a la envergadura del proyecto.
468	5.1 Criterios de Calificación (IAO 38.1)	Capital de trabajo	**2. Capital de trabajo en relación con el presupuesto estimado** **Requisito actual:** (Activo Corriente – Pasivo Corriente) / Presupuesto estimado **≥ 0,05** **Requisito propuesto:** (Activo Corriente – Pasivo Corriente) / Presupuesto estimado **≥ 1,0** **Fundamento jurídico y normativo:** La presente observación se sustenta en el Marco de Política de Adquisiciones del Banco Interamericano de Desarrollo (GN-2349-15), el cual establece como principios rectores de los procesos de adquisiciones la economía, la eficiencia, la transparencia y la proporcionalidad de los requisitos de calificación respecto de la naturaleza, complejidad y magnitud del contrato a adjudicar. Asimismo, las Regulaciones de Adquisiciones para Prestatarios del BID disponen que los criterios de calificación financiera deben ser diseñados de manera que permitan verificar objetivamente la capacidad del oferente para cumplir con las obligaciones contractuales durante la totalidad del plazo de ejecución. En particular, los Documentos Estándar de Adquisiciones del BID, en la sección relativa a los requisitos de calificación financiera, prevén que el organismo ejecutor establezca umbrales mínimos de capital de trabajo neto y de recursos financieros disponibles que resulten proporcionales al valor estimado del contrato y a los flujos de caja proyectados. Dichos documentos estándar reconocen que la fijación de un nivel adecuado de capital de trabajo constituye un mecanismo esencial para mitigar el riesgo de incumplimiento contractual derivado de insolvencia o iliquidez del contratista. **Justificación técnica:** Considerando el presupuesto estimado del proceso y la criticidad operativa de los servicios de SOC a prestar, un umbral de capital de trabajo equivalente a apenas el 5% del presupuesto estimado resulta manifiestamente insuficiente para acreditar la solidez financiera que exige un contrato de esta naturaleza. Un requisito tan bajo no permite verificar de manera razonable la capacidad del oferente para soportar la operación de forma continua, realizar las inversiones iniciales en infraestructura tecnológica y capital humano especializado, absorber eventuales retrasos en los flujos de pago por parte de la entidad contratante y garantizar la continuidad ininterrumpida del servicio sin afectaciones a los niveles de servicio comprometidos. En contraste, un capital de trabajo neto equivalente o superior al 100% del presupuesto estimado se encuentra alineado con las mejores prácticas en procesos de adquisiciones financiados por organismos multilaterales y constituye un parámetro proporcional a la magnitud, duración y nivel de responsabilidad del servicio requerido. Esta exigencia fortalece la mitigación del riesgo financiero del contrato al garantizar que el adjudicatario cuente con recursos propios suficientes para financiar la totalidad de la operación sin depender exclusivamente de los desembolsos del contratante. De esta forma, se favorece la participación de oferentes con capacidad financiera real y demostrable, en plena concordancia con los principios de economía, eficiencia y valor por dinero que rigen las adquisiciones bajo financiamiento del BID. **Consideraciones adicionales** * Los ajustes propuestos no disminuyen los estándares de solvencia, sino que los hacen más coherentes con el tamaño y naturaleza del contrato. *Permiten la participación de empresas con alto patrimonio, experiencia internacional y capacidad comprobada, que podrían quedar excluidas por umbrales excesivamente restrictivos. *Se alinean con los principios de selección objetiva, pluralidad de oferentes y eficiencia del gasto público, sin comprometer la sostenibilidad financiera del proyecto. *Resultan consistentes con la complejidad técnica y el carácter estratégico de un Centro de Operaciones de Seguridad (SOC) para una entidad de la envergadura de la DIAN.	. **Solicitud:** Se solicita respetuosamente que el organismo ejecutor ajuste el requisito de capital de trabajo neto, elevando el umbral mínimo de 0,05 a 1,0 en relación con el presupuesto estimado del proceso, a fin de asegurar condiciones de calificación financiera proporcionales al objeto contractual y coherentes con el marco normativo aplicable del BID.	En atención a la observación. no se acepta la solicitud, el indicador se mantiene debido a la envergadura del proyecto.
469	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf C. Preparación de las Ofertas IAO 11.1(j)	El Oferente presentará los siguientes documentos adicionales junto con su Oferta: • Certificado de existencia y representación legal Estados financieros correspondientes a 2024 con corte a 31 de diciembre, los cuales deberán estar suscritos por un Contador Público y un Revisor Fiscal, cuando las normas que los regulan así lo exigen en el caso de los Oferentes Nacionales. En el caso de los Oferentes que provengan de países diferentes al país del comprador, deberán presentar los documentos o sus equivalentes de acuerdo con las normas del país de origen: a. Balance General comparado por las vigencias 2023-2024 b. Estado de Resultados comparado en los años terminados 2023 – 2024 c. Notas a los Estados Financieros. d. Dictamen o Informe anual de auditoría sobre cada uno de los estados financieros	Se solicita al Contratante permitir la presentación de estados financieros del ejercicio 2025, debidamente certificados y dictaminados, en sustitución o adicionalmente a los correspondientes a los años 2023-2024, admitiendo el último período fiscal disponible al momento de la presentación de la oferta. Fundamentos de la solicitud Actualidad y pertinencia de la información financiera Entre los ejercicios 2023 y 2025 pueden producirse cambios financieros, operativos y patrimoniales relevantes (crecimiento, reorganizaciones, ampliación de capacidades, inversiones en infraestructura, cambios en endeudamiento), especialmente en empresas vinculadas a servicios de ciberseguridad y SOC, sectores altamente dinámicos. Limitar el análisis a información con un rezago de hasta uno y dos años, para un proceso cuya presentación de ofertas es en mayo de 2026, puede reducir la precisión y actualidad en la evaluación de la capacidad financiera real del oferente. Impacto sobre los indicadores financieros exigidos Los indicadores establecidos en la Sección III – Capacidad financiera (liquidez, endeudamiento, capital de trabajo, patrimonio, apalancamiento) son altamente sensibles al periodo evaluado, por lo que estados financieros 2025 reflejarían de mejor manera: - Capacidad actual de ejecución - Solvencia financiera vigente - Sostenibilidad del contrato durante su horizonte de ejecución Principio de favorecimiento al oferente La admisión de estados financieros más recientes: - No reduce exigencias técnicas ni financieras - No genera ventaja indebida - Evita exclusiones por formalidades temporales - Favorece la participación de oferentes técnicamente robustos cuya evolución reciente es positiva Este enfoque es coherente con los principios de razonabilidad, proporcionalidad y maximización de la competencia, alineados con las Políticas de Adquisición del BID.	• Certificado de existencia y representación legal Estados financieros correspondientes a 2025 con corte a 31 de diciembre, los cuales deberán estar suscritos por un Contador Público y un Revisor Fiscal, cuando las normas que los regulan así lo exigen en el caso de los Oferentes Nacionales. En el caso de los Oferentes que provengan de países diferentes al país del comprador, deberán presentar los documentos o sus equivalentes de acuerdo con las normas del país de origen: a. Balance General comparado por las vigencias 2024-2025 b. Estado de Resultados comparado en los años terminados 2024 – 2025 c. Notas a los Estados Financieros. d. Dictamen o Informe anual de auditoría sobre cada uno de los estados financieros	De acuerdo con la observación, mediante adenda se realizará el siguiente ajuste a la IAO 11.(j), quedando así: El Oferente presentará los siguientes documentos adicionales junto con su Oferta: •Certificado de existencia y representación legal •Estados financieros correspondientes a 2025 con corte a 31 de diciembre, los cuales deberán estar suscritos por un Contador Público y un Revisor Fiscal, cuando las normas que los regulan así lo exigen en el caso de los Oferentes Nacionales. En el caso de los Oferentes que provengan de países diferentes al país del comprador, cuyos cierres fiscales correspondan a otros meses, deberán presentar los últimos documentos aprobados por la Junta directiva o quien haga sus veces aportando la normatividad que sustenta dicha fecha de cierre de acuerdo con las normas del país de origen: a.Balance General comparado por las vigencias 2024-2025 b.Estado de Resultados comparado en los años terminados 2024 – 2025 c.Notas a los Estados Financieros. d.Dictamen o Informe anual de auditoría sobre cada uno de los estados financieros e.Tarjeta Profesional y certificado de antecedentes disciplinarios del Contador Público y/o Revisor Fiscal, firmantes de los estados financieros, para las firmas nacionales o por quien exija la normatividad del país de oferente. •La oferta propuesta deberá suscribirse por el representante legal autorizado para el efecto y en caso de presentar alguna limitación deberá adjuntar la autorización del órgano societario correspondiente o el poder debidamente otorgado. En caso de APCAS todos sus miembros deberán suscribir la oferta o presentar el documento constitutivo de la figura asociativa o la promesa de sociedad futura suscrita por todos los miembros en donde se otorgue la facultad de suscribir la propuesta. En caso de requerir autorización para conformar la figura asociativa o firmar el acuerdo de conformación deberá presentar la autorización otorgada por el órgano societario correspondiente.

470	Sección VII. Condiciones Generales del Contrato (CGC)	11. Inspecciones y Auditorias	Se observa que la cláusula impone al contratista y sus subcontratistas la obligación de permitir el acceso irrestricto a cuentas y registros contables por parte del Banco o sus delegados, sin establecer requisitos mínimos de procedimiento como notificación previa, delimitación del alcance o protección de información confidencial. Esta redacción representa un riesgo jurídico y comercial, ya que podría permitir la revisión de información sensible no relacionada con el contrato, incluyendo datos de otros proyectos o clientes. Se sugiere ajustar la cláusula para garantizar que las auditorías se limiten exclusivamente a documentación vinculada al contrato, se realicen con previo aviso formal de mínimo 5 días , y se respete la confidencialidad de la información del proveedor.		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.
471	Sección VII. Condiciones Generales del Contrato (CGC)	19. Derechos de Autor	Se recomienda ajustar la cláusula para dejar claro que la propiedad intelectual del contratista sobre sus aportes técnicos, metodológicos y conceptuales se mantiene intacta, y que únicamente se transfiere al comprador el derecho de uso sobre los entregables desarrollados específicamente en ejecución del contrato, y que incorporen información o requerimientos del contratante.		Se aclara al observante que la cláusula de propiedad intelectual prevista en el documento contractual debe interpretarse en el sentido de que los entregables, documentos y desarrollos elaborados específicamente para la Entidad en ejecución del contrato serán de propiedad del Contratante, en los términos previstos en el documento de Solicitud de Ofertas. No obstante, dicha disposición no implica la transferencia de titularidad sobre metodologías, marcos conceptuales, herramientas, know-how, software, licencias, desarrollos, modelos o demás componentes preexistentes o de propiedad del Contratista, utilizados como base para la prestación de los servicios. En consecuencia, el Contratista conservará la titularidad sobre sus aportes técnicos, metodológicos y conceptuales preexistentes, otorgando al Contratante los derechos de uso necesarios sobre aquellos elementos incorporados en los entregables desarrollados específicamente en ejecución del contrato.
472	Sección VII. Condiciones Generales del Contrato (CGC)	20. Confidencialidad de la Información	Se observa que la cláusula sobre confidencialidad de la información establece una obligación indefinida en el tiempo, sin delimitar un periodo específico de vigencia posterior a la terminación del contrato. Esta redacción genera incertidumbre jurídica y puede afectar la planeación contractual del proveedor, especialmente en lo relacionado con la gestión documental, la protección de datos y la liberación de compromisos con subcontratistas. Se recomienda ajustar la cláusula para establecer un plazo definido de vigencia de la obligación de confidencialida, máximo de 5 años posteriores a la finalización del contrato, garantizando así seguridad jurídica y proporcionalidad en la aplicación de esta obligación		No se modificará como quiera que hace parte de las condiciones generales del contrato y son disposiciones estándares del Banco.
473	Sección VII. Condiciones Generales del Contrato (CGC)	27. Liquidación por Daños y Perjuicios	Se recomienda ajustar la cláusula para incluir un mecanismo de revisión previa, permitir justificaciones documentadas, y excluir retrasos derivados de causas no imputables al proveedor.		No se modificará como quiera que hace parte de las condiciones generales del contrato y son disposiciones estándares del Banco.
474	Sección VII. Condiciones Generales del Contrato (CGC)	30. Limitación de Responsabilidad	En particular, se recomienda que la cláusula excluya expresamente la reclamación de lucro cesante, daños indirectos, consecuenciales, especiales o punitivos, así como cualquier otro perjuicio que no corresponda a daños directos y comprobables derivados del incumplimiento contractual. Adicionalmente, debe precisarse que el límite máximo de responsabilidad del proveedor será del 10 % del valor total del contrato, salvo en casos de dolo o culpa grave, en los cuales no aplicará dicha limitación. Esta precisión evita interpretaciones amplias que puedan generar cargas desproporcionadas para el proveedor y asegura que las reclamaciones se circunscriban a daños reales, directos y verificables, manteniendo la proporcionalidad y la equidad en la ejecución del contrato.		No se modificará como quiera que hace parte de las condiciones generales del contrato y son disposiciones estándares del Banco.
475	Sección VII. Condiciones Generales del Contrato (CGC)	35, Terminación (i) si el Proveedor no entrega parte o ninguno de los Bienes dentro del período establecido en el Contrato, o dentro de alguna prórroga otorgada por el Comprador de conformidad con la Cláusula 34 de las CGC; o	Solicitamos considerar que la Sala Civil de la Corte Suprema de Justicia ha reiterado que la terminación de un contrato por incumplimiento procede únicamente cuando dicho incumplimiento recae sobre obligaciones esenciales del mismo. Resulta contrario a la buena fe, además de una medida desproporcionada y drástica, dar por terminado un negocio jurídico por la inobservancia de prestaciones secundarias. En este orden de ideas, la terminación contractual solo sería procedente cuando el incumplimiento consista en la no entrega de la totalidad de los bienes pactados, mas no por la falta de entrega parcial de los mismos.		No se acoge la solicitud. Las condiciones contractuales establecidas en la Solicitud de Ofertas corresponden a los Documentos Estándar de Licitación del Banco Interamericano de Desarrollo y se rigen por las Políticas de Adquisiciones GN-2349-15, las cuales son de aplicación obligatoria y no pueden ser modificadas en su contenido esencial. En este marco, las disposiciones relativas a la terminación contractual responden a estándares internacionales aplicables a este tipo de procesos y permiten al comprador adoptar las medidas necesarias frente a incumplimientos que afecten la ejecución del contrato, de conformidad con las condiciones pactadas.
476	Sección VII. Condiciones Generales del Contrato (CGC)	35, Terminación (ii) si el Proveedor no cumple con cualquier otra obligación en virtud del Contrato; o	La terminación del contrato por incumplimiento no puede derivarse de la inobservancia de cualquier obligación accesoria o secundaria, pues ello resultaría contrario al principio de buena fe y desproporcionado frente a la naturaleza del negocio jurídico. En consecuencia, la causal de terminación solo debería operar cuando el incumplimiento recaiga sobre obligaciones esenciales del contrato, de manera que la falta de cumplimiento de deberes secundarios o complementarios no sea considerada suficiente para dar por terminado el vínculo contractual.		No se acoge la solicitud. Las condiciones contractuales establecidas en la Solicitud de Ofertas corresponden a los Documentos Estándar de Licitación del Banco Interamericano de Desarrollo y se rigen por las Políticas de Adquisiciones GN-2349-15, las cuales son de aplicación obligatoria y no pueden ser modificadas en su contenido esencial. En este marco, las disposiciones relativas a la terminación contractual responden a estándares internacionales aplicables a este tipo de procesos y permiten al comprador adoptar las medidas necesarias frente a incumplimientos que afecten la ejecución del contrato, de conformidad con las condiciones pactadas.
477	Sección VII. Condiciones Generales del Contrato (CGC)	35, Terminación (iii) si el Proveedor, a juicio del Comprador, durante el proceso de licitación o de ejecución del Contrato, ha participado en Prácticas Prohibidas, según se define en la Cláusula 3 de las CGC.	Lo citado otorga al comprador una facultad subjetiva y discrecional, sin requerir verificación previa, procedimiento formal de investigación, ni derecho de defensa por parte del proveedor. Tal ambigüedad representa un riesgo jurídico significativo, al permitir la terminación unilateral sin garantías mínimas de debido proceso. Se recomienda ajustar la cláusula para condicionar dicha facultad a la existencia de una decisión debidamente probada, emitida por autoridad competente o por el Banco, y garantizar al proveedor la posibilidad de presentar descargos antes de que se adopte cualquier medida definitiva		No se acoge la solicitud. Las condiciones contractuales establecidas en la Solicitud de Ofertas corresponden a los Documentos Estándar de Licitación del Banco Interamericano de Desarrollo y se rigen por las Políticas de Adquisiciones GN-2349-15, las cuales son de aplicación obligatoria y no pueden ser modificadas en su contenido esencial. En este marco, las disposiciones relativas a la terminación contractual responden a estándares internacionales aplicables a este tipo de procesos y permiten al comprador adoptar las medidas necesarias frente a incumplimientos que afecten la ejecución del contrato, de conformidad con las condiciones pactadas.
478	Sección VII. Condiciones Generales del Contrato (CGC)	35.3 Terminación pro conveniencia (a) El Comprador, mediante comunicación enviada al Proveedor, podrá terminar el Contrato total o parcialmente, en cualquier momento por razones de conveniencia. La comunicación de terminación deberá indicar que la terminación es por conveniencia del Comprador, el alcance de la terminación de las responsabilidades del Proveedor en virtud del Contrato y la fecha de efectividad de dicha terminación.	La redacción propuesta genera un riesgo jurídico y financiero para el proveedor, al facultar al comprador para terminar unilateralmente el contrato por razones de conveniencia, incluso en escenarios de cumplimiento adecuado, sin prever mecanismos de compensación proporcional por las inversiones realizadas. Esta disposición resulta desequilibrada y contraria a la seguridad jurídica, pues permite la terminación sin causa objetiva y sin salvaguardar los derechos del proveedor. Por ello, se recomienda ajustar la cláusula para definir criterios mínimos de procedencia, establecer una compensación razonable que cubra las inversiones y costos asumidos, y garantizar el derecho del proveedor a presentar descargos o reclamaciones antes de la efectividad de la terminación, de manera que la terminación por conveniencia no se convierta en una facultad arbitraria sino en una medida excepcional sujeta a condiciones de proporcionalidad y equidad.		No se acoge la solicitud. Las condiciones contractuales establecidas en la Solicitud de Ofertas corresponden a los Documentos Estándar de Licitación del Banco Interamericano de Desarrollo y se rigen por las Políticas de Adquisiciones GN-2349-15, las cuales son de aplicación obligatoria y no pueden ser modificadas en su contenido esencial. En este marco, las disposiciones relativas a la terminación contractual responden a estándares internacionales aplicables a este tipo de procesos y permiten al comprador adoptar las medidas necesarias frente a incumplimientos que afecten la ejecución del contrato, de conformidad con las condiciones pactadas.
479	C. Preparación de las Ofertas	Estados financieros correspondientes a 2024 con corte a 31 de diciembre, los cuales deberán estar suscritos por un Contador Público y un Revisor Fiscal, cuando las normas que los regulan así lo exigen en el caso de los Oferentes Nacionales. En el caso de los Oferentes que provengan de países diferentes al país del comprador, deberán presentar los documentos o sus equivalentes de acuerdo con las normas del país de origen:	Se solicita a la entidad precisar la Tasa Representativa del Mercado (TRM) que deberá utilizarse para el cálculo de los indicadores financieros, considerando que el presupuesto oficial se encuentra definido en moneda extranjera (USD).		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.
480	Sección III — Criterios de Evaluación y Calificación	5 | Apalancamiento a corto plazo | Pasivo Corriente/Patrimonio | Menor o igual a 0,5	El índice de apalancamiento a corto plazo exigido (Pasivo Corriente / Patrimonio ≤ 0,5) penaliza estructuralmente a empresas en fase de crecimiento acelerado que invierten activamente en capacidad operativa, infraestructura tecnológica y talento especializado. Un nivel de apalancamiento elevado no implica necesariamente riesgo de incumplimiento contractual; por el contrario, puede ser indicador de una estrategia de expansión respaldada por flujos de caja positivos y contratos en ejecución. Este indicador, considerado de manera aislada de los demás índices de solvencia y liquidez ya exigidos en este proceso (liquidez, endeudamiento, patrimonio/presupuesto y capital de trabajo/presupuesto), puede excluir a empresas financieramente sanas pero en etapa de consolidación, reduciendo la competencia efectiva.	Se solicita amablemente a la Entidad evaluar la posibilidad de eliminar el índice de apalancamiento a corto plazo como requisito habilitante, considerando que los cuatro (4) índices restantes ofrecen una visión suficientemente completa de la solidez financiera del oferente. Como alternativa, se sugiere elevar el umbral permitido a un valor menor o igual a 1,0, o sustituir este indicador por un índice de cobertura de servicio de deuda que refleje con mayor precisión la capacidad real de pago del oferente frente a sus obligaciones contractuales.	En atención a la observación no se acepta la solicitud, el indicador se mantiene debido a la envergadura del proyecto.
481	Sección II — Datos de la Licitación (DDL)	IAO 22.1: "La fecha límite para presentar las ofertas es: Fecha: 14 de mayo de 2026. Hora: hasta las 10:00 am (hora legal colombiana)." Anuncio específico de adquisiciones: La audiencia de aclaraciones se celebrará el 15 de abril de 2026 a las 10:30 a.m. hora legal colombiana. [El Anuncio de Adquisiciones referencia las 10:30 a.m. como hora de cierre del proceso, en conflicto con las 10:00 a.m. de la SDO].	Existe una contradicción entre los documentos del proceso respecto a la hora de cierre para la presentación de ofertas el día 14 de mayo de 2026. La Solicitud de Ofertas (DDL, IAO 22.1) establece las 10:00 a.m. como hora límite, mientras que el Anuncio Específico de Adquisiciones hace referencia a las 10:30 a.m. Esta diferencia de treinta (30) minutos puede generar confusión entre los interesados y constituye un riesgo real de rechazo de propuestas presentadas entre las 10:00 y las 10:30 a.m., con el consecuente perjuicio para los oferentes que actúen de buena fe basándose en el Anuncio publicado.	Se solicita amablemente a la Entidad confirmar mediante adenda la hora exacta de cierre para la presentación de ofertas el 14 de mayo de 2026, garantizando que todos los documentos del proceso sean consistentes entre sí, y comunicar la hora definitiva con suficiente antelación para que los interesados puedan ajustar su logística de presentación.	Medinate Adenda, se modificó la IAO 22.1, la cual quedará así: La fecha límite para presentar las ofertas es: Fecha: 9 de junio de 2026 Hora: hasta las 10:00 am (hora legal colombiana) Los Oferentes podrán presentar sus ofertas electrónicamente (de manera virtual).
482	410-Solicitud-de-Oferta-VSD-SdO-SOC		Se evidencia una posible ambigüedad en la interpretación de los requisitos relacionados con la Garantía de Mantenimiento de la Oferta, toda vez que: 1. El numeral 11 establece que la oferta debe contener una Garantía de Mantenimiento de la Oferta o una Declaración de Mantenimiento de la Oferta. 2. El numeral 19.1 indica que el oferente deberá presentar una Declaración de Mantenimiento de la Oferta o bien una Garantía de Mantenimiento de la Oferta, según lo especificado en los DDL. 3. Sin embargo, dentro de los formatos del pliego se indica expresamente que los formatos de Garantía de Mantenimiento de la Oferta (Garantía Bancaria y Fianza) "No aplican", mientras que sí se incluye el formato de Declaración de Mantenimiento de la Oferta. En ese sentido, no resulta claro si: • Para la presentación de la oferta es obligatorio constituir una Garantía de Mantenimiento de la Oferta (instrumento financiero), o • Si únicamente debe presentarse la Declaración de Mantenimiento de la Oferta, conforme al formato incluido en la Sección V. Adicionalmente, en caso de requerirse la Garantía de Mantenimiento de la Oferta, solicitamos se precise: • Si esta debe ser gestionada directamente por el proponente ante una entidad financiera o aseguradora, • O si existe algún procedimiento específico establecido por la entidad contratante o por el Banco Interamericano de Desarrollo (BID) para su emisión. Por lo anterior, respetuosamente solicitamos a la entidad aclarar de manera expresa cuál es el documento válido y exigible para la presentación de la oferta, con el fin de evitar interpretaciones erróneas que puedan derivar en el rechazo de propuestas por requisitos formales.		Se precisa al observante que no existe ambigüedad en relación con la Declaración de Mantenimiento de la Oferta. La IAO 19.1 establece expresamente que para el presente proceso se requiere la presentación de dicha declaración. Asimismo, en la Sección V – Formularios de la Oferta, se incluye el formato denominado "Declaración de Mantenimiento de la Oferta", el cual no presenta anotación alguna de "no aplica". En consecuencia, el oferente deberá diligenciar y presentar dicho formulario conforme a las instrucciones previstas en el mismo.
483	410-Solicitud-de-Oferta-VSD-SdO-SOC		Solicitan Estados financieros correspondientes a 2024 con corte a 31 de diciembre, para lo cual se solicita a la entidad confirmar si para la presentación de la oferta, efectivamente se solicitaran Estados Financieros del 2024, por el corte en el que nos presentamos, donde las renovaciones de matriculas se encuentran actualizados con los Estados financieros a corte del año 2025		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.
484	410-Solicitud-de-Oferta-VSD-SdO-SOC		En relación con el indicador financiero de apalancamiento a corto plazo establecido en el pliego de condiciones (≤ 0,5), nos permitimos presentar la siguiente observación: Respetuosamente solicitamos a la entidad evaluar la pertinencia de ajustar el umbral definido para este indicador, considerando que en diversos sectores económicos es habitual que empresas con adecuada capacidad operativa y financiera presenten niveles de apalancamiento superiores, sin que ello represente un riesgo en el cumplimiento de las obligaciones contractuales. Es importante señalar que el indicador de apalancamiento a corto plazo, por sí solo, no refleja de manera integral la solidez financiera de un proponente. Este puede verse influenciado por estrategias de financiamiento eficientes, dinámicas propias del capital de trabajo o ciclos operativos del negocio. En este sentido, niveles superiores al umbral propuesto pueden coexistir con adecuados índices de liquidez, respaldo patrimonial y capacidad de generación de flujo de caja. Por lo anterior, sugerimos a la entidad considerar la posibilidad de ampliar el rango permitido para este indicador a 0,86 La anterior solicitud se formula con el propósito de promover una mayor pluralidad de oferentes y garantizar los principios de selección objetiva y libre concurrencia, sin comprometer la adecuada ejecución del contrato.		En atención a la observación. no se acepta la solicitud, el indicador se mantiene en las mismas condiciones debido a la envergadura del proyecto.
485	Sección III. Criterios de Evaluación y Calificación	Apalancamiento a corto plazo Menor o igual a 0.5	Principio de Proporcionalidad: Se solicita que los requisitos exigidos sean proporcionales al riesgo. Dado que el contrato es de ejecución sucesiva y por fases, la carga financiera debe medirse frente a la obligación inmediata y no al valor total.	Ajustar el indicador de apalancamiento a <= 0.7	En atención a la observación. no se acepta la solicitud, el indicador se mantiene en las mismas condiciones debido a la envergadura del proyecto.
486	Numeral 20.4 de la Sección I. Carta de Oferta Técnica	20.4 Cuando el Oferente sea una APCA, la Oferta debe estar firmada por un representante autorizado de la APCA en nombre de esta, de manera que sea jurídicamente vinculante para todos los miembros, como lo demuestre un poder suscrito por sus representantes legalmente autorizados.	Con relación al numeral citado y a la carta de oferta técnica en la que se precisa "La persona que firme la Oferta deberá contar con el poder otorgado por el Oferente. El poder deberá adjuntarse a los Formularios de la Oferta , entendemos que el poder al que allí se hace referencia puede incorporarse en el documento constitutivo de la APCA, esto es, en el acuerdo consorcial, siempre que en dicho documento los representantes legales de las sociedades integrantes designen expresamente al representante legal del consorcio (APCA), y le confieran las facultades suficientes para presentar la Oferta y realizar todos los actos que se deriven de esta, de manera que la Oferta resulte jurídicamente vinculante para la totalidad de los miembros. Les agradecemos confirmar si nuestro entendido es correcto.	N/A	Se precisa al observante que su entendido es correcto. En el caso de las APCA, el poder al que hace referencia la IAO 20.4 podrá estar incorporado dentro del documento constitutivo de la APCA (acuerdo consorcial o documento equivalente), siempre que dicho documento: (i) esté suscrito por los representantes legalmente autorizados de todos sus integrantes; (ii) designe expresamente al representante de la APCA; y (iii) le otorgue facultades suficientes para presentar la Oferta y adelantar todas las actuaciones derivadas del proceso de selección y de la eventual ejecución contractual, de manera que la Oferta resulte jurídicamente vinculante para todos los miembros de la APCA.
487	Sección VI (numeral 8)	Los Acuerdos de Niveles de Servicio (ANS) en el ámbito de este proyecto son una herramienta que pretende mejorar la calidad del servicio del SOC y a su vez nivelar las expectativas de las partes involucradas definiendo claramente las reglas que se deben cumplir y las consecuencias en caso de incumplimiento. La formulación y aplicación de los ANS deberá garantizar trazabilidad técnica y jurídica sobre el cumplimiento de cada indicador, su evidencia asociada y su trazabilidad a lo largo del contrato. Las consecuencias económicas por incumplimiento son acumulables en caso de que no se cumpla con más de uno de los ANS descritos, pero en ningún caso podrá superar el 10 % del valor de costo del contrato, en este supuesto la DIAN podrá iniciar la aplicación de las cláusulas de incumplimiento al CONTRATISTA. Para el efecto del pago de estas penalizaciones el CONTRATISTA podrá optar por cubrir estas penalizaciones con servicios adicionales en la operación del SOC, para lo cual el CONTRATISTA podrá proponer la unidad de equivalencia correspondiente entregando a la DIAN un análisis detallado el cual será sujeto a validación y aprobación. Dicho análisis deberá incluir criterios verificables y medibles que permitan a la DIAN validar técnica y jurídicamente la compensación ofrecida, sin alterar la equivalencia real ni sustituir obligaciones sustanciales del contrato.	Con relación a los Acuerdos de Niveles de Servicio (ANS) previstos en el documento, agradeceríamos a la Entidad confirmar su naturaleza jurídica, en particular si estos deben entenderse como un mecanismo de liquidación anticipada de perjuicios. Así mismo, de nuestra lectura los ANS y las deducciones económicas asociadas se encontrarían comprendidos dentro de lo establecido en el numeral 21.7 de la Sección VII Condiciones Generales del Contrato.	N/A	Se precisa al observante que los Acuerdos de Niveles de Servicio (ANS) corresponden a mecanismos de medición y control del desempeño contractual, orientados a verificar el cumplimiento de los niveles de servicio exigidos para la operación del SOC, así como a establecer consecuencias económicas proporcionales frente a eventuales incumplimientos de dichos niveles. No obstante, se aclara que los ANS y las deducciones económicas asociadas son distintos de la liquidación por daños y perjuicios prevista en la Cláusula 27.1 de las Condiciones Generales del Contrato, toda vez que esta última corresponde específicamente a penalidades derivadas del retraso en la entrega de los bienes o en la prestación de los servicios conexos, estableciendo un valor del uno por ciento (1 %) por semana y un tope máximo del diez por ciento (10 %) del valor correspondiente.
488	Sección VIII (numeral 16.4)	La ENTIDAD FIDUCIARIA cancelará el valor del contrato dentro del tiempo previsto en el Reglamento Operativo del Fondo, de acuerdo con los servicios prestados, facturados y recibidos a satisfacción por el Supervisor designado por la DIAN, siempre y cuando el Contratista haya cumplido con la obligación de realizar el pago de sus obligaciones en materia de seguridad social y parafiscales en cumplimiento de la normatividad vigente que regule la materia de acuerdo con leyes del país del Contratista. Documentos soportes para el pago: a) Factura dando estricto cumplimiento a las exigencias legales que establece el artículo 617 del Estatuto Tributario Colombiano, incluyendo en la misma el número del contrato objeto de facturación; b) Acreditación de conformidad con la ley vigente aplicable, de cumplimiento del Contratista de sus obligaciones ante el Sistema de Seguridad Social Integral en Salud y Pensión, aportes parafiscales: Sena, ICBF y Cajas de Compensación Familiar, cuando corresponda, y Administradora de Riesgos Laborales (si es firma nacional) c) la certificación de cumplimiento a satisfacción expedida por el supervisor del contrato en la cual conste el valor a pagar al Contratista; d) Demás documentos requeridos por la Fiduciaria.	Frente la cláusula de condiciones y documentos para el pago, agradecemos a la Entidad precisar cuáles son los "demás documentos requeridos por la Fiduciaria" a los que se hace referencia en el numeral correspondiente, indicando de manera expresa su alcance y listado, con el fin de que los proponentes y el futuro Contratista puedan prever y cumplir oportunamente con dichos requisitos.	N/A	Se aclara al observante que los "demás documentos requeridos por la Fiduciaria" corresponden a aquellos soportes administrativos, financieros o tributarios que, de conformidad con sus procedimientos internos y la normatividad aplicable, puedan resultar necesarios al momento de la ejecución contractual para efectuar los respectivos pagos. En todo caso, dichos documentos serán informados oportunamente al contratista durante la etapa de ejecución del contrato, según corresponda a cada trámite de pago, sin que ello implique la imposición de requisitos adicionales a los previstos en el documento de Solicitud de Ofertas.
489	Sección VIII (numeral 27.1)	El valor de la liquidación por daños y perjuicios será: 1 % por semana	En virtud del principio de proporcionalidad, y considerando la cuantía del Contrato y su plazo de ejecución, solicitamos respetuosamente que el valor de las penalidades semanales se establezca en un porcentaje de hasta el 0,01 % del valor total del contrato. Así mismo, agradecemos a la Entidad confirmar el procedimiento que se aplicará para hacer efectivas dichas penalidades, precisando las etapas, plazos y responsables, y confirmando que en dicho proceso el Contratista contará con el derecho a la defensa, incluida la posibilidad de presentar las explicaciones correspondientes y un plan de acción o de mejora, previo a la aplicación de cualquier deducción.	El valor de la liquidación por daños y perjuicios será: 0,01 % por semana	Se aclara al observante que el porcentaje establecido para la liquidación por daños y perjuicios corresponde a una condición contractual definida por la Entidad en atención a la naturaleza, criticidad y alcance de los servicios requeridos, razón por la cual no se considera procedente modificar el porcentaje señalado en el documento de Solicitud de Ofertas. No obstante, se precisa que la eventual aplicación de dichas penalidades se realizará observando el debido proceso, garantizando al Contratista el derecho de defensa y contradicción. En ese sentido, previo a la imposición de cualquier medida, el supervisor y/o la Entidad pondrán en conocimiento del Contratista los presuntos incumplimientos identificados, otorgándole la posibilidad de presentar las explicaciones, soportes y acciones correctivas o planes de mejora que considere pertinentes para su evaluación.
490	Sección I	Para el caso de Experiencia y Capacidad Técnica, todas las firmas deberán demostrar experiencia, sin perjuicio de la sumatoria que puede realizarse para el cumplimiento del requisito exigido.	Si se presentar a través de una Asociación en Participación, consorcio o asociación -APCA, esto quiere decir que necesariamente las empresas participantes deben demostrar experiencia? No bastaria con que una de ellas la tenga?	Favor responder la Observación / Comentario.	El entendimiento es correcto. Se aclara al observante que, en caso de presentarse una Asociación en Participación, Consorcio o Asociación (APCA), todas las firmas integrantes deberán acreditar experiencia relacionada con el objeto del proceso, sin perjuicio de que la experiencia exigida pueda acreditarse de manera conjunta mediante la sumatoria de las experiencias aportadas por sus integrantes. En consecuencia, no basta con que únicamente uno de los integrantes de la APCA acredite experiencia, toda vez que la condición establecida en el documento requiere que cada una de las firmas participantes demuestre experiencia y capacidad técnica relacionada con los servicios objeto de la contratación.
491	Sección I	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.	Esta condición es aplicable si para esta licitación se participa atraves de un asociación en participación, consorcio, unión temporal, asociación o cualquier otra figura asociativa	Favor responder la Observación / Comentario.	El entendimiento es correcto. La nota aplica para APCAS.
492	Sección I	Estatutos de la Sociedad (o documentos equivalentes de constitución o asociación) o documentos de registro de la persona jurídica antes mencionada, y de conformidad con las IAO 4.1.	Lo correspondiente al aporte de los estatutos, estos deben ser de todos los miembros que conformen esociación en participación, consorcio, unión temporal, asociación o cualquier otra figura asociativa	Favor responder la Observación / Comentario.	Se aclara al observante que, en caso de presentarse una Asociación en Participación, Consorcio, Unión Temporal, Asociación o cualquier otra figura asociativa permitida, deberán aportarse los estatutos, documentos equivalentes de constitución o documentos de registro correspondientes a cada uno de los integrantes que conformen dicha estructura asociativa, de conformidad con lo establecido en las IAO 4.1 y demás disposiciones aplicables del documento de Solicitud de Ofertas.
493	Sección I	GARANTÍA DE MANTENIMIENTO DE LA OFERTA Garantía Bancaria y Fianza	Se debe aportar dos garantias o se es viable escoger alguna de estas dos opciones.	Favor responder la Observación / Comentario.	Se aclara al observante que, de conformidad con lo establecido en la IAO 19.1 de los Datos de la Licitación (DDL), para el presente proceso no se exige la presentación de una Garantía de Mantenimiento de la Oferta, sino únicamente una Declaración de Mantenimiento de la Oferta. En consecuencia, no se requiere aportar simultáneamente garantía bancaria y fianza, ni escoger entre estas modalidades, toda vez que para este proceso el requisito aplicable corresponde exclusivamente a la Declaración de Mantenimiento de la Oferta en los términos previstos en el documento de Solicitud de Ofertas.

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