Cons	Sección	Texto de la sección comentada	Observación / Comentario	Sugerencia de Ajuste	Respuesta
1	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.	Respecto al requisito que exige certificación de vinculación directa y activa con FIRST con una antigüedad mínima de doce (12) meses, se solicita a la entidad revisar dicho condicionamiento. Lo anterior, considerando que la exigencia de una antigüedad específica no necesariamente constituye un factor determinante de la capacidad técnica actual del proponente, en tanto que la membresía activa vigente ya acredita el cumplimiento de estándares internacionales en gestión de incidentes de seguridad. En este sentido, el requisito podría generar una limitación innecesaria a la participación, al incorporar una condición temporal que no aporta de manera proporcional a la evaluación de la idoneidad técnica. Adicionalmente, frente a la participación mediante APCA, exigir que todos los integrantes cumplan este requisito desconoce la lógica de complementariedad propia de estas estructuras, en las cuales las capacidades pueden ser acreditadas de manera conjunta.	1. Eliminar la exigencia de antigüedad mínima de doce (12) meses en la certificación de vinculación a FIRST, manteniendo únicamente la condición de membresía activa; 2. Permitir que, en caso de participación mediante APCA, al menos uno de sus integrantes acredite el cumplimiento de dicho requisito.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la certificación FIRST se solicitad con doce (12) meses de antiguedad, por lo tanto no es posible aceptar su sugerencia, se aclara que en caso de APCA con que uno de los integrantes tenga las certificaciones solicitadas se dará como valida.
2	SECCIÓN III	Entre los contratos presentados se debe cumplir que: Al menos uno (1) debe haber sido ejecutado para el sector Financiero	En relación con el requisito que establece que al menos uno (1) de los contratos debe haber sido ejecutado para el sector financiero, se solicita a la entidad precisar su alcance y los criterios de verificación aplicables. Lo anterior, considerando que el concepto de "sector financiero" no se encuentra definido en el documento, lo que puede dar lugar a interpretaciones disímiles y, en consecuencia, a escenarios de evaluación no uniformes. En particular, se requiere aclarar si dicho concepto: Se limita exclusivamente a entidades formalmente reconocidas dentro del sistema financiero, O si incluye organizaciones con actividades financieras, tales como fintech, cooperativas u otras estructuras con operación financiera. Así mismo, resulta necesario establecer los medios de acreditación válidos para verificar el cumplimiento de este requisito, tales como certificaciones contractuales, naturaleza del contratante u otros elementos objetivos.	Precisar de manera expresa la definición de "sector financiero" aplicable al proceso, así como los criterios y soportes mediante los cuales se verificará su cumplimiento, con el fin de asegurar una evaluación clara, objetiva y consistente.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa que al referirse a "sector financiero" se refiere a lo definido en el Estatuto Orgánico del Sistema Financiero (EOSF) de Colombia, DECRETO <LEY> 663 DE 1993.
3	2,8		Debe tener autoaprendizaje de inventario de activos (CMDB) contando con capacidades de descubrimiento automático para alimentar y mantener actualizada la Base de Datos de Gestión de Configuración (CMDB). Esto implica que el sistema debe ser capaz de identificar, clasificar y registrar de forma dinámica los activos tecnológicos presentes en la infraestructura, incluyendo servidores, estaciones de trabajo, dispositivos de red, aplicaciones y servicios, sin intervención manual constante. Para tal efecto se informa que actualmente la Entidad cuenta con un ITSM del fabricante ARANDA. Características mínimas requeridas: - Descubrimiento automático de nuevos activos en la red. - Actualización continua de la CMDB ante cambios en la infraestructura. - Integración con herramientas de escaneo de red y agentes locales. - Capacidad de correlación entre activos y eventos de seguridad. - Soporte para múltiples entornos (on-premise, nube, híbrido).	La solucion debe integrarse con soluciones para autoaprendizaje de inventario de activos (CMDB) contando con capacidades de descubrimiento automático para alimentar y mantener actualizada la Base de Datos de Gestión de Configuración (CMDB). Para tal efecto se informa que actualmente la Entidad cuenta con un ITSM del fabricante ARANDA. Características mínimas requeridas: - Integrar con la solucion Aranda, para descubrimiento automático de nuevos activos en la red. - Integración con herramientas de escaneo de red y agentes locales. - Capacidad de correlación entre activos y eventos de seguridad. - Soporte para múltiples entornos (on-premise, nube, híbrido).	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas por la Entidad son mínimas y son homologables siempre y cuando cumpla con los requerimientos de la Entidad. Por lo tanto, no es posible ajustar según su sugerencia.
4	2,23		Supervisión del cambio de configuraciones en tiempo real, como mínimo 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.	Supervisión del cambio de configuraciones en tiempo real, como mínimo debe incluir los siguientes elementos: - 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.	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.

5	2,25		Analítica - Búsqueda de eventos en real - sin necesidad de indexación. - Búsquedas por palabras clave basadas en atributos de eventos analizados. - Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API. - Match de patrones complejos en tiempo real. - Uso de objetos CMDB y datos de usuario/identidad y ubicación en búsquedas y reglas. - Programación de informes y entregas de resultados por correo electrónico a los principales interesados. - Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.). - Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico. - Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes. - Análisis escalable mediante la adición de nodos worker en caliente. - Posibilidad de priorización de los informes de incidentes.	Analítica - Búsqueda de eventos en real - Búsquedas por palabras clave basadas en atributos de eventos analizados. - Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API. - Match de patrones complejos en tiempo real. - Uso de objetos CMDB y datos de usuario/identidad y ubicación en búsquedas y reglas. - Programación de informes y entregas de resultados por correo electrónico a los principales interesados. - Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.). - Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico. - Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes. - Análisis escalable - Posibilidad de priorización de los informes de incidentes.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem se ajusta mediante adenda quedando de la siguiente manera: Analítica - Búsquedas por palabras clave basadas en atributos de eventos analizados. - Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API. - Match de patrones complejos en tiempo real. - Programación de informes y entregas de resultados por correo electrónico a los principales interesados. - Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.). - Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico. - Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes.. - Posibilidad de priorización de los informes de incidentes.
6	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.	Paneles de control personalizados, como mínimo debe incluir los siguientes elementos: - Dashboards configurables para monitoreo y analsis de seguridad, con capacidad de realizar integracion para realizar slide-show. - Informes y análisis exportables entre organizaciones y usuarios. - Identificación rápida los problemas críticos, por ejemplo, a través de un código de colores. - Dashboards especializados para servicios empresariales, infraestructura virtualizada y aplicaciones especializadas.	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.
7	2,34		Almacenamiento - Soporte de archivado de logs tanto para NFS como HDFS. - Creación de políticas de retención de logs tanto por espacio como por periodos de tiempo.	Almacenamiento - Soporte de archivado de logs tanto para NFS como HDFS o mediante opcion de almacenamiento escalable como un data-lake que pueda ofrecer la solucion. - Creación de políticas de retención de logs tanto por espacio como por periodos de tiempo.	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.
8	2.37		Nuevo	La solucion de SIEM entregada debe construir reglas basadas en Machine Learning e Inteligencia Artificial	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.
9	2.38		Nuevo	La correlacion debe estar basada en Identidad, no estatica	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.
10	2.39		Nuevo	Cuando se utilicen agentes para los sistemas operativos windows de la DIAN, estos deben realizar telemetria profunda.	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.
11	2.40		Nuevo	El uso del agente debe proveer analisis de comportamiento (UEBA)	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.
12	2.41		Nuevo	El agente en los sistemas operativos windows, debe -realizar analisis de registro. -inspeccion command line -analisis procesos parent/child -analisis de memoria -analisis comportamiento	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.
13	2.42		Nuevo	El agente en windows/linux, debe proveer respuesta automatizada -Aislamiento del dispositivo -Eliminar/detener procesos -bloqueo del usuario	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.
14	2.43		Nuevo	La solucion debe brindar - Hunting queries - Analisis historico - Correlacion Avanzada	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.
15	**5.15**		**Remediacion - Virtual Patching**	Vacia	Vacia
16	5.15.1		El componente debe realizar remediacion multi-vendedor, actuando sobre el stack de seguridad de la DIAN (Fortinet, Palo Alto, Trend Micro). Permitiendo aplicar cambios y parches virtuales desde la consola de gestion.	Importancia Incluir en el capitulo de gestion de vulnerabilidades, un apartado nuevo, en donde se incluya la remediacion de los incidentes, no a traves de los sistemas de ticketing y herramientas de gestion, sino directamente sobre las plataformas de seguridad de la DIAN, via API y de forma automatica. Con esto evitando procesos manuales, que ralenticen la operacion de la DIAN.	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.
17	5.15.2		Este componente, debe verificar que cualquier regla o parche a ser instalados en las soluciones de seguridad, no tendra impacto en la operación de la DIAN, previniendo caidas del servicio.		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.
18	5.15.3		La solucion debe garantizar, que no se activaran protecciones que den lugar a falsos positivos		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.
19	5.15.4		La solucion debe tener la capacidad de evaluar si no existen configuraciones en los controles de seguridad existentes, para que las politicas se cumplan en tiempo real		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.
20	5.15.5		La solucion, debe tener la capacidad de identificar protecciones en el firewall que sean redundantes o esten en desuso.		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.
21	5.15.6		La solucion debera dar recomendaciones para los componentes de IPS en las soluciones existentes en la DIAN (ej, Fortinet, Palto Alto, etc)		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.
22	5.15.7		La solucion debera ofrecer la capacidad de hacer correcciones y remediaciones desde la consola		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.
23	5.15.8		La solucion debera realizar una verificacion, en la cual la aplicación de correcciones, no degraden el servicio.		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.

24	5.15.9		El componente debera tener una facilidad para realizar rollbacks de forma automatica, ante algun fallo en los servicios de la DIAN		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.
25	5.15.10		El componente debe poder realizar correcciones en la postura de la red, teniendo en cuenta los hallazgos de los endpoint		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.
26	5.15.11		El componente debe realizar la remediacion via agentless (sin agentes), via API		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.
27	9.12		La solución debe detectar automáticamente dominios similares (lookalike) y sitios de phishing que abusen de la marca.	Nuevo Se incluyen caracteristicas que generan valor al capitulo de proteccion de marca para la DIAN. Se da un foco sobre la inteligencia y remediacion de incidentes que puedan afectar de forma externa a la DIAN.	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.
28	9.13		Capacidad de detectar perfiles falsos en redes sociales y aplicaciones móviles maliciosas dirigidas a personas clave.		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.
29	9.14		Debe permitir dar de baja sitios fraudulentos y perfiles sociales con pocos clics y de forma escalable.		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.
30	9.15		Despliegue de instancias de detección (beacons) en subdominios para identificar interfaces de login fraudulentas.		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.
31	9.16		la solucion debe monitorear activamente foros de actores de amenazas, grupos de chat ocultos, mercados negros y sitios TOR (.onion)		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.
32	9.17		La solucion debe alertar inmediatamente sobre exposición de correos y contraseñas de funcionarios para prevenir la toma de control de cuentas.		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.
33	9.18		La solucion debe tener capacidad de detectar filtraciones de código fuente, números de tarjetas de crédito y documentos confidenciales de la DIAN		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.
34	9.19		La solucion debe garantizar el acceso a un repositorio histórico y en tiempo real (Data Lake) para realizar investigaciones personalizadas en la Dark Web.		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.
35	9.20		La solucion debe proveer Inteligencia especifica sobre tácticas y actividades recientes de grupos de ransomware y hacktivistas.		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.
36	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.	Respecto al requisito que exige certificación de vinculación directa y activa con FIRST con una antigüedad mínima de doce (12) meses, se solicita a la entidad revisar dicho condicionamiento. Lo anterior, considerando que la exigencia de una antigüedad específica no necesariamente constituye un factor determinante de la capacidad técnica actual del proponente, en tanto que la membresía activa vigente ya acredita el cumplimiento de estándares internacionales en gestión de incidentes de seguridad. En este sentido, el requisito podría generar una limitación innecesaria a la participación, al incorporar una condición temporal que no aporta de manera proporcional a la evaluación de la idoneidad técnica. Adicionalmente, frente a la participación mediante APCA, exigir que todos los integrantes cumplan este requisito desconoce la lógica de complementariedad propia de estas estructuras, en las cuales las capacidades pueden ser acreditadas de manera conjunta.	1. Eliminar la exigencia de antigüedad mínima de doce (12) meses en la certificación de vinculación a FIRST, manteniendo únicamente la condición de membresía activa; 2. Permitir que, en caso de participación mediante APCA, al menos uno de sus integrantes acredite el cumplimiento de dicho requisito.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la certificación FIRST se solicita con doce (12) meses de antiguedad, por lo tanto no es posible aceptar su sugerencia, se aclara que en caso de APCA en caso de que uno de los integrantes tenga las certificaciones solicitadas se dará como valida.
37	SECCIÓN III	(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	Se solicita a la entidad definir de manera expresa la TRM aplicable para la conversión del requisito de experiencia establecido en USD (1.000.000), con el propósito de garantizar condiciones homogéneas y objetivas en la evaluación. Lo anterior, teniendo en cuenta que el requisito permite acreditar experiencia dentro de los últimos siete (7) años, periodo en el cual la TRM ha presentado variaciones relevantes que impactan directamente el valor equivalente en pesos colombianos.	Definir expresamente la TRM aplicable para la conversión (por ejemplo, la TRM del año de ejecución, de suscripción o de liquidación del contrato)	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 se hará el análisis de las certificaciones de acuerdo a lo expuesto en el mismo ítem, no se permite pesos constantes o ajustados.
38	SECCIÓN III	Entre los contratos presentados se debe cumplir que: Al menos uno (1) debe haber sido ejecutado para el sector Financiero	FIN	Precisar de manera expresa la definición de "sector financiero" aplicable al proceso, así como los criterios y soportes mediante los cuales se verificará su cumplimiento, con el fin de asegurar una evaluación clara, objetiva y consistente.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa que al referirse a "sector financiero" se refiere a lo definido en el Estatuto Orgánico del Sistema Financiero (EOSF) de Colombia, DECRETO <LEY> 663 DE 1993.
39	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 amablemente a la entidad ajustar el pliego de condiciones para permitir la participación de soluciones NDR (Network Detection and Response) con arquitecturas híbridas (On Premise y Cloud). Es fundamental que el sistema pueda contar con sensores en las premisas (on-premises, vía appliance o VM) para la captura y retención local de datos, pero permitiendo el uso de componentes de nube para procesos de análisis avanzado del comportamiento que tiene en la red.	Favor responder la Observación / Comentario.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
40	7.18	El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 17727 dispositivos por (3) años.	Se sugiere a la entidad ajustar la opción de contemplar licenciamiento para aceptar modelos basados en ancho de banda o capacidad (throughput). En entornos de red dinámicos, el licenciamiento por capacidad permite una visibilidad completa del tráfico sin las limitaciones administrativas de un conteo de activos variable, asegurando que la solución de NDR opere bajo los estándares óptimos	Favor responder la Observación / Comentario.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
41	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.	Solicitamos a la entidad tener en cuenta soluciones que permitan otras integraciones de seguridad, ya que los formatros aquí mencionados se refieren a un fabricante, lo que no cuenta con pluralidad en los participantes	Favor responder la Observación / Comentario.	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.
42	8.20	En el ciclo de desarrollo las herramientas del CONTRATISTA deben utilizar SASE (Secure Access Services Edge), buscando seguridad en dispositivos móviles, Internet de la cosas y migración de aplicaciones on-premise hacia Cloud.	Solicitamos a la entidad indicar la cantidad de usuarios que deben contar con la solución de SASE, para acotar el requerimiento de acuerdo a la necesidad de la entidad	Favor responder la Observación / Comentario.	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.

43	Sobre la Pluralidad de Oferentes y Sesgo Tecnológico		Respetuosamente solicitamos a la entidad aclarar si, en aras de garantizar el principio de pluralidad de oferentes, la arquitectura técnica y los puntajes de evaluación permitirán la participación de fabricantes distintos a Fortinet y Darktrace como los que se evidencian en las fichas técnicas, siempre que cumplan con la capacidad de integración y migración exigida, evitando que los requerimientos técnicos se conviertan en una limitante para marcas competidoras con capacidades equivalentes.	Respetuosamente solicitamos a la entidad aclarar si, en aras de garantizar el principio de pluralidad de oferentes, la arquitectura técnica y los puntajes de evaluación permitirán la participación de fabricantes distintos a Fortinet y Darktrace como los que se evidencian en las fichas técnicas, siempre que cumplan con la capacidad de integración y migración exigida, evitando que los requerimientos técnicos se conviertan en una limitante para marcas competidoras con capacidades equivalentes.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la Entidad ha estructurado el proceso con base en criterios técnicos orientados a satisfacer sus necesidades operativas y de seguridad, los proponentes podrán presentar sus ofertas con las herramientas, plataformas o software que consideren pertinentes, siempre y cuando cumplan integralmente con los requerimientos técnicos mínimos establecidos en los documentos del proceso.
44	Sobre los Centros de Datos y Conectividad Referencia: Sección VI - Anexo Inventario (Hoja Infraestructura IT).	Texto Original SDO: "Infraestructura Servidores y Almacenamiento... Sitio 1 y 2, SITO".	¿Podría la entidad precisar el número exacto de Centros de Datos activos y si la infraestructura de interconexión para el monitoreo de tráfico (puertos espejo / SPAN-TAP) está basada en medios de Fibra Óptica o Cobre?Dentro de la infraestructura de red, ¿se puede contar con un puerto espejo?	¿Podría la entidad precisar el número exacto de Centros de Datos activos y si la infraestructura de interconexión para el monitoreo de tráfico (puertos espejo / SPAN-TAP) está basada en medios de Fibra Óptica o Cobre?Dentro de la infraestructura de red, ¿se puede contar con un puerto espejo?	La Dirección de Impuestos y Aduanas Nacionales (DIAN) aclara al observante que la conexión entre los dos centros de datos (sitio 1 y sitio 2) se hace mediante fibra oscura, , el interesado podrá presentar en su oferta una propuesta de solución, siempre y cuando cumpla con las condiciones exigidas para este ITEM.
45	2.7 . Sobre la Retención de Información (SIEM) Referencia: Sección VI - Ítem 2 (SIEM).		Respecto al requisito de retención de logs de 12 meses en línea: ¿Aceptaría la entidad una solución que combine un periodo de retención en caliente (Hot Storage) de un mes y el resto del tiempo en almacenamiento de archivo (Cold Storage), siempre que se garantice la integridad forense y un tiempo de recuperación (retrieval) no mayor a pocos minutos para auditorías?	Respecto al requisito de retención de logs de 12 meses en línea: ¿Aceptaría la entidad una solución que combine un periodo de retención en caliente (Hot Storage) de un mes y el resto del tiempo en almacenamiento de archivo (Cold Storage), siempre que se garantice la integridad forense y un tiempo de recuperación (retrieval) no mayor a pocos minutos para auditorías?	La Dirección de Impuestos y Aduanas Nacionales (DIAN) aclara al observante que las características solicitadas por la Entidad corresponden a requerimientos mínimos. En consecuencia, el interesado podrá presentar en su oferta una propuesta de solución, siempre y cuando cumpla con las condiciones exigidas para este ITEM.
46	7. Sobre el Ethical Hacking y Re-Test Referencia: Anexo Técnico Administrativo - Ítem 10.	Texto Original SDO: "10.1 Se deben realizar como mínimo dos (2) ejercicios de ethical hacking por año... como mínimo cien (100) activos".	¿Se requiere que dentro del alcance de cada uno de los dos ejercicios anuales de Ethical Hacking se incluya una fase de re-test para verificar la efectividad de las mitigaciones aplicadas tras el informe inicial?	¿Se requiere que dentro del alcance de cada uno de los dos ejercicios anuales de Ethical Hacking se incluya una fase de re-test para verificar la efectividad de las mitigaciones aplicadas tras el informe inicial?	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, los ejercicios de ethical hacking solicitado deben cumplir con los requerimientos mínimos solicitados en este ítem, no se solicitan retest.
47	8. Sobre el Threat Hunting Referencia: Sección VI - Ítem 6 (Caza de Amenazas)		¿Podría la entidad precisar la periodicidad requerida para los ejercicios de Threat Hunting y si existe un número mínimo de 'hipótesis de caza' que se deban desarrollar mensualmente?	¿Podría la entidad precisar la periodicidad requerida para los ejercicios de Threat Hunting y si existe un número mínimo de 'hipótesis de caza' que se deban desarrollar mensualmente?	La Dirección de Impuestos y Aduanas Nacionales (DIAN) informa al observante que, no se menciona una periodicidad ni cantidad mínima, las características deben funcionar de manera proactiva.
48			¿Tienen alguna herramienta de DFB o DAM para integrar como fuente de datos para monitorear las bases de datos?	¿Tienen alguna herramienta de DFB o DAM para integrar como fuente de datos para monitorear las bases de datos?	La Dirección de Impuestos y Aduanas Nacionales (DIAN) informa al observante que, la Entidad cuenta con firewall de bases de datos que el futuro proveedor del SOC deberá gestionar y administrar.
49	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.	El requisito de exigir una antigüedad mínima de doce (12) meses en la certificación de vinculación a FIRST introduce una barrera que no evidencia una relación directa con la capacidad técnica actual del proponente. La membresía activa vigente ya implica el cumplimiento de estándares internacionales en gestión de incidentes de seguridad, por lo que adicionar una condición temporal no incrementa la idoneidad técnica, pero sí reduce el universo de posibles oferentes sin una justificación técnica clara. Adicionalmente, en el caso de estructuras bajo APCA, exigir este requisito a todos los integrantes desconoce la lógica de complementariedad propia de estas figuras, generando una exigencia más gravosa de la necesaria. En conjunto, estas condiciones pueden derivar en una restricción artificial de la competencia, al limitar la participación de oferentes que cuentan con las capacidades técnicas requeridas.	Se solicita eliminar la exigencia de antigüedad mínima en la certificación FIRST, manteniendo únicamente la condición de membresía activa, y permitir que, en el caso de APCA, el requisito sea acreditado por al menos uno de sus integrantes.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem en mención es puntuable la antigüedad exigida se mantiene en 12 meses, en caso de APCA con que uno de los integrantes de la unión temporal lo acredite se dará como válido.
50	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.	El requisito que exige una antigüedad mínima de doce (12) meses en la certificación de vinculación a FIRST introduce una condición temporal que no necesariamente se traduce en una mejor capacidad técnica para la ejecución del contrato. En la práctica, la membresía activa vigente ya acredita el cumplimiento de estándares internacionales en gestión de incidentes de seguridad, por lo que exigir un tiempo mínimo adicional no aporta un valor diferencial verificable, pero sí puede restringir la participación de oferentes que actualmente cumplen con dichas condiciones técnicas. Adicionalmente, tratándose de esquemas de participación mediante APCA, exigir este requisito a todos los integrantes desconoce la naturaleza de estas estructuras, donde las capacidades son complementarias y pueden ser acreditadas de manera conjunta.	Se solicita eliminar la exigencia de antigüedad mínima en la certificación FIRST, manteniendo únicamente la membresía activa, y permitir que, en estructuras APCA, el requisito sea acreditado por al menos uno de sus integrantes.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la certificación FIRST se solicitad con doce (12) meses de antiguedad, por lo tanto no es posible aceptar su sugerencia, se aclara que en caso de APCA con que uno de los integrantes tenga las certificaciones solicitadas se dará como valida.
51	SECCIÓN III	Entre los contratos presentados se debe cumplir que: Al menos uno (1) debe haber sido ejecutado para el sector Financiero	El requisito que establece que al menos uno de los contratos debe haber sido ejecutado en el "sector financiero" presenta un nivel de indeterminación que puede generar dificultades en su aplicación. La ausencia de una definición concreta del término permite múltiples interpretaciones sobre qué entidades o actividades pueden ser consideradas dentro de dicho sector, lo cual puede traducirse en criterios disímiles durante la evaluación. Así mismo, no se establecen parámetros claros sobre la forma en que dicha condición debe ser acreditada, lo que incrementa el riesgo de inconsistencias en la verificación.	Se solicita precisar el alcance del concepto de "sector financiero", indicando de manera expresa qué tipo de entidades o actividades se consideran válidas, así como los criterios y soportes mediante los cuales se verificará su cumplimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa que al referirse a "sector financiero" se refiere a lo definido en el Estatuto Orgánico del Sistema Financiero (EOSF) de Colombia, DECRETO <LEY> 663 DE 1993.

52	Estrategia de implementación (40 puntos)	Los oferentes deberán allegar como parte de la oferta técnica las siguientes certificaciones vigentes y que sean verificables para lograr la puntuación de la que trata este ítem: • ISO 27001:2022 en los procesos asociados a la operación del SOC • ISO 22301:2019 o superior. • FIRST, 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	En relación con el numeral 2 "Estrategia de implementación (40 puntos)", especificamente en el literal c., donde se solicita la presentación de certificaciones como ISO 27001:2022, ISO 22301:2019, FIRST y otras certificaciones internacionales aplicables al SOC, respetuosamente solicitamos a la entidad aclarar el siguiente aspecto: En caso de que la oferta sea presentada bajo una figura asociativa (APCA, Consorcio o Unión Temporal), entendemos que dichas certificaciones pueden ser acreditadas por cualquiera de los integrantes de la estructura asociativa, siempre que este participe directamente en la ejecución de las actividades relacionadas con la operación del SOC. Agradecemos confirmar si esta interpretación es correcta. Lo anterior, considerando que este tipo de certificaciones suelen estar asociadas a capacidades específicas dentro de los integrantes del equipo, y su acreditación individual dentro de la estructura asociativa permite garantizar la idoneidad técnica sin restringir la participación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en caso de APCA con que uno de los integrantes tenga las certificaciones solicitadas se dará como valida.
53	Anexo Tecnico		En relación con el equipo de trabajo requerido en el Anexo Técnico del proyecto, respetuosamente solicitamos a la entidad aclarar el siguiente aspecto: ¿Es obligatorio presentar, junto con la oferta, la totalidad del equipo de trabajo con sus respectivos soportes (hojas de vida, certificaciones, etc.)? O, en su defecto, ¿es válido presentar una carta de compromiso suscrita por el proponente, en la cual se garantice la disponibilidad del equipo de trabajo requerido para la ejecución del contrato, aportando los soportes correspondientes con posterioridad a la suscripción del acta de inicio? Lo anterior, considerando que en este tipo de proyectos es práctica común permitir la acreditación del equipo mediante compromisos formales en etapa de oferta, garantizando su disponibilidad en la ejecución, lo cual favorece la participación y la estructuración eficiente de las propuestas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el equipo mínimo exigido y sus hojas de vida será presentado por el oferente ganador para la adjudicación.
54	Nota 1	Descripción General y Requerimientos para la DIAN La Dian requiere adquirir, instalar, configurar e implementar un Centro de Operaciones de Seguridad - SOC, el cual debe constar como mínimo de los siguientes componentes y servicios: 1. SIEM - Correlacionador de Eventos (Ver características en el Ítem 2). 2. SOAR - Orquestación, automatización y respuesta de seguridad) (Ver características en el Ítem 3). 3. Herramienta de protección de bases de datos (Ver características en el ítem 4). 4. Monitoreo a la Gestión de Vulnerabilidades (Ver características en el ítem 5). 5. Caza de amenazas (Ver características en el ítem 6). 6. NDR - Detección y respuesta en red e Inteligencia de amenazas (Ver características en el ítem 7). 7. Solución de análisis de código estático y dinámico para aplicaciones (Ver características en el ítem 8). 8. Protección de marca (Ver características en el ítem 9). 9. Ethical hacking (Ver características Hoja Administrativos en ítem 10). 10. Implementación de toda la plataforma y los dispositivos adquiridos (Ver características Hoja Administrativos en ítem 11). 11. Servicios de Monitoreo (Ver características Hoja Administrativos en ítem 12). 12. Garantía y Soporte técnico de tres (3) años (Ver características Hoja Administrativos en ítem 13). 13. Capacitación (Ver características en Hoja Administrativos en ítem 14). 14. Transferencia de Conocimiento (Ver características en Hoja Administrativos en ítem 15). 15. Documentación (Ver características en Hoja Administrativos en ítem 16). 16. Equipo Mínimo de Trabajo (Ver características en Hoja Administrativos en ítem 17). 17. Certificaciones (Ver características en Hoja Administrativos en ítem 18). 18. Gestión de Incidentes (Ver características en Hoja Administrativos en ítem 19). 19. Devolución del servicio (Ver características en Hoja Administrativos en ítem 20). NOTA 1: Se entiende que es un contrato llave en mano. NOTA 2: Todos los elementos adquiridos y entregados producto del presente proceso contractual serán de propiedad de la DIAN.	Respecto a la Nota 1 (Contrato llave en mano) ¿se solicita indicar los crecimientos proyectados a 3 años y en que tiempos aproximados de la vida del proyecto ? , o indicar cual es el crecimiento total al final 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.
55	Nota 1	Descripción General y Requerimientos para la DIAN La Dian requiere adquirir, instalar, configurar e implementar un Centro de Operaciones de Seguridad - SOC, el cual debe constar como mínimo de los siguientes componentes y servicios: 1. SIEM - Correlacionador de Eventos (Ver características en el Ítem 2). 2. SOAR - Orquestación, automatización y respuesta de seguridad) (Ver características en el Ítem 3). 3. Herramienta de protección de bases de datos (Ver características en el ítem 4). 4. Monitoreo a la Gestión de Vulnerabilidades (Ver características en el ítem 5). 5. Caza de amenazas (Ver características en el ítem 6). 6. NDR - Detección y respuesta en red e Inteligencia de amenazas (Ver características en el ítem 7). 7. Solución de análisis de código estático y dinámico para aplicaciones (Ver características en el ítem 8). 8. Protección de marca (Ver características en el ítem 9). 9. Ethical hacking (Ver características Hoja Administrativos en ítem 10). 10. Implementación de toda la plataforma y los dispositivos adquiridos (Ver características Hoja Administrativos en ítem 11). 11. Servicios de Monitoreo (Ver características Hoja Administrativos en ítem 12). 12. Garantía y Soporte técnico de tres (3) años (Ver características Hoja Administrativos en ítem 13). 13. Capacitación (Ver características en Hoja Administrativos en ítem 14). 14. Transferencia de Conocimiento (Ver características en Hoja Administrativos en ítem 15). 15. Documentación (Ver características en Hoja Administrativos en ítem 16). 16. Equipo Mínimo de Trabajo (Ver características en Hoja Administrativos en ítem 17). 17. Certificaciones (Ver características en Hoja Administrativos en ítem 18). 18. Gestión de Incidentes (Ver características en Hoja Administrativos en ítem 19). 19. Devolución del servicio (Ver características en Hoja Administrativos en ítem 20). NOTA 1: Se entiende que es un contrato llave en mano. NOTA 2: Todos los elementos adquiridos y entregados producto del presente proceso contractual serán de propiedad de la DIAN.	Considerando que se solicitan 19 componentes y servicios distintos, se solicita confirmar si la DIAN requiere que exista una integración nativa y bidireccional entre todas las plataformas (ej. que el NDR alimente al SIEM y el SOAR orqueste al escáner de vulnerabilidades). ¿La falta de compatibilidad nativa entre marcas de diferentes fabricantes será considerada un incumplimiento técnico, o se permite el uso de desarrollos a medida (APIs) para lograr la interoperabilidad?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se deberá cumplir con todos y cada uno de los requerimientos solicitados.

56	12	Descripción General y Requerimientos para la DIAN La Dian requiere adquirir, instalar, configurar e implementar un Centro de Operaciones de Seguridad - SOC, el cual debe constar como mínimo de los siguientes componentes y servicios: 1. SIEM - Correlacionador de Eventos (Ver características en el Ítem 2). 2. SOAR - Orquestación, automatización y respuesta de seguridad) (Ver características en el Ítem 3). 3. Herramienta de protección de bases de datos (Ver características en el ítem 4). 4. Monitoreo a la Gestión de Vulnerabilidades (Ver características en el ítem 5). 5. Caza de amenazas (Ver características en el ítem 6). 6. NDR - Detección y respuesta en red e Inteligencia de amenazas (Ver características en el ítem 7). 7. Solución de análisis de código estático y dinámico para aplicaciones (Ver características en el ítem 8). 8. Protección de marca (Ver características en el ítem 9). 9. Ethical hacking (Ver características Hoja Administrativos en ítem 10). 10. Implementación de toda la plataforma y los dispositivos adquiridos (Ver características Hoja Administrativos en ítem 11). 11. Servicios de Monitoreo (Ver características Hoja Administrativos en ítem 12). 12. Garantía y Soporte técnico de tres (3) años (Ver características Hoja Administrativos en ítem 13). 13. Capacitación (Ver características en Hoja Administrativos en ítem 14). 14. Transferencia de Conocimiento (Ver características en Hoja Administrativos en ítem 15). 15. Documentación (Ver características en Hoja Administrativos en ítem 16). 16. Equipo Mínimo de Trabajo (Ver características en Hoja Administrativos en ítem 17). 17. Certificaciones (Ver características en Hoja Administrativos en ítem 18). 18. Gestión de Incidentes (Ver características en Hoja Administrativos en ítem 19). 19. Devolución del servicio (Ver características en Hoja Administrativos en ítem 20). NOTA 1: Se entiende que es un contrato llave en mano. NOTA 2: Todos los elementos adquiridos y entregados producto del presente proceso contractual serán de propiedad de la DIAN.	Respecto al Ítem 19 (Devolución del servicio), se solicita a la Entidad definir el alcance y duración del periodo de transición. ¿Se espera que el contratista mantenga la operación y el soporte técnico (Ítem 12) sin costo adicional durante el empalme con un nuevo proveedor? Asimismo, ¿cuál es el formato y la profundidad de la data histórica (logs y casos) que debe ser entregada para garantizar la continuidad del negocio?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, dentro del anexo técnico se menciona una fase de devolución que detalla los requerimientos para esta actividad.
57		**Descripción General y Requerimientos para la DIAN** 1.3 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.	Respecto a la administración de IBM QRadar e IBM Guardium hasta sus fechas de retiro, se solicita a la Entidad aclarar si el contratista será responsable únicamente de la operación lógica (configuración de reglas, monitoreo y gestión de incidentes) o si también debe asumir el soporte de hardware y la renovación de suscripciones ante el fabricante IBM hasta el momento de la transición. ¿Se exime al proponente de responsablilidad ante fallos catastróficos de hardware o falta de parches de seguridad si el fabricante ya no provee soporte oficial para esas versiones específicas, o no se tiene activo este componente de soporte en el servicio por la entidad o sus terceros ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor del SOC será responsable de la gestión, administración y demás actividades propias de la operación de las plataformas SIEM y Firewall de bases de datos de la Entidad, se aclara que dichas plataformas cuentan con el respectivo soporte del fabricante.
58	2.5	**Especificaciones Técnicas SIEM** 2.5 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.	En relación con el requerimiento de licenciamiento mínimo para 2.467 dispositivos (incluyendo el 20% de crecimiento proyectado), se solicita a la DIAN aclarar el mecanismo de gestión en caso de que durante la operación se supere dicho umbral. Específicamente: ¿se contempla un modelo de ajuste contractual y presupuestal para el incremento de dispositivos y/o consumo (por ejemplo, EPS u otra métrica equivalente), considerando que estos implican licenciamiento y recursos adicionales? Asimismo, ¿se acepta que el contratista notifique estos incrementos mediante reportes periódicos (mensuales) y que, previa validación por parte de la Entidad, se proceda con la ampliación correspondiente bajo un esquema de costos adicionales?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las cantidades solicitadas son requerimientos mínimos por lo tanto la Entidad no exigirá cumplimiento más allá de esas cantidades.
59	2.7	**Especificaciones Técnicas SIEM** 2.7 Debe manejar tasa de retención de doce (12) meses en línea y doce (12) meses fuera de línea.	En relación con los requerimientos de retención de logs (12 meses en línea y 12 meses fuera de línea), se solicita a la DIAN aclarar si la infraestructura de almacenamiento deberá ser provista por el contratista o por la Entidad. En caso de ser responsabilidad del contratista, ¿existe alguna restricción sobre la ubicación de dichos datos (on-premise en las instalaciones de la DIAN / Proveedor o posibilidad de uso de servicios en la nube), particularmente en términos de regulación, residencia de datos y conectividad? Asimismo, se solicita confirmar si se permite el uso de arquitecturas híbridas (almacenamiento local + nube) para optimizar costos y desempeño.		La Dirección de Impuestos y Aduanas Nacionales (DIAN) aclara al observante que las características solicitadas por la Entidad corresponden a requerimientos mínimos. En consecuencia, el interesado deberá proveer lo suficiente y necesario para cumplirlas con las soluciones que estime conveniente siempre y cuando se cumpla con lo solicitado.
60	2.8	**Especificaciones Técnicas SIEM** 2.8 Debe tener autoaprendizaje de inventario de activos (CMDB) contando con capacidades de descubrimiento automático para alimentar y mantener actualizada la Base de Datos de Gestión de Configuración (CMDB). Esto implica que el sistema debe ser capaz de identificar, clasificar y registrar de forma dinámica los activos tecnológicos presentes en la infraestructura, incluyendo servidores, estaciones de trabajo, dispositivos de red, aplicaciones y servicios, sin intervención manual constante. Para tal efecto se informa que actualmente la Entidad cuenta con un ITSM del fabricante ARANDA. Características mínimas requeridas: - Descubrimiento automático de nuevos activos en la red. - Actualización continua de la CMDB ante cambios en la infraestructura. - Integración con herramientas de escaneo de red y agentes locales. - Capacidad de correlación entre activos y eventos de seguridad. - Soporte para múltiples entornos (on-premise, nube, híbrido).	En relación con el requerimiento de autoaprendizaje de inventario de activos (CMDB) y su integración con la plataforma ITSM actual Aranda ITSM, se solicita a la DIAN aclarar cuál será el modelo de gobierno y responsabilidad sobre la calidad, actualización y consistencia de la información de activos. Específicamente: ¿el contratista será responsable únicamente de alimentar y correlacionar la información descubierta o también de la depuración, normalización y mantenimiento de la CMDB institucional?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, solo será responsable de alimentar y correlacionar la información
61	2.8	**Especificaciones Técnicas SIEM** 2.8 Debe tener autoaprendizaje de inventario de activos (CMDB) contando con capacidades de descubrimiento automático para alimentar y mantener actualizada la Base de Datos de Gestión de Configuración (CMDB). Esto implica que el sistema debe ser capaz de identificar, clasificar y registrar de forma dinámica los activos tecnológicos presentes en la infraestructura, incluyendo servidores, estaciones de trabajo, dispositivos de red, aplicaciones y servicios, sin intervención manual constante. Para tal efecto se informa que actualmente la Entidad cuenta con un ITSM del fabricante ARANDA. Características mínimas requeridas: - Descubrimiento automático de nuevos activos en la red. - Actualización continua de la CMDB ante cambios en la infraestructura. - Integración con herramientas de escaneo de red y agentes locales. - Capacidad de correlación entre activos y eventos de seguridad. - Soporte para múltiples entornos (on-premise, nube, híbrido).	Adicionalmente, se solicita confirmar si la Entidad garantizará los accesos, permisos y condiciones técnicas necesarias para la ejecución de descubrimiento automático (escaneo de red, despliegue de agentes, integraciones vía API), así como posibles restricciones en segmentos de red o entornos (on-premise, nube o híbridos).		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la Entidad garantizará los respectivos accesos y permisos necesarios para la ejecución de las diferentes actividades.

62	2.8	**Especificaciones Técnicas SIEM** 2.8 Debe tener autoaprendizaje de inventario de activos (CMDB) contando con capacidades de descubrimiento automático para alimentar y mantener actualizada la Base de Datos de Gestión de Configuración (CMDB). Esto implica que el sistema debe ser capaz de identificar, clasificar y registrar de forma dinámica los activos tecnológicos presentes en la infraestructura, incluyendo servidores, estaciones de trabajo, dispositivos de red, aplicaciones y servicios, sin intervención manual constante. Para tal efecto se informa que actualmente la Entidad cuenta con un ITSM del fabricante ARANDA. Características mínimas requeridas: - Descubrimiento automático de nuevos activos en la red. - Actualización continua de la CMDB ante cambios en la infraestructura. - Integración con herramientas de escaneo de red y agentes locales. - Capacidad de correlación entre activos y eventos de seguridad. - Soporte para múltiples entornos (on-premise, nube, híbrido).	Finalmente, se solicita aclarar cómo se gestionarán las discrepancias entre la información descubierta automáticamente y la registrada en la CMDB, y si estas tendrán algún impacto en los niveles de servicio o responsabilidades del contratista.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, no tendrán impacto en los niveles de servicio o responsabilidades del contratista.
63	2.9	**Especificaciones Técnicas SIEM** 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	En relación con el requerimiento de correlación cruzada entre SOC y NOC, y la integración con la plataforma de monitoreo actual SolarWinds Orion, se solicita a la DIAN aclarar el alcance, nivel de acceso y responsabilidades asociadas a dicha integración. Específicamente: ¿el contratista contará con acceso completo a las APIs, bases de datos, métricas y eventos necesarios para realizar la correlación en tiempo real, o existirán restricciones técnicas o de seguridad que deban considerarse?		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.
64	2.9	**Especificaciones Técnicas SIEM** 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	Adicionalmente, se solicita confirmar si la Entidad garantizará la disponibilidad, calidad y consistencia de los datos provenientes del NOC, y cómo se gestionarán escenarios en los que dicha información sea incompleta, inconsistente o no esté disponible, confirmando que esto no es un cumplimiento de los niveles de servicio por parte del contratista del presente contrato.		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.
65	2.9	**Especificaciones Técnicas SIEM** 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	Finalmente, se solicita aclarar si los casos de uso de correlación SOC/NOC serán definidos y priorizados por la DIAN o si se espera que el contratista los diseñe e implemente, así como el mecanismo de gestión de nuevos requerimientos durante la fase operativa, así como cuantos casos se deben cumplir durante la vida de contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclarar que, los casos de uso serán definidos y diseñados por el proveedor del SOC, en las cantidades mínimas requeridas por la Entidad, los demás serán bajo demanda de la Entidad, y no tiene un número máximo.
66	2.12	**Especificaciones Técnicas SIEM** 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 relación con el requerimiento de monitoreo de transacciones sintéticas, se solicita a la DIAN aclarar el alcance funcional y responsabilidades asociadas a esta capacidad. Específicamente: ¿cuáles son las aplicaciones, y sistemas críticos que deberán ser incluidos dentro de este monitoreo y si existe un inventario priorizado de los mismos?, y confirmar si este puede variar y porcentualmente cuanto durante la vida del contrato ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem en mención 2.12 se elimina mediante adenda.
67	2.12	**Especificaciones Técnicas SIEM** 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.	Se solicita confirmar si la Entidad proveerá los accesos, credenciales, flujos transaccionales y ambientes necesarios para la construcción y ejecución de dichas transacciones, así como la infraestructura requerida para desplegar los agentes o puntos de monitoreo desde la perspectiva de usuario final (internos y/o externos).		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem en mención 2.12 se elimina mediante adenda.
68	2.12	**Especificaciones Técnicas SIEM** 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.	Se solicita aclarar que el contratista será responsable únicamente de la generación y correlación de las métricas obtenidas, y no del análisis y gestión de incidentes derivados de degradaciones de rendimiento o disponibilidad detectadas en las aplicaciones, considerando que estas pueden depender de componentes fuera del alcance del SOC.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem en mención 2.12 se elimina mediante adenda.
69	2.14	**Especificaciones Técnicas SIEM** 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.	En relación con el requerimiento de desarrollar y ejecutar 20 casos de uso durante la fase de implementación, se solicita a la Entidad aclarar si existe un catálogo predefinido de casos de uso o si estos deben ser diseñados desde cero por el contratista.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, serán diseñados desde cero por el contratista.
70	2.14	**Especificaciones Técnicas SIEM** 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.	Adicionalmente, se solicita definir el procedimiento de gestión de cambios y los tiempos de respuesta (SLA) para la creación de nuevos casos de uso, dado que su implementación puede depender de la integración de nuevas fuentes de datos o ajustes en la arquitectura que no fueron contemplados inicialmente.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los tiempos serán acordados con la Entidad.

71	2.14	**Especificaciones Técnicas SIEM** 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.	Sobre el requerimiento de que el know-how y las parametrizaciones queden para la Entidad, se solicita a la DIAN confirmar los entregables esperados para cumplir con este punto (ej. manuales de configuración, diccionarios de datos, guías de usuario, sesiones de transferencia técnica).		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los entregables serán acordados con la Entidad.
72	2.14	**Especificaciones Técnicas SIEM** 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.	Asimismo, se solicita aclarar si esta transferencia se limita a la configuración específica sobre la plataforma suministrada o si implica la entrega de scripts, conectores personalizados o desarrollos de software propietarios que el proponente pueda utilizar como valor agregado.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se deberá entregar todo lo necesario asegurando know how y las respectivas parametrizaciones, según lo acordado con la Entidad.
73	2.17	**Especificaciones Técnicas SIEM** 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")	Considerando que la infraestructura tecnológica es dinámica, se solicita a la Entidad aclarar, si la cantidad de dispositivos en el anexo "Inventario Infraestructura IT" se considera la línea base definitiva para el dimensionamiento de la oferta económica, o los crecimientos estimados durante la vida del contrato y como se manejaría dicho incremento en cuanto al componente de precios, la entidad lo cancela como un servicio adicional ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las cantidades solicitadas son las mínimas, y será lo exigido por la Entidad.
74	2.17	**Especificaciones Técnicas SIEM** 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")	Se solicita a la DIAN definir el nivel de profundidad del monitoreo requerido para los activos del inventario. ¿Se espera un monitoreo básico de disponibilidad (Up/Down) o se requiere el monitoreo detallado de métricas de rendimiento (CPU, Memoria, E/S de disco), estados de salud de hardware y cumplimiento de configuración?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, será un monitoreo detallado basado en lo requerido en el anexo técnico.
75	2.17	**Especificaciones Técnicas SIEM** 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")	En relación con el anexo "Inventario Infraestructura IT", se solicita a la Entidad confirmar si la totalidad de los activos allí listados cuentan con protocolos estándar de gestión (SNMP v2/v3, WMI, SSH, Syslog) habilitados y con las credenciales necesarias disponibles para el contratista desde el inicio de la ejecución, adicionalmete confirmar que para IT o recursos de usuario final que no cuenten con estas capacidades , no seran causal de penalidad hacia el contratista durante la vida del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, infraestructura tecnológica de la Entidad cuenta con los protocolos estándar y se darán los respectivos accesos.
76	2.18	**Especificaciones Técnicas SIEM** 2.18 Una vez integrada toda la plataforma tecnológica, se debe configurar y afinar la herramienta de correlación para mejorar su funcionalidad, tomando como base al menos los siguientes eventos: - Actividades asociadas a la administración de cuentas de usuario final (UserID) - Actividades asociadas a cuentas de altos privilegios, automáticas de procesos o asignadas a usuarios administradores (root, sa, administrator). - Ejecución de comandos especiales sobre sistemas operativos - Ejecución de comandos especiales sobre bases de datos (dump,drop, delete, insert, update) - Cambios de parámetros técnicos, de configuración o de seguridad - Cambios de configuración horaria. - Cambios no autorizados en recursos tecnológicos críticos - Actividades de conexión de cuentas de usuario final o administradores. - Actividades asociadas a manipulación de bitácoras técnicas (LOGs) o interrupciones en el envío de los LOGs. - Actividades asociadas a conexión de acceso remoto. - Actividades asociadas a la no efectividad de controles en el ejercicio del monitoreo transaccional.	Respecto al listado de eventos de correlación requeridos (ej. comandos en SO, comandos en BD, cambios de configuración), se solicita a la Entidad confirmar si los activos tecnológicos del inventario ya cuentan con las políticas de auditoría y niveles de logging (verbose/debug) necesarios para generar dichos evento		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, infraestructura tecnológica de la Entidad cuenta con los protocolos estándar y se darán los respectivos accesos.
77	2.18	**Especificaciones Técnicas SIEM** 2.18 Una vez integrada toda la plataforma tecnológica, se debe configurar y afinar la herramienta de correlación para mejorar su funcionalidad, tomando como base al menos los siguientes eventos: - Actividades asociadas a la administración de cuentas de usuario final (UserID) - Actividades asociadas a cuentas de altos privilegios, automáticas de procesos o asignadas a usuarios administradores (root, sa, administrator). - Ejecución de comandos especiales sobre sistemas operativos - Ejecución de comandos especiales sobre bases de datos (dump,drop, delete, insert, update) - Cambios de parámetros técnicos, de configuración o de seguridad - Cambios de configuración horaria. - Cambios no autorizados en recursos tecnológicos críticos - Actividades de conexión de cuentas de usuario final o administradores. - Actividades asociadas a manipulación de bitácoras técnicas (LOGs) o interrupciones en el envío de los LOGs. - Actividades asociadas a conexión de acceso remoto. - Actividades asociadas a la no efectividad de controles en el ejercicio del monitoreo transaccional.	¿En caso de que un sistema crítico no soporte técnicamente la generación de alguno de los eventos listados (ej. comandos dump en versiones específicas de BD o cambios de configuración horaria en equipos cerrados), se considerará este punto como una excepción técnica ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el plan solicitado debe cumplir con los requerimientos mínimos solicitados en este ítem, el futuro contratista deberá tenerlos en cuenta, y desde allí diseñar su propuesta de acuerdo a la experticia del interesado conforme a los escenarios que considere necesarios para este fin.
78	2.18	**Especificaciones Técnicas SIEM** 2.18 Una vez integrada toda la plataforma tecnológica, se debe configurar y afinar la herramienta de correlación para mejorar su funcionalidad, tomando como base al menos los siguientes eventos: - Actividades asociadas a la administración de cuentas de usuario final (UserID) - Actividades asociadas a cuentas de altos privilegios, automáticas de procesos o asignadas a usuarios administradores (root, sa, administrator). - Ejecución de comandos especiales sobre sistemas operativos - Ejecución de comandos especiales sobre bases de datos (dump,drop, delete, insert, update) - Cambios de parámetros técnicos, de configuración o de seguridad - Cambios de configuración horaria. - Cambios no autorizados en recursos tecnológicos críticos - Actividades de conexión de cuentas de usuario final o administradores. - Actividades asociadas a manipulación de bitácoras técnicas (LOGs) o interrupciones en el envío de los LOGs. - Actividades asociadas a conexión de acceso remoto. - Actividades asociadas a la no efectividad de controles en el ejercicio del monitoreo transaccional.	Con el fin de dimensionar correctamente el esfuerzo de afinación y evitar falsos positivos, se solicita aclarar si la DIAN entregará una Matriz de Control donde se detallen las cuentas de administración autorizadas para evitar alertas innecesarias durante la fase de afinación.		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.
79	2.19	**Especificaciones Técnicas SIEM** 2.19 Contexto en tiempo real para análisis de seguridad que incluya como mínimo: - Actualización continua del contexto, de los dispositivos, su software y parches instalados, así como los servicios en ejecución. - Análisis del rendimiento de aplicaciones y sistemas junto con datos del entorno para identificar rápidamente problemas de seguridad. - Contexto de usuario, en tiempo real, con seguimiento de direcciones IP, cambios de identidad de usuario, contexto de datos de ubicación física y geo-localización. - Detección de dispositivos, aplicaciones de red y cambios de configuración no autorizados.	Relacionado con el "seguimiento de direcciones IP, cambios de identidad de usuario y geolocalización", se solicita aclarar: Si la Entidad proveerá acceso a los logs de Active Directory y servidores DHCP para realizar la correlación usuario-IP de manera precisa. Si para la geolocalización es aceptable el uso de bases de datos de reputación IP públicas/estándar. ¿Cómo se espera capturar el "contexto de datos de ubicación física" para dispositivos dentro de la red corporativa (ej. por puerto de switch, AP inalámbrico o GPS del dispositivo),? adicionalmente en caso de que un activo no lo permita no sera causal de penalidad al contratista.		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.

80	2.20	**Especificaciones Técnicas SIEM** 2.20 - 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 .	Sobre el contexto de aplicaciones y servicios de infraestructura (DNS, DHCP, Web, DB, etc.), se solicita confirmar que el alcance implica unicamente el monitoreo del estado del proceso/servicio en el servidor.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el alcance está descrito en el respectivo ítem.
81	2.20	**Especificaciones Técnicas SIEM** 2.20 - 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 .	Para los dispositivos ambientales (UPS, HVAC) y el hardware del dispositivo, se solicita confirmar si todos los equipos cuentan con tarjetas de gestión de red (NMC) y si soportan el protocolo SNMP (v2c o v3), y en caso que no se tengan se pide confirmar que no sera responsabilidad del oferente del servicio el garantizar estos recursos ni configuraciones.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, infraestructura tecnológica de la Entidad cuenta con los protocolos estándar y se darán los respectivos accesos.
82	2.22	**Especificaciones Técnicas SIEM** 2.22 Supervisión de rendimiento, como mínimo debe incluir los siguientes elementos: - Monitor de métricas de sistema (almacenamiento, rendimiento, memoria, etc). - Estado del sistema a través de SNMP, WMI, PowerShell. - Estado de aplicaciones a través de JMX, WMI, PowerShell. - Supervisión de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster. - Monitorización del rendimiento de aplicaciones a medida. - Microsoft Active Directory y Exchange a través de WMI y Powershell. - Posibilidad de agregar métricas personalizadas.	Respecto al requerimiento de supervisión mediante PowerShell, WMI y JMX, se solicita a la Entidad confirmar si las políticas de endurecimiento (hardening) de los servidores permiten la ejecución de scripts remotos y el uso de WinRM. Asimismo, para el monitoreo de aplicaciones Java vía JMX, ¿se garantiza que las máquinas virtuales Java (JVM) de la DIAN están configuradas para permitir conexiones de monitoreo ?		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.
83	2.22	**Especificaciones Técnicas SIEM** 2.22 Supervisión de rendimiento, como mínimo debe incluir los siguientes elementos: - Monitor de métricas de sistema (almacenamiento, rendimiento, memoria, etc). - Estado del sistema a través de SNMP, WMI, PowerShell. - Estado de aplicaciones a través de JMX, WMI, PowerShell. - Supervisión de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster. - Monitorización del rendimiento de aplicaciones a medida. - Microsoft Active Directory y Exchange a través de WMI y Powershell. - Posibilidad de agregar métricas personalizadas.	Sobre la monitorización de "aplicaciones a medida", se solicita a la DIAN definir el alcance técnico esperado. ¿Se refiere al monitoreo de disponibilidad del proceso y consumo de recursos del servidor, o se requiere una integración profunda tipo APM (Application Performance Monitoring) para medir tiempos de respuesta de transacciones, latencia de consultas a bases de datos o errores a nivel de código?		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.
84	2.22	**Especificaciones Técnicas SIEM** 2.22 Supervisión de rendimiento, como mínimo debe incluir los siguientes elementos: - Monitor de métricas de sistema (almacenamiento, rendimiento, memoria, etc). - Estado del sistema a través de SNMP, WMI, PowerShell. - Estado de aplicaciones a través de JMX, WMI, PowerShell. - Supervisión de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster. - Monitorización del rendimiento de aplicaciones a medida. - Microsoft Active Directory y Exchange a través de WMI y Powershell. - Posibilidad de agregar métricas personalizadas.	En relación con la supervisión de virtualización (VMware y Hyper-V), se solicita confirmar que el alcance se limita únicamente a la visualización del estado actual y alertas de rendimiento.		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.
85	2.22	**Especificaciones Técnicas SIEM** 2.22 Supervisión de rendimiento, como mínimo debe incluir los siguientes elementos: - Monitor de métricas de sistema (almacenamiento, rendimiento, memoria, etc). - Estado del sistema a través de SNMP, WMI, PowerShell. - Estado de aplicaciones a través de JMX, WMI, PowerShell. - Supervisión de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster. - Monitorización del rendimiento de aplicaciones a medida. - Microsoft Active Directory y Exchange a través de WMI y Powershell. - Posibilidad de agregar métricas personalizadas.	Para el monitoreo de Active Directory y Exchange, se solicita confirmar si la Entidad proveerá cuentas de servicio con los privilegios mínimos necesarios (ej. View-Only Organization Management en Exchange o permisos de lectura en el contenedor de auditoría de AD).		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.
86	2.22	**Especificaciones Técnicas SIEM** 2.22 Supervisión de rendimiento, como mínimo debe incluir los siguientes elementos: - Monitor de métricas de sistema (almacenamiento, rendimiento, memoria, etc). - Estado del sistema a través de SNMP, WMI, PowerShell. - Estado de aplicaciones a través de JMX, WMI, PowerShell. - Supervisión de virtualización para VMware, HyperV - guest, host, pool de recursos y estado del clúster. - Monitorización del rendimiento de aplicaciones a medida. - Microsoft Active Directory y Exchange a través de WMI y Powershell. - Posibilidad de agregar métricas personalizadas.	Se solicita a la Entidad aclarar si estas metricas serán definidas durante la fase de implementación inicial o si el contratista debe contemplar una bolsa de horas o soporte recurrente para la creación de nuevos monitores personalizados durante la fase de operación, en caso contrario indicar cuantas metricas personalizadas y de que tipo se deben incluir durante la vida del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las métricas se mencionan en el ítem y las demás serán definidas durante la implementación.
87	2.23	**Especificaciones Técnicas SIEM** 2.23 Supervisión del cambio de configuraciones en tiempo real, como mínimo 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.	Respecto al requerimiento de 'Recopilar archivos de configuración de red almacenados en un repositorio versionado', se solicita aclarar si la DIAN aceptará que el SIEM cumpla esta función mediante la captura y almacenamiento de los logs de cambio (diff) o si la solución propuesta debe incluir obligatoriamente un módulo de gestión de configuraciones (NCM) que realice la descarga proactiva y el almacenamiento físico del archivo de configuración completo.		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.
88	2.23	**Especificaciones Técnicas SIEM** 2.23 Supervisión del cambio de configuraciones en tiempo real, como mínimo 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.	Sobre la recopilación de versiones de software instaladas, se solicita a la Entidad confirmar si es aceptable que el SIEM genere un inventario basado en los logs de instalación/actualización recolectados, o si se requiere que la herramienta realice un escaneo activo (crawling) de los sistemas de archivos de todos los servidores para versionar cada ejecutable instalado.		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.

89	2.23	**Especificaciones Técnicas SIEM** 2.23 Supervisión del cambio de configuraciones en tiempo real, como mínimo 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.	Para la detección de cambios en archivos y carpetas (quién y qué), se solicita a la DIAN aclarar si se requiere la visualización de la diferencia de contenido (payload) antes y después del cambio. De ser así, se solicita confirmar si la Entidad permitirá la instalación de agentes con capacidades FIM en los servidores críticos, dado que los logs estándar de sistema operativo solo informan que el archivo fue modificado, pero no el contenido del cambio.		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.
90	2.23	**Especificaciones Técnicas SIEM** 2.23 Supervisión del cambio de configuraciones en tiempo real, como mínimo 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.	En relación con la detección de cambios en el registro de Windows, y con el fin de no afectar el rendimiento de los servidores ni saturar el volumen de eventos (EPS) del SIEM, se solicita a la Entidad definir las ramas (hives) o llaves específicas del registro que se consideran críticas para el monitoreo. ¿Se aceptará una política de monitoreo basada únicamente en llaves de configuración del sistema y seguridad?		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.
91	2.23	**Especificaciones Técnicas SIEM** 2.23 Supervisión del cambio de configuraciones en tiempo real, como mínimo 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 aclarar el alcance de 'Detección automatizada de cambios desde un archivo de configuración'. ¿Se refiere a que el SIEM debe detectar cambios en sus propios archivos de configuración (autoprotección) o que debe monitorear archivos de configuración de aplicaciones de terceros? En caso de ser lo segundo, ¿la DIAN entregará la estructura y ubicación de dichos archivos para la creación de las reglas de correlac		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.
92	2.24	**Especificaciones Técnicas SIEM** 2.24 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	Respecto al establecimiento de patrones de comportamiento base para usuarios finales, se solicita a la Entidad indicar la cantidad exacta de usuarios nominales (identidades únicas) que deberán ser analizados por la plataforma desde el inicio. Esto es indispensable para dimensionar el motor de analítica, el licenciamiento de UEBA y el almacenamiento de perfiles históricos.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, no se maneja una cantidad exacta de usuarios nominales, las características solicitadas deben cubrir la infraestructura tecnológica de la Entidad.
93	2.24	**Especificaciones Técnicas SIEM** 2.24 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	Se solicita aclarar el procedimiento técnico y económico si el número de usuarios finales supera la cantidad inicialmente proyectada. ¿Deberá la Entidad suministrar hardware adicional para mantener el rendimiento del análisis de anomalías, o se establecerá un umbral de crecimiento máximo permitido (ej. 10%) dentro de la oferta original para cubrir el licenciamiento y recursos de cómputo, y en caso que se supere se costeara como algo adicional ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, no se maneja una cantidad exacta de usuarios nominales, las características solicitadas deben cubrir la infraestructura tecnológica de la Entidad, sin incurrir en costos adicionales para la Entidad.
94	2.24	**Especificaciones Técnicas SIEM** 2.24 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	En caso de presentarse crecimientos de usuarios no indicados, se solicita confirmar que el contratista no será penalizado por degradación en tiempos de respuesta o pérdida de visibilidad de anomalías hasta que se realice el ajuste en hardware y licencias		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el plan solicitado debe cumplir con los requerimientos mínimos solicitados en este ítem, el futuro contratista deberá tenerlos en cuenta, y desde allí diseñar su propuesta de acuerdo a la experticia del interesado conforme a los escenarios que considere necesarios para este fin.
95	2.24	**Especificaciones Técnicas SIEM** 2.24 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	Para establecer patrones base con granularidad de hora y día de la semana, se solicita confirmar cuál es el periodo de aprendizaje (learning phase) mínimo aceptado (ej. 60 días) antes de que las alertas de anomalías se consideren válidas para efectos de cumplimiento de SLA		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, el plan solicitado debe cumplir con los requerimientos mínimos solicitados en este ítem, el futuro contratista deberá tenerlos en cuenta, y desde allí diseñar su propuesta con los respectivos valores agregados de acuerdo a la experticia del interesado.
96	2.25	**Especificaciones Técnicas SIEM** 2.25 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	Respecto a la búsqueda de eventos en tiempo real sin indexación, se solicita a la Entidad aclarar si existe un límite de volumen de datos (GB) o un periodo de tiempo máximo sobre el cual se realizarán estas consultas para garantizar los tiempos de respuesta.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem 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: Analítica - Búsquedas por palabras clave basadas en atributos de eventos analizados. - Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API. - Match de patrones complejos en tiempo real. - Programación de informes y entregas de resultados por correo electrónico a los principales interesados. - Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.). - Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico. - Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes.. - Posibilidad de priorización de los informes de incidentes.
97	2.25	**Especificaciones Técnicas SIEM** 2.25 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	Asimismo, sobre la adición de nodos worker en caliente, ¿la Entidad suministrará la infraestructura de hardware/virtualización de forma inmediata ante un crecimiento del flujo de datos, o el contratista debe incluir desde el inicio una reserva de recursos para garantizar la escalabilidad sin interrupciones?, si es el contratista se solicita se confirme cuantos se deben contemplar durante la vida del contrato ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem 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: Analítica - Búsquedas por palabras clave basadas en atributos de eventos analizados. - Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API. - Match de patrones complejos en tiempo real. - Programación de informes y entregas de resultados por correo electrónico a los principales interesados. - Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.). - Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico. - Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes.. - Posibilidad de priorización de los informes de incidentes. Adicionalmente aclara al observante que el contrato es bajo la modalidad llave en mano, por lo cual el oferente deberá suministrar, instalar y poner en operación todos los elementos requeridos para la implementación de la solución, incluyendo infraestructura, hardware, software, racks, cableado y demás recursos necesarios. No obstante lo anterior, se entiende que la Entidad dispondrá de los servicios básicos de infraestructura en sus sedes, particularmente suministro de energía eléctrica y conectividad a Internet, los cuales estarán disponibles para la correcta operación de la solución implementada.
98	2.25	**Especificaciones Técnicas SIEM** 2.25 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	Sobre el uso de objetos CMDB y datos de identidad en búsquedas y reglas, ¿la DIAN garantizará la disponibilidad de APIs o conectores con sus bases de datos de activos y usuarios (ej. Service Now, Active Directory)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.

99	2.25	**Especificaciones Técnicas SIEM** 2.25 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	En caso de que la información de la CMDB esté incompleta odesactualizada, ¿cómo afectará esto la responsabilidad del contratista sobre la precisión de los informes y la efectividad de las reglas de correlación, bajo el entednimiento que no sera el contratista el responsable de la CMDB ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el futuro proveedor del SOC deberá realizar la respectiva integración como fuente para el servicio SIEM, no tendrá injerencia en desactualizaciones.
100	2.25	**Especificaciones Técnicas SIEM** 2.25 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	¿Existe una cantidad máxima de informes personalizados que el contratista deba diseñar durante la fase de implementación,y operacion ?"		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá generar los reportes básicos estándar de la industria al inicio, posteriormente se adicionarán más reportes de acuerdo con las necesidades del servicio.
101	2.25	**Especificaciones Técnicas SIEM** 2.25 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	Para el dimensionamiento de las capacidades de analitica y la generación de reportes, se solicita indicar la cantidad de usuarios finales y dominios lógicos actuales		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.
102	2.25	**Especificaciones Técnicas SIEM** 2.25 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	¿Qué impacto tendrá en los niveles de servicio (SLA) de búsqueda y entrega de informes si el número de usuarios finales crece más allá de lo indicado en este requerimiento? Se solicita confirmar que cualquier crecimiento no previsto en la base de usuarios requerirá una revisión de la capacidad de procesamiento de los nodos worker, y en caso de un posible impacto en la inversion de recursos no contemplados en la oferta inicial estos seran considerados como un requerimiento adicional con un valor que no esta en la oferta base.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
103	2.27	**Especificaciones Técnicas SIEM** 2.27 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	Respecto a la integración con el sistema de ticketing Aranda, se solicita a la Entidad confirmar si dispone de las licencias de API (Web Services) y la documentación técnica de los esquemas de datos necesaria para la integración bidireccional, y en caso que no se tenga o no se pueda ejecutar el requerimiento por causas atribuibles a la herramienta de ticketing no sera causa de penalización al contratista.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad, para el caso, el proveedor deberá consumir y utilizar las APIS de la respectiva plataforma, generando los desarrollos en caso de ser necesario.
104	2,24	**Especificaciones Técnicas SIEM** 2.27 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	¿Se solicita a la entidad confirmar que es únicamente de un envío de alertas vía correo electrónico hacia la mesa de ayuda?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, "disparadores incorporados y personalizables sobre anomalías de comportamiento", se refiere a la capacidad de la herramienta para identificar automáticamente acciones inusuales de usuarios o sistemas, y generar alertas basadas tanto en reglas preconfiguradas como en reglas adaptadas a las necesidades específicas de la empresa, por lo tanto, su comentario no concuerda con lo requerido en este ítem.
105	2.27	**Especificaciones Técnicas SIEM** 2.27 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	Sobre la secuencia de comandos de corrección', se solicita aclarar si la DIAN entregará los protocolos de autorización y los scripts pre-aprobados para estas acciones		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se deberán realizar mesas técnicas para establecer los métodos de automatización de casos estándar.
106	2.27	**Especificaciones Técnicas SIEM** 2.27 - Establecimiento de patrones de comportamiento base de endpoint/servidor/usuario - granularidad de la hora/día de la semana/fin de semana. - Altamente flexible - cualquier conjunto de claves y métricas puede ser usado como patrón base. - Disparadores incorporados y personalizables sobre anomalías de comportamiento	Para el dimensionamiento del sistema de gestión de incidentes, ¿cuál es el volumen promedio mensual de tickets/incidentes que la DIAN gestiona y proyecta gestionar?		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.
107	2.28	**Especificaciones Técnicas SIEM** 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.	Sobre los 'Dashboards especializados para servicios empresariales', se solicita aclarar si la DIAN entregará el mapa de dependencias de sus servicios de negocio (ej. qué servidores, bases de datos y balanceadores componen cada servicio crítico)		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad, la cual es amplia y suficiente para dimensionar su ofrecimiento.
108	2.29	**Especificaciones Técnicas SIEM** 2.29 Integración con fuentes de Inteligencia Externas - API para integrar inteligencia externa de amenazas - como mínimo con Dominios de malware, IPs, URL, hashes, nodos Tor, etc. - Integración para fuentes de inteligencia de amenazas populares - Como mínimo con ThreatStream, CyberArk, SANS, Zeus, etc. - Tecnología para manejar grandes fuentes de información de amenazas - descarga incremental y compartición entre nodos, coincidencia de patrones en tiempo real.	Respecto a la integración con fuentes populares como ThreatStream y CyberArk, se solicita a la Entidad confirmar que la DIAN ya cuenta con las suscripciones activas y pagas a estos servicios de inteligencia, y el contratista no debe incluir el costo de dichas suscripciones comerciales dentro de su oferta económica por la duración del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el oferente deberá incluir este tipo de suscripciones en su oferta por la duración del contrato.
109	2.29	**Especificaciones Técnicas SIEM** 2.29 Integración con fuentes de Inteligencia Externas - API para integrar inteligencia externa de amenazas - como mínimo con Dominios de malware, IPs, URL, hashes, nodos Tor, etc. - Integración para fuentes de inteligencia de amenazas populares - Como mínimo con ThreatStream, CyberArk, SANS, Zeus, etc. - Tecnología para manejar grandes fuentes de información de amenazas - descarga incremental y compartición entre nodos, coincidencia de patrones en tiempo real.	Se solicita a la Entidad aclarar el volumen esperado de Indicadores de Compromiso (IoCs) que la plataforma deberá procesar simultáneamente.		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.
110	2.29	**Especificaciones Técnicas SIEM** 2.29 Integración con fuentes de Inteligencia Externas - API para integrar inteligencia externa de amenazas - como mínimo con Dominios de malware, IPs, URL, hashes, nodos Tor, etc. - Integración para fuentes de inteligencia de amenazas populares - Como mínimo con ThreatStream, CyberArk, SANS, Zeus, etc. - Tecnología para manejar grandes fuentes de información de amenazas - descarga incremental y compartición entre nodos, coincidencia de patrones en tiempo real.	Dado que la inteligencia de amenazas se aplica sobre el comportamiento de los usuarios finales (ej. URLs visitadas, hashes de archivos descargados), ¿cómo se ajustará la capacidad de procesamiento de inteligencia ante un crecimiento no previsto de la base de usuarios? Se solicita confirmar que el contratista no será responsable por la omisión de alertas si el flujo de eventos supera la capacidad de consulta de las APIs de inteligencia contratadas		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
111	2.29	**Especificaciones Técnicas SIEM** 2.29 Integraciones de Tecnología Externa - Integración con cualquier sitio web externo para la búsqueda de direcciones IP. - Integración basada en API para fuentes externas de inteligencia de amenazas. - Integración bidireccional basada en API con sistemas de help desk como ARANDA - Integración bidireccional basada en API con CMDB externas – directamente soportado. - Soporte de Apache Kafka para la integración con informes mejorados de análisis, por ejemplo, PowerBI, ELK, Tableau y Hadoop. - API para una fácil integración con sistemas de aprovisionamiento. - API para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervisión.	Respecto al soporte de Apache Kafka para integración con herramientas como PowerBI o Tableau, se solicita a la Entidad que el contratista en su solución SIEM solo debe tener la capacidad técnica de conectarse a un bus de datos ya existente en la DIAN., y que la entidad suministra e implementa el clúster de Kafka completo (nodos, brokers, zookeepers)		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.

112	2.29	**Especificaciones Técnicas SIEM** 2.29 Integraciones de Tecnología Externa - Integración con cualquier sitio web externo para la búsqueda de direcciones IP. - Integración basada en API para fuentes externas de inteligencia de amenazas. - Integración bidireccional basada en API con sistemas de help desk como ARANDA - Integración bidireccional basada en API con CMDB externas – directamente soportado. - Soporte de Apache Kafka para la integración con informes mejorados de análisis, por ejemplo, PowerBI, ELK, Tableau y Hadoop. - API para una fácil integración con sistemas de aprovisionamiento. - API para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervisión.	Sobre la integración bidireccional basada en API con Aranda y CMDB externas, se solicita a la Entidad confirmar si proporcionará los esquemas de datos, la documentación de los Web Services y los tokens de acceso con permisos de escritur		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
113	2.29	**Especificaciones Técnicas SIEM** 2.29 Integraciones de Tecnología Externa - Integración con cualquier sitio web externo para la búsqueda de direcciones IP. - Integración basada en API para fuentes externas de inteligencia de amenazas. - Integración bidireccional basada en API con sistemas de help desk como ARANDA - Integración bidireccional basada en API con CMDB externas – directamente soportado. - Soporte de Apache Kafka para la integración con informes mejorados de análisis, por ejemplo, PowerBI, ELK, Tableau y Hadoop. - API para una fácil integración con sistemas de aprovisionamiento. - API para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervisión.	Se solicita confirmar con la entidad que el desarrollo de conectores no son parte de la implementación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, efectivamente, esto hace parte de la automatización.
114	2.29	**Especificaciones Técnicas SIEM** 2.29 Integraciones de Tecnología Externa - Integración con cualquier sitio web externo para la búsqueda de direcciones IP. - Integración basada en API para fuentes externas de inteligencia de amenazas. - Integración bidireccional basada en API con sistemas de help desk como ARANDA - Integración bidireccional basada en API con CMDB externas – directamente soportado. - Soporte de Apache Kafka para la integración con informes mejorados de análisis, por ejemplo, PowerBI, ELK, Tableau y Hadoop. - API para una fácil integración con sistemas de aprovisionamiento. - API para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervisión.	Respecto a las APIs para agregar organizaciones y activar descubrimiento, se solicita aclarar si se requiere la integración con sistemas de orquestación (ej. Ansible, Terraform, Kubernetes)		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
115	2.30	**Integraciones de Tecnología Externa** 2.30 - Integración con cualquier sitio web externo para la búsqueda de direcciones IP. - Integración basada en API para fuentes externas de inteligencia de amenazas. - Integración bidireccional basada en API con sistemas de help desk como ARANDA - Integración bidireccional basada en API con CMDB externas – directamente soportado. - Soporte de Apache Kafka para la integración con informes mejorados de análisis, por ejemplo, PowerBI, ELK, Tableau y Hadoop. - API para una fácil integración con sistemas de aprovisionamiento. - API para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervi	Respecto al soporte de Apache Kafka para integración con herramientas como PowerBI o Tableau, se solicita a la Entidad que el contratista en su solución SIEM solo debe tener la capacidad técnica de conectarse a un bus de datos ya existente en la DIAN., y que la entidad suministra e implementa el clúster de Kafka completo (nodos, brokers, zookeepers)		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.
116	2.30	**Integraciones de Tecnología Externa** 2.30 - Integración con cualquier sitio web externo para la búsqueda de direcciones IP. - Integración basada en API para fuentes externas de inteligencia de amenazas. - Integración bidireccional basada en API con sistemas de help desk como ARANDA - Integración bidireccional basada en API con CMDB externas – directamente soportado. - Soporte de Apache Kafka para la integración con informes mejorados de análisis, por ejemplo, PowerBI, ELK, Tableau y Hadoop. - API para una fácil integración con sistemas de aprovisionamiento. - API para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervi	Sobre la integración bidireccional basada en API con Aranda y CMDB externas, se solicita a la Entidad confirmar si proporcionará los esquemas de datos, la documentación de los Web Services y los tokens de acceso con permisos de escritura		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
117	2.30	**Integraciones de Tecnología Externa** 2.30 - Integración con cualquier sitio web externo para la búsqueda de direcciones IP. - Integración basada en API para fuentes externas de inteligencia de amenazas. - Integración bidireccional basada en API con sistemas de help desk como ARANDA - Integración bidireccional basada en API con CMDB externas – directamente soportado. - Soporte de Apache Kafka para la integración con informes mejorados de análisis, por ejemplo, PowerBI, ELK, Tableau y Hadoop. - API para una fácil integración con sistemas de aprovisionamiento. - API para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervi	Se solicita confirmar a la entidad que el desarrollo de conectores no son parte de la implementación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, efectivamente, esto hace parte de la automatización.
118	2.30	**Integraciones de Tecnología Externa** 2.30 - Integración con cualquier sitio web externo para la búsqueda de direcciones IP. - Integración basada en API para fuentes externas de inteligencia de amenazas. - Integración bidireccional basada en API con sistemas de help desk como ARANDA - Integración bidireccional basada en API con CMDB externas – directamente soportado. - Soporte de Apache Kafka para la integración con informes mejorados de análisis, por ejemplo, PowerBI, ELK, Tableau y Hadoop. - API para una fácil integración con sistemas de aprovisionamiento. - API para agregar organizaciones, crear credenciales, activar descubrimiento, modificar eventos de supervi	Respecto a las APIs para agregar organizaciones y activar descubrimiento, se solicita aclarar si se requiere la integración con sistemas de orquestación (ej. Ansible, Terraform, Kubernetes)		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
119	2.31	**Integraciones de Tecnología Externa** 2.31 - GUI basada en web, a ser posible HTML5. - Control de acceso basada en roles para restringir el acceso a la GUI y a los datos. - Todas las comunicaciones entre módulos están protegidas por HTTPS. - Auditoría completa de la actividad del usuario. - Fácil actualización de software con un mínimo tiempo de inactividad y pérdida de eventos. - Actualización de la base de conocimientos (analizadores, reglas, informes) sencilla. - Archivado basado en políticas. - Hashing de registros a tiempo para no repudio y verificación de integridad. - Autenticación de usuario flexible – local, y externa a través de Microsoft AD y OpenLDAP, Cloud SSO/SAML a través de Okta	Sobre la autenticación vía Cloud SSO/SAML (Okta), se solicita a la Entidad confirmar si garantiza la visibilidad de red y apertura de puertos hacia los proveedores externos de identidad. Asimismo, ¿la Entidad proveerá los metadatos y certificados necesarios para la federación? Se solicita aclarar si se requiere únicamente autenticación o si también se espera el aprovisionamiento dinámico de usuarios (SCIM); en caso de ser esto último, se solicita indicar si la DIAN dispone de los conectores necesarios.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, La conectividad interna deberá ser garantizada por la Entidad, la autenticación SCIM hace parte de otro proyecto, esta funcionalidad no está incluida en este proceso.
120	2.31	**Integraciones de Tecnología Externa** 2.31 - GUI basada en web, a ser posible HTML5. - Control de acceso basada en roles para restringir el acceso a la GUI y a los datos. - Todas las comunicaciones entre módulos están protegidas por HTTPS. - Auditoría completa de la actividad del usuario. - Fácil actualización de software con un mínimo tiempo de inactividad y pérdida de eventos. - Actualización de la base de conocimientos (analizadores, reglas, informes) sencilla. - Archivado basado en políticas. - Hashing de registros a tiempo para no repudio y verificación de integridad. - Autenticación de usuario flexible – local, y externa a través de Microsoft AD y OpenLDAP, Cloud SSO/SAML a través de Okta	En relación con el 'archivado basado en políticas', se solicita a la Entidad definir formalmente el tiempo de retención para datos 'calientes' (en línea) y datos 'fríos' (archivados). De igual forma, se solicita aclarar si el almacenamiento para el archivado histórico (ej. NAS, S3 o Tape Library) será provisto por la Entidad o si el proponente debe incluirlo en su oferta,en caso que sea el proveedor se solicita confirmar actualmente cual es la capacidad utilizada.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la retención en línea deberá ser mínimo de un mes, en frio de al menos tres años y el histórico de al menos cinco años, el Contratista tendrá que proporcionar el almacenamiento para cumplir dichos parámetros.

121	2.31	**Integraciones de Tecnología Externa** 2.31 - GUI basada en web, a ser posible HTML5. - Control de acceso basada en roles para restringir el acceso a la GUI y a los datos. - Todas las comunicaciones entre módulos están protegidas por HTTPS. - Auditoría completa de la actividad del usuario. - Fácil actualización de software con un mínimo tiempo de inactividad y pérdida de eventos. - Actualización de la base de conocimientos (analizadores, reglas, informes) sencilla. - Archivado basado en políticas. - Hashing de registros a tiempo para no repudio y verificación de integridad. - Autenticación de usuario flexible – local, y externa a través de Microsoft AD y OpenLDAP, Cloud SSO/SAML a través de Okta	Sobre el 'hashing de registros para no repudio', se solicita aclarar si se requiere la integración con una Autoridad de Sellado de Tiempo (TSA) certificada o si es suficiente el uso de la hora del sistema sincronizada por NTP.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, es suficiente el uso de la hora del sistema sincronizada por NTP
122	2.33	**Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos:** 2.33 Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos: - Sistema de monitorización de estado - a través de Ping, SNMP, WMI, Uptime Analysis, interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento. - Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP. - Monitorización del hardware y del entorno. - Calendario para la programación de las ventanas de mantenimiento. - Cálculo de SLA – consideración de las horas normales de trabajo y fuera de horas.	Respecto al requerimiento de 'Synthetic Transaction Monitoring', se solicita a la Entidad aclarar si la solución debe realizar estas pruebas de forma nativa o si se permite la integración con herramientas de monitoreo ya existentes. En caso de ser nativo, ¿se garantiza que el contratista contará con cuentas de servicio y permisos de red para realizar consultas directas a bases de datos (JDBC), servidores de correo y aplicaciones transaccionales sin que estas acciones sean bloqueadas o alertadas como ataques por los sistemas de seguridad perimetral?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem permite equivalencia, las características solicitadas se pueden cumplir con herramientas similares o equiparables, sin embargo, para evitar equívocos en el requerimiento de la Entidad, el ítem en mención 2.33 será eliminado del respectivo anexo técnico, cambio que se verá reflejado en la adenda a publicar en los próximos días.
123	2.33	**Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos:** 2.33 Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos: - Sistema de monitorización de estado - a través de Ping, SNMP, WMI, Uptime Analysis, interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento. - Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP. - Monitorización del hardware y del entorno. - Calendario para la programación de las ventanas de mantenimiento. - Cálculo de SLA – consideración de las horas normales de trabajo y fuera de horas.	Sobre la 'monitorización del hardware y del entorno', se solicita confirmar si la totalidad de los activos (incluyendo UPS y HVAC) cuentan con tarjetas de gestión que soporten SNMP v2/v3 y si las MIBs propietarias serán suministradas por la Entidad. ¿Se exime al proponente de la responsabilidad de monitoreo sobre aquellos dispositivos que no posean interfaces de red o que utilicen protocolos de comunicación cerrados/propietarios?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
124	2.33	**Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos:** 2.33 Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos: - Sistema de monitorización de estado - a través de Ping, SNMP, WMI, Uptime Analysis, interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento. - Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP. - Monitorización del hardware y del entorno. - Calendario para la programación de las ventanas de mantenimiento. - Cálculo de SLA – consideración de las horas normales de trabajo y fuera de horas.	En relación con la supervisión de cambios de estado en BGP, OSPF y EIGRP, se solicita aclarar si se espera que el SIEM reciba únicamente los Traps de SNMP o Syslogs enviados por los routers, o si la solución debe participar activamente en el plano de control de red para detectar los cambios. Se solicita confirmar que la responsabilidad del contratista se limita a la visualización y alerta del evento una vez el dispositivo de red lo reporte.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el servicio de SIEM administrado deberá alertar sobre cambios en las tablas de ruteo de los diferentes dispositivos con el fin de identificar cambios no controlados o autorizados.
125	2.33	**Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos:** 2.33 Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos: - Sistema de monitorización de estado - a través de Ping, SNMP, WMI, Uptime Analysis, interfaz crítica, proceso crítico y servicio, cambio de estado en BGP/OSPF/EIGRP, cambios de estado del puerto de almacenamiento. - Modelos de disponibilidad de servicios a través de Synthetic Transaction Monitoring - Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, ruta de rastreo y para puertos genéricos TCP/UDP. - Monitorización del hardware y del entorno. - Calendario para la programación de las ventanas de mantenimiento. - Cálculo de SLA – consideración de las horas normales de trabajo y fuera de horas.	Respecto al 'Cálculo de SLA', se solicita a la Entidad confirmar si ya dispone de una definición formal de los Servicios de Negocio y sus horarios de operación. ¿El proponente es responsable únicamente de entregar la funcionalidad técnica de cálculo o también de la consultoría para definir qué activos componen cada nivel de servicio? Asimismo, en caso de crecimiento de usuarios o activos no previstos, ¿se aceptará una revisión de los umbrales de SLA si la carga operativa excede la capacidad de cómputo inicial?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
126	2.34	**Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos:** 2.34 - 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.	En relación con el requerimiento de almacenamiento y archivado de logs (soporte para NFS y HDFS), así como la definición de políticas de retención por tiempo y capacidad, se solicita a la DIAN confirmar que la infraestructura de almacenamiento requerida sera provista en su totalidad por la Entidad o se dispondrá de plataformas existentes para este fin, en caso contrario se solicita indicar que capacidades actualmente se tienen para este fin.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, estas capacidades solicitadas estarán a cargo del Contratista
127	2.34	**Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos:** 2.34 - 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.	Adicionalmente, se solicita confirmar los volúmenes estimados de generación de logs (GB/TB por día) y su proyección de crecimiento, con el fin de dimensionar adecuadamente la arquitectura de almacenamiento y definir las políticas de retención (en línea y fuera de línea) sin afectar el desempeño de la solución.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el promedio diario aproximado de eventos es de 150 millones y el uso de almacenamiento promedio diario aproximado es de 13 GB sin compresión. se estima un crecimiento anual de 20% como máximo, indicando que se deben cumplir todos los requisitos solicitados para este servicio descritos en los documentos del proyecto.
128	2.34	**Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos:** 2.34 - 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.	Asimismo, se solicita aclarar si se permite la implementación de arquitecturas de almacenamiento por niveles (tiering), incluyendo esquemas híbridos (on-premise y nube), así como el uso de mecanismos de compresión y optimización, garantizando el cumplimiento de los tiempos de consulta y recuperación requeridos por la Entidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, este aspecto queda a discreción del oferente, así como todas las consideraciones técnicas derivadas del mismo.
129	2.34	**Supervisión de disponibilidad, como mínimo debe incluir los siguientes elementos:** 2.34 - 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.	Finalmente, se solicita confirmar si los tiempos de acceso a la información histórica (logs fuera de línea) están sujetos a algún nivel de servicio específico, y cómo se gestionarán escenarios en los que limitaciones de infraestructura o crecimiento de datos impacten dichos tiempos.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, este aspecto queda a discreción del oferente, así como todas las consideraciones técnicas derivadas del mismo.
130	2.35	**Licenciamiento, como mínimo debe incluir los siguientes elementos::** 2.35 - 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.	Sobre la posibilidad de desplegar 'tantos colectores virtuales como se quiera sin coste adicional', se solicita aclarar si esta gratuidad aplica únicamente al licenciamiento del software. En ese sentido, ¿se confirma que la Entidad será la responsable de proveer el licenciamiento de los Sistemas Operativos (Windows/Linux) y la infraestructura virtual donde residirán dichos colectores, así como el ancho de banda necesario para su operación?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, es un contrato llave en mano, el futuro proveedor del SOC deberá proporcionar lo necesario para poner en operación los servicios requeridos.
131	2.35	**Licenciamiento, como mínimo debe incluir los siguientes elementos::** 2.35 - 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.	Respecto al licenciamiento de UEBA para equipos Windows, se solicita a la Entidad definir la cantidad nominal de usuarios/equipos que conforman la línea base. Dado que el UEBA se dimensiona por identidades, ¿qué procedimiento técnico-económico se seguirá si durante la ejecución el número de usuarios finales supera lo indicado en el inventario inicial? Se solicita confirmar que cualquier crecimiento no previsto requerirá una adición presupuestal para cubrir las nuevas licencias.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.

132	2.35	**Licenciamiento, como mínimo debe incluir los siguientes elementos::** 2.35 - 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.	En relación con el monitoreo de servidores en ambientes híbridos (Cloud), se solicita aclarar si los costos de transferencia de salida (Data Egress Fees) cobrados por los proveedores de nube (AWS, Azure, GCP) al enviar logs hacia la plataforma central serán asumidos por la Entidad, o si el proponente debe estimar y cubrir estos costos operativos por la duración del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, es un contrato llave en mano, el futuro proveedor del SOC deberá proporcionar lo necesario para poner en operación los servicios requeridos.
133	2.35	**Licenciamiento, como mínimo debe incluir los siguientes elementos::** 2.35 - 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.	Respecto a la posibilidad de 'añadir EPS adicionales sin necesidad de contratar soporte asociado', se solicita a la Entidad aclarar si, en caso de presentarse una falla técnica o degradación del rendimiento derivada directamente del procesamiento de estos eventos excedentes, . ¿Se exime al proponente de responsabilidad si el volumen de eventos no soportados afecta la estabilidad de la plataforma o la integridad de los datos		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el exceso de eventos debería encolarse y procesarse con posterioridad.
134	2.35	**Licenciamiento, como mínimo debe incluir los siguientes elementos::** 2.35 - 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.	Sobre el despliegue de 'tantos colectores virtuales como se quiera sin coste adicional', se solicita confirmar que el alcance del proponente se limita al suministro de la licencia del software. ¿Será responsabilidad de la Entidad proveer la infraestructura de hardware, el hipervisor y el licenciamiento de los Sistemas Operativos (Windows/Linux) para cada nuevo colector? Asimismo, se solicita aclarar si el soporte para la configuración de nuevos colectores durante la fase de operación se manejará bajo una bolsa de horas o si está incluido de forma ilimitada.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
135	2.35	**Licenciamiento, como mínimo debe incluir los siguientes elementos::** 2.35 - 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.	Respecto al suministro de 'otras suscripciones como Indicadores de Compromiso (IoC)', se solicita a la Entidad definir si se refiere únicamente a fuentes de inteligencia abiertas (Open Source) o si el proponente debe incluir el costo de suscripciones comerciales de pago, En caso de ser comerciales, ¿se solicita un número mínimo de fuentes de inteligencia a integrar?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, es un contrato llave en mano, el futuro proveedor del SOC deberá proporcionar lo necesario para poner en operación los servicios requeridos.
136	2.35	**Especificaciones Técnicas Plataforma SOAR** 3.5 En la solución SOAR entregada como mínimo debe integrar el SIEM, firewalls, plataforma antivirus y las demás plataformas de seguridad de la Entidad y que sean susceptibles de integración, para lo cual el oferente se apoyará en los inventarios incluidos en el archivo excel Anexo Técnico Proyecto SOC DIAN.	¿El inventario incluido en el anexo corresponde a un listado definitivo, actualizado y validado de las plataformas a integrar, o podrá ser modificado durante la ejecución del contrato? En caso de cambios, ¿cómo se gestionará el impacto en alcance, tiempos y costos, esto se asumira como un costo adicional ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperado.
137	2.35	**Especificaciones Técnicas Plataforma SOAR** 3.5 En la solución SOAR entregada como mínimo debe integrar el SIEM, firewalls, plataforma antivirus y las demás plataformas de seguridad de la Entidad y que sean susceptibles de integración, para lo cual el oferente se apoyará en los inventarios incluidos en el archivo excel Anexo Técnico Proyecto SOC DIAN.	Para cada una de las soluciones a integrar, ¿la Entidad garantizará la disponibilidad de APIs, documentación técnica, licencias necesarias y accesos requeridos (credenciales, ambientes de prueba, etc.) para realizar las integraciones de manera efectiva, en todos los casos que sea tecnologia del la entidad o sus terceros ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
138	2.35	**Especificaciones Técnicas Plataforma SOAR** 3.5 En la solución SOAR entregada como mínimo debe integrar el SIEM, firewalls, plataforma antivirus y las demás plataformas de seguridad de la Entidad y que sean susceptibles de integración, para lo cual el oferente se apoyará en los inventarios incluidos en el archivo excel Anexo Técnico Proyecto SOC DIAN.	En los casos donde las plataformas oriopiedad de la entidad o sus terceros no cuenten con conectores nativos o APIs estándar, y no se puedan desarrollar o entregar por la entidad ,se solicita confirmar que esto no sera causal de imcumplimiento del contratista de la presente invitacion a cotizar en ninguna fase de la vida del proyecto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
139	2.35	**Especificaciones Técnicas Plataforma SOAR** 3.5 En la solución SOAR entregada como mínimo debe integrar el SIEM, firewalls, plataforma antivirus y las demás plataformas de seguridad de la Entidad y que sean susceptibles de integración, para lo cual el oferente se apoyará en los inventarios incluidos en el archivo excel Anexo Técnico Proyecto SOC DIAN.	Para cada una de las soluciones a integrar, ¿la Entidad garantizará la disponibilidad de APIs, documentación técnica, licencias necesarias y accesos requeridos (credenciales, ambientes de prueba, etc.) para realizar las integraciones de manera efectiva, en todos los casos que sea tecnologia del la entidad o sus terceros ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
140	2.35	**Especificaciones Técnicas Plataforma SOAR** 3.5 En la solución SOAR entregada como mínimo debe integrar el SIEM, firewalls, plataforma antivirus y las demás plataformas de seguridad de la Entidad y que sean susceptibles de integración, para lo cual el oferente se apoyará en los inventarios incluidos en el archivo excel Anexo Técnico Proyecto SOC DIAN.	¿Se solicita confirmar que la responsabilidad sobre la calidad, disponibilidad y consistencia de los datos provenientes de las diferentes plataformas provistas por la entidad o sus terceros será asumida por la Entidad, especialmente en escenarios donde dichas limitaciones afecten la automatización de playbooks y la respuesta a incidentes?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá crear las excepciones correspondientes para mejorar la calidad de la ingesta.
141	2.35	**Especificaciones Técnicas Plataforma SOAR** 3.5 En la solución SOAR entregada como mínimo debe integrar el SIEM, firewalls, plataforma antivirus y las demás plataformas de seguridad de la Entidad y que sean susceptibles de integración, para lo cual el oferente se apoyará en los inventarios incluidos en el archivo excel Anexo Técnico Proyecto SOC DIAN.	Se solicita precisar el número mínimo y máximo de integraciones esperadas dentro del alcance base del contrato, así como el criterio de priorización de las mismas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el mínimo está definido en el mismo texto "el SIEM, firewalls, plataforma antivirus y las demás plataformas de seguridad de la Entidad y que sean susceptibles de integración" no hay máximo, dependerá de las tecnologías y recursos disponibles hasta el fin del contrato.
142	3.59	**Especificaciones Técnicas Plataforma SOAR** 3.59 Debería ser posible que la solución SOAR permita la ejecución simultánea de múltiples playbooks, garantizando la capacidad de respuesta ante varios incidentes de seguridad en paralelo, con nodos o licencias adicionales o su equivalente de acuerdo a la solución ofrecida, sin que ello implique costos adicionales para la Entidad, cumliendo como mínimo: - Capacidad de ejecutar varios playbooks al mismo tiempo, sin afectar el rendimiento del sistema. - Soporte para playbooks anidados o encadenados, permitiendo modularizar tareas complejas. - Arquitectura escalable que permita aumentar la capacidad de ejecución mediante la adición de nodos, instancias o licencias adicionales. - Gestión eficiente de recursos para evitar cuellos de botella en la ejecución de automatizaciones. - Monitoreo y visualización del estado de ejecución de cada playbook en tiempo real.	¿Cuáles son los volúmenes esperados que debe soportar la solución en términos de Número máximo de playbooks ejecutándose concurrentemente?		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 establecer la cantidad de playbooks que eventualmente se requieran para dicha operación.

143	3.59	**Especificaciones Técnicas Plataforma SOAR** 3.59 Debería ser posible que la solución SOAR permita la ejecución simultánea de múltiples playbooks, garantizando la capacidad de respuesta ante varios incidentes de seguridad en paralelo, con nodos o licencias adicionales o su equivalente de acuerdo a la solución ofrecida, sin que ello implique costos adicionales para la Entidad, cumliendo como minimo: - Capacidad de ejecutar varios playbooks al mismo tiempo, sin afectar el rendimiento del sistema. - Soporte para playbooks anidados o encadenados, permitiendo modularizar tareas complejas. - Arquitectura escalable que permita aumentar la capacidad de ejecución mediante la adición de nodos, instancias o licencias adicionales. - Gestión eficiente de recursos para evitar cuellos de botella en la ejecución de automatizaciones. - Monitoreo y visualización del estado de ejecución de cada playbook en tiempo real.	En relación con la exigencia de escalabilidad sin costos adicionales,se solicita indicar cuantos nodos ro licencias espera la entidad se cubran durante la vida del contrato esto con vista a poder tener un dimensionamiento claro que se refleja en el valor de la propuesta ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
144	3.59	**Especificaciones Técnicas Plataforma SOAR** 3.59 Debería ser posible que la solución SOAR permita la ejecución simultánea de múltiples playbooks, garantizando la capacidad de respuesta ante varios incidentes de seguridad en paralelo, con nodos o licencias adicionales o su equivalente de acuerdo a la solución ofrecida, sin que ello implique costos adicionales para la Entidad, cumliendo como minimo: - Capacidad de ejecutar varios playbooks al mismo tiempo, sin afectar el rendimiento del sistema. - Soporte para playbooks anidados o encadenados, permitiendo modularizar tareas complejas. - Arquitectura escalable que permita aumentar la capacidad de ejecución mediante la adición de nodos, instancias o licencias adicionales. - Gestión eficiente de recursos para evitar cuellos de botella en la ejecución de automatizaciones. - Monitoreo y visualización del estado de ejecución de cada playbook en tiempo real.	Se solicita confirmar cómo se evaluará el cumplimiento del requerimiento de "no afectación del rendimiento", y qué herramientas o mecanismos de monitoreo serán considerados válidos para evidenciar dicho cumplimiento.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se realizará mediante análisis de throwput y consumo de recursos, para ello se definirán umbrales máximos.
145	3.59	**Especificaciones Técnicas Plataforma SOAR** 3.59 Debería ser posible que la solución SOAR permita la ejecución simultánea de múltiples playbooks, garantizando la capacidad de respuesta ante varios incidentes de seguridad en paralelo, con nodos o licencias adicionales o su equivalente de acuerdo a la solución ofrecida, sin que ello implique costos adicionales para la Entidad, cumliendo como minimo: - Capacidad de ejecutar varios playbooks al mismo tiempo, sin afectar el rendimiento del sistema. - Soporte para playbooks anidados o encadenados, permitiendo modularizar tareas complejas. - Arquitectura escalable que permita aumentar la capacidad de ejecución mediante la adición de nodos, instancias o licencias adicionales. - Gestión eficiente de recursos para evitar cuellos de botella en la ejecución de automatizaciones. - Monitoreo y visualización del estado de ejecución de cada playbook en tiempo real.	En escenarios donde el incremento en la carga operativa supere las condiciones inicialmente previstas, ¿cómo se gestionará el ajuste de capacidad sin afectar el equilibrio económico del contrato?, se requiere que la entidad confirme que esto sera un visto como un servicio adicional con su correspondiente costo.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
146	3.70	**Especificaciones Técnicas Plataforma SOAR** 3.70 La solución SOAR debe contar con una amplia biblioteca de conectores de integración preexistentes, que permitan la interoperabilidad con diversas herramientas de seguridad, infraestructura, nube, gestión de incidentes, inteligencia de amenazas, y otros sistemas relevantes. Estos conectores deben facilitar la automatización de tareas, el intercambio de información y la ejecución de acciones dentro de los playbooks, cumpliendo como mínimo con lo siguiente: -La solución debe incluir al menos 300 conectores de integración preconfigurados o funcionalidades equivalentes, que cubran herramientas de seguridad, TI, nube, mensajería, bases de datos, APIs REST, entre otros. - Los conectores deben estar documentados y actualizados regularmente por el fabricante o comunidad. - La solución debe permitir el desarrollo de nuevos conectores a demanda, utilizando herramientas de desarrollo, SDKs o APIs proporcionadas por el fabricante, sin que esto implique nuevos costos para la Entidad. - La solución debe contar con los conectores necesarios para integrar los sistemas actuales de la DIAN, así como tener la flexibilidad para integrar sistemas futuros, mediante desarrollo propio o expansión de la biblioteca existente. - Debe existir soporte para conectores personalizados, autenticación segura, y gestión de versiones.	En relación con los sistemas actuales de la DIAN, ¿se cuenta con un listado priorizado de integraciones obligatorias (derivado del inventario del anexo técnico), y cuál es el número esperado de conectores a implementar dentro del alcance base del contrato?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
147	3.70	**Especificaciones Técnicas Plataforma SOAR** 3.70 La solución SOAR debe contar con una amplia biblioteca de conectores de integración preexistentes, que permitan la interoperabilidad con diversas herramientas de seguridad, infraestructura, nube, gestión de incidentes, inteligencia de amenazas, y otros sistemas relevantes. Estos conectores deben facilitar la automatización de tareas, el intercambio de información y la ejecución de acciones dentro de los playbooks, cumpliendo como mínimo con lo siguiente: -La solución debe incluir al menos 300 conectores de integración preconfigurados o funcionalidades equivalentes, que cubran herramientas de seguridad, TI, nube, mensajería, bases de datos, APIs REST, entre otros. - Los conectores deben estar documentados y actualizados regularmente por el fabricante o comunidad. - La solución debe permitir el desarrollo de nuevos conectores a demanda, utilizando herramientas de desarrollo, SDKs o APIs proporcionadas por el fabricante, sin que esto implique nuevos costos para la Entidad. - La solución debe contar con los conectores necesarios para integrar los sistemas actuales de la DIAN, así como tener la flexibilidad para integrar sistemas futuros, mediante desarrollo propio o expansión de la biblioteca existente. - Debe existir soporte para conectores personalizados, autenticación segura, y gestión de versiones.	Respecto a la exigencia de desarrollo de nuevos conectores "sin costos adicionales", se solicita aclarar, si ¿cual es la cantidad de conectores personalizados a desarrollar?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información disponible que entregue la Entidad, no hay máximo, depende de las tecnologías y recursos disponibles hasta el fin del contrato.
148	3.70	**Especificaciones Técnicas Plataforma SOAR** 3.70 La solución SOAR debe contar con una amplia biblioteca de conectores de integración preexistentes, que permitan la interoperabilidad con diversas herramientas de seguridad, infraestructura, nube, gestión de incidentes, inteligencia de amenazas, y otros sistemas relevantes. Estos conectores deben facilitar la automatización de tareas, el intercambio de información y la ejecución de acciones dentro de los playbooks, cumpliendo como mínimo con lo siguiente: -La solución debe incluir al menos 300 conectores de integración preconfigurados o funcionalidades equivalentes, que cubran herramientas de seguridad, TI, nube, mensajería, bases de datos, APIs REST, entre otros. - Los conectores deben estar documentados y actualizados regularmente por el fabricante o comunidad. - La solución debe permitir el desarrollo de nuevos conectores a demanda, utilizando herramientas de desarrollo, SDKs o APIs proporcionadas por el fabricante, sin que esto implique nuevos costos para la Entidad. - La solución debe contar con los conectores necesarios para integrar los sistemas actuales de la DIAN, así como tener la flexibilidad para integrar sistemas futuros, mediante desarrollo propio o expansión de la biblioteca existente. - Debe existir soporte para conectores personalizados, autenticación segura, y gestión de versiones.	En relación con la actualización y mantenimiento de conectores, se solicita confirmar que no sera causa de incumplimiento por parte del contratista el esfuerzo asociado a cambios no controlados por el contratista (por ejemplo, modificaciones en APIs de terceros)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información disponible que entregue la Entidad, no hay máximo, depende de las tecnologías y recursos disponibles hasta el fin del contrato.

149	3.70	**Especificaciones Técnicas Plataforma SOAR** 3.70 La solución SOAR debe contar con una amplia biblioteca de conectores de integración preexistentes, que permitan la interoperabilidad con diversas herramientas de seguridad, infraestructura, nube, gestión de incidentes, inteligencia de amenazas, y otros sistemas relevantes. Estos conectores deben facilitar la automatización de tareas, el intercambio de información y la ejecución de acciones dentro de los playbooks, cumpliendo como mínimo con lo siguiente: -La solución debe incluir al menos 300 conectores de integración preconfigurados o funcionalidades equivalentes, que cubran herramientas de seguridad, TI, nube, mensajería, bases de datos, APIs REST, entre otros. - Los conectores deben estar documentados y actualizados regularmente por el fabricante o comunidad. - La solución debe permitir el desarrollo de nuevos conectores a demanda, utilizando herramientas de desarrollo, SDKs o APIs proporcionadas por el fabricante, sin que esto implique nuevos costos para la Entidad. - La solución debe contar con los conectores necesarios para integrar los sistemas actuales de la DIAN, así como tener la flexibilidad para integrar sistemas futuros, mediante desarrollo propio o expansión de la biblioteca existente. - Debe existir soporte para conectores personalizados, autenticación segura, y gestión de versiones.	Se solicita confirmar que la incorporación de nuevas plataformas o tecnologías futuras no contempladas en el inventario inicial, y que afecten términos de alcance, tiempos y valor económico del contrato, seran vistas como requerimientos adicionales		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información disponible que entregue la Entidad, no hay máximo, depende de las tecnologías y recursos disponibles hasta el fin del contrato.
150	4.2	**Especificaciones Técnicas herramienta de protección de Bases de Datos** 4.2 La solución deberá contar con tecnología de autoaprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo esquemas, objetos, tablas, sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario; todo esto para el establecimiento de un comportamiento base de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.	¿Cuál es el período esperado de operación en modo aprendizaje para la construcción de la línea base (baseline), y si este será definido por la Entidad en conjunto con el contratista en función del comportamiento observado?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la Línea base estará en construcción durante toda la ejecución del proyecto, sobre todo teniendo en cuenta que se van a incluir nuevos sistemas a lo largo de su ciclo de vida.
151	4.2	**Especificaciones Técnicas herramienta de protección de Bases de Datos** 4.2 La solución deberá contar con tecnología de autoaprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo esquemas, objetos, tablas, sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario; todo esto para el establecimiento de un comportamiento base de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.	¿La Entidad definirá políticas o casos de uso específicos que deban ser considerados dentro del modelo de aprendizaje, o se espera que el contratista los proponga y configure?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se deben tener en cuenta ambas consideraciones.
152	4.4	**Especificaciones Técnicas herramienta de protección de Bases de Datos** 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".	¿El inventario de bases de datos corresponde a un listado cerrado, validado y actualizado? En caso contrario, ¿cómo se gestionarán las inclusiones, exclusiones o modificaciones durante la ejecución del contrato en términos de alcance, cronograma y valor económico?, La entidad cancelaran valores adicionales a aumentos en cantidades no dimensionadas con base al listado de activos entregado en la invitacion a cotizar ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
153	4.4	**Especificaciones Técnicas herramienta de protección de Bases de Datos** 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".	En escenarios donde existan limitaciones técnicas (versiones no soportadas, ausencia de agentes, restricciones de acceso, incompatibilidades), ¿ cual sera el alcance esperado por parte de la entidad si dichas bases de datos seran excluidas del alcance base ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, si se presentare el caso, se realizará exclusión documentada.
154	4.4	**Especificaciones Técnicas herramienta de protección de Bases de Datos** 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".	En relación con el crecimiento futuro, ¿cómo se gestionará la incorporación de nuevas bases de datos o cambios en el inventario durante la vigencia del contrato?, seran requerimientos adicionales		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
155	4.4	**Especificaciones Técnicas herramienta de protección de Bases de Datos** 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".	¿Cómo se evaluará el cumplimiento del monitoreo "total", especialmente en escenarios donde existan restricciones ajenas al contratista (accesos, disponibilidad, dependencias con terceros)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
156	4.52	**Especificaciones Técnicas herramienta de protección de Bases de Datos** 4.52 Incluir una consola de reportería basada en big data, que retenga los datos siempre en tiempo real y permita generar búsquedas y analítica forense, como mínimo debe manejar una retención de seis (6) meses.	¿Aplica para la totalidad de los datos recolectados o solo para un subconjunto (ej. eventos críticos, alertas, auditoría)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el alcance abarca todos los tipos de evento
157	4.52	**Especificaciones Técnicas herramienta de protección de Bases de Datos** 4.52 Incluir una consola de reportería basada en big data, que retenga los datos siempre en tiempo real y permita generar búsquedas y analítica forense, como mínimo debe manejar una retención de seis (6) meses.	¿Se requiere almacenamiento en línea (hot) durante todo el período o se permiten esquemas de almacenamiento jerárquico (hot/warm/cold)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la retención en línea deberá ser mínimo de un mes, en frio de al menos tres años y el histórico de al menos cinco años, el Contratista tendrá que proporcionar el almacenamiento para cumplir dichos parámetros.
158	4.54.9	**4.54.9 Consola de Administración de la Plataforma de Monitoreo de Bases de Datos** La solución deberá ser capaz de poder desplegarse en nubes públicas como Amazon Web Services o Microsoft Azure	En relación con la capacidad de despliegue en nube pública: ¿Se requiere que la solución opere obligatoriamente en nube, o solo que tenga la capacidad de hacerlo?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las característica indica que tenga la capacidad de hacerlo.
159	4.54.9	**4.54.9 Consola de Administración de la Plataforma de Monitoreo de Bases de Datos** La solución deberá ser capaz de poder desplegarse en nubes públicas como Amazon Web Services o Microsoft Azure	¿La Entidad proveerá la infraestructura en nube (cuentas, suscripciones, redes, seguridad), o deberá ser incluida por el contratista?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, para todas las capacidades asociadas directamente al SOC el Contratista deberá proveer toda la infraestructura relacionada.
160	4.54.9	**4.54.9 Consola de Administración de la Plataforma de Monitoreo de Bases de Datos** La solución deberá ser capaz de poder desplegarse en nubes públicas como Amazon Web Services o Microsoft Azure	¿Se espera un modelo de arquitectura específico (on-premise, cloud, híbrido), o queda a criterio del oferente? En caso de ser híbrido, ¿cómo se gestionarán los requisitos de latencia entre componentes distribuidos?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, este aspecto queda a discreción del oferente, así como todas las consideraciones técnicas derivadas del mismo.
161	4.54.9	**4.54.9 Consola de Administración de la Plataforma de Monitoreo de Bases de Datos** La solución deberá ser capaz de poder desplegarse en nubes públicas como Amazon Web Services o Microsoft Azure	¿Existen restricciones de residencia de datos, seguridad o cumplimiento normativo que limiten el uso de nubes públicas para el almacenamiento o procesamiento de información sensible?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no existen restricciones de residencia de datos, sin embargo, se deben implementar todos los controles correspondientes para garantizar Integridad, disponibilidad y confidencialidad.
162	5.3	**Especificaciones Técnicas Gestión y Monitoreo de Vulnerabilidades.** **5.3 Alcance del Requerimiento** Debe ser en modalidad software como servicio. (SaaS), con capacidad de aprovisionamiento rápido y elasticidad automática de servicios. No se aceptan soluciones de código abierto o similares. Debe integrarse con las plataformas SIEM, SOAR a considerar en el Proyecto. El servicio SaaS incluye la operación y mantenimiento de la plataforma, su monitoreo, actualizaciones, soporte técnico con ingeniero de fabricante dedicado con Tecnical Account Manager TAMy optimización continua.	¿ Se solicita aclarar la solución deberá ser completamente multi-tenant o se requiere un esquema dedicado (single-tenant)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, este aspecto queda a discreción del oferente, así como todas las consideraciones técnicas derivadas del mismo.
163	5.3	**Especificaciones Técnicas Gestión y Monitoreo de Vulnerabilidades.** **5.3 Alcance del Requerimiento** Debe ser en modalidad software como servicio. (SaaS), con capacidad de aprovisionamiento rápido y elasticidad automática de servicios. No se aceptan soluciones de código abierto o similares. Debe integrarse con las plataformas SIEM, SOAR a considerar en el Proyecto. El servicio SaaS incluye la operación y mantenimiento de la plataforma, su monitoreo, actualizaciones, soporte técnico con ingeniero de fabricante dedicado con Tecnical Account Manager TAMy optimización continua.	En relación con la restricción de "no se aceptan soluciones de código abierto o similares", se solicita aclarar: ¿Esta restricción aplica únicamente a la plataforma principal o también a componentes subyacentes (motores, agentes, librerías)? ¿Se permiten soluciones comerciales que incorporen componentes open source como parte de su arquitectura?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la restricción aplica para la solución principal, aclarando que el futuro proveedor del SOC, deberá responder por la implementación integral de los servicios requeridos.

164	5.3	**Especificaciones Técnicas Gestión y Monitoreo de Vulnerabilidades.** **5.3 Alcance del Requerimiento** Debe ser en modalidad software como servicio. (SaaS), con capacidad de aprovisionamiento rápido y elasticidad automática de servicios. No se aceptan soluciones de código abierto o similares. Debe integrarse con las plataformas SIEM, SOAR a considerar en el Proyecto. El servicio SaaS incluye la operación y mantenimiento de la plataforma, su monitoreo, actualizaciones, soporte técnico con ingeniero de fabricante dedicado con Tecnical Account Manager TAMy optimización continua.	En relación con el soporte técnico con ingeniero del fabricante (TAM se solicita aclarar): ¿Se requiere dedicación exclusiva o compartida? ¿Cuál es la disponibilidad esperada (horario, cobertura 7x24, idioma)? ¿Qué tipo de actividades se espera que realice (operación, optimización, acompañamiento estratégico, resolución de incidentes)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Oferente deberá tener en cuenta todos los aspectos de la operación a este respecto para garantizar el correcto funcionamiento dentro de los tiempos y cumplimientos de los SLA's, el esquema de cobertura deberá ajustarse en concordancia.
165	5.3	**Especificaciones Técnicas Gestión y Monitoreo de Vulnerabilidades.** **5.3 Alcance del Requerimiento** Debe ser en modalidad software como servicio. (SaaS), con capacidad de aprovisionamiento rápido y elasticidad automática de servicios. No se aceptan soluciones de código abierto o similares. Debe integrarse con las plataformas SIEM, SOAR a considerar en el Proyecto. El servicio SaaS incluye la operación y mantenimiento de la plataforma, su monitoreo, actualizaciones, soporte técnico con ingeniero de fabricante dedicado con Tecnical Account Manager TAMy optimización continua.	Se solicita aclarar cómo se gestionarán La incorporación de nuevos activos o entornos (cloud, on-premise, híbrido) y Cambios en el alcance durante la vigencia del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, todo cambio introducido deberá obedecer a los principios de planeación y acuerdo, de forma que si existen recursos disponibles y mientras el contrato esté en ejecución el Contratista deberá estar disponible para realizar la integración.
166	5.32	**Especificaciones Técnicas Gestión y Monitoreo de Vulnerabilidades.** 5.32 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.	En relación con el número total de 25.000 activos: ¿Corresponde a un máximo fijo o puede variar durante la ejecución del contrato? ¿Cómo se gestionarán incrementos en el inventario de activos en términos de licenciamiento y costos, esto se vera como un requerimiento adicional o se limita a la cantidad indicada desde esta fase del proceso?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
167	5.32	**Especificaciones Técnicas Gestión y Monitoreo de Vulnerabilidades.** 5.32 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.	En escenarios donde la reasignación de licencias afecte la cobertura de monitoreo o protección de activos críticos, ¿cómo se gestionará el riesgo operativo asociado?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá informar previamente cuando se cumpla el umbral de cobertura, la Entidad dará las directrices para la asignación y reutilización en caso de requerirse.
168	5.32	**Especificaciones Técnicas Gestión y Monitoreo de Vulnerabilidades.** 5.32 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 confirmar cómo se medirá el cumplimiento del licenciamiento total de 25.000 activos, especialmente en entornos dinámicos como nube, virtualización o usuarios de directorio activo.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la plataforma deberá tener el control de la cantidad de sensores desplegados.
169	5.4.11	**Especificaciones Técnicas Gestión y Monitoreo de Vulnerabilidades.** 5.4.11 La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	¿Qué tratamiento se dará a fabricantes que no estén incluidos en dichas evaluaciones por razones de alcance del estudio, pero que cuenten con capacidades equivalentes o superiores técnicament		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, su cumplimiento es obligatorio al ser requisitos mínimos exigidos.
170	5.4.11	**Especificaciones Técnicas Gestión y Monitoreo de Vulnerabilidades.** 5.4.11 La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	Se solicita aclarar si este requisito es habilitante (excluyente) o de carácter ponderable dentro del proceso de evaluación.		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, su cumplimiento es obligatorio al ser requisitos mínimos exigidos.
171	5.4.11	**Especificaciones Técnicas Gestión y Monitoreo de Vulnerabilidades.** 5.4.11 La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	Se solicita confirmar si la Entidad contempla mecanismos de validación objetiva adicionales a los reportes de Gartner/Forrester para evaluar capacidades funcionales 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, su cumplimiento es obligatorio al ser requisitos mínimos exigidos.
172	6.3.1	**Especificaciones Técnicas Caza de Amenazas** 6.3.1 Para el monitoreo y alertamiento temprano sobre nuevas vulnerabilidades, ataques. amenazas externas y del ciberespacio que puedan afectar a la infraestructura interna de la entidad el CONTRATISTA debe adelantar el despliegue, configuración y afinamiento de herramientas para cacería de amenazas, las cuales permitan tener una visual horizontal y vertical en el caso de incidentes de seguridad de la información. Debe tener por lo menos las siguientes componentes: Herramientas de caza de amenazas: herramienta para buscar e interceptar ataques ocultos de una manera proactiva. Se puede desplegar una sola herramienta siempre y cuando tanto la inteligencia como la caza sean completamente identificables y a nivel de mercado sea aceptada como tal. Hay que tener en cuenta que el despliegue de herramientas que no tengan las capacidades de cacería de amenazas completas, no serán evaluadas. Parametrizar y/o configurar la herramienta adquirida, a partir de las mejores prácticas definidas por el fabricante y las exigencias de la entidad.	Se solicita precisar el significado técnico de "interceptar ataques ocultos", indicando si implica capacidades de respuesta activa (bloqueo/contención) o únicamente detección y alertamiento sin intervención sobre tráfico o sistemas productivos.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la capacidad esperada es bloqueo o contención, derivada de la detección y alertamiento.
173	6.3.1	**Especificaciones Técnicas Caza de Amenazas** 6.3.1 Para el monitoreo y alertamiento temprano sobre nuevas vulnerabilidades, ataques. amenazas externas y del ciberespacio que puedan afectar a la infraestructura interna de la entidad el CONTRATISTA debe adelantar el despliegue, configuración y afinamiento de herramientas para cacería de amenazas, las cuales permitan tener una visual horizontal y vertical en el caso de incidentes de seguridad de la información. Debe tener por lo menos las siguientes componentes: Herramientas de caza de amenazas: herramienta para buscar e interceptar ataques ocultos de una manera proactiva. Se puede desplegar una sola herramienta siempre y cuando tanto la inteligencia como la caza sean completamente identificables y a nivel de mercado sea aceptada como tal. Hay que tener en cuenta que el despliegue de herramientas que no tengan las capacidades de cacería de amenazas completas, no serán evaluadas. Parametrizar y/o configurar la herramienta adquirida, a partir de las mejores prácticas definidas por el fabricante y las exigencias de la entidad.	Se solicita precisar qué capacidades mínimas conforman una "caza de amenazas completa" y bajo qué metodología objetiva se evaluará este criterio para evitar interpretaciones subjetivas durante la evaluación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, esta característica hace referencia al ciclo de gestión de amenazas, que incluye (no limitada a) detección, alertamiento, clasificación, contención, erradicación y lecciones aprendidas.
174	6.3.1	**Especificaciones Técnicas Caza de Amenazas** 6.3.1 Para el monitoreo y alertamiento temprano sobre nuevas vulnerabilidades, ataques. amenazas externas y del ciberespacio que puedan afectar a la infraestructura interna de la entidad el CONTRATISTA debe adelantar el despliegue, configuración y afinamiento de herramientas para cacería de amenazas, las cuales permitan tener una visual horizontal y vertical en el caso de incidentes de seguridad de la información. Debe tener por lo menos las siguientes componentes: Herramientas de caza de amenazas: herramienta para buscar e interceptar ataques ocultos de una manera proactiva. Se puede desplegar una sola herramienta siempre y cuando tanto la inteligencia como la caza sean completamente identificables y a nivel de mercado sea aceptada como tal. Hay que tener en cuenta que el despliegue de herramientas que no tengan las capacidades de cacería de amenazas completas, no serán evaluadas. Parametrizar y/o configurar la herramienta adquirida, a partir de las mejores prácticas definidas por el fabricante y las exigencias de la entidad.	Se solicita aclarar si la Entidad suministrará casos de uso, escenarios y reglas de detección, o si el contratista deberá diseñarlos, implementarlos y mantenerlos durante toda la operación del servicio.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se deberán tener en cuenta ambas consideraciones.
175	6.4.2	**Especificaciones Técnicas Caza de Amenazas** 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.	¿Estos valores corresponden a mínimos obligatorios o a capacidad máxima de la solución? Adicionalmente, ¿la infraestructura de virtualización y VLANs será provista por la Entidad o debe ser incluida dentro del alcance del contratista?		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, son requisitos mínimos. El oferente podrá exceder la expectativa sin que esto implique puntuación extra. Para todas las capacidades asociadas directamente al SOC el Contratista deberá proveer toda la infraestructura relacionada.

176	6.4.2	**Especificaciones Técnicas Caza de Amenazas** 6.4.3 El licenciamiento de la solución debe ser como mínimo ciento veinte (120) vlans.	Se solicita aclarar si el licenciamiento es fijo o escalable, y cómo se gestionarán incrementos o cambios en la arquitectura de red durante la vigencia del contrato , se solicita aclarar cual es maximo esperado e indicar que si se alcanza , y en caso de requerir mas , este incremento sera una solicitud adicional .		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
177	6.4.21	**6.4.12 Especificaciones Técnicas Caza de Amenazas** 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.	Se solicita precisar el fabricante, modelo y versión del Firewall de Nueva Generación de la Entidad, así como las capacidades reales de integración disponibles (APIs, syslog, webhooks u otros mecanismos). Adicionalmente, ¿el firewall cuenta actualmente con soporte nativo para visualización tipo dashboard extensible o se espera un desarrollo adicional por parte del contratista dentro del alcance? ¿Qué nivel de detalle debe mostrarse en el dashboard (telemetría, eventos, estado de señuelos, ataques, correlación) y cuál será la fuente de datos oficial para dicha visualización?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Firewall de nueva generación instalado actualmente en la Entidad permite la integración con componentes de terceros por medio de APIs, el Contratista deberá desarrollar los servicios necesarios para ser consumidos desde el NGFW. Toda la documentación correspondiente se encuentra disponible en la página web del fabricante.
178	6.5.1	**6.4.12 Especificaciones Técnicas Caza de Amenaza** 6.5.1 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).	Se solicita precisar si las 4 capas de decepción son obligatorias simultáneamente en todos los escenarios o si pueden implementarse de forma progresiva. Adicionalmente, ¿cuáles son los criterios de validación para determinar que cada capa está correctamente implementada y operativa en producción?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, este aspecto queda a discreción del oferente, así como todas las consideraciones técnicas derivadas del mismo.
179	8.20	**8 Especificaciones Técnicas Solución de análisis de código estático y dinámico para aplicaciones** 8.20 En el ciclo de desarrollo las herramientas del CONTRATISTA 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 solicita aclarar si el requerimiento de SASE aplica únicamente como control de acceso seguro en el entorno de desarrollo (SDLC) o si implica la implementación de una arquitectura SASE completa a nivel corporativo (ZTNA, SWG, CASB, FWaaS).		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.
180	8.20	**8 Especificaciones Técnicas Solución de análisis de código estático y dinámico para aplicaciones** 8.20 En el ciclo de desarrollo las herramientas del CONTRATISTA deben utilizar SASE (Secure Access Services Edge), buscando seguridad en dispositivos móviles, Internet de la cosas y migración de aplicaciones on-premise hacia Cloud.	Adicionalmente, ¿la Entidad ya cuenta con una solución SASE implementada o se espera que el contratista la suministre como parte del alcance? ¿Cómo se delimita el uso de SASE frente a otras soluciones ya existentes de seguridad perimetral, nube y endpoint para evitar solapamientos funcionales y costos duplicados?		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.
181	9.9	**9 Especificaciones Técnicas Protección de Marca (Deep&Dark Web)** 9.9 Generar informes detallados mensualmente o bajo demanda cuando la Entidad así lo requiera, sobre actividades de protección de marca, incluidas estadísticas de monitoreo, acciones tomadas y resultados obtenidos.	Se solicita indicar el límite de frecuencia para solicitudes , esto para delimitar los recursos a asignar los cuales son base para el componente economico de la oferta y cómo se gestionará el impacto operativo y de costos asociado a generación continua de reportes que sobrepase el umbral que se defina ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem es claro al referir el término bajo demanda, por lo tanto, la Entidad puede requerir o no las cantidades que estime conveniente y/o necesarias.
182	7.3	**Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas** 7.3 Se debe licenciar como mínimo para 25000 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web)	Se solicita a la Entidad aclarar el modelo de licenciamiento esperado para la solución de NDR, dado que el requerimiento se expresa en número de activos, pero estas soluciones típicamente se dimensionan en función de tráfico de red (Gbps) y capacidad de procesamiento.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la Entidad requiere licenciamiento para 25000 dispositivos, el proveedor del SOC deberá cumplir con las cantidades solicitadas independientemente de la forma de licenciar del o lo fabricantes ofrecidos.
183	7.3	**Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas** 7.3 Se debe licenciar como mínimo para 25000 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web)	Se solicita confirmar si la cifra de 25.000 activos corresponde a un inventario referencial o si será utilizada como base contractual para dimensionamiento, facturación y niveles de servicio, adicionalmente confirmar si se pasa ese indicador de activos y se incluyen mas , esto sera un requerimieto adicional		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
184	7.3	**Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas** 7.3 Se debe licenciar como mínimo para 25000 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web)	En relación con los 260 aplicativos web incluidos como "activos", se solicita aclarar cómo se espera su monitoreo dentro del alcance NDR, dado que este tipo de soluciones no necesariamente inspeccionan lógica de aplicación sino tráfico de red.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, "260 aplicaciones Web" se informa solo como referencia, el requerimiento mínimo es de 25000 activos.
185	7.3	**Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas** 7.3 Se debe licenciar como mínimo para 25000 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web)	Se solicita especificar el volumen estimado de tráfico de red (promedio y pico en Gbps), así como la distribución del tráfico (norte-sur vs. este-oeste), necesario para dimensionar correctamente la solución NDR.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la Entidad requiere licenciamiento para 25000 dispositivos, el proveedor del SOC deberá cumplir con las cantidades solicitadas independientemente de la forma de licenciar del o lo fabricantes ofrecidos, dato que es suficiente para dimensionar su ofrecimiento.
186	7.3	**Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas** 7.3 Se debe licenciar como mínimo para 25000 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web)	Se solicita aclarar los requerimientos de retención de metadata de red y capacidad de análisis histórico, dado que esto impacta directamente el almacenamiento y dimensionamiento de la solución		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la retención en línea deberá ser mínimo de un mes, en frio de al menos tres años y el histórico de al menos cinco años, el Contratista tendrá que proporcionar el almacenamiento para cumplir dichos parámetros.
187	7.3	**Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas** 7.3 Se debe licenciar como mínimo para 25000 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web)	Finalmente, se solicita confirmar cómo se gestionarán escenarios en los que el crecimiento del tráfico supere la capacidad inicialmente dimensionada, y si esto será considerado un ajuste de alcance.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la Entidad requiere licenciamiento para 25000 dispositivos, es la cantidad mínima solicitada, por lo tanto, no se exigirá más de lo solicitado en la vigencia contractual.
188	11.9	**Especificaciones Técnicas Ethical Hacking** 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).	Considerando que el alcance se define bajo modalidad de "contrato llave en mano", lo cual implica la provisión por parte del contratista de todos los recursos tecnológicos, físicos y logísticos necesarios para la implementación, se solicita a la Entidad aclarar si existe un dimensionamiento máximo o límites definidos para la expansión de infraestructura, capacidad o servicios asociados durante la ejecución del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
189	11.9	**Especificaciones Técnicas Ethical Hacking** 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).	En caso de no existir dichos límites, se solicita indicar cuál será el umbral de crecimiento permitido (en términos porcentuales o de consumo incremental sobre la línea base del diseño inicial) y el mecanismo mediante el cual la Entidad gestionará y aprobará las ampliaciones de capacidad o demanda adicional.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
190	11.9	**Especificaciones Técnicas Ethical Hacking** 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).	Adicionalmente, se solicita confirmar si los incrementos que excedan dichos umbrales serán considerados como servicios adicionales sujetos a reconocimiento económico independiente o si deberán ser asumidos dentro del valor global del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.

191	11.17	**Especificaciones Técnicas Ethical Hacking** 11.17 Todos los recursos tecnológicos, logísticos, de infraestructura, humanos y demás que se requieran para la implementación de los servicios incluidos en este documento, serán por cuenta del contratista, modalidad "llave en mano".	Considerando que el alcance se define bajo modalidad de "contrato llave en mano", lo cual implica la provisión por parte del contratista de todos los recursos tecnológicos, físicos y logísticos necesarios para la implementación, se solicita a la Entidad aclarar si existe un dimensionamiento máximo o límites definidos para la expansión de infraestructura, capacidad o servicios asociados durante la ejecución del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
192	11.17	**Especificaciones Técnicas Ethical Hacking** 11.17 Todos los recursos tecnológicos, logísticos, de infraestructura, humanos y demás que se requieran para la implementación de los servicios incluidos en este documento, serán por cuenta del contratista, modalidad "llave en mano".	En caso de no existir dichos límites, se solicita indicar cuál será el umbral de crecimiento permitido (en términos porcentuales o de consumo incremental sobre la línea base del diseño inicial) y el mecanismo mediante el cual la Entidad gestionará y aprobará las ampliaciones de capacidad o demanda adicional.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
193	11.17	**Especificaciones Técnicas Ethical Hacking** 11.17 Todos los recursos tecnológicos, logísticos, de infraestructura, humanos y demás que se requieran para la implementación de los servicios incluidos en este documento, serán por cuenta del contratista, modalidad "llave en mano".	Adicionalmente, se solicita confirmar si los incrementos que excedan dichos umbrales serán considerados como servicios adicionales sujetos a reconocimiento económico independiente o si deberán ser asumidos dentro del valor global del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el inventario ya tiene incluida holgura, con esto no deberían presentarse crecimientos inesperados.
194	11.20	**Especificaciones Técnicas Ethical Hacking** 11.20 Implementar las diferentes fases del proyecto bajo los estándares del PMBOK o metodologías agiles o híbrido, con el objeto de garantizar la aplicación de conocimientos, habilidades, herramientas y técnicas estandarizadas en todas las actividades que se van a desarrollar durante el proyecto.	Se solicita a la Entidad aclarar el alcance de responsabilidad del contratista frente a la compatibilidad e interoperabilidad con las tecnologías actualmente instaladas en la Entidad, considerando que dichas plataformas corresponden a infraestructura de terceros bajo su administración.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
195	11.20	**Especificaciones Técnicas Ethical Hacking** 11.20 Implementar las diferentes fases del proyecto bajo los estándares del PMBOK o metodologías agiles o híbrido, con el objeto de garantizar la aplicación de conocimientos, habilidades, herramientas y técnicas estandarizadas en todas las actividades que se van a desarrollar durante el proyecto.	En particular, se requiere precisar qué sucede en los casos en los que, por restricciones técnicas, versiones obsoletas, limitaciones de fabricante o configuraciones propias del entorno existente, no sea posible garantizar la interoperabilidad con la solución propuesta. En estos escenarios, se solicita confirmar si la Entidad asumirá las adecuaciones, actualizaciones o ajustes necesarios sobre su infraestructura base, o si estos serán considerados como requerimientos adicionales con impacto en costos, cronograma o alcance del contrato		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
196	11.22	**Especificaciones Técnicas Ethical Hacking** 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.	Se solicita aclarar si la informacion técnica tipo datasheets o documentación pública del fabricante (incluyendo referencia a página y párrafo de cumplimiento), es exigible en la etapa de presentación de oferta, durante la evaluación técnica, o como parte de la etapa de perfeccionamiento y/o ejecución del contrato.?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la documentación será exigible: en cualquier etapa para consulta, en la presentación y evaluación como requisito, en la firma como obligación contractual y en la ejecución como documentación.
197	11.22	**Especificaciones Técnicas Ethical Hacking** 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.	Adicionalmente, se solicita confirmar si durante la evaluación se aceptarán compromisos del fabricante o documentación preliminar, o si el cumplimiento debe estar soportado exclusivamente en documentación pública vigente y verificable al momento de la presentación de la propuesta		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, para la evaluación solo será tenida en cuenta la documentación pública verificable.
198	Nota 1 ,Nota 2 , Nota3	Anexo Técnico – Ítems Verificables, ítem 1.1, Notas 1, 2 y 3	Dado que el Anexo Técnico establece que el contrato es "llave en mano" y que todos los elementos, plataformas, soluciones y servicios deberán ser prestados por el contratista, ¿confirma la DIAN que el alcance incluye infraestructura física, eléctrica, climatización, racks, enlaces de conectividad y seguridad física del SOC en Bogotá, o estos elementos serán provistos parcial o totalmente por la Entidad?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, para todas las capacidades asociadas directamente al SOC el Contratista deberá proveer toda la infraestructura relacionada.
199	1.2	Anexo Técnico – Ítems Verificables, ítem 1.2	¿El SOC físico en Bogotá requerido debe ser 100% del CONTRATISTA o puede corresponder a una infraestructura híbrida (propia del contratista + infraestructura DIAN)? En caso de ser híbrido, ¿qué componentes físicos y lógicos son responsabilidad directa de la DIAN?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, para todas las capacidades asociadas directamente al SOC el Contratista deberá proveer toda la infraestructura relacionada.
200	1.3	Anexo Técnico – Ítems Verificables, ítem 1.3	Durante el período en el que el CONTRATISTA debe operar el SIEM actual IBM QRadar (hasta el 31 de agosto de 2027), ¿la DIAN suministrará: -Licenciamiento vigente -Soporte fabricante -Infraestructura asociada?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la consideración corresponde a las condiciones actuales.
201	1.3	Anexo Técnico – Ítems Verificables, ítem 1.3	¿La DIAN espera que exista un período de coexistencia entre el SIEM actual (IBM QRadar) y el nuevo SIEM a implementar a partir del 1 de septiembre de 2027? En caso afirmativo: - ¿Por cuánto tiempo? - ¿Debe existir sincronización de logs, casos de uso e históricos?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que: a) Habrá un periodo de coexistencia de las dos tecnologías, sin embargo, solo una estará recibiendo registros. b) hasta que se cumplan los periodos de retención en caliente. c) No habrá sincronización de logs entre plataformas.
202	1.3	Anexo Técnico – Ítems Verificables, ítem **1.3** y sección **4**	Para el firewall de bases de datos IBM Guardium vigente hasta el 31 de diciembre de 2027, ¿el CONTRATISTA deberá únicamente operar la plataforma existente y/o también asumir actividades de afinamiento, creación de nuevas políticas y soporte extendido? ¿Existe alguna restricción para que el nuevo firewall de BD sea de un fabricante diferente al actual?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que: a) El Contratista debe asumir la operación completa de la herramienta, que implica todas las gestiones relacionadas (no limitadas) como son: gestión del sistema operativo de los componentes (gestión de parches y actualizaciones, cambios de configuración, corrección de errores, afinamiento, control de tareas administrativas, generación de scripts, etc.), gestión de la configuración de los componentes (Despliegue de políticas, afinamiento, creación de exclusiones, evaluación de desempeño, ajustes de umbrales, etc.), gestión del ciclo de monitoreo (análisis, alertamiento, clasificación, generación de informes, verificación de cierre de brechas, etc.) b) este aspecto queda a discreción del oferente, así como todas las consideraciones técnicas derivadas del mismo.
203	1.3	Anexo Técnico – Ítems Verificables, ítem 1.3 y sección 7	Considerando que la capacidad NDR inicia operación a partir de enero de 2028, ¿se requiere que la infraestructura, licencias y sensores estén desplegados previamente? ¿Se deberia realizar una fase de aprendizaje antes de la fecha oficial de puesta en marcha?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la capacidad NDR deberá estar implementada, licenciada, configurada, probada y lista para su puesta en operación conforme a las fechas establecidas en los documentos del proceso. Las actividades de despliegue, afinamiento, aprendizaje o estabilización que sean necesarias deberán ser contempladas por el contratista dentro del plan de implementación, sin afectar la continuidad del servicio ni generar costos adicionales para la Entidad.
204	2.8	Anexo Técnico – Ítems Verificables, ítem 2.8	La integración del SIEM con el ITSM ARANDA debe ser nativa certificada por el fabricante, o es aceptable mediante APIs/conectores desarrollados por el CONTRATISTA ¿La DIAN suministrará documentación técnica/API de ARANDA para dicha integración?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la integración con el ITSM institucional podrá realizarse mediante capacidades nativas, APIs, conectores o desarrollos requeridos por el contratista, siempre que se cumpla con la funcionalidad solicitada. La información técnica disponible para dicha integración será suministrada durante la fase de implementación, bajo los controles de seguridad y confidencialidad aplicables.
205	2.9	Anexo Técnico – Ítems Verificables, ítem 2.9	Respecto a la correlación cruzada SOC–NOC con la plataforma ORION, la DIAN espera correlación directa de eventos ORION hacia SIEM o únicamente consumo de métricas/alertas ya procesadas ¿Existe acceso a ambientes de prueba de ORION para validaciones técnicas previas?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la correlación SOC–NOC deberá permitir el consumo, integración y análisis de eventos, métricas o alertas relevantes para enriquecer el contexto de seguridad, conforme a las capacidades definidas en los documentos del proceso. Los detalles técnicos de integración con la plataforma ORION y la disponibilidad de ambientes de validación serán definidos durante la fase de implementación, de acuerdo con las condiciones técnicas y de seguridad de la Entidad.

206	2.14	Anexo Técnico – Ítems Verificables, ítem 2.14	Los 20 casos de uso requeridos en la fase de implementación son definidos exclusivamente por la DIAN o pueden ser propuestos por el oferente y validados por la Entidad ¿Existe un catálogo base de casos de uso prioritarios definidos?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los veinte (20) casos de uso requeridos para la fase de implementación podrán ser propuestos por el contratista y deberán ser revisados, priorizados y validados por la Entidad, conforme a sus necesidades de monitoreo, riesgos y capacidades tecnológicas. Durante la operación podrán definirse casos de uso adicionales según las necesidades del servicio.
207	3.4	Anexo Técnico – Ítems Verificables, ítem 3.4	Se solicita licenciamiento mínimo requerido para 3 analistas.Estos corresponden a analistas concurrentes, analistas nombrados o sesiones simultáneas Es posible que durante el contrato la ampliación de analistas debe estar contemplada dentro de la oferta?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los requerimientos solicitados son mínimos en este caso tres (3) analistas o su equivalente de acuerdo al servicio entregado, no se contemplan crecimientos a futuro, se respetan las cantidades solicitadas.
208	3.52	Anexo Técnico – Ítems Verificables, ítems 3.52 – 3.70	Cuando se indica un mínimo de 300 playbooks y 300 conectores, la DIAN acepta playbooks/comunidades oficiales del fabricante, playbooks desarrollados por el oferente, ambas opciones son válidas ¿Debe entregarse evidencia documental de cada playbook/conector en la propuesta técnica?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento mínimo es de 300 playbooks y 300 conectores oficiales del fabricante. El oferente deberá aportar la documentación técnica que permita verificar el cumplimiento de las capacidades ofertadas.
209	5.11	Anexo Técnico – Ítems Verificables, ítems 5.11.1 – 5.11.5	¿La DIAN exige que todas las capacidades CNAPP (CWPP, CSPM, CIEM, DSPM, IaC) sean del mismo fabricante, o se aceptan integraciones siempre que exista consola unificada?		La Dirección de Impuestos y Aduanales Nacionales - DIAN aclara al observante que las capacidades CNAPP deberán cumplir integralmente con lo solicitado en los documentos del proceso, garantizando integración, visibilidad y operación centralizada.
210	5.5.3	Anexo Técnico – Ítems Verificables, ítem 5.5.3	Respecto a la auditoría de Active Directory sin agentes, ¿existe alguna excepción controlada para escenarios donde el fabricante requiera componentes livianos solo de lectura?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento de auditoría de Active Directory sin agentes se mantiene en los términos definidos en los documentos del proceso.
211	6.4.2	Anexo Técnico – Ítems Verificables, ítems 6.4.2 – 6.4.3	Para el requisito de 400 señuelos y 120 VLANs, ¿la DIAN espera despliegue total desde el inicio o un despliegue progresivo basado en criticidad ¿Las VLAN serán suministradas por la DIAN o deberán ser creadas por el CONTRATISTA?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las capacidades mínimas de señuelos, máquinas virtuales y despliegue en VLAN deberán estar disponibles conforme a los requerimientos técnicos establecidos. El despliegue podrá organizarse de forma progresiva y priorizada durante la implementación, de acuerdo con la criticidad de los entornos y la arquitectura aprobada por la Entidad. Las VLAN existentes serán definidas por la DIAN; cualquier ajuste técnico requerido deberá coordinarse y aprobarse durante la fase de implementación.
212	6.5.7	Anexo Técnico – Ítems Verificables, ítems 6.5.7 – 6.5.10	La DIAN podría confirmar por favor cuáles ambientes OT/SCADA están actualmente en operación. Así mismo aclarar si existe inventario técnico detallado para estos entornos ¿Se permite realizar pilotos controlados antes del despliegue completo?		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, actualmente no se cuenta con entornos OT, la característica se solicita para futuros proyectos, sin embargo, se aclara que el servicio solicitado debe cumplir con esta característica.
213	7.3	Anexo Técnico – Ítems Verificables, ítems 7.3 y 7.18	Se observa una diferencia entre el licenciamiento mínimo para 25.000 activos (ítem 7.3) y licenciamiento para 17.727 dispositivos por 3 años (ítem 7.18) ¿Puede la DIAN aclarar cuál es el número definitivo y vinculante para efectos de licenciamiento y costos?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la cantidad de dispositivos es 25000, para lo cual se procederá a modificar la cantidad expresada en este ítem quedando de la siguiente manera, cambio que se verá reflejado en la adenda a publicar en los próximos días: 7.18 El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 25000 dispositivos por (3) años.
214	7.14	Anexo Técnico – Ítems Verificables, ítem 7.14	¿Los 6 meses de retención mínima de tráfico NDR deben ser en almacenamiento local del appliance o se acepta almacenamiento híbrido (local + frío)? ¿Existe expectativa de ampliar este período durante el contrato?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la retención mínima de seis (6) meses deberá garantizar la consulta y disponibilidad de los datos capturados conforme a lo solicitado en los documentos del proceso, así mismo el ítem es claro "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".
215	8.4	Anexo Técnico – Ítems Verificables, ítems 8.4 – 8.7	¿Existe actualmente una metodología formal de SDLC documentada por DIGIT. Hay un pipeline CI/CD estándar institucional? ¿La DIAN suministrará acceso y lineamientos técnicos para integraciones CI/CD?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la interacción con entornos SDLC, CI/CD y DevSecOps deberá realizarse conforme a los lineamientos, herramientas y accesos que la Entidad disponga durante la fase de implementación. El contratista deberá proponer los mecanismos de integración, monitoreo y acompañamiento requeridos, los cuales deberán ser validados y autorizados por la Entidad.
216	8.17	Anexo Técnico – Ítems Verificables, ítems 8.17 – 8.21	¿El acompañamiento en remediación de vulnerabilidades debe ser bajo modalidad bolsa de horas o atención ilimitada durante la vigencia del contrato?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el acompañamiento en la remediación de vulnerabilidades hace parte del alcance del servicio durante la vigencia contractual. El contratista deberá disponer los recursos necesarios para apoyar la priorización, análisis, generación de planes de acción, seguimiento y acompañamiento técnico, sin que ello implique la intervención directa sobre plataformas de la Entidad, salvo autorización expresa.
217		Solicitud de Oferta, Sección VII y VIII (Condiciones Contractuales)	Los pagos estarán asociados a hitos de implementación, operación mensual o un esquema mixto. ¿Se contempla algún pago inicial por fase de transición?	Pago mixto , según la capcaidad	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los pagos se realizarán a medida de que el futuro proveedor de SOC vaya realizando la implementación y puesta en operación de cada uno de los servicios y capacidades SOC requeridas por la Entidad, así mismo, se aclara que la gestión, operación y administración se pagará mensualmente.
218		Anexo Técnico – Administrativo, ítems ANS / SLA	¿Las penalidades por incumplimiento SLA se aplican por evento individual, por acumulado mensual o por incumplimiento reiterado? ¿Existe un tope máximo de penalización 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) están definidas las condiciones de aplicación de los ANS frente a los valores por mes y frente al valor tal del contrato.
219	17	Anexo Técnico – Administrativo, ítem 17 – Equipo mínimo de trabajo	¿Confirma la DIAN que, para el ítem 17 "Equipo mínimo de trabajo", no es obligatorio anexar hojas de vida nominativas del personal, y que es suficiente con la descripción de perfiles, roles, experiencia mínima y certificaciones exigidas?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las hojas de vida y soportes del equipo mínimo deberán ser presentados por el oferente ganador en la etapa que corresponda, conforme a lo establecido en los documentos del proceso. En la oferta deberán acreditarse las condiciones exigidas para los perfiles, roles, experiencia mínima y certificaciones requeridas.
220	1.3	Anexo Técnico – Ítems Verificables, ítem 1.3	¿Confirma la DIAN que las plataformas actualmente en operación (SIEM IBM QRadar y Firewall de Bases de Datos IBM Guardium) son de propiedad de la Entidad, y que el contratista no debe asumir costos de licenciamiento, renovación o infraestructura de dichas soluciones durante el período de operación transitoria?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las plataformas IBM QRadar e IBM Guardium actualmente en operación son de propiedad de la Entidad. El futuro contratista deberá recibirlas, gestionarlas, administrarlas y operarlas durante el periodo transitorio definido en los documentos del proceso, conforme al soporte vigente y a las condiciones allí establecidas.
221	5	Anexo Técnico – Ítems 5, 6, 7, 8, 9	Se entiende que las demás soluciones relacionadas para ser incluidas no son soluciones actuales que hoy en día tenga la entidad sino que se trata de soluciones nuevas, que debe proveer el contratista y que deben ser en su totalidad propiedad de la DIAN, es esto correcto?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, todas las soluciones solicitadas son nuevas, sólo que el SIEM, FIREWALL DE BASES DE DATOS e INTELIGENCIA DE AMENAZAS, deberán ser implementadas en fechas diferentes de acuerdo a lo estipulado en los documentos del proyecto.
222		N/A	Teniendo en cuenta la criticidad del proyecto SOC, ¿confirma la DIAN si, durante la etapa de evaluación técnica, negociación o previa a la implementación, podrá requerir demostraciones técnicas controladas (PoC, demostraciones funcionales o laboratorios) de algunas de las capacidades ofertadas, tales como SIEM, SOAR, NDR, Caza de Amenazas o Protección de Bases de Datos? En caso afirmativo, ¿estas demostraciones serían oosteriores a la evaluación documental o serán solicitadas únicamente al oferente mejor evaluado o no se contemplan de carácter obligatorio para la presentación de la oferta?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, no se contemplan demostraciones o cualquier otro tipo de prueba.
223		N/A	¿Existen restricciones actuales o políticas internas DIAN que limiten la ejecución de acciones automatizadas por parte del SOAR (por ejemplo, bloqueo de usuarios, aislamiento de activos, cambios en firewall)?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las acciones automatizadas ejecutadas mediante SOAR deberán estar previamente definidas, autorizadas y coordinadas con la Entidad, especialmente cuando puedan impactar usuarios, activos, reglas de seguridad, conectividad, ambientes productivos o continuidad operativa. La automatización deberá implementarse bajo flujos aprobados, controles de auditoría y mecanismos de reversión cuando aplique.
224		N/A	¿El inventario de activos suministrado en el Anexo Técnico refleja el estado real y actualizado de la infraestructura o debe considerarse como una referencia inicial susceptible de ajustes durante la implementación?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el inventario suministrado corresponde a la información de referencia disponible para la estructuración de la oferta. Durante la fase de implementación podrán realizarse validaciones, ajustes o actualizaciones propias del levantamiento técnico, sin que ello modifique las obligaciones mínimas establecidas en los documentos del proceso.

225		N/A	¿La DIAN puede indicar tasas de crecimiento estimadas (anuales o plurianuales) de activos, eventos, aplicaciones y servicios cloud, para efectos de planeación de capacidad del SOC?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las tasas de crecimiento ya se encuentran estipuladas en las cantidades mínimas solicitadas en los documentos del proceso.
226		N/A	Durante eventos críticos (fechas tributarias, cierres fiscales, picos operativos), ¿se requerirán esquemas de refuerzo operativo del SOC o aumento temporal de capacidad?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el servicio SOC deberá operar conforme a los ANS/SLA definidos en los documentos del proceso, incluyendo la atención de eventos críticos, picos operativos o periodos de alta demanda institucional. El contratista deberá contemplar dentro de su modelo operativo la capacidad necesaria para mantener la continuidad y oportunidad del servicio.
227		N/A	¿Confirma la DIAN que los casos de uso, playbooks, scripts, dashboards, modelos de correlación y cualquier desarrollo específico realizado durante el contrato serán de propiedad exclusiva de la Entidad al finalizar el contrato?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los casos de uso, playbooks, scripts, dashboards, reglas, modelos de correlación, parametrizaciones, documentación y demás desarrollos específicos realizados para la Entidad en ejecución del contrato deberán quedar documentados y disponibles para la DIAN, conforme a lo establecido en los documentos del proceso y a las condiciones de propiedad, uso y transferencia que resulten aplicables.
228		N/A	Durante la fase de devolución del servicio, ¿la DIAN espera que el CONTRATISTA entregue únicamente documentación y configuraciones, o también acompañamiento operativo activo durante un período de transición?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la devolución del servicio deberá incluir la entrega de documentación, configuraciones, respaldos, procedimientos, evidencias, licenciamiento, transferencia de conocimiento y acompañamiento operativo requerido para asegurar la continuidad del servicio, conforme a lo previsto en los documentos del proceso.
229		N/A	¿Las integraciones con plataformas que no se encuentren actualmente en los inventarios suministrados deberán considerarse parte del alcance contractual sin costo adicional, siempre que estén dentro del ecosistema tecnológico de la DIAN?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las integraciones deberán realizarse conforme al alcance, cantidades, capacidades y ecosistema tecnológico definidos en los documentos del proceso. Las integraciones adicionales que sean requeridas durante la ejecución deberán ser analizadas, priorizadas y aprobadas por la Entidad, conforme a las condiciones técnicas y contractuales aplicables.
230		N/A	¿El SOC deberá atender auditorías técnicas o requerimientos de información por parte de entes externos (BID, Contraloría, Auditorías TIC) como parte del alcance estándar del servicio?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el contratista deberá apoyar la atención de auditorías, requerimientos de información, revisiones técnicas o solicitudes relacionadas con los servicios prestados por el SOC, cuando estas se encuentren asociadas al alcance contractual. Dicho apoyo deberá realizarse bajo los lineamientos, autorizaciones y canales definidos por la Entidad.
231		N/A	En caso de cambios tecnológicos relevantes durante la vigencia del contrato (por ejemplo, salida de soporte de un fabricante, adquisición de nuevas plataformas institucionales), ¿cómo se gestionará el impacto contractual y técnico?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los cambios tecnológicos relevantes que se presenten durante la vigencia contractual deberán ser gestionados conforme a los mecanismos de seguimiento, control, aprobación y gestión de cambios definidos para el proyecto. En todo caso, el contratista deberá mantener la continuidad, soporte y cumplimiento de las capacidades mínimas requeridas en los documentos del proceso.
232	1.3 Nota 5 Nota 7 Nota 8	Anexo Técnico – Ítems Verificables, ítem 1.3 Formulario de Lista de Precios, Notas 5, 7 y 8	Teniendo en cuenta que el Anexo Técnico establece que el CONTRATISTA deberá operar soluciones actualmente licenciadas de propiedad de la DIAN (SIEM IBM QRadar hasta agosto de 2027 y Firewall de Bases de Datos IBM Guardium hasta diciembre de 2027), y que las nuevas soluciones deberán implementarse posteriormente (a partir de septiembre de 2027 y enero de 2028 respectivamente), solicitamos a la Entidad confirmar cuál es la expectativa real respecto a la cotización de estas nuevas soluciones desde la etapa de oferta. En particular, se solicita aclarar si la DIAN espera que los oferentes: (i) Coticen desde ahora soluciones cuya implementación y entrada en operación se realizará dentro de 18 a 24 meses, entendiendo que dichas condiciones comerciales, tecnológicas y de mercado difícilmente pueden mantenerse inalteradas en el tiempo; o (ii) Presenten una estructura referencial de costos, sujeta a ajustes debidamente regulados contractualmente, al momento de la implementación efectiva.		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, sin que se contemple una estructura meramente referencial sujeta a ajustes posteriores.
233	1.3 Nota 5 Nota 7 Nota 8	Anexo Técnico – Ítems Verificables, ítem 1.3 Formulario de Lista de Precios, Notas 5, 7 y 9	Adicionalmente, solicitamos a la DIAN indicar si dentro de su planeación tecnológica se contempla como alternativa la renovación anticipada o extensión del licenciamiento actual de las soluciones existentes (SIEM y Firewall de Bases de Datos), con el fin de llevar dichas plataformas a un esquema de coterminо con las nuevas soluciones a incluir, reduciendo así los riesgos tecnológicos, contractuales y económicos tanto para la Entidad como para los oferentes. En caso afirmativo, ¿estas eventuales renovaciones formarían parte del alcance del contrato objeto de la licitación o serían gestionadas directamente por la DIAN?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el alcance del proceso corresponde a lo definido en los documentos de la licitación. El contratista deberá recibir, gestionar, administrar y operar las soluciones existentes durante los periodos transitorios señalados, y posteriormente implementar las nuevas capacidades requeridas conforme a las fechas y condiciones allí establecidas.
234	1.3 Nota 5 Nota 7 Nota 10	Anexo Técnico – Ítems Verificables, ítem 1.3 Formulario de Lista de Precios, Notas 5, 7 y 10	Considerando que la cotización anticipada de soluciones cuya implementación se materializará en 2027 y 2028 expone a riesgos significativos asociados a variaciones en precios de mercado, cambios en modelos de licenciamiento de los fabricantes, obsolescencia tecnológica o incluso discontinuidad de productos, solicitamos a la DIAN precisar si el contrato contemplará mecanismos explícitos para gestionar estos riesgos, tales como: Ajustes contractuales por cambios sustanciales en las condiciones de licenciamiento de los fabricantes Sustitución tecnológica por soluciones equivalentes o superiores Actualización del alcance sin afectar el equilibrio económico del contrato		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los riesgos asociados a variaciones de mercado, modelos de licenciamiento o evolución tecnológica deberán ser considerados por el oferente al estructurar su propuesta. Cualquier sustitución tecnológica deberá cumplir con condiciones equivalentes o superiores a las requeridas y estar previamente aprobada por la Entidad, sin afectar el alcance, continuidad, soporte, garantía ni condiciones económicas ofertadas.
235	14 15 18	Anexo Técnico – Administrativo, ítems 14 (Capacitación), 15 (Transferencia de Conocimiento) y 18 (Certificaciones)	En relación con los ítems de Capacitación y Transferencia de Conocimiento solicitados en el Anexo Técnico Administrativo, solicitamos a la DIAN precisar cuál es el alcance esperado de la transferencia de conocimiento hacia su equipo interno. En particular, se solicita aclarar si la transferencia de conocimiento debe enfocarse principalmente en: (i) El uso operativo de las plataformas (SIEM, SOAR, NDR, CNAPP, Deception, AppSec, etc.) (ii) La administración técnica avanzada de las soluciones (iii) El diseño de casos de uso, playbooks y modelos de respuesta (iv) O una combinación integral de los anteriores Así mismo, se solicita confirmar si esta transferencia está orientada a habilitar a la DIAN para una operación autónoma futura del SOC, o si se entiende como una transferencia de conocimiento funcional limitada al acompañamiento durante la vigencia del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la transferencia de conocimiento deberá contemplar una combinación integral de uso operativo, administración técnica, configuración, optimización, diseño de casos de uso, playbooks, modelos de respuesta y demás actividades propias de las capacidades y servicios entregados para el SOC, conforme a lo establecido en los documentos del proceso.

236	14 15 18	Anexo Técnico – Administrativo, ítems 14 (Capacitación), 15 (Transferencia de Conocimiento) y 18 (Certificaciones)	El Anexo Técnico Administrativo menciona la realización de certificaciones internacionales para personal de la DIAN. Al respecto, solicitamos a la Entidad precisar la expectativa real asociada a dichas certificaciones. En particular, agradecercemos nos confirmen: ¿Qué objetivo persigue la DIAN con estas certificaciones (formación estratégica, fortalecimiento institucional, reemplazo progresivo del proveedor, cumplimiento de auditorías, entre otros)? ¿Las certificaciones solicitadas son obligatorias y habilitantes dentro del contrato, o se entienden como un valor agregado deseable?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las certificaciones y capacitaciones solicitadas hacen parte integral del alcance contractual y buscan fortalecer las capacidades institucionales de la Entidad en seguridad de la información, operación SOC, gestión de incidentes, continuidad, auditoría y demás temáticas relacionadas con el proyecto. Por tanto, deberán ser contempladas por el oferente conforme a lo establecido en los documentos del proceso.
237	14 15 18	Anexo Técnico – Administrativo, ítems 14 (Capacitación), 15 (Transferencia de Conocimiento) y 18 (Certificaciones)	Dado que las certificaciones referenciadas son de carácter internacional y suelen implicar costos elevados (derechos de examen, entrenamientos oficiales, materiales, renovaciones y posibles recertificaciones), solicitamos a la DIAN aclarar si se espera que dichas certificaciones sean asumidas económicamente en su totalidad por el CONTRATISTA como parte del contrato. En caso afirmativo, ¿la Entidad ha estimado o definido un número máximo de certificaciones a financiar, con el fin de permitir a los oferentes estructurar una oferta económica realista y comparable?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los costos asociados a las capacitaciones, certificaciones, vouchers, materiales y demás elementos requeridos para cumplir con este componente deberán ser considerados por el oferente dentro de su propuesta, conforme a las cantidades y condiciones establecidas en los documentos del proceso.
238	14 15 18	Anexo Técnico – Administrativo, ítems 14 (Capacitación), 15 (Transferencia de Conocimiento) y 18 (Certificaciones)	Solicitamos a la DIAN precisar el número de funcionarios beneficiarios de los esquemas de capacitación y certificación, así como el tipo de perfiles a los que estaría dirigido este componente del contrato.. ¿Las certificaciones están dirigidas a perfiles técnicos, operativos, estratégicos o mixtos? ¿Existe un número definido o estimado de personas por certificar, o se deja a criterio del oferente dentro del alcance contractual?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el número mínimo de beneficiarios, capacitaciones, reentrenamientos y vouchers se encuentra definido en los documentos del proceso. Los funcionarios beneficiarios serán designados por la Entidad de acuerdo con sus necesidades institucionales, perfiles técnicos, operativos o estratégicos relacionados con el alcance del proyecto.
239	14 15 18	Anexo Técnico – Administrativo, ítems 14 (Capacitación), 15 (Transferencia de Conocimiento) y 18 (Certificaciones)	¿Las certificaciones y capacitaciones solicitadas deben estar directamente asociadas a las tecnologías específicas que se oferten dentro del contrato (por ejemplo, certificaciones oficiales de fabricantes), o la DIAN acepta certificaciones de carácter transversal en ciberseguridad (ISO, gestión de incidentes, SOC, threat hunting, etc.) siempre que cumplan el objetivo de fortalecimiento de capacidades institucionales?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las capacitaciones, certificaciones y transferencia de conocimiento deberán atender tanto las tecnologías ofertadas como los estándares, buenas prácticas y temáticas transversales de ciberseguridad definidas en los documentos del proceso. El contratista deberá asegurar que estas actividades contribuyan al fortalecimiento de capacidades institucionales asociadas al SOC.
240	14 15 18	Anexo Técnico – Administrativo, ítems 14 (Capacitación), 15 (Transferencia de Conocimiento) y 18 (Certificaciones)	Solicitamos a la DIAN aclarar la modalidad esperada para las capacitaciones y certificaciones, indicando si se espera que estas sean: presenciales, virtuales, híbridas Así mismo, agradeceremos confirmar si las capacitaciones y certificaciones deben realizarse: En un único momento del contrato De forma periódica O bajo un esquema flexible a demanda durante la vigencia del servicio		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las capacitaciones, certificaciones y actividades de transferencia de conocimiento podrán desarrollarse en modalidad presencial, virtual o híbrida, siempre que cumplan con las condiciones oficiales, certificables y de calidad exigidas en los documentos del proceso. La programación se coordinará con la supervisión del contrato durante la ejecución.
241	14 15 18	Anexo Técnico – Administrativo, ítems 14 (Capacitación), 15 (Transferencia de Conocimiento) y 18 (Certificaciones)	Ssolicitamos a la entidad confirmar cuáles serán las evidencias y entregables esperados para dar por cumplidos los componentes de Capacitación, Certificación y Transferencia de Conocimiento, tales como: Certificados oficiales emitidos por fabricantes o entidades certificadoras: actas de asistencia, materiales de entrenamiento, evaluaciones de conocimiento, con el fin de evitar interpretaciones posteriores durante la ejecución contractual.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las evidencias mínimas esperadas para acreditar el cumplimiento de los componentes de capacitación, certificación y transferencia de conocimiento podrán incluir, entre otras, actas de asistencia, certificados, vouchers, materiales de entrenamiento, evaluaciones, registros de participación, informes de ejecución y demás soportes que permitan verificar el cumplimiento de las actividades realizadas.
242	11.9	**Especificaciones Implementación de todas las Capacidades y Servicios Entregados** 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).	Considerando que el alcance se define bajo modalidad de "contrato llave en mano", lo cual implica la provisión por parte del contratista de todos los recursos tecnológicos, físicos y logísticos necesarios para la implementación, se solicita a la Entidad aclarar si existe un dimensionamiento máximo o límites definidos para la expansión de infraestructura, capacidad o servicios asociados durante la ejecución del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, no existe un dimensionamiento máximo, todos los ítems de los servicios requeridos contemplan cantidades mínimas que es lo que exige la Entidad para su cumplimiento.
243	11.9	**Especificaciones Implementación de todas las Capacidades y Servicios Entregados** 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).	En caso de no existir dichos límites, se solicita indicar cuál será el umbral de crecimiento permitido (en términos porcentuales o de consumo incremental sobre la línea base del diseño inicial) y el mecanismo mediante el cual la Entidad gestionará y aprobará las ampliaciones de capacidad o demanda adicional		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, no existe un dimensionamiento máximo, todos los ítems de los servicios requeridos contemplan cantidades mínimas que es lo que exige la Entidad para su cumplimiento, no se solicitarán cantidades que excedan lo requerido.
244	11.9	**Especificaciones Implementación de todas las Capacidades y Servicios Entregados** 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).	Adicionalmente, se solicita confirmar si los incrementos que excedan dichos umbrales serán considerados como servicios adicionales sujetos a reconocimiento económico independiente o si deberán ser asumidos dentro del valor global del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, no existe un dimensionamiento máximo, todos los ítems de los servicios requeridos contemplan cantidades mínimas que es lo que exige la Entidad para su cumplimiento, no se solicitarán cantidades que excedan lo requerido.
245	11.17	**Especificaciones Implementación de todas las Capacidades y Servicios Entregados** 11.17 Todos los recursos tecnológicos, logísticos, de infraestructura, humanos y demás que se requieran para la implementación de los servicios incluidos en este documento, serán por cuenta del contratista, modalidad "llave en mano".	Considerando que el alcance se define bajo modalidad de "contrato llave en mano", lo cual implica la provisión por parte del contratista de todos los recursos tecnológicos, físicos y logísticos necesarios para la implementación, se solicita a la Entidad aclarar si existe un dimensionamiento máximo o límites definidos para la expansión de infraestructura, capacidad o servicios asociados durante la ejecución del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, no existe un dimensionamiento máximo, todos los ítems de los servicios requeridos contemplan cantidades mínimas que es lo que exige la Entidad para su cumplimiento, no se solicitarán cantidades que excedan lo requerido.

246	11.17	**Especificaciones Implementación de todas las Capacidades y Servicios Entregados** 11.17 Todos los recursos tecnológicos, logísticos, de infraestructura, humanos y demás que se requieran para la implementación de los servicios incluidos en este documento, serán por cuenta del contratista, modalidad "llave en mano".	En caso de no existir dichos límites, se solicita indicar cuál será el umbral de crecimiento permitido (en términos porcentuales o de consumo incremental sobre la línea base del diseño inicial) y el mecanismo mediante el cual la Entidad gestionará y aprobará las ampliaciones de capacidad o demanda adicional.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, no existe un dimensionamiento máximo, todos los ítems de los servicios requeridos contemplan cantidades mínimas que es lo que exige la Entidad para su cumplimiento, no se solicitarán cantidades que excedan lo requerido.
247	11.17	**Especificaciones Implementación de todas las Capacidades y Servicios Entregados** 11.17 Todos los recursos tecnológicos, logísticos, de infraestructura, humanos y demás que se requieran para la implementación de los servicios incluidos en este documento, serán por cuenta del contratista, modalidad "llave en mano".	Adicionalmente, se solicita confirmar si los incrementos que excedan dichos umbrales serán considerados como servicios adicionales sujetos a reconocimiento económico independiente o si deberán ser asumidos dentro del valor global del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, no existe un dimensionamiento máximo, todos los ítems de los servicios requeridos contemplan cantidades mínimas que es lo que exige la Entidad para su cumplimiento, no se solicitarán cantidades que excedan lo requerido.
248	11.20	**Especificaciones Implementación de todas las Capacidades y Servicios Entregados** 11.20 Implementar las diferentes fases del proyecto bajo los estándares del PMBOK o metodologías agiles o híbrido, con el objeto de garantizar la aplicación de conocimientos, habilidades, herramientas y técnicas estandarizadas en todas las actividades que se van a desarrollar durante el proyecto.	Se solicita a la Entidad aclarar el alcance de responsabilidad del contratista frente a la compatibilidad e interoperabilidad con las tecnologías actualmente instaladas en la Entidad, considerando que dichas plataformas corresponden a infraestructura de terceros bajo su administración.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se discrimina un inventario de infraestructura tecnológica detallado de la Entidad para que los interesados puedan dimensionar y revisar su matriz de compatibilidad frente a lo solicitado.
249	11.20	**Especificaciones Implementación de todas las Capacidades y Servicios Entregados** 11.20 Implementar las diferentes fases del proyecto bajo los estándares del PMBOK o metodologías agiles o híbrido, con el objeto de garantizar la aplicación de conocimientos, habilidades, herramientas y técnicas estandarizadas en todas las actividades que se van a desarrollar durante el proyecto.	En particular, se requiere precisar qué sucede en los casos en los que, por restricciones técnicas, versiones obsoletas, limitaciones de fabricante o configuraciones propias del entorno existente, no sea posible garantizar la interoperabilidad con la solución propuesta. En estos escenarios, se solicita confirmar si la Entidad asumirá las adecuaciones, actualizaciones o ajustes necesarios sobre su infraestructura base, o si estos serán considerados como requerimientos adicionales con impacto en costos, cronograma o alcance del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se discrimina un inventario de infraestructura tecnológica detallado de la Entidad para que los interesados puedan dimensionar y revisar su matriz de compatibilidad frente a lo solicitado.
250	11.20	**Especificaciones Implementación de todas las Capacidades y Servicios Entregados** 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.	técnica tipo datasheets o documentación pública del fabricante (incluyendo referencia a página y párrafo de cumplimiento), es decir, si dicho requisito es exigible en la etapa de presentación de oferta, durante la evaluación técnica, o como parte de la etapa de perfeccionamiento y/o ejecución del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la documentación técnica, datasheets o documentación pública del fabricante deberá ser aportada con la oferta, en los términos establecidos en los documentos del proceso, con el fin de permitir la verificación del cumplimiento de los requerimientos técnicos exigidos.
251	11.22	**Especificaciones Implementación de todas las Capacidades y Servicios Entregados** 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.	Adicionalmente, se solicita confirmar si durante la evaluación se aceptarán compromisos del fabricante o documentación preliminar, o si el cumplimiento debe estar soportado exclusivamente en documentación pública vigente y verificable al momento de la presentación de la propuesta.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el cumplimiento técnico deberá estar soportado en documentación pública vigente, datasheets, certificaciones o documentación verificable del fabricante, conforme a lo exigido en los documentos del proceso.
252	12.6	**Especificaciones Técnicas Servicios de Monitoreo** 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 precisar el mecanismo de aprobación para la incorporación de nuevos dispositivos: ¿existirá un flujo formal de solicitud, validación técnica, impacto en capacidad y autorización previa por parte de la Entidad?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la incorporación de nuevos dispositivos se realizará mediante solicitud de la Entidad y conforme a los procedimientos de gestión, validación técnica, autorización y control definidos durante la ejecución contractual, hasta ocupar el licenciamiento y capacidades contratadas.
253	12.6	**Especificaciones Técnicas Servicios de Monitoreo** 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).	Dado que el numeral sugiere crecimiento dinámico sobre múltiples plataformas (SIEM, SOAR, NDR, etc.), se solicita aclarar si el modelo de licenciamiento es realmente "ilimitado hasta el máximo contratado" o si existen restricciones diferenciadas por tecnología o tipo de dato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la inclusión de dispositivos adicionales deberá realizarse hasta el límite del licenciamiento, capacidades y cantidades contratadas para cada solución o servicio.
254		**Capacitación** 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.	Se solicita a la Entidad precisar el alcance total del componente de formación, indicando de manera explícita cuántas capacitaciones o sesiones se deben ejecutar durante la vigencia del contrato por cada una de las certificaciones requeridas. Lo anterior, considerando que actualmente el requerimiento solo establece un mínimo de veinte (20) funcionarios por capacitación y la entrega de "al menos 2 vouchers de certificación por capacitación" (NOTA 2), sin definir el número total de eventos formativos ni su distribución en el tiempo.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las capacitaciones deberán realizarse conforme a los temas, cantidades mínimas, funcionarios beneficiarios y vouchers establecidos en los documentos del proceso. La distribución y programación de las actividades será coordinada con la supervisión del contrato durante la ejecución.
255	15.3	**Transferencia de Conocimiento** 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 a la Entidad precisar el alcance del "entrenamiento gratuito en línea", indicando si corresponde a plataformas oficiales del fabricante, si incluye certificaciones oficiales o solo acceso a contenido		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el entrenamiento gratuito en línea deberá ser impartido por el fabricante de las soluciones y plataformas entregadas, y estará orientado a la administración, gestión, operación, optimización, actualización, configuración y demás actividades propias de las capacidades y servicios entregados. Este entrenamiento no sustituye las certificaciones exigidas en otros apartados, salvo que así esté expresamente previsto en los documentos del proceso.
256	18.1	**Certificaciones** 18.1 Se deben presentar las siguientes certificaciones expedidas y firmadas por el fabricante de la solución, plataformas, servicios y dispositivos entregados, entre otros:	Se solicita a la Entidad aclarar en qué fase del proceso deben presentarse estas certificaciones (oferta, evaluación o ejecución), y si se aceptan cartas de compromiso preliminares sujetas a adjudicación. Adicionalmente, se requiere confirmar si el requisito aplica de manera estricta a todos los componentes, incluyendo software, soluciones SaaS y servicios, considerando que estos no siempre manejan concepto de "fin de venta" ni ciclos de vida tradicionales de hardware.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las certificaciones exigidas deberán presentarse en la etapa definida en los documentos del proceso y deberán acreditar el cumplimiento de las condiciones solicitadas para las soluciones, plataformas, servicios o dispositivos ofertados. En soluciones SaaS, virtualizadas o servicios que no manejen ciclos tradicionales de hardware, el oferente deberá aportar certificación o soporte equivalente del fabricante que permita verificar soporte, vigencia y condiciones aplicables.
257	18.2	**Certificaciones** 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.	Se solicita aclarar si es el no contar con el nivel mas alto con los fabricantes es motivo descalificante ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el requerimiento es claro al referir los tres niveles más altos ante el fabricante de las soluciones y plataformas ofertadas, en ningún momento se exige el más alto nivel.
258	18.2	**Certificaciones** 18.2 Certificación expedida por el fabricante, donde se indique el compromiso del suministro de piezas y partes de repuestos por un periodo mínimo de cinco (5) años posteriores a la declaración de obsolescencia de los equipos ofrecidos la cual debe quedar consignada en la respectiva garantía entregada a la entidad.	Se solicita aclarar si este requerimiento aplica únicamente a componentes de hardware y cómo se gestionará en soluciones virtualizadas o SaaS donde no existen repuestos físicos. Adicionalmente, se requiere confirmar que la responsabilidad del suministro recae exclusivamente en el fabricante y no se traslada al contratista.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requerimiento de suministro de piezas, partes y repuestos aplica cuando por la naturaleza de la solución existan componentes físicos sujetos a obsolescencia o reemplazo. Para soluciones virtualizadas, SaaS o servicios sin componentes físicos, el oferente deberá aportar certificación o soporte equivalente sobre continuidad, soporte, garantía, vigencia y disponibilidad del servicio. En todo caso, el contratista será responsable frente a la Entidad por las garantías y soportes ofrecidos.

259	18.2	**Certificaciones** 18.2 Certificación expedida por el fabricante en donde avalen la garantía y soporte técnico de tres (3) años ofrecida por el proponente para la plataformas, soluciones y dispositivos ofertados.	Se solicita precisar si el soporte debe ser brindado directamente por el fabricante o si puede ser prestado por el contratista con respaldo del fabricante.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el soporte y garantía debe ser prestado por el proveedor del SOC como primer respondiente, los demás niveles los adelantará el proveedor ante el fabricante o fabricantes, siempre que se garantice la cobertura, niveles de servicio, vigencia, escalamiento, garantía y demás condiciones exigidas en los documentos del proceso.
260	19.2.1	**Gestión de Incidentes** 19.2.1 Gestionar y canalizar las alertas a los diferentes grupos de interés y partes interesadas.	Se solicita a la Entidad definir el listado formal de grupos de interés y partes interesadas, así como los canales oficiales de comunicación, niveles de criticidad y tiempos de notificación esperados, con el fin de evitar ambigüedad en la gestión de alertas y posibles reprocesos o incumplimientos de SLA.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los grupos de interés, partes interesadas, canales oficiales de comunicación, niveles de criticidad y tiempos de notificación serán definidos durante la fase de implementación y operación del servicio, conforme al modelo de gestión de incidentes, los procedimientos internos y las necesidades de la Entidad. El contratista deberá contemplar esta definición dentro de las actividades de parametrización y operación del servicio.
261	19.2.2	**Gestión de Incidentes** 19.2.2 Definir los casos de uso (eventos externos), sobre posibles ataques de ciberseguridad que se lleguen a presentar.	Se solicita aclarar si los casos de uso serán definidos, priorizados y aprobados por la Entidad o si esta responsabilidad recae completamente en el contratista, así como el número mínimo esperado y el mecanismo de gestión de cambios o nuevos casos durante la operación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los casos de uso asociados a eventos externos podrán ser propuestos por el contratista y deberán ser revisados, priorizados y aprobados por la Entidad, conforme a sus necesidades de monitoreo, riesgos, fuentes de información y capacidades tecnológicas. Durante la operación podrán definirse nuevos casos de uso, de acuerdo con las necesidades del servicio y los mecanismos de gestión que se establezcan.
262	19.2.3	**Gestión de Incidentes** 19.2.3 Definir los casos de uso (eventos internos), generados por los usuarios al interior de la DIAN.	Se solicita precisar si la Entidad proporcionará información de contexto (roles, perfiles de usuario, riesgos, políticas internas) necesaria para la definición de casos de uso, así como el nivel de responsabilidad del contratista en caso de falsos positivos o negativos derivados de dichos casos.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la Entidad suministrará, en la medida de su disponibilidad y bajo los controles de seguridad aplicables, la información de contexto necesaria para apoyar la definición de casos de uso internos. El contratista será responsable de diseñar, configurar, documentar, afinar y ajustar dichos casos de uso, así como de apoyar la reducción de falsos positivos y falsos negativos durante la operación del servicio.
263	19.3.2	**Lecciones aprendidas** 19.3.2 Se deberá entregar una base de conocimiento sobre las lecciones aprendidas en los diferentes proceso que se tenga en SOC, pensando en la transferencia de conocimiento al equipo interno de la DIAN y enmarcado en las mejores prácticas del mejoramiento continuo, estas lecciones aprendidas deberá ser revisadas al menos una vez al mes en el transcurso del contrato, Generando los respectivos reportes y artefactos para la el entendimiento de la DIAN.	Se solicita aclarar el alcance y nivel de detalle esperado de la base de conocimiento (procedimientos, playbooks, casos de uso, indicadores, etc.), así como el formato (herramienta, repositorio, wiki) y si debe integrarse con plataformas existentes de la Entidad		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la base de conocimiento deberá incluir, como mínimo, documentación técnica y operativa relacionada con incidentes, procedimientos, lecciones aprendidas, casos de uso, playbooks, indicadores, recomendaciones, acciones ejecutadas y oportunidades de mejora. El formato, repositorio o herramienta será definido durante la ejecución, conforme a los lineamientos de la Entidad.
264	19.3.2	**Lecciones aprendidas** 19.3.2 Se deberá entregar una base de conocimiento sobre las lecciones aprendidas en los diferentes proceso que se tenga en SOC, pensando en la transferencia de conocimiento al equipo interno de la DIAN y enmarcado en las mejores prácticas del mejoramiento continuo, estas lecciones aprendidas deberá ser revisadas al menos una vez al mes en el transcurso del contrato, Generando los respectivos reportes y artefactos para la el entendimiento de la DIAN.	Se solicita precisar el mecanismo de transferencia (sesiones formales, talleres, documentación, entrenamiento práctico), la frecuencia, duración y si existe un número mínimo de horas o sesiones obligatorias durante el contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la transferencia de conocimiento podrá realizarse mediante sesiones formales, talleres, documentación, ejercicios prácticos, socialización de lecciones aprendidas y demás mecanismos que permitan asegurar la apropiación del conocimiento por parte de la Entidad. La frecuencia y duración se coordinarán con la supervisión del contrato, sin perjuicio de las revisiones mínimas previstas en los documentos del proceso.
265	19.3.2	**Lecciones aprendidas** 19.3.2 Se deberá entregar una base de conocimiento sobre las lecciones aprendidas en los diferentes proceso que se tenga en SOC, pensando en la transferencia de conocimiento al equipo interno de la DIAN y enmarcado en las mejores prácticas del mejoramiento continuo, estas lecciones aprendidas deberá ser revisadas al menos una vez al mes en el transcurso del contrato, Generando los respectivos reportes y artefactos para la el entendimiento de la DIAN.	Se solicita confirmar si las revisiones mensuales implican sesiones formales con la Entidad, quiénes deben participar y si estas sesiones hacen parte del esfuerzo operativo contratado o requieren una dedicación adicional específica.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las revisiones mensuales de lecciones aprendidas hacen parte del esfuerzo operativo contratado y deberán coordinarse con la supervisión del contrato y los equipos que la Entidad determine. Estas sesiones deberán generar los reportes, evidencias y artefactos correspondientes.
266	19.3.2	**Lecciones aprendidas** 19.3.2 Se deberá entregar una base de conocimiento sobre las lecciones aprendidas en los diferentes proceso que se tenga en SOC, pensando en la transferencia de conocimiento al equipo interno de la DIAN y enmarcado en las mejores prácticas del mejoramiento continuo, estas lecciones aprendidas deberá ser revisadas al menos una vez al mes en el transcurso del contrato, Generando los respectivos reportes y artefactos para la el entendimiento de la DIAN.	Se solicita precisar qué se considera "artefactos" (dashboards, matrices, playbooks, informes ejecutivos, indicadores), así como el nivel de profundidad técnica esperado (ejecutivo vs operativo) y si existe un estándar de presentación definido por la Entidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los artefactos podrán incluir, entre otros, informes ejecutivos, informes técnicos, dashboards, matrices, playbooks, procedimientos, indicadores, registros de seguimiento, recomendaciones y documentos de lecciones aprendidas. El nivel de profundidad deberá ajustarse al público objetivo, incluyendo vistas ejecutivas y operativas cuando corresponda.
267	19.4.2	**Relacionamiento con terceros nacionales e internacionales (CSIRT – FIRST)** 19.4.2 Realizar con los entes de control en Colombia tales como el CSIRT, COLCERT, Centro Cibernético Policial, Fiscalía, entre otros, el escalamiento, retroalimentación e implementación de las recomendaciones dadas por un tercero. Si no es posible realizar la implementación deberá realizar el escalamiento a las áreas responsables, de igual forma será el responsable de tomar y aportar las evidencias necesarias.	Se solicita a la Entidad aclarar si el contratista actuará como vocero oficial autorizado para el reporte de incidentes ante terceros o si deberá existir validación previa y expresa por parte de la Entidad antes de cualquier comunicación externa, considerando las implicaciones legales, reputacionales y regulatorias.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el contratista no actuará como vocero oficial autónomo de la Entidad frente a terceros. Cualquier comunicación, reporte o escalamiento ante CSIRT, COLCERT, Centro Cibernético Policial, Fiscalía u otros terceros deberá realizarse conforme a los lineamientos, autorizaciones y canales definidos por la DIAN, sin perjuicio del apoyo técnico, recolección de información y preparación de evidencias que deba realizar el contratista dentro del alcance del servicio.
268	19.4.2	**Relacionamiento con terceros nacionales e internacionales (CSIRT – FIRST)** 19.4.2 Realizar con los entes de control en Colombia tales como el CSIRT, COLCERT, Centro Cibernético Policial, Fiscalía, entre otros, el escalamiento, retroalimentación e implementación de las recomendaciones dadas por un tercero. Si no es posible realizar la implementación deberá realizar el escalamiento a las áreas responsables, de igual forma será el responsable de tomar y aportar las evidencias necesarias.	Se solicita definir cuáles son las áreas responsables dentro de la Entidad, los tiempos de respuesta esperados y el mecanismo formal de transferencia de responsabilidad una vez el contratista haya realizado el escalamiento.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las áreas responsables, tiempos de respuesta y mecanismos de escalamiento serán definidos durante la implementación del modelo operativo del SOC, conforme a la estructura interna, criticidad del incidente y procedimientos de atención definidos por la Entidad. El contratista deberá documentar y operar dichos flujos una vez sean aprobados.
269	19.4.2	**Relacionamiento con terceros nacionales e internacionales (CSIRT – FIRST)** 19.4.2 Realizar con los entes de control en Colombia tales como el CSIRT, COLCERT, Centro Cibernético Policial, Fiscalía, entre otros, el escalamiento, retroalimentación e implementación de las recomendaciones dadas por un tercero. Si no es posible realizar la implementación deberá realizar el escalamiento a las áreas responsables, de igual forma será el responsable de tomar y aportar las evidencias necesarias.	Se solicita aclarar el alcance de la responsabilidad sobre la cadena de custodia de la evidencia digital, responsable legal de su recolección, preservación y entrega confirmando que esta responsabilidad recae sobre la Entidad o autoridades competentes.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la gestión de evidencias digitales deberá realizarse conforme a las políticas, procedimientos, protocolos definidos por la Entidad y la normatividad aplicable. El contratista deberá apoyar la identificación, registro, preservación y entrega de evidencias en el marco del servicio SOC, bajo las instrucciones de la Entidad, sin que ello implique asumir competencias propias de autoridades judiciales o de control.
270	19.4.2	**Relacionamiento con terceros nacionales e internacionales (CSIRT – FIRST)** 19.4.2 Realizar con los entes de control en Colombia tales como el CSIRT, COLCERT, Centro Cibernético Policial, Fiscalía, entre otros, el escalamiento, retroalimentación e implementación de las recomendaciones dadas por un tercero. Si no es posible realizar la implementación deberá realizar el escalamiento a las áreas responsables, de igual forma será el responsable de tomar y aportar las evidencias necesarias.	Se solicita precisar el alcance del relacionamiento internacional (ej. FIRST u otros organismos), indicando si la Entidad ya cuenta con membresías activas o si se espera que el contratista las provea, incluyendo costos y responsabilidades asociadas.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el relacionamiento con terceros nacionales e internacionales deberá realizarse conforme a los lineamientos definidos por la Entidad y al alcance contractual. En relación con FIRST, se precisa que deberá atenderse lo dispuesto en los documentos del proceso y en los ajustes realizados mediante adenda, según corresponda.
271	19.4.3	**Relacionamiento con terceros nacionales e internacionales (CSIRT – FIRST)** 19.4.2 Realizar con los entes de control en Colombia tales como el CSIRT, COLCERT, Centro Cibernético Policial, Fiscalía, entre otros, el escalamiento, retroalimentación e implementación de las recomendaciones dadas por un tercero. Si no es posible realizar la implementación deberá realizar el escalamiento a las áreas responsables, de igual forma será el responsable de tomar y aportar las evidencias necesarias.	Se solicita confirmar si el contratista será el único autorizado para reportar incidentes o si esta función requiere validación previa de la Entidad, así como definir el nivel de autonomía y responsabilidad frente a errores u omisiones en el reporte.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el contratista no será el único autorizado para reportar incidentes. Los reportes y comunicaciones con terceros deberán realizarse bajo validación, autorización y lineamientos de la Entidad. El contratista deberá apoyar técnicamente la preparación, documentación, análisis y seguimiento de dichos reportes, conforme al alcance del servicio.
272	19.4.3	**Relacionamiento con terceros nacionales e internacionales (CSIRT – FIRST)** Realizar monitoreo, reporte y/o relacionamiento con terceros nacionales e internacionales. 19.4.3	Se solicita a la Entidad precisar el alcance exacto del "relacionamiento con terceros nacionales e internacionales", indicando qué tipos de organizaciones unicamente están incluidas (CSIRT, ISAC, FIRST, o esto incluye fabricantes, autoridades, entre otros, cuales), si la Entidad cuenta actualmente con membresías o convenios vigentes o si se espera que el contratista los provea. Adicionalmente, se requiere confirmar si este relacionamiento implica representación formal de la Entidad ante terceros y bajo qué lineamientos de autorización, así como los límites de responsabilidad del contratista frente a la información compartida y las acciones derivadas de dicha interacción.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el relacionamiento con terceros nacionales e internacionales podrá incluir, según el caso, CSIRT, COLCERT, Centro Cibernético Policial, Fiscalía, FIRST, fabricantes, comunidades técnicas u otros actores relevantes para la gestión de incidentes y amenazas. Dicho relacionamiento no implica representación formal autónoma del contratista y deberá realizarse bajo lineamientos, autorización y control de la Entidad.
273	20.1	**Devolución del servicio (licenciamiento posterior a la terminación del contrato)** 20.1 Realizar y entregar el plan de trabajo detallado para la devolución del servicio, por lo menos cuatro meses antes de la finalización del servicio.	Se solicita a la Entidad precisar si el proceso de devolución formal del servicio inicia posterior a la fecha de terminación del contrato y, en caso afirmativo, establecer el plazo máximo obligatorio para su ejecución (en días o meses), independiente de la disponibilidad, aceptación o capacidad de recepción de la Entidad o del nuevo proveedor. Adicionalmente, se solicita confirmar si, una vez cumplido dicho plazo de reversión, el contratista queda formalmente exonerado de cualquier responsabilidad técnica, operativa o de continuidad sobre la plataforma, independientemente de si la Entidad o el tercero designado ha recibido, validado o puesto en operación la información, configuraciones y recursos entregados.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la devolución del servicio deberá planearse e iniciarse por lo menos cuatro (4) meses antes de la finalización del servicio, conforme a lo establecido en los documentos del proceso. Esta actividad hace parte del alcance contractual y deberá ejecutarse hasta la entrega, validación y cierre conforme a los procedimientos definidos por la Entidad, sin que la sola entrega formal de información implique exoneración automática de responsabilidades.

274	20.3	**Devolución del servicio (licenciamiento posterior a la terminación del contrato)** 20.3 Entregar la estrategia a seguir para la devolución del servicio, este proceso se debe iniciar con un tiempo mínimo de cuatro meses antes de la fecha de finalización y deberá incluir como mínimo: las copias de las configuraciones actuales, diseños físicos y lógicos de la prestación de los servicios, procedimientos, instructivos, manuales y de más documentos de estrategia, copia en formato standard de la configuración de los logs de las herramientas utilizadas durante el servicio prestado, evidencias o registros de las licencias a nombre de la DIAN y demás información administrativa asociada al servicio prestado.	Se solicita a la Entidad precisar si el proceso de devolución del servicio corresponde a una fase obligatoria dentro del alcance contractual o si se trata de una actividad independiente posterior a la finalización del contrato. Adicionalmente, se requiere confirmar si el periodo mínimo de cuatro (4) meses previo a la finalización hace parte del contrato y su valor económico, o si corresponde a una extensión operativa adicional. Asimismo, se solicita establecer de manera expresa el momento en el cual se considera cumplida y aceptada la obligación de reversión, definiendo si dicha aceptación depende de la Entidad o de terceros designados, o si por el contrario el contratista se libera de toda responsabilidad una vez entregada la información dentro del plazo establecido, independientemente de su validación o puesta en operación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la devolución del servicio corresponde a una fase obligatoria dentro del alcance contractual y deberá iniciarse mínimo cuatro (4) meses antes de la finalización del servicio. Este periodo hace parte de las obligaciones del contratista y deberá contemplar la entrega de configuraciones, diseños, procedimientos, documentación, evidencias, licencias y demás información requerida, sujeta a validación por parte de la Entidad.
275	20.4	**Devolución del servicio (licenciamiento posterior a la terminación del contrato)** 20.4 Realizar los procesos administrativos de cierre de contrato que haya lugar.	Se solicita a la Entidad precisar el alcance exacto de los "procesos administrativos de cierre de contrato", indicando cuáles actividades específicas están incluidas (actas de cierre, informes finales, paz y salvos, liquidación, transferencias técnicas, entre otros) y cuáles corresponden exclusivamente a la Entidad. Adicionalmente, se requiere confirmar los plazos máximos para la ejecución de dichas actividades posteriores a la finalización del servicio, y si durante este periodo el contratista mantiene responsabilidades operativas o únicamente obligaciones documentales y administrativas sin continuidad técnica del servicio.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los procesos administrativos de cierre comprenden las actividades documentales, técnicas, administrativas y de soporte necesarias para finalizar ordenadamente el contrato, incluyendo informes finales, actas, soportes, paz y salvos cuando apliquen, transferencia de información, devolución del servicio y demás entregables definidos por la Entidad. El alcance operativo durante este periodo será el previsto en los documentos del proceso y en el plan de devolución aprobado.
276		**Canales de Comunicación** A nivel nacional no hay canales de internet, son enlaces mpls y tienen diferentes anchos de banda están asignados según la cantidad de funcionarios de la sede. Así mismo hay medios diferentes pueden ser por fibra o satélite En total son 137 enlaces a nivel nacional	Entedemos que los canales aquí mencionados ya se encuentran instalados en la entidad y no hacen parte de los servicios a ofertar.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los enlaces nacionales mencionados corresponden a infraestructura de comunicaciones existente de la Entidad. No obstante, el contratista deberá proveer los canales, componentes, integraciones o capacidades adicionales que requiera para la prestación del servicio SOC, conforme al alcance llave en mano definido en los documentos del proceso.
277	6.2	Item 6 Especificaciones Técnicas Caza de Amenazas 6.2 Referencia o Modelo (Especificar el modelo ofrecido)	Solicitamos a la entidad indicar si la solucion puede ser ofertada ya sea como appliance dedicado, una plataforma software, un servicio gestionado o una arquitectura hibrida (plataforma + operación), siempre que cumpla capacidades funcionales equivalentes.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la solución podrá ser ofertada como appliance dedicado, plataforma software, servicio gestionado o arquitectura hibrida, siempre que cumpla integralmente con las capacidades funcionales, técnicas, operativas, de seguridad, soporte y garantía exigidas en los documentos del proceso.
278	6.3.1	Item 6 Especificaciones Técnicas Caza de Amenazas 6.3 Alcance 6.3.1 Para el monitoreo y alertamiento temprano sobre nuevas vulnerabilidades, ataques. amenazas externas y del ciberespacio que puedan afectar a la infraestructura interna de la entidad el CONTRATISTA debe adelantar el despliegue, configuración y afinamiento de herramientas para cacería de amenazas, las cuales permitan tener una visual horizontal y vertical en el caso de incidentes de seguridad de la información. Debe tener por lo menos las siguientes componentes: Herramientas de caza de amenazas: herramienta para buscar e interceptar ataques ocultos de una manera proactiva. Se puede desplegar una sola herramienta siempre y cuando tanto la inteligencia como la caza sean completamente identificables y a nivel de mercado sea aceptada como tal. Hay que tener en cuenta que el despliegue de herramientas que no tengan las capacidades de cacería de amenazas completas, no serán evaluadas. Parametrizar y/o configurar la herramienta adquirida, a partir de las mejores prácticas definidas por el fabricante y las exigencias de la entidad.	Solicitamos a la entidad indicar qué capacidades de las mencionadas son obligatorias desde el inicio y cuáles pueden ser progresivas, debido a que esto impacta en el dimensionamiento de analistas dedicados, horas de operación proactiva e infraestructura de decepción		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las capacidades mínimas requeridas para caza de amenazas deberán estar disponibles desde la implementación y puesta en operación del servicio. El contratista podrá proponer una estrategia progresiva de afinamiento, maduración y optimización, siempre que no limite el cumplimiento de las funcionalidades mínimas exigidas ni afecte la operación del SOC.
279	6.4	Item 6 Especificaciones Técnicas Caza de Amenazas 6.4Aspectos Generales 6.4.1Debe permitir la creación de trampas de alta interacción, con capacidad de clonar activos existentes	Solicitamos a la entidad definir qué se considera una trampa de alta interacción, indicando si se espera la clonación de servicios, sistemas completos o credenciales, y bajo qué controles de seguridad		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que una trampa de alta interacción corresponde a un señuelo con capacidad de simular, emular o reproducir comportamientos, servicios o características de activos reales, de forma suficiente para permitir la interacción controlada de un atacante y generar alertamiento, análisis y trazabilidad de la actividad maliciosa. Su configuración deberá realizarse bajo controles de seguridad y conforme a la arquitectura aprobada por la Entidad.
280	6.4	Item 6 Especificaciones Técnicas Caza de Amenazas 6.4Aspectos Generales 6.4.2El 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 caracteristicas similares o superiores en las tecnologias ofrecidas.	Solicitamos a la entidad confirmar si los valores de 400 señuelos, 20 máquinas virtuales y 120 VLANs corresponden a un mínimo obligatorio, un máximo esperado, o una capacidad referencial, y si estos valores se encuentran alineados con la arquitectura actual de la DIAN		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los valores de cuatrocientos (400) señuelos, veinte (20) máquinas virtuales y ciento veinte (120) VLAN corresponden a capacidades mínimas requeridas o equivalentes/superiores conforme a la tecnología ofertada. El diseño y despliegue deberán alinearse con la arquitectura aprobada por la Entidad durante la fase de implementación.
281	7.2	Item 7 Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas 7.2Referencia o Modelo (Especificar el modelo de la herramienta del servicio ofrecido)	Solicitamos a la entidad indicar si el modelo debe ser dedicado por segmento o centralizado, si se aceptan appliances físicos, virtuales o mixtos y si existen restricciones de país de origen o certificaciones adicionales		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la solución NDR podrá implementarse mediante modelo centralizado, distribuido, físico, virtual o mixto, siempre que cumpla con las capacidades requeridas, cobertura, retención, análisis, integración, soporte y niveles de servicio definidos en los documentos del proceso. Cualquier restricción técnica deberá atender la normativa aplicable y los lineamientos de seguridad de la Entidad.
282	7.3	Item 7 Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenaza 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).	solicitamos a la entidad aclarar la cantidad de activos para la cual se requiere el licenciamiento pues en el item 7.18 se indican 17.727 y en este item 25.000		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la cantidad definitiva para el licenciamiento de la capacidad NDR corresponde a veinticinco mil (25.000) dispositivos, conforme a los ajustes realizados mediante adenda.
283	7.4	7 Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas 7.4Se debe suministrar una solución para Monitoreo de Red con Inteligencia Artificial con el objetivo de revisar el tráfico de red y alertar ciberamenazas que existan en la red de la entidad, favor tener en cuenta los procedimientos al respecto incluidos en el Manual de políticas de seguridad de la información de la Entidad, con código MN-IIT-0072	Solicitamos a la entidad indicarnos si dentro del Manual de políticas de seguridad de la información de la Entidad, existe algun control especifico que la solucion de NDR debe cubrir con el fin de contemplarlo dentro del licenciamiento		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la referencia al Manual de Políticas y Lineamientos de Seguridad de la Información debe entenderse como marco de cumplimiento de los lineamientos institucionales de seguridad y privacidad aplicables. La solución NDR deberá contribuir al monitoreo, detección, análisis, alertamiento y respuesta frente a amenazas de red, conforme a los requerimientos técnicos definidos en el anexo.
284	7.8	7 Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas 7.8 La solución debe realizar un análisis completo del tráfico.	Solicitamos a la entidad se indique mayor claridad del analisis completo de trafico requerido, para definir si este hace referencia o puede interpretarse como Full Packet Capture, Metadata (L3–L7), Flow-based (NetFlow/IPFIX), entre otros		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el análisis completo de tráfico deberá permitir visibilidad suficiente para identificar, correlacionar y alertar comportamientos anómalos, amenazas y eventos relevantes en la red de la Entidad. El oferente podrá implementar enfoques basados en metadatos, flujos, paquetes u otros mecanismos equivalentes o superiores, siempre que cumpla con las capacidades requeridas en los documentos del proceso.
285	7.8	7 Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas 7.10La 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	solicitamos a la entidad indicarnos o definirnos los criterior tecnicos equivalentes aceptables como Behavioral analytics, Modelos estadísticos dinámicos y ML híbrido (heurística + ML) y con este definir un alcance mas especifico		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que se aceptarán modelos de analítica de comportamiento, modelos estadísticos, machine learning, heurística, correlación multidimensional u otros mecanismos equivalentes o superiores, siempre que permitan identificar comportamientos anómalos y amenazas en la red conforme a las capacidades solicitadas en los documentos del proceso.
286	7.10	7 Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas 7.14Capacidad 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 a la entidad indicarnos si la retencion mencionada es estrictamente local o puede ser offload a SIEM, o alguna otra opción		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la retención mínima de seis (6) meses deberá garantizar la consulta y disponibilidad de los datos capturados conforme a lo solicitado en los documentos del proceso. Así mismo, el ítem es claro al señalar la capacidad de realizar consultas a los datos capturados y almacenados en el hardware de uso específico, sin conectarse a la nube.
287	7.14	7 Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas 7.28La 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	solicitamos a la entidad de acuerdo al nivel solicitado de IA, definir periocidad, entregables, hunting automático continuo, hunting manual periódico, número mínimo de informes mensuales, entre otros.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las actividades de hunting, analítica, generación de informes y seguimiento deberán ejecutarse conforme al modelo operativo SOC, los ANS/SLA, entregables e informes definidos en los documentos del proceso. La periodicidad específica y priorización de actividades será coordinada con la supervisión del contrato durante la operación.
288	7.28	8Especificaciones Técnicas Solución de análisis de código estático y dinámico para aplicaciones 8.3La 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 definir la frecuencia mínima esperada de análisis por aplicación y los criterios de priorización de las 50 aplicaciones		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la frecuencia de análisis para las aplicaciones será definida conforme a la criticidad, priorización, ciclo de desarrollo, exposición y necesidades de la Entidad. El contratista deberá contemplar dentro del servicio la ejecución de los análisis requeridos para las cincuenta (50) aplicaciones conforme al alcance definido en los documentos del proceso.
289	8.6	8 Especificaciones Técnicas Solución de análisis de código estático y dinámico para aplicaciones 8.6 Debe dar soporte a las fábricas de desarrollo y pruebas en el proceso de Desarrollo Seguro	Entendemos que el soporte requerido es el soporte de fabricante y no un soprote especializado o bolsa de servicios para brindar este tipo de soporte		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el soporte a las fábricas de desarrollo y pruebas comprende el acompañamiento técnico requerido para el uso de la herramienta, interpretación de hallazgos, buenas prácticas de desarrollo seguro y gestión de vulnerabilidades identificadas. Lo anterior deberá prestarse conforme al alcance definido en los documentos del proceso y no se limita únicamente al soporte estándar del fabricante.

290	8.7	8 Especificaciones Técnicas Solución de análisis de código estático y dinámico para aplicaciones 8.7 El CONTRATISTA debe estar en la capacidad de dar transferencia de conocimiento para la correcta ejecución de pruebas y del uso de la herramienta	Entendemos que esta transferencia de conocimiento es aparte al item de capacitaciones por lo que esta transferencia de conocimiento puede brindarse de forma remota.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la transferencia de conocimiento asociada al uso de la herramienta podrá realizarse de forma presencial, virtual o híbrida, siempre que permita cumplir el objetivo de apropiación, uso correcto y operación de la solución. Esta actividad es independiente de las capacitaciones y certificaciones exigidas en otros apartados, salvo que los documentos del proceso dispongan lo contrario.
291	8	8 Especificaciones Técnicas Solución de análisis de código estático y dinámico para aplicaciones 8.8 Se deben crear los soportes requeridos en las auditorias	Solicitamos a la entidad nos indique a que tipo de auditorias hace referencia, si internas o externas		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los soportes requeridos en auditorías podrán corresponder a auditorías internas, externas, de entes de control, contractuales, técnicas, de seguridad o de cumplimiento, siempre que estén relacionadas con el alcance del servicio y las capacidades implementadas.
292	8.17	8 Especificaciones Técnicas Solución de análisis de código estático y dinámico para aplicaciones 8.17Apoyar con los recursos necesarios (personal idóneo) constantemente a la Dian realizando el respectivo acompañamiento, apoyo, experticia, experiencia, conocimiento en la resolución y remediación de todas y cada una de las vulnerabilidades encontradas durante la ejecución del contrato, se aclara que el personal de la Dian estará al frente de dichas actividades	Entendemos que estos recursos mencionados son los mismos que se emplean dentro de equipo de trabajo y el cual realizará la administración de la solución		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el acompañamiento en resolución y remediación de vulnerabilidades deberá ser realizado por el contratista con personal idóneo, conforme al alcance del servicio. El personal podrá corresponder al equipo asignado al contrato, siempre que se garantice la disponibilidad, especialidad, oportunidad y suficiencia requeridas para atender las actividades solicitadas.
293	9.11	9 Especificaciones Técnicas Protección de Marca (Deep&Dark Web) 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	Solicitamos a la entidad nos indique si tienen definiciones de las métricas y fuentes esperadas para el análisis de percepción de marca.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las métricas y fuentes para el análisis de percepción de marca deberán ser propuestas por el contratista conforme a las mejores prácticas del servicio, fuentes abiertas, monitoreo de superficie digital, redes, web, deep web, dark web y demás fuentes pertinentes. Estas deberán ser revisadas y validadas por la Entidad durante la implementación y operación.
294	10.1	10Especificaciones Técnicas Ethical Hacking 10.1Se 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	Solicitamos a la Entidad precisar la distribución temporal esperada de dichos ejercicios (por ejemplo, semestral), la duración estimada de cada uno y si los ejercicios deben considerarse independientes o acumulativos en alcance y resultados?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los ejercicios de ethical hacking deberán realizarse como mínimo dos (2) veces por año durante la vigencia del servicio, conforme a la planeación acordada con la Entidad. La distribución temporal, duración, alcance específico y priorización de activos serán definidos en el cronograma correspondiente, garantizando las etapas de preparación, ejecución, análisis e informe.
295	10.1	10 Especificaciones Técnicas Ethical Hacking 10.2El 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).	Respecto al cronograma y las etapas indicadas en el numeral 10.1 (preparación, ejecución de pruebas, análisis y elaboración de informes), ¿podría la Entidad definir los entregables mínimos y criterios de aceptación esperados para cada una de estas etapas?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los entregables mínimos de cada ejercicio de ethical hacking deberán incluir, según aplique, plan de trabajo, alcance aprobado, metodología, evidencias de ejecución, hallazgos, clasificación de criticidad, análisis de impacto, recomendaciones, informe técnico, informe ejecutivo y plan de remediación o seguimiento. Los criterios de aceptación serán definidos con la supervisión del contrato conforme al alcance aprobado para cada ejercicio.
296		11Especificaciones Implementación de todas las Capacidades y Servicios Entregados 11.5Pruebas de Servicio de las plataformas ofertadas.	Solicitamos a la entidad indicar la frecuencia de las pruebas planteadas o si por el contrario el contratista puede estimarlas y proponer 1 visita anual.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las pruebas de servicio deberán realizarse durante la implementación, puesta en operación, ajustes relevantes, actualizaciones o cuando la Entidad lo requiera para verificar la adecuada operación de las plataformas. La frecuencia y alcance serán definidos en el plan de pruebas aprobado, sin que resulte procedente limitarlo a una visita anual, aclarando que se deben 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
297	11.20	ITEM 11Especificaciones Implementación de todas las Capacidades y Servicios Entregados 11.20Implementar las diferentes fases del proyecto bajo los estándares del PMBOK o metodologías agiles o híbrido, con el objeto de garantizar la aplicación de conocimientos, habilidades, herramientas y técnicas estandarizadas en todas las actividades que se van a desarrollar durante el proyecto.	Solicitamos a la Entidad indicar si existe una metodología de gestión de proyectos preferente (PMBOK, ágil o híbrida) y los entregables mínimos esperados para la supervisión del proyecto		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el contratista podrá implementar el proyecto bajo estándares PMBOK, metodologías ágiles o un enfoque híbrido, conforme a lo establecido en los documentos del proceso. Los entregables mínimos deberán incluir, entre otros, plan de proyecto, cronograma, matriz de riesgos, plan de comunicaciones, actas, informes de avance, seguimiento de hitos, gestión de cambios y cierre de fase.
298	12.1	ITEM 12Especificaciones Técnicas Servicios de Monitoreo 12.1"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."	Solicitamos a la Entidad precisar la frontera técnica y operativa entre las plataformas y herramientas que son propiedad de la DIAN y aquellas que son propiedad del contratista, así como indicar la titularidad de las configuraciones, reglas, casos de uso y datos generados durante la prestación del servicio?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la frontera técnica y operativa entre plataformas de la Entidad y plataformas provistas por el contratista será definida en el diseño de la arquitectura y el modelo operativo del servicio. Las configuraciones, reglas, casos de uso, datos, documentación y parametrizaciones desarrolladas específicamente para la DIAN deberán quedar disponibles para la Entidad, conforme a lo establecido en los documentos del proceso y a las condiciones de propiedad y uso aplicables.
299	12.3	ITEM 12Especificaciones Técnicas Servicios de Monitoreo 12.3La administración, operación, gestión de los servicios y demás actividades de las plataformas, soluciones, software, hardware, entre otros, que hacen parte de las capacidades requeridas por la Entidad en este proyecto, deben ser realizadas por el futuro oferente, por el tiempo de duración del proyecto.	En relación con el numeral 12.3, entendemos que la administración, operación y gestión de las plataformas incluye únicamente la operación funcional del SOC, sin embargo solicitamos se aclare cómo se articula esta responsabilidad con el área de TI de la DIAN.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la administración, operación y gestión de las plataformas y servicios del SOC deberá articularse con las áreas técnicas de la Entidad mediante los procedimientos, canales, roles y responsabilidades definidos en el modelo operativo aprobado. El contratista será responsable de la operación funcional del SOC y del escalamiento oportuno a las áreas responsables cuando se requieran intervenciones sobre infraestructura institucional.
300	12.60	ITEM 12Especificaciones Técnicas Servicios de Monitoreo 12.6Dispositivos 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).	En relación con el numeral 12.6, que permite la inclusión de dispositivos adicionales hasta copar el licenciamiento, Solicitamos a la Entidad aclarar el procedimiento, tiempos de integración y el impacto esperado en los SLA cuando se incorporen nuevos dispositivos durante la operación		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la incorporación de dispositivos adicionales deberá realizarse mediante un procedimiento de solicitud, validación, priorización, planeación e integración acordado con la Entidad, hasta ocupar el licenciamiento y capacidades contratadas. Los tiempos e impactos operativos deberán ser evaluados caso a caso y gestionados sin afectar injustificadamente los ANS/SLA definidos para el servicio.
301	12.8	ITEM 12Especificaciones Técnicas Servicios de Monitoreo 12.8Se 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.	Solicitamos a la Entidad detallar el alcance técnico de la integración con la herramienta GRC NOVASEC, especificando si la integración debe ser unidireccional o bidireccional, qué tipos de eventos, riesgos o controles deben intercambiarse y si se espera automatización.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la integración con la herramienta GRC NOVASEC deberá permitir el intercambio de información relevante sobre riesgos, controles tecnológicos, eventos o cambios asociados a las herramientas que soportan dichos controles. El detalle técnico, direccionalidad, campos, eventos y nivel de automatización será definido durante la fase de diseño e implementación, conforme a las capacidades de las plataformas y los lineamientos de la Entidad.
302	12.14	ITEM 12Especificaciones Técnicas Servicios de Monitoreo 12.14El servicio debe incluir apoyo en la definición de estrategias de seguridad, que permitan fortalecer las políticas y controles de seguridad de la información.	Solicitamos a la Entidad delimitar el alcance del apoyo en la definición de estrategias de seguridad, aclarando si corresponde a asesorías puntuales, recomendaciones tácticas, o participación en diseño estratégico		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el apoyo en la definición de estrategias de seguridad comprende asesoría técnica, recomendaciones, análisis, insumos para el fortalecimiento de políticas y controles, y acompañamiento en la mejora continua de la postura de seguridad de la información, conforme al alcance del servicio SOC y bajo la orientación de la Entidad.
303	13.7	ITEM 13 Garantía y Soporte Técnico por tres (3) años. 13.7Realizar 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.	Solicitamos a la entidad indicar la frecuencia de las visitas de seguimiento planteadas o si por el contrario el contratista puede estimarlas y proponer 1 visita anual		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las visitas de seguimiento técnico para mantenimiento preventivo deberán realizarse con periodicidad cuatrimestral, conforme a lo establecido en los documentos del proceso. Por lo anterior, no se acepta la solicitud de limitar esta actividad a una visita anual.
304	14.2	14Capacitación 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."	Se indica que las capacitaciones se dicten en centros de capacitación certificados, pero no se precisa: Quién certifica (fabricante, entidad internacional, academia). Si el centro debe estar en Colombia. Si se aceptan modalidades virtuales oficiales. Solicitamos a la entidad aclarar y definir estos criterios o indicar que sean de acuerdo a lo que el contratista incluya en su oferta.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el componente de capacitación fue ajustado mediante adenda, por lo cual las capacitaciones deberán desarrollarse conforme a los temas, cantidades, modalidad, condiciones y soportes allí establecidos. En todo caso, deberán ser oficiales y certificables, impartidas por fabricantes, centros, entidades certificadoras o instituciones autorizadas según la naturaleza de cada capacitación.

305	15.3	ITEM 15 Transferencia de Conocimiento 15.3Se 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	Solicitamos a la Entidad confirmar las modalidades permitidas para la transferencia de conocimiento (presencial, virtual o híbrida), así como si existen temáticas que deban impartirse de manera presencial obligatoria, indicando la ubicación y condiciones aplicables		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la transferencia de conocimiento podrá desarrollarse en modalidad presencial, virtual o híbrida, de acuerdo con la naturaleza de la actividad, la tecnología implementada y la programación aprobada por la supervisión del contrato. Las temáticas, alcance y condiciones deberán asegurar la apropiación sobre administración, gestión, operación, optimización, actualización y configuración de las capacidades entregadas.
306		18Certificaciones 18.1Se deben presentar las siguientes certificaciones expedidas y firmadas por el fabricante de la solución, plataformas, servicios y dispositivos entregados, entre otros:	Solicitamos a la entidad indicar si la certificación debe presentarse por cada solución/capacidad individual (SIEM, SOAR, NDR, DB Firewall, etc.) o si es aceptable una certificación general del fabricante que cubra varias soluciones.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las certificaciones deberán acreditar el respaldo del fabricante respecto de las soluciones, plataformas, servicios o dispositivos ofertados. Podrán presentarse certificaciones individuales o certificaciones generales que cubran varias soluciones, siempre que permitan identificar claramente las capacidades incluidas, su vigencia, alcance, soporte y correspondencia con los requerimientos del proceso.
307	19.1.1	ITEM 19 Gestión de Incidentes 19.1Análisis y detección 19.1.1Realizar la evaluación de los eventos y detectar aquellos que sean potencialmente un incidente evaluando su impacto después de la detección en el menor tiempo posible	En relación con el numeral 19.1.1, donde se indica la evaluación de eventos para detectar incidentes potenciales, ¿podría la Entidad aclarar cuál es el marco de referencia oficial para la evaluación del impacto del incidente (por ejemplo, matriz de riesgos institucional, criterios CIA – confidencialidad, integridad, disponibilidad –, criticidad del activo o clasificación de la información), y si dicho marco será suministrado como insumo oficial a los proponentes?		La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que se debe dar cumplimiento a lo establecido en el respectivo ítem. La Entidad no ha definido un marco de referencia único para la evaluación de este aspecto; no obstante, el proceso de análisis contempla inicialmente la criticidad del activo involucrado y el impacto potencial que el evento pueda generar.
308	19.1.2	ITEM 19 Gestión de Incidentes 19.1.2Gestionar los tiempos de notificación del incidente después de la evaluación del impacto, según propuesta realizada por el PROPONENTE y deberá alinearse con lo definido en el SGSPI en relación con los tiempos de atención del incidente	Se menciona la alineación con el SGSI, pero el pliego no incorpora ni referencia explícitamente los tiempos oficiales del SGSI aplicables a incidentes, solicitamos a la Entidad indicar: Los tiempos exactos de notificación esperados por severidad y si estos tiempos corresponden a: Notificación, Atención, Contención y Resolución		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los tiempos de atención que tiene el SGSI para incidentes son los siguientes: Nivel de prioridad / Tiempo de atención Crítico / 1 hora Alto / 2 horas Medio / 4 horas Bajo / 8 horas Informe / 16 horas
309	19.1.3	ITEM 19 Gestión de Incidentes 19.1Análisis y detección 19.1.3Generar propuesta de solución del incidente después de la evaluación del impacto.	De acuerdo con la generación de una propuesta de solución del incidente, entendemos que dicha propuesta implica únicamente recomendaciones técnicas y no la ejecucion de acciones directas en equipos y servicios fuera del alcance del contratista en este proyecto, por favor indicarnos si nuestro entendimiento es correcto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se debe cumplir con lo requerido en el respectivo ítem, el futuro proveedor del SOC no realizará intervenciones directas o acciones en los equipos e infraestructura tecnológica de la Entidad para solucionar incidentes.
310	19.1.4	ITEM 19 Gestión de Incidentes 19.1.4En caso de ser necesario, realizar el escalamiento del o los incidentes de seguridad de la información a un nivel de servicio de soporte especializado, nivel 3 o 4 que pueda realizar el análisis y solución del incidente	Con respecto al numeral 19.1.4, que menciona el escalamiento a niveles de soporte especializado nivel 3 o 4, solicitamos a la entidad precisar qué se entiende por niveles 3 y 4, si estos corresponden a recursos propios del contratista, fabricantes, terceros especializados o CSIRT externos, y si dichos niveles se consideran incluidos dentro del alcance contractual sin costos adicionales		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se debe cumplir con lo requerido en el respectivo ítem, el futuro proveedor del SOC en caso de requerirse deberá realizar el escalamiento del o los incidentes a nivel de fabricante, CSIRT o cualquier otro soporte especializado sin generar costo alguno para la Entidad.
311	19.1.6	ITEM 19 Gestión de Incidentes 19.1.6Detectar si en los sistemas de información existen eventos anómalos que deban ser reportados, bloqueados y/o escalados a incidentes, e integrarlos a casos de uso si necesario	En relación con el numeral 19.1.6, donde se solicita integrar eventos anómalos a casos de uso, solicitamos a la entidad indicar si se espera un número mínimo o estimado de nuevos casos de uso derivados de incidentes durante la operación del SOC y si dichos casos deben quedar formalmente documentados y transferidos a la DIAN		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, dentro del documento anexo técnico se encuentran las respectivas especificaciones para cada uno de los servicios requeridos, en el caso mencionado hay unos mínimos que se deben cumplir, así mismo no existe un límite en los casos de uso, estos se harán de acuerdo a las necesidades de la Entidad, por demanda o según las situaciones que se pueden llegar a presentar, quedando documentados formalmente para transferir a la DIAN.
312	19.1.9	ITEM 19 Gestión de Incidentes 19.1Análisis y detección 19.1.9Detectar de manera temprana los incidentes de seguridad de la información, basado en la inteligencia y cacería de amenazas que permita a la DIAN la contención de posibles incidentes	En cuanto al numeral 19.1.9, referido a la detección temprana basada en inteligencia y cacería de amenazas, solicitamos a la entidad precisar si la cacería de amenazas proactiva es obligatoria, con qué periodicidad debe ejecutarse y si se esperan informes formales de Threat Hunting como entregables del contrato		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características de la caza e inteligencia de amenazas, así como de los demás servicios requeridos por la Entidad, están claramente definidos en el anexo de características técnicas.
313	19.2	ITEM 19 Gestión de Incidentes 19.2Escalamiento y seguimiento 19.2.1Gestionar y canalizar las alertas a los diferentes grupos de interés y partes interesadas.	En relación con los numerales 19.2.1 y 19.2.7, donde se indica la canalización de alertas a los diferentes grupos de interés, ¿podría la Entidad especificar cuáles áreas internas o partes interesadas participan en el proceso de gestión de incidentes y el rol esperado de cada una de ellas en las diferentes fases del incidente?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las áreas involucradas serían la Dirección de Tecnología y la Oficina de Seguridad de la Información.
314	19.2	ITEM 19 Gestión de Incidentes 19.2.2Definir los casos de uso (eventos externos), sobre posibles ataques de ciberseguridad que se lleguen a presentar.	Frente a los numerales 19.2.2 y 19.2.3, que hacen referencia a la definición de casos de uso externos e internos, ¿podría la Entidad aclarar si dichos casos de uso serán propiedad intelectual exclusiva de la DIAN, si podrán ser reutilizados por el contratista en otros contextos y si su entrega es obligatoria como parte de la transferencia de conocimiento?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, serían de uso exclusivo de la Entidad y su entrega es obligatoria.
315	19.2.2	ITEM 19 Gestión de Incidentes 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.	En relación con los numerales 19.2.1 y 19.2.7, donde se indica la canalización de alertas a los diferentes grupos de interés, ¿podría la Entidad especificar cuáles áreas internas o partes interesadas participan en el proceso de gestión de incidentes y el rol esperado de cada una de ellas en las diferentes fases del incidente?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las áreas involucradas serían la Dirección de Tecnología y la Oficina de Seguridad de la Información.
316	19.4	ITEM 19 Gestión de Incidentes 19.4 Relacionamiento con terceros nacionales e internacionales (CSIRT – FIRST) 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/	En relación con los numerales 19.4.1 a 19.4.4, donde se establece que el SOC es el único autorizado para reportar incidentes de seguridad a entes externos, ¿podría la Entidad precisar si este reporte se realizará de manera autónoma por parte del contratista o previa autorización expresa de la DIAN, así como el alcance de la representación del contratista ante entidades como ColCERT, CSIRT Gobierno y otros organismos nacionales o internacionales?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el contratista no actuará como vocero oficial autónomo de la Entidad frente a terceros. Cualquier comunicación, reporte o escalamiento ante CSIRT, COLCERT, Centro Cibernético Policial, Fiscalía u otros terceros deberá realizarse conforme a los lineamientos, autorizaciones y canales definidos por la DIAN, sin perjuicio del apoyo técnico, recolección de información y preparación de evidencias que deba realizar el contratista dentro del alcance del servicio.
317	Sección VI	"Las arquitecturas propuestas... deben venir acompañadas por una carta o certificación del fabricante..."	La exigencia no define contenido mínimo, alcance, formato, vigencia, destinatario, ni si debe presentarse una carta por cada fabricante involucrado. Esto puede generar rechazos por aspectos meramente formales.	Se solicita amablemente a la entidad definir el contenido mínimo de la carta o certificación del fabricante, indicando si debe ir dirigida al proceso, incluir nombre del oferente, fabricante, soluciones ofertadas, vigencia y manifestación expresa de cumplimiento.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las certificaciones en mención corresponden a las del ítem 18 del anexo técnico.
318	Sección VI / Anexo Técnico	Tabla de infraestructura con 24.284 activos aproximados vs. licenciamiento mínimo SIEM para 2.467 dispositivos.	Se observa una posible inconsistencia entre el universo total de activos de la DIAN y la cantidad mínima a licenciar o integrar en SIEM, lo que dificulta dimensionar correctamente la solución y la cobertura esperada por capacidad.	Se solicita amablemente a la entidad precisar por cada capacidad y herramienta el alcance exacto de cobertura, indicando cantidades por tipo de activo, fuentes a integrar obligatoriamente, exclusiones y proyección de crecimiento aplicable.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el requerimiento es claro en la medida que solicita licenciamiento de 2467 dispositivos para el servicio de SIEM, así mismo, se indica que para otras capacidades y servicios se solicita licenciamiento para 25000 activos, para lo cual Entidad refiere el inventario de la infraestructura tecnológica de la Entidad en los documentos del proceso.
319	Sección VI / Anexo Técnico	Retención SIEM de "doce (12) meses en línea y doce (12) meses fuera de línea" y entrega final de "logs de los últimos seis (6) meses".	Se evidencia una posible inconsistencia entre la obligación de retención histórica y el alcance de entrega al cierre del contrato, sin que se precise el medio, formato, custodio ni la infraestructura asociada a dicha conservación.	Se solicita amablemente a la entidad unificar y aclarar el requerimiento de retención y entrega de logs, indicando tiempos definitivos, responsabilidades de almacenamiento, formato de exportación, custodio de la información y alcance de la reversión.	La Dirección de Impuestos y Aduanas Nacionales (DIAN) aclara al observante que, se trata de dos conceptos distintos: por un lado, los logs que deben entregarse al finalizar el contrato, correspondientes a seis (6) meses; y, por otro, la retención de logs que debe mantener el sistema SIEM durante la ejecución contractual, la cual corresponde a doce (12) meses en línea y doce (12) meses fuera de línea

320	Sección VI	"El tiempo esperado para la implementación del proyecto SOC... es de máximo cuatro meses."	Considerando el alcance integral del proyecto, la validación de inventario, la integración multicloud/on premise, las aprobaciones de la OSI y la puesta en operación, se requiere mayor precisión sobre el punto de inicio y las dependencias para medir dicho plazo.	Se solicita amablemente a la entidad aclarar que el plazo de implementación se contará a partir del acta de inicio y de la disponibilidad de accesos, información, ventanas y aprobaciones requeridas por la DIAN, así como definir las dependencias a cargo de cada parte.	La Dirección de Impuestos y Aduanas Nacionales (DIAN) aclara al observante que, el tiempo máximo de implementación es de cuatro (4) y comienza a partir del acta de inicio.
321	Sección VI / Anexo Técnico	Equipo mínimo exclusivo, continuidad obligatoria y restricción de modificación de perfiles durante el proyecto.	La exigencia de inmutabilidad del equipo, sumada a la exclusividad, puede resultar excesiva para un contrato de larga duración, aun cuando el contratista garantice continuidad del servicio con reemplazos de perfil igual o superior.	Se solicita amablemente a la entidad permitir sustituciones por perfiles equivalentes o superiores, previa aprobación de la supervisión, y aclarar el porcentaje de dedicación exigido por rol, así como si la atención puede prestarse en modalidad remota, híbrida u onsite según la necesidad del servicio.	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.
322	Sección VI	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.	Dado al requisito de paneles de control personalizados, en particular aquellos orientados a servicios empresariales, infraestructura virtualizada y aplicaciones especializadas, describe funcionalidades tradicionalmente asociadas a herramientas NOC u observabilidad de infraestructura, las cuales pueden encontrarse desacopladas del núcleo de una plataforma SIEM moderna. Actualmente, existen soluciones SIEM de nueva generación que no concentran todas estas capacidades de manera nativa, pero que las cubren plenamente mediante esquemas de integración con plataformas especializadas.	Se solicita respetuosamente a la Entidad evaluar que el requisito de dashboards especializados para servicios empresariales, infraestructura virtualizada y aplicaciones, sea considerado como Opcional, o Compatible mediante mecanismos de integración con herramientas de monitoreo, observabilidad o gestión existentes o complementarias.	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.
323	Sección VI	Recolección de logs escalable y flexible, como mínimo 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.	Se solicita respetuosamente a la Entidad si puede suministrar, de manera referencial o estimada, la información necesaria para dimensionar adecuadamente el volumen promedio y máximo estimado de eventos o logs diarios, adicional Volumen estimado de ingesta de datos diarios (DAI, GB/día o equivalente). Dado que los modelos de licenciamiento, dimensionamiento de infraestructura, costos de almacenamiento, retención y capacidad de procesamiento del SIEM dependen directamente del volumen de datos a recolectar.	Suministrar información sobre volumen promedio y máximo estimado de eventos o logs diarios y volumen estimado de ingesta de datos diarios (DAI, GB/día o equivalente).	"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 frío. 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. "
324	Sección VI	La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	Se solicita respetuosamente a la Entidad evaluar la posibilidad de ajustar o complementar el requisito, permitiendo que la solución de Gestión de Riesgo de Vulnerabilidades pueda ser provista por fabricantes que demuestren el cumplimiento integral de las capacidades técnicas y funcionales exigidas en el Anexo Técnico.	Aceptar criterios equivalentes de madurez técnica y capacidad operativa sin restringir obligatoriamente la participación a fabricantes incluidos en el cuadrante de líderes de reportes de analistas específicos.	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.
325	Sección VI	La solución ofertada deberá realizar una evaluación de vulnerabilidades en entornos web de manera automatizada de manera completa y precisa.	Realizar la evaluación automatizada de vulnerabilidades en entornos web se encuentra formulado de manera tal que condiciona implícitamente la solución de Gestión de Vulnerabilidades a incorporar de forma nativa capacidades completas de escaneo web, lo cual limita la libre concurrencia y excluye arquitecturas técnicas ampliamente adoptadas en la industria.	Se solicita que la Entidad permita explícitamente que la evaluación de vulnerabilidades web sea provista como una solución complementaria e integrada a la plataforma de Gestión de Vulnerabilidades, manteniendo la automatización, centralización y trazabilidad de los hallazgos.	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.
326	Sección VI	La solución ofertada permitirá gestionar la superficie de ataque externa, con el fin de identificar y reducir riesgo, brindando a la entidad la visión de un atacante.	Gestionar la superficie de ataque externa para identificar y reducir el riesgo desde la visión de un atacante se encuentra formulado de manera que asocia implícitamente esta capacidad a una única plataforma de Gestión de Vulnerabilidades, cuando en la práctica la gestión de la superficie de ataque externa (External Attack Surface Management – ASM) se realiza de forma más efectiva mediante soluciones especializadas adicionales.	Se solicita que la Entidad permita explícitamente que esta funcionalidad sea provista como una solución complementaria e integrada, y que se defina el número de dominios, subdominios o activos externos que la Entidad requiere monitorear dentro del alcance de ASM.	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.
327	Sección VI	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.	El requisito de gestionar de manera conjunta CWPP, CSPM, CIEM, CDR, DSPM e IaC/DevSecOps bajo una arquitectura CNAPP, provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades, define un modelo tecnológico altamente específico que condiciona la arquitectura de la solución y restringe la participación de alternativas especializadas.	Se solicita que la Entidad permita que estas capacidades CNAPP puedan ser cumplidas mediante soluciones complementarias e integradas, siempre que se garantice la visibilidad unificada, la correlación del riesgo, la automatización y la gestión centralizada requeridas.	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.
328	Sección VI	La solución debe ser capaz de realizar auditorías y Gestión de Seguridad del Directorio Activo sin la necesidad de un agente instalado en la Infraestructura de Directorio.	Para el requisito de realizar auditorías y gestión de seguridad del Directorio Activo sin agente, exigido además como parte de una solución de Gestión de Vulnerabilidades provista por un único fabricante, corresponde de manera directa a capacidades específicas de la solución Tenable, lo cual orienta el requerimiento hacia un fabricante y arquitectura determinados.	Se solicita que la Entidad permita que esta capacidad pueda cumplirse mediante soluciones especializadas adicionales e integrables, siempre que se garantice la automatización, la evaluación integral de la postura de seguridad del Directorio Activo y la gestión centralizada del riesgo.	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.
329	SDO - Sección III	Sobre Experiencia y/o Capacidades relacionadas con contratos terminados o iniciados (mínimo 40% de ejecución) dentro de los últimos siete (7) años	Es lógico y coherente que se requiera dentro de este importante proceso, que el oferente o algún integrante del oferente demuestre contar con un SOC PROPIO. Puede suceder que uno de los oferentes (individual o plural) pueda certificar experiencias obtenidas en forma conjunta sin tener un SOC propio, lo cual debería ser motivo de análisis por el seleccionador de este proceso, pues no reflejaría experiencia real para esta Licitación Internacional. El solicitar que se cuente con SOC PROPIO garantiza conocimiento, experiencia, capacidad, respaldo, entre otros factores críticos para este proceso y su objeto a contratar.	MODIFICACION: que se requiera dentro de este importante proceso, que el oferente o algún integrante del oferente demuestre contar con un SOC PROPIO.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los interesados deben contar con SOC propio en la ciudad de Bogotá.

330	SDO - Sección III	Enfoque Técnico y metodología (60 puntos) - Modelo operacional de servicios SOC	ACLARACIÓN: Se solicita definir claramente qué se considera "aspectos diferenciadores y valores agregados" para obtener la máxima puntuación (12 puntos). ¿Existe una lista indicativa de elementos que la DIAN valoraría como diferenciadores?	No	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.
331	SDO - Sección III	Nivel de partner más alto en las capacidades ofertadas (items 2 al 9 del anexo técnico)	ACLARACIÓN: Se solicita definir qué se entiende por 'nivel de partner más alto'. ¿Se refiere a Gold Partner, Platinum Partner, Premier Partner según cada fabricante? Algunos fabricantes tienen nomenclaturas diferentes (Tier 1, Elite, etc.)	No	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: • 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.
332	SDO - Sección III	Nivel de partner más alto en las capacidades ofertadas (items 2 al 9 del anexo técnico)	ACLARACION / MODIFICACION: Se solicita aclarar / modificar si el "nivel de partner mas alto" aclarado con la solicitud anterior, entendemos puede o pueda ser demostrado por Filiales, Sucursales o Controladas otorgados a su casa Matriz ? Es decir que si la Casa Matriz cuenta con estas certificaciones de fabricante, las sucursales, filiales y/o controladas pueden aportarlas y son validas.	No	La Dirección de Impuestos y Aduanas Nacionales (DIAN) informa al observante que este ítem se evaluará con base en los mecanismos mediante los cuales se anexe la información soporte, con el fin de corroborar su cumplimiento.
333	SDO - Sección III	Incluye servicios TAM (Technical Account Manager) en 5 o más de las capacidades para obtener 12 puntos	ACLARACIÓN: ¿El servicio TAM debe estar incluido sin costo adicional durante todo el proyecto (3 años) o solo durante la fase de implementación? ¿Se requiere carta del fabricante confirmando la inclusión del TAM?	No	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: • 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.
334	SDO - Sección III	Metodología para el cálculo de ROSI con facilidad de uso y comunicación ante la alta dirección para 12 puntos	ACLARACIÓN: Se solicita indicar si existe algún estándar o framework preferido por la DIAN para el cálculo del ROSI (ej. FAIR, Gordon-Loeb) o si se acepta metodología propia del oferente.	No	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.
335	SDO - Sección III	Estrategia de Monitoreo recreando posibles escenarios de ciberataques para 12 puntos	ACLARACIÓN: ¿Los escenarios de ciberataques deben basarse en amenazas específicas identificadas para el sector tributario/aduanero colombiano? ¿Se requiere alineación con el catálogo de amenazas del CoICERT?	No	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"". En este contexto, los escenarios deberán construirse con base en inteligencia de amenazas contextualizada, considerando el entorno operativo de la Entidad, y alinearse con las alertas, tipologías y tendencias de amenazas vigentes emitidas por fuentes oficiales.
336	Anexo Técnico	SIEM debe ser cotizado a tres (3) años, implementación a partir de septiembre 1 de 2027	ACLARACIÓN: Se solicita confirmar si el SIEM nuevo debe estar completamente implementado y operativo el 1 de septiembre 2027, o si esa es la fecha de inicio de implementación. ¿Hay período de transición con QRadar operando en paralelo?	No	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.
337	SDO - TDR	El futuro contratista debe operar, administrar y gestionar IBM QRadar e IBM Guardium hasta vencimiento del licenciamiento	ACLARACIÓN: Se solicita confirmar el alcance de la responsabilidad sobre QRadar y Guardium. ¿El contratista asume responsabilidad total sobre estas herramientas o solo operación bajo supervisión DIAN? ¿Qué soporte proporciona IBM durante este período?	No	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.
338	Anexo Técnico	Endpoints: 21.000 - Esta cantidad incluye proyección de crecimiento por el tiempo del proyecto	ACLARACIÓN: Se solicita confirmar la metodología de licenciamiento para los 21.000 endpoints. ¿Se licencia desde el inicio por la cantidad máxima o existe mecanismo de escalamiento progresivo según crecimiento real?	No	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, son 25000 activos la cantidad mínima requerida.
339	Lista de Precios	Monitoreo a la Gestión de Vulnerabilidades - 18.000 Activos de información - IVA N/A	ACLARACIÓN: Se solicita confirmar que el Monitoreo a Gestión de Vulnerabilidades está exento de IVA. El formulario indica 'N/A' en la columna IVA. ¿Es correcto o debe aplicarse IVA?	No	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, son 25000 activos la cantidad mínima requerida, y depende del tipo de licenciamiento estará exento de IVA en los casos donde aplique.
340	SDO - TDR	Implementación en máximo cuatro (4) meses	Considerando la complejidad de la infraestructura híbrida (Azure, AWS, on-premises, 2 datacenters), y establecido el plazo de 4 meses para implementación.	MODIFICACIÓN: Se sugiere un plazo de 7 u 8 meses que permita una implementación más segura y con menor riesgo de errores.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los tiempos de implementación solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
341	SDO - TDR	Equipo mínimo de trabajo: Gerente, Líder SOC, Threat Hunter, QA, IR, Analistas N1-N2-N3	ACLARACIÓN: Se solicita confirmar si todos los perfiles del equipo mínimo deben estar dedicados 100% exclusivamente a DIAN o si algunos pueden tener dedicación parcial compartida con otros clientes.	No	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.
342	Anexo Técnico	Requisitos específicos de certificaciones para cada perfil	ACLARACIÓN: Se solicita confirmar si las certificaciones requeridas para el equipo mínimo son todas obligatorias desde el inicio del contrato o si hay plazo para que el personal las obtenga durante la ejecución.	No	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, las hojas de vida del equipo mínimo de trabajo deberán ser presentadas por el oferente ganador.
343	SDO - TDR	Procedimiento de Cambio de Perfiles - 10 días hábiles para presentar reemplazo	ACLARACIÓN: En caso de renuncia intempestiva de un recurso, ¿los 10 días hábiles aplican desde la renuncia o desde que el contratista notifica a la DIAN? ¿Hay penalidad por vacancy temporal mientras se gestiona el reemplazo?	No	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que el término de diez (10) días se aplicará a partir de la ocurrencia de cualquiera de las dos situaciones descritas, esto es, la renuncia intempestiva o la notificación previa a la DIAN por parte del contratista.

344	SDO - TDR	Capacitaciones: CISSP, CISM, ECES, CEH, CCNA para 5 ingenieros cada una con vouchers	ACLARACIÓN: Se solicita confirmar si los 5 ingenieros pueden ser los mismos para todas las certificaciones o deben ser diferentes, lo que implicaría capacitar a 25 personas diferentes. ¿Los ingenieros deben ser funcionarios DIAN o pueden ser del contratista?	No	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el plan de capacitación están claramente detallados en la páginas 117 sección VI del documento "410-Solicitud-de-Oferta-VSD-SdO-SOC", que a la letra menciona: El CONTRATISTA deberá proponer y realizar un plan de capacitación general dirigido a los grupos específicos que la OSI considere: 1. Se deberán realizar cinco (5) capacitaciones para la obtención de los certificados relacionados a continuación. Las capacitaciones serán dictadas para cinco (5) ingenieros cada una, los cuales serán designados por la DIAN. Cada capacitación deberá contar con sus respectivos vouchers para la certificación y serán dictadas en un centro de capacitación certificado. En este sentido, se aclara que se contemplan veinticinco (25) cupos en total, distribuidos en cinco (5) capacitaciones de cinco (5) participantes cada una, los cuales serán designados por la DIAN a través de la OSI.
345	SDO - TDR	Programa de apropiación para mínimo 20 funcionarios por capacitación	ACLARACIÓN: Se solicita definir la duración mínima de cada capacitación del programa de apropiación. ¿Hay intensidad horaria mínima requerida para las 10 certificaciones listadas?	No	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el plan de capacitación están claramente detallados en la páginas 117 y 118 sección VI del documento "410-Solicitud-de-Oferta-VSD-SdO-SOC", que a la letra menciona: 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. I. CompTIA PenTest+ - CompTIA. J. Cybersecurity Practitioner - CSX-P - ISACA. 3. Acorde al punto anterior se dará prioridad a la modalidad presencial para las capacitaciones, bajo ese escenario, se deberán dictar en centros de enseñanza 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. 4. El CONTRATISTA deberá presentar evidencia de que las entidades certificadoras se encuentran activas, autorizadas y con contenidos actualizados al momento de impartir la formación.
346	SDO - Sección VIII CEC	Pagos por fases con límites máximos: 38% capacidades iniciales, 39% capacidades posteriores	ACLARACIÓN: Se solicita confirmar si los límites de 38% y 39% son techos máximos o porcentajes exactos. ¿Qué sucede con el 23% restante? ¿Corresponde a operación mensual, capacitaciones y ethical hacking?	No	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, 125 y 126, allí se describen los detalles y los entregables para hacer el pago y son techos máximos.
347	SDO - TDR	ANS 03 - Incidentes: P1: 1hr contención/8hr solución; P2: 4hr/16hr; P3: 8hr/48hr	ACLARACIÓN: Se solicita definir claramente qué se entiende por 'solución' de un incidente. ¿Es contención, erradicación, recuperación o cierre completo del caso? Algunos incidentes pueden requerir acciones de mediano plazo para solución definitiva.	No	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características están claramente definidas en los documentos del proceso.
348	SDO - TDR	Deducciones acumulables hasta máximo 10% del valor de costo del contrato	ACLARACIÓN: Se solicita confirmar si el 10% máximo se refiere al valor total del contrato o al valor de cada pago mensual. También se solicita definir 'valor de costo' versus 'precio del contrato'.	No	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, refiere al valor del pago mensual.
349	SDO - TDR	ANS 01 - Retraso en entrega productos: 2-4 SMMLV por cada día hábil de retraso	ACLARACIÓN: Se solicita confirmar el valor del SMMLV a utilizar. ¿Será el vigente a la fecha de la penalidad o el vigente a la fecha del contrato? Para proyectos de 3 años esto puede variar significativamente.	No	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, refiere al valor vigente a la fecha de la penalidad.
350	SDO - Sección VIII CEC	Plazo de ejecución: 36 meses o hasta el 30 de octubre de 2028	ACLARACIÓN: Existe aparente contradicción. Si el contrato inicia en septiembre 2026, 36 meses serían hasta septiembre 2029, pero se indica fecha máxima 30 octubre 2028 (25 meses). Se solicita aclarar cuál es el plazo real de ejecución.	No	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la operación, seguimiento, gestión, monitoreo y administración por parte del futuro proveedor de todos los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho a uso, licenciamiento, suscripciones, actualizaciones, soporte y garantía irá por tres (3) años y sus periodos se contabilizarán a partir de la puesta en operación de cada uno de los servicios requeridos, incluyendo lo siguiente: Tener en cuenta que desde el inicio del contrato se deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 nuevo SIEM (solicitado en el ítem 2) que hace parte integral de este proyecto por el tiempo solicitado (Tres años) con licenciamiento soporte, garantía y derecho a uso hasta agosto 31 de 2030. La protección de bases de datos (Firewall de bases de datos) irá a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031. El futuro contratista deberá, recibir, gestionar, administrar y operar desde el inicio del contrato el actual firewall de bases de datos propiedad de la DIAN del fabricante IBM Referencia GUARDIUM hasta diciembre 31 de 2027 tiempo en el que termina el soporte de este dispositivo por parte del fabricante, una vez esto ocurra deberá implementar el nuevo firewall de bases de datos solicitado en las capacidades requeridas por la DIAN. Para la capacidad de NDR se deberá tener en cuenta que este comenzará a operar a partir de enero de 2028 previamente autorización de la DIAN, para lo cual deberá implementar, administrar, operar, soportar y garantizar el servicio mencionado, con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031.
351	SDO - TDR	DIAN cuenta con 16.000 funcionarios y 3.000 contratistas aproximadamente	ACLARACIÓN: Para efectos del licenciamiento de endpoint (21.000 según anexo), ¿la cifra incluye proyección de crecimiento? ¿Hay dispositivos móviles corporativos que deban incluirse en el monitoreo?	No	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la cantidad mínima requerida son 25000, y dentro de la misma están las proyecciones de crecimiento.
352	SDO - TDR	Servicios tipo SaaS, PaaS, IaaS, XaaS. Todo licenciamiento debe estar a nombre de la DIAN	ACLARACIÓN: Para servicios SaaS de fabricantes internacionales, ¿cómo se garantiza que las licencias queden a nombre de DIAN si el contrato es con el oferente? Se solicita definir el mecanismo de registro de licencias.	No	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la Fase 1 - Diseño, planeación y estrategia del SOC están claramente detallados en la páginas 111 sección VI del documento "410-Solicitud-de-Oferta-VSD-SdO-SOC", que a la letra menciona: 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. En este sentido, el mecanismo de garantía se basa en que el oferente deberá gestionar con los fabricantes o proveedores internacionales el registro, asignación y titularidad de las licencias a nombre de la DIAN, asegurando que estas queden directamente asociadas a la entidad como cliente final. Esto implica que, desde el proceso de activación y administración de licencias, se deberá reflejar a la DIAN como titular, sin perjuicio de que el oferente actúe como intermediario contractual o integrador del servicio.

353	Lista de Precios VSD	OBJETO: DISEÑAR, IMPLEMENTAR Y OPERAR vs. TDR: PRESTAR LOS SERVICIOS	ACLARACIÓN: Existe diferencia en la descripción del objeto entre el formulario de precios y los TDR. Se solicita confirmar cuál es el objeto oficial del contrato para efectos de la propuesta.	No	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que no existe inconsistencia entre las expresiones "Diseñar, implementar y operar" y "Prestar los servicios", en la medida en que esta última comprende integralmente todas las actividades necesarias para la ejecución del contrato. Lo anterior se encuentra desarrollado en el numeral 4. Enfoque metodológico para el cumplimiento del contrato, así como en las fases subsiguientes, contenidas entre las páginas 110 y 114, Sección VI del documento "410-Solicitud-de-Oferta-VSD-SdO-SOC", donde se establece de manera expresa que: Fase 1 - Diseño, planeación y estrategia del SOC: El CONTRATISTA deberá entregar el diseño para la implantación de los servicios de un Centro de Operaciones de Seguridad – SOC, conforme a los lineamientos de la Oficina de Seguridad de la Información. Fase 2 - Implementación del SOC: El CONTRATISTA deberá ejecutar todas las actividades definidas en el plan de implementación, conforme a los servicios y capacidades adquiridas en el proceso de contratación. Fase 3 - Operación del SOC: El CONTRATISTA deberá operar el SOC de acuerdo con el Modelo Operacional de Servicios, siguiendo los lineamientos definidos por la OSI como supervisor del contrato. En este sentido, el objeto contractual debe entenderse como la prestación integral de los servicios de diseño, implementación y operación del SOC, conforme a lo establecido en los Términos de Referencia.
354	SDO - TDR	Forma de pago especifica hasta 38% para capacidades iniciales y hasta 39% para capacidades posteriores	ACLARACIÓN: La suma de los límites máximos indicados (38%+39%=77%) más pagos mensuales de operación no clarifica la distribución del 100%. Se solicita tabla de pagos detallada con porcentajes exactos por concepto.	No	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, 125 y 126, allí se describen los detalles y los entregables para hacer el pago.
355	Anexo Técnico	Capacitación - Unidad: Cursos - Cantidad: 15	ACLARACIÓN: En los TDR se listan 5 certificaciones oficiales para 5 personas cada una (=25 cursos potenciales) más el programa de apropiación. ¿Cómo se concilia con las 15 unidades del formulario de precios?	No	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que el plan de capacitación se encuentra claramente definido en las páginas 117 y 118, Sección VI del documento "410-Solicitud-de-Oferta-VSD-SdO-SOC", donde se establecen los lineamientos, alcance y condiciones aplicables.
356	SDO - TDR	Fase 4 Devolución del servicio: entregar componentes tecnológicos con licencias a perpetuidad con soporte actualizado por mínimo un año	ACLARACIÓN: ¿Las licencias que se entreguen como perpetuas al cierre deben incluirse en el precio del contrato, o DIAN adquiere estas licencias por separado? ¿El año de soporte post-contrato está incluido en el alcance?	No	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se deberá licenciar por un (1) año más, sólo se contemplan tres (3) años, 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.
357	SDO - TDR	Normativa vigente a tener en cuenta incluye manuales internos DIAN	ACLARACIÓN: Se solicita acceso a los documentos de normativa interna listados (MN-IIT-0072, MN-IIT-0062, IN-IIT-0253, etc.) para que los oferentes puedan dimensionar correctamente los requisitos de cumplimiento.	No	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, en la Sección VI del documento "410-Solicitud-de-Oferta-VSD-SdO-SOC", página 125 y 126, se establece que la normativa será entregada en la fase de diseño, planeación y estrategia.
358	SDO - TDR	Herramientas SIEM, Guardium e Inteligencia de Amenazas actuales deben ser operadas hasta sus fechas de vencimiento	En el anexo Técnico no estan las especificaciones detalladas de las herramientas IBM actuales (versiones, configuraciones, casos de uso implementados).	MODIFICACIÓN: Se solicita incluir en el Anexo Técnico las especificaciones detalladas de las herramientas IBM actuales (versiones, configuraciones, casos de uso implementados) para garantizar una transición adecuada.	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.
359	SDO - TDR	Equipo mínimo de trabajo incluye 3 Analistas SOC Nivel I para cobertura 7x24x365	ACLARACIÓN: Con solo 3 analistas Nivel I para cobertura 7x24x365, el esquema de turnos sería de 56 horas semanales por persona, excediendo límites legales. Se solicita confirmar si se requieren más analistas para turnos o si hay flexibilidad en la cantidad.	No	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, en la Sección VI del documento "410-Solicitud-de-Oferta-VSD-SdO-SOC", página 115, se establece la cantidad mínima requerida de personas. En este sentido, no se limita la inclusión de un mayor número de personas por parte del oferente, siempre que se garantice el cumplimiento integral de las condiciones técnicas, operativas y de los niveles de servicio definidos.
360	Lista de Precios VSD	SIEM implementación desde sept 2027, licenciamiento hasta sept 2030 (3 años)	ACLARACIÓN: Si el contrato es hasta octubre 2028, pero el licenciamiento SIEM es hasta sept 2030, ¿quién operará/administrará el SIEM entre oct 2028 y sept 2030? Se solicita aclarar la transición.	No	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, finalizando 2028 el proveedor del SOC deberá entregar los servicios a la DIAN.
361	SOLICITUD DE OFERTAS LICITACIÓN PÚBLICA INTERNACIONAL PAMD – 410-LPI-25 (P226834) / PRIMERA PARTE. Procedimientos de Licitación / Sección III. Criterios de Evaluación y Calificación / Reglas generales / 3.1. Criterios de Evaluación (IAO 34.6) / Evaluación Técnica / 1. Enfoque Técnico y metodología (60 puntos) IAO 34.6	"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 (...)"	Respetuosamente solicitamos a la Entidad modificar este requisito, por las siguientes razones: La exigencia de contar con la más alta membresía respecto de todos los fabricantes involucrados constituye una restricción injustificada a la libre concurrencia y pluralidad de oferentes. Contar con niveles inferiores de membresía no implica una afectación en la idoneidad técnica ni en la correcta ejecución del objeto contractual.	Permitir la acreditación de membresías o certificaciones vigentes de nivel intermedio o autorizado por los fabricantes, siempre que estas habiliten al oferente para la correcta provisión, implementación y soporte de los bienes y servicios requeridos; o ajustar la redacción del requisito de manera que se garantice la idoneidad técnica sin restringir injustificadamente la participación.	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.

362	SOLICITUD DE OFERTAS LICITACIÓN PÚBLICA INTERNACIONAL PAMD – 410-LPI-25 (P226834) / PRIMERA PARTE. Procedimientos de Licitación / Sección III. Criterios de Evaluación y Calificación / Reglas generales / 3.1. Criterios de Evaluación (IAO 34.6) / Evaluación Técnica / 2. Estrategia de implementación (40 puntos) IAO 34.6	"Los oferentes deberán allegar como parte de la oferta técnica las siguientes certificaciones vigentes y verificables para lograr la puntuación de la que trata este ítem: • ISO 27001:2022 en los procesos asociados a la operación del SOC • ISO 22301:2019 o superior."	Respetuosamente solicitamos a la Entidad eliminar o no considerar la certificación ISO 22301:2019 como criterio de evaluación, con fundamento en que: Ésta certificación no guarda una relación directa ni necesaria con el objeto del presente proceso (SOC). La certificación ISO/IEC 27001:2022 resulta plenamente pertinente para la gestión de la seguridad de la información. La exigencia de ISO 22301 introduce una barrera de entrada para potenciales oferentes.	Eliminar la certificación ISO 22301:2019 como requisito puntuable; o permitir acreditar la continuidad mediante mecanismos equivalentes, tales como planes de continuidad, pruebas, políticas y certificaciones ya exigidas.	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.
363	410-20260220-ANEXO- TECNICO PROYECTO-SOC-DIAN	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.	Amablemente solicitamos a la entidad se suprima la "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.". Y se permita "certificación en plataformas gestión de la superficie de ataque" o certificaciones de industria tales como por ejemplo ISO 27001 o ethical hacking, entre otros o experiencia en plataformas de gestión de la superficie de ataque.	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 en Plataformas Gestión de la Superficie de Ataque o certificaciones de industria tales como ISO 27001 o ethical hacking o otros o experiencia en plataformas de 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.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las certificaciones solicitadas para el perfil de Analista SOC Nivel II obedecen a las necesidades técnicas y operativas definidas por la Entidad para la prestación del servicio SOC. En consecuencia, el perfil deberá acreditar las condiciones de formación, experiencia y certificaciones establecidas en los documentos del proceso. Por lo anterior, no se acepta la solicitud.
364	410-20260220-ANEXO- TECNICO PROYECTO-SOC-DIAN /EQUIPO MINIMO DE TRABAJO	Tres (03) Analistas SOC Nivel I Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 2 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: -Cédula de Ciudadanía -Tarjeta Profesional -Certificación vigente como analista o profesional o especialista o arquitecto en seguridad de operaciones o su equivalente en las soluciones ofertadas (SIEM, SOAR, caza de amenazas o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. - Certificación en Plataformas de Gestión de la Superficie de Ataque. - Certificaciones de experiencia mínima de dos (2) años en implementación y/o soporte y/o administración de soluciones de seguridad. NOTA: Estos tres perfiles (analista I) deben cumplir los ANS de 7x24x365	Teniendo presente que los tres analistas corresponden a un nivel I y no corresponde a un nivel II o III de especialistas, amablemente solicitamos a la entidad no requerir certificación vigente como analista o profesional o especilista o arquitecto en seguridad de operaciones o su equivalente en las soluciones ofertadas (SIEM, SOAR, caza de amenazas o protección de marca) emitidad por el fabricante con el cual se presenta el oferente, así mismo solicitamos no se requiera tampoco certificación en plataformas de gestión de la superficie de ataque.	Tres (03) Analistas SOC Nivel I Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 2 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: -Cédula de Ciudadanía -Tarjeta Profesional - Certificaciones de experiencia mínima de dos (2) años en implementación y/o soporte y/o administración de soluciones de seguridad y/o plataformas de gestión de superficie de ataque. NOTA: Estos tres perfiles (analista I) deben cumplir los ANS de 7x24x365	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los requisitos exigidos para los Analistas SOC Nivel I fueron definidos conforme a las necesidades de operación, monitoreo y cumplimiento de los ANS 7x24x365 requeridos por la Entidad. Las certificaciones solicitadas permiten acreditar capacidades mínimas para la adecuada prestación del servicio. Por lo anterior, no se acepta la solicitud.
365	410-20260220-ANEXO- TECNICO PROYECTO-SOC-DIAN	**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.**	Teniendo presente el perfil requerido y las funciones a realizar por el especialista de respuesta a Incidentes amablemente sugerimos a la entidad se modifique la experiencia del perfil haciendo que esta sea más ajustada a las necesidades del contrato para lo cual sugerimos quede como se expresa en la columna de sugerencia de ajuste.	**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 tres (3) años de experiencia profesional en atención de incidentes de cuales uno(1) año 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.**	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la experiencia mínima solicitada para el Especialista de Respuesta a Incidentes - IR obedece a la criticidad del servicio, al alcance de las actividades de análisis, acompañamiento, remediación y respuesta, y a las necesidades puntuales de la Entidad. Por lo anterior, no se acepta la solicitud de reducción de experiencia.
366	410-20260220-ANEXO- TECNICO PROYECTO-SOC-DIAN	**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.	Teniendo presente el perfil requerido y las funciones a realizar por el gerente de proyecto y las diferentes personas que aran parte del proyecto, amablemente sugerimos a la entidad se modifique la experiencia del perfil haciendo que esta sea más ajustada a las necesidades del contrato para lo cual sugerimos quede como se expresa en la columna de sugerencia de ajuste.	**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 tres (3) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales dos (2) años en Gerencia de proyectos de seguridad de la información , plan de recuperación de desastres o continuidad de negocio.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los requisitos de formación, certificación y experiencia definidos para el Gerente de Proyecto responden a la complejidad, criticidad, alcance y duración del proyecto SOC. En consecuencia, se mantienen las condiciones establecidas en los documentos del proceso. Por lo anterior, no se acepta la solicitud

367	410-20260220-ANEXO- TECNICO PROYECTO-SOC-DIAN	**Lider /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	Teniendo presente el perfil requerido y las funciones a realizar por el líder/Coordinador SOC y las diferentes personas que aran parte del proyecto, amablemente sugerimos a la entidad se modifique la experiencia del perfil haciendo que esta sea más ajustada a las necesidades del contrato para lo cual sugerimos quede como se expresa en la columna de sugerencia de ajuste.	Lider /Coordinador SOC Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Gerencia de proyectos Certificaciones vigentes: •PMP Mínimo tres (3) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales dos (2) años en Gerencia de proyectos de seguridad de la información, plan de recuperación de desastres o continuidad de negocio.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los requisitos definidos para el Líder / Coordinador SOC corresponden a las necesidades de dirección, coordinación, seguimiento y control operativo del servicio SOC. En consecuencia, se mantienen las condiciones de formación, certificación y experiencia establecidas en los documentos del proceso. Por lo anterior, no se acepta la solicitud.
368	410-20260220-ANEXO- TECNICO PROYECTO-SOC-DIAN	**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	Amablemente solicitamos además de los posgrados requeridos adicionar el posgrado en ciberseguridad el cual es también muy ajustado al proyecto, así mismo solicitamos a la entidad se admita la certificación WAHS o la certificación certified ethical hacker, como opcional a la licensed penetration tester	**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 o ciberseguridad Certificaciones vigentes: • Licensed Penetration Tester (LPT) y/o WAHS Web applicaton hacking and security y/o certified ethical hacker 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	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, después de validar la información, el ítem en mención será ajustado en el anexo técnico mediante adenda que se publicará en los próximos días, quedando de la siguiente manera: • Licensed Penetration Tester (LPT), CPENT o LPT (Master).
369	410-20260220-ANEXO- TECNICO PROYECTO-SOC-DIAN	**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	Amablemente solicitamos a la entidad teniendo en cuenta que el perfil a ejecutar es de analista no se requiera postgrado en gerencia de proyectos, se adicione la carrera de ingeniería de producción la cual esta relacionada con la ingeniería industrial y se adicione el requerir la certificación de ISO 27001	**QA / Analista de Calidad SOC.** Ingeniería industrial , de sistemas o, telemática o, electrónica o, telecomunicaciones o de producción Certificaciones vigentes: • ISO 9001 ISO 27001 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	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
370	410-20260220-ANEXO- TECNICO PROYECTO-SOC-DIAN	**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.	Amablemente solicitamos a la entidad se permita homologar las certificaciones requeridas con experiencia en seguridad, así mismo solicitamos a la entidad disminuir el tiempo de experiencia mínima requerida	**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 o dos años de experiencia en seguridad -Certificación en gestión o administración de plataformas de seguridad informática o un (1) año adicional a la minima requerida en soluciones de seguridad. Certificaciones de experiencia mínima de 3 años en implementar y/o soportar y/o administrar soluciones de seguridad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
371	6. Equipo de Trabajo	El CONTRATISTA deberá conformar y mantener un equipo de trabajo para la ejecución del contrato, compuesto por perfiles especializados ajustados al proyecto. Este equipo deberá organizarse según los roles, perfiles, componentes o soluciones a desarrollar/implementar, e integrarse por recurso humano propio y, cuando se requiera, por expertos externos	Entendemos que las hojas de vida y soportes del equipo mínimo requerido deberán ser presentadas por el contratista adjudicado del proceso, es correcta nuestra apreciación.?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, es correcto su entendimiento los perfiles y hojas de vida solicitados deberán presentarse por parte del oferente ganador.
372	Equipo mínimo de trabajo Anexo Técnico de proyecto	Gerente de Proyecto: Posgrado en Gerencia de proyectos	Solicitamos respetuosamente a la entidad ampliar el pregrado a gerencia de tecnología, alta gerencia, gerencia del servicio o áreas afines a la ingeniería.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
373	Equipo mínimo de trabajo Anexo Técnico de proyecto	Gerente de Proyecto:Posgrado en Gerencia de proyectos Certificaciones vigentes: • PMP • Scrum Master	Solicitamos de manera atenta a entidad permitir que la formación pueda ser acreditada de la la siguiente manera: Posgrado en Gerencia de proyectos y/o certificado PMP Contar con certificación vigente: • Scrum Master		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
374	Equipo mínimo de trabajo Anexo Técnico de proyecto	Gerente de Proyecto: 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.	Amablemente solicitamos a la entidad evaluar la posibilidad de flexibilizar el requisito de experiencia específica, permitiendo experiencia equivalente en gestión de proyectos TI, gestión de servicios o proyectos relacionados con continuidad operativa.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
375	Equipo mínimo de trabajo Anexo Técnico de proyecto	Lider /Coordinador SOC Posgrado en Gerencia de proyectos	Solicitamos respetuosamente a la entidad ampliar el pregrado a gerencia de tecnología, alta gerencia, gerencia del servicio o áreas afines a la ingeniería.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
376	Equipo mínimo de trabajo Anexo Técnico de proyecto	Lider /Coordinador SOC Posgrado en Gerencia de proyectos Certificaciones vigentes: • PMP	Solicitamos de manera atenta a entidad permitir que la formación pueda ser acreditada de la la siguiente manera: Posgrado en Gerencia de proyectos y/o certificado PMP		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
377	Equipo mínimo de trabajo Anexo Técnico de proyecto	Lider /Coordinador SOC 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	Respetuosamente solicitamos a la entidad permitir que la experiencia específica sea acreditada en seguridad de la información o continuidad de negocio o recuperación de desastres, y no de manera conjunta.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.

378	Garantía de mantenimiento de la oferta (Fianza) No Aplica Declaración de mantenimiento de la oferta	Garantía de mantenimiento de la oferta Declaración de mantenimiento de la oferta	En la sección de "Garantía de Mantenimiento de la Oferta" se indica que la fianza no aplica. En ese sentido, entendemos que el único documento que debe presentar el proponente es la "Declaración de Mantenimiento de la Oferta", la cual establece compromisos en caso de retiro o incumplimiento de la propuesta. Agradecemos se pueda confirmar si efectivamente para el presente proceso aplica únicamente la Declaración de Mantenimiento de la Oferta. Lo anterior, con el fin de tener claridad sobre el alcance de las obligaciones exigidas a los proponentes y asegurar el adecuado cumplimiento de los requisitos del proceso.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, para el presente proceso, deberá atenderse lo establecido en los Datos de la Licitación - DDL respecto de la Declaración de Mantenimiento de la Oferta y la Garantía de Mantenimiento de la Oferta. En caso de indicarse que la garantía o fianza no aplica, el oferente deberá presentar la Declaración de Mantenimiento de la Oferta en los términos previstos en los documentos del proceso.
379	Anexo-Tecnico-Proyecto-SOC-DIAN Anexo Técnico ItemsVerificables	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.	Se cuentan con estadisticas o datos estimados de la cantidad de data en GB que debe ser considerada para la ingesta del SIEM		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el volumen mensual aproximado de eventos es de 4.6 mil millones, y el almacenamiento promedio mensual aproximado es de 390 GB sin compresión, indicando que se deben cumplir todos los requisitos solicitados para este servicio descritos en los documentos del proyecto.
380	Sección III. Criterios de Evaluación y Calificación	c. Los oferentes deberán allegar como parte de la oferta técnica las siguientes certificaciones vigentes y que sean verificables para lograr la puntuación de la que trata este ítem: …….. Otras certificaciones internacionales y reconocidas de SOC relevantes para el proyecto	Agradecemos confirmar si en la opción de otras certificaciones internacionales se pueden incluir asociones nacionales a CSIRT o CERT, certificaciones de protección de datos de los clientes tales como SOC 2 Type II, certificaciones que demuestren conformidad con requisitos de seguridad de la información, gobierno y niveles de protección según el riesgo.	Los oferentes deberán allegar como parte de la oferta técnica las siguientes certificaciones vigentes y que sean verificables para lograr la puntuación de la que trata este ítem: …….. Otras certificaciones internacionales y/o incluir asociones nacionales a CSIRT o CERT, certificaciones de protección de datos de los clientes tales como SOC 2 Type II, certificaciones que demuestran conformidad con requisitos de seguridad de la información, gobierno y niveles de protección según el riesgo. y reconocidas de SOC relevantes para el proyecto	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las certificaciones que se pretendan acreditar como "otras certificaciones internacionales y reconocidas de SOC relevantes para el proyecto" deberán ser vigentes, verificables y guardar relación directa con la operación, gestión, seguridad, continuidad, protección de datos o madurez del servicio SOC. La evaluación se realizará conforme a los criterios establecidos en los documentos del proceso.
381	Sección III. Criterios de Evaluación y Calificación	c. Los oferentes deberán allegar como parte de la oferta técnica las siguientes certificaciones vigentes y que sean verificables para lograr la puntuación de la que trata este ítem: …….. Otras certificaciones internacionales y reconocidas de SOC relevantes para el proyecto	Agradecemos confirmar si en la opción de otras certificaciones internacionales se pueden incluir asociones nacionales a CSIRT o CERT, certificaciones de protección de datos de los clientes tales como SOC 2 Type II, certificaciones que demuetren conformidad con requisitos de seguridad de la información, gobierno y niveles de protección según el riesgo.	Sugerimos a la entidad incluir otras certificaciones internacionales tales como: CSIRT o CERT, certificaciones de protección de datos de los clientes tales como SOC 2 Type II, certificaciones que demuetren conformidad con requisitos de seguridad de la información, gobierno y niveles de protección según el riesgo.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las certificaciones que se pretendan acreditar como "otras certificaciones internacionales y reconocidas de SOC relevantes para el proyecto" deberán ser vigentes, verificables y guardar relación directa con la operación, gestión, seguridad, continuidad, protección de datos o madurez del servicio SOC. La evaluación se realizará conforme a los criterios establecidos en los documentos del proceso.
382	Sección III. Criterios de Evaluación y Calificación 1. Enfoque Técnico y metodología (60 puntos)	b. 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.	Con el fin de que se me permita la pluralidad de oferentes solicitamos que este requisito sea aplicable para un número mínimo de plataformas a integrar o que se permita la pertenencia a dos de los niveles más altos de membresia.	b. 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 como mínimo para dos de las plataformas que deban integrarse. Para tal efecto, el oferente deberá informar los mecanismos suficientes para corroborar dicha información.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el criterio de evaluación asociado al nivel de partner o membresía de fabricante se aplicará conforme a lo establecido en los documentos del proceso y a los mecanismos de verificación allí previstos. La Entidad no acoge la solicitud de limitar el requisito a un número mínimo de plataformas o a niveles diferentes de membresía, toda vez que el criterio definido responde a las necesidades de respaldo, soporte y capacidad técnica requeridas para las soluciones ofertadas. Por lo anterior, no se acepta la solicitud.
383	Anexo Técnico – Ítem 1.1 / Sección VI TDR	NOTA 1: Se entiende que es un contrato llave en mano. NOTA 3: Todos los elementos, plataformas, soluciones, servicios y demás capacidades requeridas deberán ser prestados por el contratista.	El requisito de contrato 'llave en mano' en el que el contratista debe proveer la totalidad de los 19 componentes y servicios. No se aclara si el contratista puede subcontratar componentes, ni qué nivel de subcontratación es aceptable.	Se Solicita a la entidad que se precise el alcance 'llave en mano': (1) ¿cuál es el proceso de aprobación de subcontratistas por parte de la DIAN?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el carácter de contrato llave en mano implica que el contratista será responsable integralmente por la provisión, implementación, integración, operación, soporte y cumplimiento de las capacidades requeridas en los documentos del proceso. Cualquier subcontratación que el contratista pretenda realizar deberá cumplir las condiciones previstas en los documentos del proceso, no podrá trasladar ni disminuir su responsabilidad frente a la Entidad y deberá contar con las aprobaciones que correspondan conforme al marco contractual aplicable.
384	Anexo técnico	"El SOC mediante el cual se prestarán los servicios debe ser miembro FIRST™" y "Certificación que acredite vinculación… como mínimo doce (12) meses de antigüedad"	La exigencia de una antigüedad específica (12 meses) de membresía en el foro FIRST™ resulta restrictiva para la libre concurrencia y la pluralidad de oferentes. Un SOC puede demostrar capacidades técnicas avanzadas y procesos maduros mediante otras certificaciones exigidas (ISO 27001 e ISO 22301) sin que la antigüedad en un foro específico sea el único determinante de su calidad	Se solicita eliminar el requisito de los 12 meses de antigüedad, permitiendo que los proponentes que cuenten con la vinculación activa al momento de la oferta puedan participar, o en su defecto, eliminar la membresía FIRST como requisito obligatorio.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requisito relacionado con FIRST fue ajustado mediante adenda, por lo cual deberá atenderse lo allí dispuesto. En ese sentido, la vinculación o membresía FIRST no se entiende como requisito habilitante obligatorio, sino conforme al tratamiento definido en los documentos del proceso y sus adendas.
385	Sección III: Criterios de Evaluación y Calificación	"El SOC mediante el cual se prestarán los servicios debe ser miembro FIRST™" y "Certificación que acredite vinculación… como mínimo doce (12) meses de antigüedad"	Existe una contradicción en la naturaleza del requisito. El numeral 12.11 lo define como una característica técnica mínima de obligatorio cumplimiento (habilitante), mientras que la Sección III lo incluye como un factor de ponderación que otorga puntaje. En los procesos de selección, los requisitos mínimos obligatorios no deben otorgar puntaje, ya que el puntaje se reserva para calidades que excedan lo mínimo solicitado	Se solicita a la Entidad aclarar de manera precisa: ¿Es la membresía FIRST™ un requisito habilitante cuya ausencia es causal de rechazo de la oferta, o es exclusivamente un factor de ponderación técnica? Se sugiere que sea solo puntuable para fomentar la competencia.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requisito relacionado con FIRST fue ajustado mediante adenda, con el fin de precisar su tratamiento dentro del proceso. En consecuencia, deberá atenderse lo previsto en los documentos del proceso y sus adendas, en donde dicha condición no se configura como requisito habilitante obligatorio, sino conforme al esquema de evaluación allí definido.
386	Propuesta de valores	CEC: "El plazo de ejecución del contrato será de 36 meses". Anexo Técnico: "…durante toda la duración del contrato que es de tres (3) años". Formulario 1: "Servicios de Monitoreo… Cantidad Mínima: 30 meses".	Se observa una inconsistencia sustancial respecto al periodo de prestación del servicio de monitoreo. Mientras que las CEC y el Anexo Técnico establecen una duración de 36 meses (3 años), el Formulario 1 de Lista de Precios solo solicita cotizar 30 meses. Esta discrepancia de 6 meses afecta la comparabilidad de las ofertas y la estimación del presupuesto total, ya que el monitoreo debe ser continuo durante toda la vigencia del contrato.	Se solicita a la Entidad aclarar el plazo real del servicio de monitoreo y operación del SOC. En consecuencia, se sugiere ajustar la cantidad del ítem 11 en el Formulario 1 de 30 a 36 meses, para que guarde estricta coherencia con el plazo de ejecución contractual definido en las CEC y las especificaciones del Anexo Técnico.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la operación, seguimiento, gestión, monitoreo y administración por parte del futuro proveedor de los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho de 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, conforme a lo establecido en los documentos del proceso.
387	Ficha tècnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	En toda la capacidad 4 del pliego de condiciones (protecciòn de Bases de datos)	Respetuosamente solicitmos a la entidad permitir la participaciòn de Guardian de IBM para la protecciòn de bases de datos, aboliendo o cambiando la forma de redacciòn de los siguientes requerimientos: 4.3 4.8 4.15 4.23 4.33 4.37 4.39 4.54.3 4.54.4 4.54.7 De no ser tenida en cuenta nuestra observaciòn en estos ìtems, Guardiam de IBM quedaria por fuera del proceso, y no tendria sentido que Guardium no pueda participar cuando justamente es la herramienta actual. ESta afirmaciòn puede ser confirmada directamente con el fabricante	eliminar y/o modificar la redacciòn del requerimiento, a fin que se permita la participaciòn de IBM con su herramienta de protecciòn de Bases de datos Guardiam (el que tiene actualmente la entidad). A continuaciòn enlistamos la recomendaciòn para cada item del sistema de protecciòn de Bases de datos	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto no se acepta su sugerencia.

388	Ficha tècnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	"La entidad requiere adquirir [...] una Herramienta de protección de bases de datos (Firewall de bases de datos).”"	El ìtem 4 describe una solución de Database Activity Monitoring (DAM) / Database Firewall de propósito específico, con características que corresponden a un mercado de nicho muy especializado (IBM Guardium, Imperva Data Security, Oracle Audit Vault). El pliego no especifica ningún fabricante para este componente, lo cual es correcto. Sin embargo, se solicita confirmar explícitamente que: (i) se acepta que este componente sea provisto por un fabricante diferente al del SIEM y el SOAR, siempre que la integración con dichas plataformas esté garantizada; y (ii) la gestión centralizada de alertas del DAM desde el SIEM y la respuesta automatizada desde el SOAR son suficientes para acreditar el cumplimiento de los ítems de integración. Esto garantiza que el oferente pueda proponer el fabricante de DAM más idóneo sin estar forzado a una marca única que concentre todos los componentes.	Respetuosamente recomendamos a la entidad "La herramienta de protección de bases de datos podrá ser de un fabricante diferente al SIEM y SOAR, siempre que se garantice integración vía API o Syslog para el reenvío de alertas al SIEM y la ejecución de respuestas automatizadas desde el SOAR. El oferente deberá demostrar la integración funcional entre todos los componentes durante las pruebas de aceptación."	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, en ningún apartado del proceso se solicita que los servicios entregados sean de un sólo fabricante, el futuro proveedor del SOC podrá entregar los servicios requeridos en las herramientas que considera, siempre y cuando cumpla con las características técnicas solicitadas.
389	Ficha tècnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	"La solución deberá contar con tecnología de autoaprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo esquemas, objetos, tablas, sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario; todo esto para el establecimiento de un comportamiento base de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta."	En aras de la pluralidad de marcas, respetuosamente solicitamos a la entidad abolir esta parte del requerimiento:	" El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.""	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
390	Ficha tècnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	"La solución no deberá requerir el instalar agentes de software en los servidores a monitorear, pero deberá tener la opción en caso de ser necesario."	En aras de la pluralidad de marcas, respetuosamente solicitamos a la entidad que este requerimiento quede así: "	La solucion deberá permitir el monitoreo de actividad en las bases de datos mediante diversos mecanismos, como uso de agente y/o agentless"	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
391	Ficha tècnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	Proveer un servicio de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.	En aras de la pluralidad de marcas, respetuosamente solicitamos a la entidad eliminar este requerimiento, ***toda vez que èsto es una caracteristica tècnica que solo cumple Imperva*** , y justamente este requerimiento fuè el quee nos motivó a escribir nuestra observacion **3 "Que la entidad nos asegure que no nos exigirá el cumplimiento de lo imposible con las herramientas otorgadas por la entidad, pues Guardium no cumple este requerimiento.** **No entendemos como si el nuevo contratista debe prestar su servicio con Guardium (la herramienta que proporciona la entidad) para la renovaciòn no le permiten la participación.**		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
392	Ficha tècnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios deberán de poder usarse en cualquier número y cualquier combinación: - Número de registros a regresar por la consulta (SQL Query) - Número de registros afectados - Tipo de datos accedido (financiero, recursos humanos, inventarios, o cualquier definición personalizada) - Acceso a datos marcados como sensibles - Base de Datos, Esquema, Tabla y Columna accedida - Estado de autenticación de la sesión - Usuario y/o grupo de usuarios de Base de Datos conectado - Usuario conectado en la capa aplicativo, a diferencia del usuario conectado a la base de datos - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier personalización por expresiones regulares) - Autenticación (login, logout) y tareas (quering) - Direcciones IP origen y destino - Nombre de Host origen, usuario firmado en el host origen - Aplicación usada para la conexión a la base de datos - Tiempo de respuesta/procesamiento de las tareas - Errores en el manejador de SQL - Número de ocurrencias en intervalos de tiempo definidos - Por operaciones básicas (Select, Insert, Update, Delete) - Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export) - Por Stored Procedure o función utilizada - Si existe evento asignado de cambios (ticket) - Fecha y hora del evento	En aras de la pluralidad de marcas, respetuosamente solicitamos a la entidad abolir este requerimiento: "**Si existe evento asignado de cambio (ticket)**; toda vez que esto no corresponde al alcance natural de una solución de protección de base de datos		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, una vez revisado el ítem en mención se ajusta en su redacción y será publicado en adenda en los próximos días quedando de la siguiente manera: 4.23 Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios deberán de poder usarse en cualquier número y cualquier combinación: - Número de registros a regresar por la consulta (SQL Query) - Número de registros afectados - Tipo de datos accedido (financiero, recursos humanos, inventarios, o cualquier definición personalizada) - Acceso a datos marcados como sensibles - Base de Datos, Esquema, Tabla y Columna accedida - Estado de autenticación de la sesión - Usuario y/o grupo de usuarios de Base de Datos conectado - Usuario conectado en la capa aplicativo, a diferencia del usuario conectado a la base de datos - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier personalización por expresiones regulares) - Autenticación (login, logout) y tareas (quering) - Direcciones IP origen y destino - Nombre de Host origen, usuario firmado en el host origen - Aplicación usada para la conexión a la base de datos - Tiempo de respuesta/procesamiento de las tareas - Errores en el manejador de SQL - Número de ocurrencias en intervalos de tiempo definidos - Por operaciones básicas (Select, Insert, Update, Delete) - Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export) - Por Stored Procedure o función utilizada - Fecha y hora del evento
393	Ficha tècnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	La solución deberá analizar los eventos generados desde diferentes bases de datos. El análisis deberá contemplar los siguientes criterios: - Deberá mostrar el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos. - Deberá contar con un sistema de correlación basado en la dirección de los ataques. Deberá determinar si los ataques provienen desde dentro de la organización hacia afuera de la misma o viceversa. - Deberá realizar una correlación automática y en tiempo real de eventos, vulnerabilidades y bases de datos. - Deberá ejecutar una correlación que permita identificar usuarios de aplicación asociados con consultas –y determinadas actividades– en bases de datos específicas sin necesidad de alterar aplicaciones o instalar APIs. - Deberá correlacionar eventos como número de errores inusuales de sentencias de SQL o al momento de hacer autenticación a las bases de datos.	En aras de la pluralidad de marcas, respetuosamente solicitamos a la entidad abolirdo de los cinco siguientes requerimientos: "- Deberá contar con un sistema de correlación basado en la dirección de los ataques. Deberá determinar si los ataques provienen desde dentro de la organización hacia afuera de la misma o viceversa. - Deberá realizar una correlación automática y en tiempo real de eventos, vulnerabilidades y bases de datos" y a que esto hace parte de la herramienta de propósito específico SIEM que corresponde a la capacidad 2 de la ficha tècnica y justamente esta funcionalidad fuè la que nos incitò a escribir nuestra observacion 24.. **(que la entidad nos asegure que no nos exigirá el cumplimiento de lo imposible con las herramientas oorgadas por la entidad, pues Guardium no cumple este requerimiento).** **No entendemos como si el nuevo contratista debe prestar su servicio con Guardium (la herramienta que proporciona la entidad) para la renovaciòn no le permiten la participación.**	La solución deberá analizar los eventos generados desde diferentes bases de datos. El análisis deberá contemplar los siguientes criterios: - Deberá mostrar el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos. - Deberá ejecutar una correlación que permita identificar usuarios de aplicación asociados con consultas –y determinadas actividades– en bases de datos específicas sin necesidad de alterar aplicaciones o instalar APIs. - Deberá correlacionar eventos como número de errores inusuales de sentencias de SQL o al momento de hacer autenticación a las bases de datos.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, una vez revisado se encuentra que las características en mención por parte del interesado para este ítem, las cumplen diferentes herramientas en el mercado, por lo tanto no se acepta su solicitud.

394	Ficha tècnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	La solución deberá contar con una base de datos de vulnerabilidades predefinida para las siguientes regulaciones: - CIS - DISA (STIG) - FISMA - HIPAA - PCI-DSS	Teniendo en cuenta que: - CIS y DISA (STIG) no son regulaciones, son marcos de referencia - FISMA aplica para agencias federales de USA - HIPAA es para protección de datos de Salud en USA - PCI-DSS aplicaría solamente si almacenan, procesan o transmiten información de tarjetahabientes. Por o anteriormente expuesto, y en aras de la pluralidad de marcas, recomendamos a la entidad requerir lo que se ajusta a su necesidad, esd eliminar CIS y DISA (STIG)	La solución deberá contar con una base de datos de vulnerabilidades predefinida para las siguientes regulaciones: - FISMA - HIPAA - PCI-DSS	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su observación.
395	Ficha tècnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	Deberá ser capaz de monitorear al menos las siguientes plataformas de bases de datos: - Oracle (Including NDE/ASO, SSL) - Oracle Exadata - Microsoft SQL Server - IBM DB2 para Linux, z/OS y DB2/400 - IBM IMS para z/OS - IBM Informix - IBM Netezza - SAP Sybase (ASE, IQ, SQL Anywhere) - SAP-HANA - Teradata - MySQL - PostgreSQL - Progress OpenEdge - Maria DB	En aras de la pluralidad de marcas, y justamente dejar participar a Guardium que es la herramienta que tiene la DIAN, respestuosamente solicitamos a la entidad dejar así: Deberá ser capaz de monitorear al menos las siguientes plataformas de bases de datos: - Oracle (Including NDE/ASO, SSL) - Oracle **(eliminar la pablabra Exadata)** - Microsoft SQL Server - IBM DB2 para Linux, z/OS y DB2/400 - IBM IMS para z/OS - IBM Informix - IBM Netezza - SAP Sybase (ASE, IQ, SQL **(eliminar la palabra Anywhere**) - SAP-HANA - Teradata - MySQL - PostgreSQL - Progress **(Eliminar la palabra OpenEdge)** - Maria DB	Deberá ser capaz de monitorear al menos las siguientes plataformas de bases de datos: - Oracle (Including NDE/ASO, SSL) - Oracle - Microsoft SQL Server - IBM DB2 para Linux, z/OS y DB2/400 - IBM IMS para z/OS - IBM Informix - IBM Netezza - SAP Sybase (ASE, IQ, SQL) - SAP-HANA - Teradata - MySQL - PostgreSQL - Progress - Maria DB	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, una vez revisado se encuentra que las características en mención por parte del interesado para este ítem, las cumplen diferentes herramientas en el mercado, por lo tanto no se acepta su solicitud.
396	Ficha tècnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	En el modo monitoreo el administrador podrá visualizar alertas, ataques, errores de servidor y otra actividad no autorizada.	Respetuosamente recomendamos a la entidad cambiar esta redacción toda vez que como está escrito está enfocado a una funcionalidad de la solución y no a una necesidad. Por lo anteriormente expuesto, y en aras de la pluralidad de marcas, recomendamos a la entidad cambiar la redacción y que quede así: "La solución deberá asignar roles específicos para el acceso a la gestión y a la administracion, es decir, asociados con la consola de administración y monitoreo de las bases de datos"		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, una vez revisado se encuentra que las características en mención por parte del interesado para este ítem, las cumplen diferentes herramientas en el mercado, por lo tanto no se acepta su solicitud.
397	Ficha tècnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	En el modo de cumplimiento de políticas, la solución deberá bloquear ataques proactivamente.	Respetuosamente recomendamos a la entidad cambiar esta redacción toda vez que como está escrito está enfocado a una funcionalidad de la solución y no a una necesidad. Por lo anteriormente expuesto, y en aras de la pluralidad de marcas, recomendamos a la entidad cambiar la redacción y que quede así: "De acuerdo a los roles definidos en el acceso a las consolas de administración y monitoreo de las Bases de datos, se deberá proporcionar de acuedo al rol del usuario la investigación de amenazas proactivamente"	"De acuerdo a los roles definidos en el acceso a las consolas de administración y monitoreo de las Bases de datos, se deberá proporcionar de acuedo al rol del usuario la investigación de amenazas proactivamente"	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, una vez revisado se encuentra que las características en mención por parte del interesado para este ítem, las cumplen diferentes herramientas en el mercado, por lo tanto no se acepta su solicitud.
398	Ficha tècnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	En modo analizador de paquetes, la solución deberá ser capaz de enviar un paquete TCP-RST a ambos extremos de la conexión. Alternativamente, si así se configura, la solución podrá reportar el comportamiento anómalo, pero no tomar acción alguna.	En aras de la pluralidad de marcas, respetuosamente solicitamos a la entidad eliminar este requerimiento, ***toda vez que èsto es una caracteristica tècnica que solo cumple Imperva*** , y justamente este requerimiento fuè el quee nos incitò a escribir nuestra observacion **3.. (que la entidad nos asegure que no nos exige el cumplimiento de lo imposible con las herramientas oorgadas por la entidad, pues Guardium no cumple este requerimiento).** **No entendemos como si el nuevo contratista debe prestar su servicio con Guardium (la herramienta que proporciona la entidad) para la renovaciòn no le permiten la participación.**		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, una vez revisado se encuentra que las características en mención por parte del interesado para este ítem, las cumplen diferentes herramientas en el mercado, por lo tanto no se acepta su solicitud.
399	II: Datos de la licitación (DDL)	El idioma utilizado será Español	Teniendo en cuenta que en algunos puntos se demostrarà el cumplimiento técnico con un link del fabricante, respetuosamente solicitamos a la entidad seleccionar el idioma español en su navegador a fin que si se toma un idioma diferente a èste, no se rechace la oferta		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.

400	Ficha tècnica llamado "3. 410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN", hoja "Anexo Técnico ItemsVerificables"	La protección de bases de datos (Firewall de bases de datos) irá a tres (3) años, y su implementación se hará a partir de enero de 2028 con licenciamiento soporte, garantía y derecho a uso hasta enero de 2031. El futuro contratista deberá, recibir, gestionar, administrar y operar desde el inicio del contrato el actual firewall de bases de datos propiedad de la DIAN del fabricante IBM Referencia GUARDIUM hasta diciembre 31 de 2027 tiempo en el que termina el soporte de este dispositivo por parte del fabricante, una vez esto ocurra deberá implementar el nuevo firewall de bases de datos solicitado en las capacidades requeridas por la DIAN.	Respetuosamente solicitamos a la entidad indicarnos si este SIEM està operando y adicionalmente compartirnos el pantallazo o evidencia que el licenciamiento està activo hasta la fecha indicada por la entidad		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el SIEM de la Entidad se encuentra operativo con soporte y garantía por parte del fabricante, con los siguientes datos: 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. "
401	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 evaluar cúales son los fabricante en el cual debera entregarse el TAM durante la vigencia del contrato, teniendo en cuenta que el servicio a ofertar contempla varios productos y fabricantes, alguno no poseen este servicio.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ofrecimiento para puntuación se validará con la presentación de la certificación expedida por el fabricante o los fabricantes de los servicios ofertados.
402	Sección III. Criterios de Evaluación y Calificación	c. Incluye servicios TAM (Thecnical account manager) (items 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 ofrecimiento para puntuación se validará con la presentación de la certificación expedida por el fabricante o los fabricantes de los servicios ofertados.
403	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 en la sesión de aclaraciones, se evidenció un esquema en donde la operación finaliza en Octtubre de 2028 (Mes 10).		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.
404	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Como parte de este proceso, el contratista deberá suministrar el licenciamiento para las nuevas herramientas por un periodo de tres años, a partir de la fecha de su implementación y acorde a las características solicitadas en el anexo de características mínimas	Solicitamos a la entidad **aclarar** quien realizara las actividades de operación del SIEM, en el periodo de 1 Septiembre 2027 a 31 Agosto de 2030, ya que en este periodo el contrato de la operación a finalizado. Se espera que el oferente entregue la solucion con derecho a uso de este item.		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.
405	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Como parte de este proceso, el contratista deberá suministrar el licenciamiento para las nuevas herramientas por un periodo de tres años, a partir de la fecha de su implementación y acorde a las características solicitadas en el anexo de características mínimas	Solicitamos a la entidad **aclarar** quien realizara las actividades de operación del Firewall de Proteccion de bases de datos, en el periodo de 1 Nov 2028 a Enero de 2031, ya que en este periodo el contrato de la operación a finalizado. Se espera que el oferente entregue la solucion con derecho a uso de este item.		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.

406	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Como parte de este proceso, el contratista deberá suministrar el licenciamiento para las nuevas herramientas por un periodo de tres años, a partir de la fecha de su implementación y acorde a las características solicitadas en el anexo de características mínimas	Solicitamos a la entidad **aclarar** quien realizara las actividades de operación del NDR, en el periodo de 1 Ene 2028 a Enero de 2031, ya que en este periodo el contrato de la operación a finalizado. Se espera que el oferente entregue la solucion con derecho a uso de este item. En el anexo tecnico se menciona este parrafo "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." Agradecmos claridad.		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 item 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.
407	Sección I. Instrucciones a los Oferentes (IAO)	10. Idioma de la Oferta	Solicitamos a la entidad permitir la traduccion simple del idioma ingles al español en la entrega de especificaciones, fichas técnicas y/o catálogos que están en idioma inglés por parte del fabricante. 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 aclara al observante que, para la revisión de las diferentes ofertas se tendrá en cuenta su comentario, y se hará la revisión de las características técnicas donde aplique en el idioma original de los catálogos del fabricante.
408	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 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 item 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.
409	Especificaciones Técnicas Solución de análisis de código estático y dinámico para aplicaciones	En el ciclo de desarrollo las herramientas del CONTRATISTA 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 solicita a la entidad establecer la cantidad de usuarios para los cuales se debe considerar el licenciamiento SASE.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la cantidad y características se encuentran estipuladas claramente en el anexo técnico.
410	Anexo-Tecnico-Proyecto-SOC-DIAN	Especialista de Respuesta a Incidentes (IR)	Se agradece a la entidad ampliar por pluralidad de oferentes ampliar la base para este perfil de la siguiente Manera: Especialista de Respuesta a Incidentes (IR) Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Seguridad Informática o Seguridad de la Información o Afines 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 En cuanto al requisito de posgrado, se propone aceptar no solo "Seguridad Informática" , sino también programas relacionados tales como Ciberseguridad, Seguridad Digital, Gestión de la Seguridad de la Información, Seguridad de la Información, Seguridad de Tecnologías de la Información, Riesgos y Seguridad de la Información, entre otros afines. En el contexto actual, estos programas comparten fundamentos, metodologías y enfoques prácticos orientados a la protección de activos digitales y la gestión de incidentes, por lo que limitar la exigencia a una denominación específica restringe la participación de profesionales con formación equivalente.		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.

411	Equipo Mínimo de Trabajo	Gerente de Proyecto	ampliar la base para este perfil de la siguiente Manera: Gerente de Proyecto Profesional en Ingeniería de sistemas, telemática, electrónica, telecomunicaciones o áreas afines. Con posgrado en Gerencia de Proyectos o en áreas relacionadas tales como: Dirección de Proyectos, Gestión de Proyectos, Administración de Proyectos, Project Management, Gerencia de Tecnologías de la Información (TI), Gerencia de Ingeniería, MBA o programas afines que incluyan formación en gestión de proyectos • PMP Mínimo cinco (5) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales cinco (3) años en Gerencia de proyectos de seguridad de la información , Lo anterior se fundamenta en la necesidad de garantizar el principio de pluralidad de oferentes, promoviendo la participación de un mayor número de proponentes idóneos en el proceso. En el mercado actual, existen múltiples programas de posgrado con enfoques equivalentes en gestión de proyectos, cuyos contenidos académicos desarrollan competencias similares en planificación, ejecución, control y cierre de proyectos, bajo estándares internacionales. Limitar el requisito exclusivamente a una denominación específica puede restringir injustificadamente la		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.
412	Equipo Mínimo de Trabajo	Threat Hunter / Analista de Ciber inteligencia	ampliar la base para este perfil de la siguiente Manera: Threat Hunter / Analista de Ciber inteligencia Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Gerencia de proyectos o Seguridad Informatica, Ciberseguridad, Seguridad Digital, Gestión de la Seguridad de la Información, Seguridad de la Información, Seguridad de Tecnologías de la Información, Riesgos y Seguridad de la Información, entre otros afines Certificaciones vigentes: • Licensed Penetration Tester (LPT) o similares 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 En cuanto al requisito de posgrado, se propone aceptar no solo "Seguridad Informática" , sino también programas relacionados tales como Ciberseguridad, Seguridad Digital, Gestión de la Seguridad de la Información, Seguridad de la Información, Seguridad de Tecnologías de la Información, Riesgos y Seguridad de la Información, entre otros afines. En el contexto actual, estos programas comparten fundamentos, metodologías y enfoques		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.
413	Equipo Mínimo de Trabajo	QA / Analista de Calidad SOC.	Ingeniería industrial , de sistemas o, telemática o, electrónica o, telecomunicaciones. Postgrado en Gerencia de proyectos o Especialización o Maestría en Gerencia de Proyectos, Gestión de Proyectos, Dirección de Proyectos, Project Management, Gerencia de Programas, Gerencia de Ingeniería, Gerencia de Tecnologías de la Información (TI), Administración de Proyectos, e incluso programas en Gerencia Estratégica o Administración (MBA) con énfasis en proyectos. Certificaciones vigentes: • ISO 9001 o similar 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 Lo anterior se fundamenta en la necesidad de garantizar el principio de pluralidad de oferentes, promoviendo la participación de un mayor número de proponentes idóneos en el proceso. En el mercado actual, existen múltiples programas de posgrado con enfoques equivalentes en gestión de proyectos, cuyos contenidos académicos desarrollan competencias similares en planificación, ejecución, control y cierre de proyectos, bajo estándares internacionales. Limitar el requisito exclusivamente a una denominación específica puede restringir injustificadamente la participación de profesionales que cuentan con formación		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.

414	8,21	El CONTRATISTA 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 desbordas que muestre la respectiva herramienta. El CONTRATISTA debe poner a disposición el recurso humano para generar planes de acción sobre la información reportada en la herramienta.	Se solicita a la entidad aclarar si es correcto entender que las actividades de remediación derivadas de los hallazgos identificados por la herramienta estarán a cargo de los equipos de desarrollo y/o de las áreas responsables de la entidad, siendo el CONTRATISTA un apoyo en la gestión, priorización y seguimiento de dichas actividades. En caso contrario, se agradece especificar si el CONTRATISTA deberá asumir directamente la ejecución de las remediaciones dentro del ciclo de DevSecOps, detallando el alcance, responsabilidades, perfiles requeridos, niveles de acceso y recursos necesarios para su ejecución, con el fin de dimensionar adecuadamente la prestación del servicio. Es importante precisar que la ejecución de actividades de remediación implica capacidades propias de equipos de desarrollo de software, incluyendo análisis, desarrollo, pruebas, gestión de ambientes (laboratorios) y despliegue de aplicaciones, aspectos que no se encuentran definidos dentro del alcance actual. En este sentido, la ausencia de dicha definición puede generar ambigüedades en la asignación de responsabilidades. Adicionalmente, se solicita a la entidad aclarar la posible inconsistencia de este requerimiento frente a lo establecido en el numeral 12.78 del Anexo Técnico Administrativo, con el fin de asegurar coherencia en el alcance contractual		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, las remediaciones y la intervenciones a las que haya lugar en la infraestructura propia de la Entidad, las realizará el personal de la DIAN, el futuro proveedor del SOC deberá realizar el acompañamiento desde el inicio y hasta la solución de las mismas, tal como se indica en el anexo técnico. Así mismo se indica que no existe inconsistencia en el ítem 12.78 del anexo técnico.
415	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	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.	Según lo establecido en el presente numeral, y conforme a lo indicado en el numeral 12.78 – 4. Respuestas, donde se señala que "se deberá reportar de manera oportuna al equipo de seguridad de la Entidad para que pueda contener, erradicar y remediar", entendemos que la ejecución de las acciones de remediación será gestionada ante el equipo de seguridad de la Entidad, quien será el responsable de llevarlas a cabo dichas labores generando los planes de acción correspondiente. Se agradece confirmar, luego una remediación puede la generara la entidad acompañado del SOC del contratista.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, su entendimiento es incorrecto, el futuro proveedor deberá generar los planes de acción correspondientes para la ejecución de las acciones de remediación, el equipo de seguridad de la Entidad será el responsable de llevar a cabo las labores propias de intervención en las plataformas tecnológicas de la Entidad.
416	Formulario 1 lista de precios VSD	Monitoreo a la Gestión de Vulnerabilidades (Ver características en el ítem 5 del anexo).	Se agradece a la entidad aclarar la cantidad de activos luego para el Formulario 1 lista de precios VSD solo indican 18000		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: ITEM | DESCRIPCIÓN | ESPECIFIQUE: REFERENCIA / MARCA | ESPECIFIQUE: REFERENCIA / 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 | | | |
417	Formulario 1 lista de precios VSD	NDR - Detección y respuesta en red e Inteligencia de amenazas (Ver características en el ítem 7 del anexo).	Se agradece a la entidad aclarar la cantidad de activos luego para el Formulario 1 lista de precios VSD solo indican 18000		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la cantidad de dispositivos es 25000, el formulario fue ajustado en sus cantidades mediante adenda.
418	Formulario 1 lista de precios VSD	Servicios de Monitoreo y operación de SOC con el personal mínimo requerido (Ver características en el ítem 12 del anexo).	Se agradece a la entidad indicar si para todo los 36 meses de servicio se facturaran 30 meses, se agradece aclarar luego esto esta estimado en el Formulario 1 lista de precios VSD		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.
419	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	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.	Se agradece a la entidad especificar si la facturación podrá realizarse una vez implementados los equipos, aun cuando el licenciamiento no se encuentre activado o los equipos no estén en operación. Lo anterior es relevante, en la medida en que esta condición impacta directamente los flujos de caja de los oferentes, incrementando el riesgo financiero asociado al contrato. Adicionalmente el incremento de los componentes como memorias y procesadores que pueden impactar el costo de los mismos en el tiempo.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los pagos de cada uno de los servicios o capacidades requeridas, se harán cuando estos se encuentren operativos.
420	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	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.	Teniendo en cuenta las fechas establecidas, se solicita a la entidad aclarar que, una vez finalizado el contrato de servicios, se defina expresamente quién será responsable de gestionar los procesos de RMA en caso de requerirse. Asimismo, se agradece precisar si, en el evento de existir un nuevo proveedor, este asumirá la gestión de dichos RMA o si la entidad reconocerá económicamente los costos asociados a cambios de partes o procesos de RMA correspondientes a equipos suministrados por el proveedor anterior.		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.

421	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	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.	Se agradece a la entidad especificar el momento exacto en que deberá activarse el incremento adicional de licenciamiento, indicando si este corresponde a la fecha de implementación, puesta en operación, acta de recibo a satisfacción u otro hito contractual definido		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor del SOC tiene cuatro (4) meses para realizar la respectiva implementación de los servicios requeridos con el licenciamiento solicitado por la Entidad en las cantidades estipuladas en el anexo técnico.
422	2,8	Debe tener autoaprendizaje de inventario de activos (CMDB) contando con capacidades de descubrimiento automático para alimentar y mantener actualizada la Base de Datos de Gestión de Configuración (CMDB). Esto implica que el sistema debe ser capaz de identificar, clasificar y registrar de forma dinámica los activos tecnológicos presentes en la infraestructura, incluyendo servidores, estaciones de trabajo, dispositivos de red, aplicaciones y servicios, sin intervención manual constante. Para tal efecto se informa que actualmente la Entidad cuenta con un ITSM del fabricante ARANDA.	Se agradece a la entidad especificar las labores administrativas de integración y Gestión con Aranda ITSM quien sera el encargado. Luego la integracion se realizara por API,	Debe tener autoaprendizaje de inventario de activos (CMDB) contando con capacidades de descubrimiento automático para alimentar y mantener actualizada la Base de Datos de Gestión de Configuración (CMDB). Esto implica que el sistema debe ser capaz de identificar, clasificar y registrar de forma dinámica los activos tecnológicos presentes en la infraestructura, incluyendo servidores, estaciones de trabajo, dispositivos de red, aplicaciones y servicios, sin intervención manual constante. Para tal efecto se informa que actualmente la Entidad cuenta con un ITSM.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor del SOC deberá realizar las respectivas labores para poder realizar la respectiva integración.
423	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 agradece a la entidad aclarar si los veinte (20) casos de uso adicionales deberán desarrollarse a lo largo de toda la ejecución del contrato o si corresponden a casos de uso ya existentes y personalizados en el SIEM actual, los cuales deberán ser migrados durante el plazo contractual.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor del SOC deberá realizar las respectivas labores para de este ítem durante la implementación.
424	2,16	Debe tener métricas de base y detección de desviaciones (comportamientos anómalos).	Se agradece a la entidad indicar el número total de activos que serán objeto de verificación de comportamiento anómalo, así como el alcance de dicha verificación (por ejemplo, endpoints, servidores, aplicaciones, entre otros), con el fin de dimensionar adecuadamente la solución requerida.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el mínimo de activos que se deben tener en cuenta para esta funcionalidad son 2467 activos.
425	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 .	Se agradece a la entidad aclarar si, para los dispositivos alojados en entornos de nube como Azure y AWS, es correcto entender que la entidad dispondrá de los recursos necesarios para su monitoreo (tales como infraestructura para la instalación de colectores, sondas, entre otros).		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor del SOC deberá aprovisionar todo lo necesario para realizar la implementación de los diferentes servicios requeridos para el SOC.
426	2,26	Recolección de logs escalable y flexible, como mínimo 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.	Se agradece a la entidad indicar la cantidad total de activos que requerirán capacidades de FIM (File Integrity Monitoring), así como su tipología (servidores, endpoints, bases de datos, entre otros), con el fin de dimensionar adecuadamente la solución.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el mínimo de activos que se deben tener en cuenta para esta funcionalidad son 2467 activos.
427	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 agradece a la entidad confirmar que el alcance se limita a la integración de la herramienta de ITSM mediante API, y que no incluye actividades de administración, implementación, configuración o provisión de una nueva herramienta de ITSM.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, lo requeridos es la integración de la herramienta ITSM, no se exige provisión de una nueva herramienta o administrar la existente.
428	2,32	Escalabilidad - Escalabilidad de recolección de datos mediante la implementación de máquinas virtuales con la función de recolección (colectores virtuales). - Los recolectores deben poder almacenar en búfer eventos cuando la conexión no esté disponible. - Escalado del análisis mediante la implementación de nuevas máquinas virtuales. - Arquitectura de balanceo integrada para recoger eventos desde sitios remotos usando recolectores	Se agradece a la entidad aclarar si, en caso de requerirse colectores o workers adicionales, esta será responsable de suministrar los recursos de infraestructura necesarios (máquinas virtuales, almacenamiento, red, entre otros) para su implementación y operación		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor del SOC deberá aprovisionar todo lo necesario para realizar la implementación de los diferentes servicios requeridos para el SOC.
429	5.4.11	La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	Se solicita a la entidad validar y actualizar la nomenclatura de los cuadrantes definidos, considerando que estos han sido modificados en versiones recientes de la metodología o herramienta de referencia, con el fin de evitar ambigüedades en la interpretación y asegurar la correcta alineación con los estándares vigentes.		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, su cumplimiento es obligatorio al ser requisitos mínimos exigidos, si se presentan actualizaciones en cuanto a lo exigido por la Entidad, el interesado deberá aportar los documentos necesarios para sustentar dicha actualización.
430	5.9.1	La solución debe realizar el escaneo para la detección de vulnerabilidades locales y remotas sin la necesidad de un agente en el dispositivo de destino.	Se solicita a la entidad confirmar si, dentro de su infraestructura on-premise y/o en entornos de nube, se permitirá el despliegue de sondas necesarias para la ejecución de las tareas de escaneo, así como precisar las condiciones, restricciones o requisitos técnicos asociados a su implementación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor del SOC deberá aprovisionar todo lo necesario para realizar la implementación de los diferentes servicios requeridos para el SOC.
431	6.5.14	La solución se debe integrar como mínimos con los siguientes elementos: - Sistema de control de acceso a la red (NAC) - Herramienta de Sandbox - Solución SIEM - Solución de respuesta automática (SOAR) - BitDefender - Solución de detección y respuesta en el endpoint (EDR)	Se solicita a la entidad suministrar el inventario detallado de soluciones NAC, Sandbox u otros dispositivos de seguridad que deban ser integrados, toda vez que estos no se encuentran reflejados en el inventario actualmente proporcionado, lo cual puede generar vacíos en la definición del alcance e integración de la solución.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el inventario de la infraestructura tecnológica de la Entidad está detallado en los diferentes documentos del proceso.
432	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).	Se agradece a la entidad Confirmar la cantidad de activos, luego esta cantidad difiere del anexo economico : Formulario 1 lista de precios VSD		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las cantidad solicitada es de 25000 activos, los documentos han sido ajustados en sus valores.
433	8,30	Determinar automáticamente los scanner de código a utilizar en función del lenguaje, atributos y configuración de la aplicación.	Se agradece a la entidad cual es el tipo de información requiere que muestre el escaneo (o Solo mostrar la información sin importar la tecnologia)		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se debe realizar lo solicitado en el respectivo ítem.
434	8,45	Debe tener la funcionalidad de visualizar en detalle las vulnerabilidades de una aplicación, en el cual se muestre: - Archivo asociado - Número de líneas (SAST) o URL(DAST) - Severidad de la vulnerabilidad - Descripción. - CWE asociado, si existe. - El número de instancias en las que se encuentra - Historia de la vulnerabilidad que incluye el tiempo de su primera y última aparición. - Estado de la Vulnerabilidad (Activa o Cerrada).	Se agradece aclarar a la entidad, cuando hablan de "El número de instancias en las que se encuentra" entendemos que hablan las aplicaciones a evaluar.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se refiere a aplicaciones.

435		Detección de Amenazas	Solicitamos a la entidad aclarar cuantos endpoints se encuentran definidos en el alcance que debe tener en cuenta el oferente para el dimensionamiento del servicio.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el inventario de la infraestructura tecnológica de la Entidad está detallado en los diferentes documentos del proceso.
436		Detección de Amenazas	Solicitamos a la entidad aclarar si la entidad cuenta con una solución EDR para servidores y equipos de computo, por favor informar el fabricante, la version del producto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el inventario de la infraestructura tecnológica de la Entidad está detallado en los diferentes documentos del proceso, también se indica que el fabricante es BITDEFENDER.
437		Detección de Amenazas	Solicitamos a la entidad informar cual es el inventario de fuentes a integrar en la solución SIEM y donde se ubican las fuentes en el alcance?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el inventario de la infraestructura tecnológica de la Entidad está detallado en los diferentes documentos del proceso.
438		Detección de Amenazas	Solicitamos a la entidad aclarar si se espera una solucion SaaS (Cloud) o On-premise de la entidad o instalaciones del oferente.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor del SOC puede implementar los servicios con la modalidad que estime conveniente, siempre y cuando se cumpla con las características solicitadas por la Entidad.
439	2	SIEM	Solicitamos a la entidad aclarar cual es la volumetria de la solucion actual de los ultimos 12 meses en la plataforma actual IBM y cuantas alertas (mensuales o diarias) se generan actualmente?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el volumen mensual aproximado de eventos es de 4.6 mil millones, y el almacenamiento promedio mensual aproximado es de 390 GB sin compresión, indicando que se deben cumplir todos los requisitos solicitados para este servicio descritos en los documentos del proyecto.
440		Code Review	Solicitamos a la entidad suministrar detalles de los códigos a revisar en el alcance, confirmar su son desarollos propios y si se cuentan con la documentacion de los codigos fuentes, necesarios para entender el tema de remediación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas para este ítem se encuentran detalladas en el anexo técnico.
441		Code Review	Solicitamos a la entidad informar cuantas líneas de código se deben revisar en el alcance dle proyecto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas para este ítem se encuentran detalladas en el anexo técnico.
442		Code Review	Solicitamos a la entidad informar si es posible hacer escaneos SAST en caso de ser un numero muy grande de líneas de codigo que tengan que revisarse en el alcance del proyecto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el servicio se requiere para cincuenta (50) aplicaciones.
443	1,3	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.	Se solicita a la entidad aclarar que no se realizaran cambios sobre la platafroma actual IBM QRADAR durante el inicio de contrato. En caso de requerirse actualización y/o cambio de versión deberá asumirlo la entidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor deberá realizar labores de gestión, administración y operación del SIEM de la Entidad, indicando que se cuenta con el respectivo soporte de fabricante.
444	Equipo Mínimo de Trabajo	NOTA 2:Todo el personal del SOC requerido para la implementación, operación, gestión, monitoreo, soporte, garantía, entre otros, deberá ser propio evitando figuras de tercerización, sin embargo se aclara que el CONTRATISTA se podrá apoyar con recursos (personal) directamente del fabricante para la etapa de implementación.	Se solicita amablemente a la entidad revisar y ajustar el presente requerimiento, con el fin de permitir el uso de esquemas de tercerización o prestación de servicios. En este sentido, se propone permitir la participación de oferentes que integren esquemas de tercerización, siempre que se asegure el cumplimiento integral de los requisitos técnicos, operativos y de seguridad establecidos por la entidad.Estos modelos son ampliamente utilizados en el entorno colombiano y se encuentran debidamente habilitados dentro del marco legal vigente.		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.
445	15	Sesión de Aclaraciones	Se solicita a la entidad especificar la profundidad y duración de la transferencia de conocimiento requerida para su equipo interno? ¿Hay certificaciones o niveles de habilidad específicos que esperan que su equipo alcance después de la transferencia?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características requeridas para la transferencia de conocimiento se encuentran detalladas en el anexo técnico.
446	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	Sugerimos respetuosamente a la Entidad que en el Anexo Tecnico Equipo de trabajo mínimo habilitante sea modificado para así garantizar pluralidad de profesionales y oferentes. -Sean agregados los siguientes posgrados al perfil, Seguridad de Redes Telemáticas o Seguridad informática o Ciberseguridad o Seguridad de las Tecnologías de la Información y de las Comunicaciones Los cuales son afines al solicitado y está relacionado según el SNIES a las actividades a desarrollar.	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 o Seguridad de Redes Telemáticas o Seguridad informática o Ciberseguridad o Seguridad de las Tecnologías de la Información y de las Comunicaciones 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	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.
447	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.	Sugerimos respetuosamente a la Entidad que en el Anexo Tecnico Equipo de trabajo mínimo habilitante sea modificado para así garantizar pluralidad de profesionales y oferentes. -Sean agregados los siguientes posgrados al perfil Gerencia de Proyectos de Telecomunicaciones o Seguridad de Redes Telemáticas o Seguridad informática o Ciberseguridad o Seguridad de las Tecnologías de la Información y de las Comunicaciones Los cuales son afines al solicitado y está relacionado según el SNIES a las actividades a desarrollar.	Especialista de Respuesta a Incidentes (IR) Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Seguridad Informática o Seguridad de Redes Telemáticas o Seguridad informática o Ciberseguridad o Seguridad de las Tecnologías de la Información y de las Comunicaciones 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.	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.

448	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.	Sugerimos respetuosamente a la Entidad que en el Anexo Tecnico Equipo de trabajo mínimo habilitante sea modificado para así garantizar pluralidad de profesionales y oferentes. -Sean agregados los siguientes posgrados al perfil, Gerencia de Proyectos de Telecomunicaciones o Seguridad de Redes Telemáticas o Seguridad informática o Ciberseguridad o Seguridad de las Tecnologías de la Información y de las Comunicaciones Los cuales son afines al solicitado y está relacionado según el SNIES a las actividades a desarrollar.	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 o Gerencia de Proyectos de Telecomunicaciones o Seguridad de Redes Telemáticas o Seguridad informática o Ciberseguridad o Seguridad de las Tecnologías de la Información y de las Comunicaciones -Certificación vigente como analista o profesional o arquitecto en seguridad de redes o su equivalente en las soluciones ofertadas (SIEM, SOAR, Caza de Amenazas, NDR o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. -Certificación en gestión o administración de plataformas de seguridad informática. Certificaciones de experiencia mínima de 5 años en implementar y/o soportar y/o administrar soluciones de seguridad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
449	III	Capacitación y transferencia de conocimiento. El CONTRATISTA deberá desarrollar e implementar actividades de capacitación y transferencia de conocimiento que incluyan, como mínimo: 7.1. Servicios de capacitación y formación en ciberseguridad. El CONTRATISTA deberá proponer y realizar un plan de capacitación general dirigido a los grupos específicos que la OSI considere: 1. Se deberán realizar cinco (5) capacitaciones para la obtención de los certificados relacionados a continuación. Las capacitaciones serán dictadas para cinco (5) ingenieros cada una, los cuales serán designados por la DIAN. Cada capacitación deberá contar con sus respectivos vouchers para la certificación y serán dictadas en un centro de capacitación certificado. • CISSP -Certified Information Systems Security Professional • Certified Information Security Manager (CISM) • EC-Council Certified Encryption Specialist (ECES) • Certified Ethical Hacker (CEH) – EC-Council • Cisco Certified Network Associate (CCNA)	Solicitamos aclarar si las capacitaciones son 5 de cada una para 5 funcionarios para un total de 25 cursos según el listado o si son 5 cualquiera del listado para 5 funcionarios según la que elija el funcionario a participar para un total de 5		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se deberán realizar cinco (5) capacitaciones para cinco (5) ingenieros cada una.
450	III	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. I. CompTIA PenTest+ - CompTIA. J. Cybersecurity Practitioner - CSX-P - ISACA.	Solicitamos aclarar si las capacitaciones son 1 de cada para 20 funcionarios para un total de 220 cursos según el listado o si se elije cualquiera del listado para 20 funcionarios		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, se deben entregar capacitaciones en los temas definidos para mínimo 20 funcionarios.
451	VIII		Teniendo las fechas que estan estipuladas de fabricantes como SIEM, bases de datos e Inteligencia de amenazas (NDR) ,como la entidad garantiza que se puede desarollar el cambio y de que manera se realizará la adquisición de estos nuevos licenciamientos ya que los fabricantes manejan una política de precios en el tiempo que suben gradualmente? como la entidad contempla el aumento de precios en el tiempo, teniendo en cuenta que solo va recibir y pagar las herramientas al momento que caduquen las existentes ?		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.
452	VIII		Si un proponente contemplara la posiblidad de adquirir en este momento el licenciamiento y entregarlos con posterioridad en las fechas esperadas, la entidad solo pagaria en las fechas en que se reciba el licencimiento ? o con el hecho de recibir la carta del fabricante certificado que fueron adquirirdas las licencias y que estas se activiran con posteriridad podria efectuarse el pago de las mismas ?		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, la forma de pago es clara en el sentido que solo se pagaría a la puesta en producción de cada uno de los servicios requeridos.
453	Sección VII. Condiciones Generales del Contrato (CGC	11.1 El Proveedor permitirá, y realizará todos los trámites para que sus Subcontratistas permitan, que el Banco y/o las personas designadas por el Banco inspeccionen todas las cuentas y registros contables del Proveedor y sus Subcontratistas relacionados con el proceso de licitación y la ejecución del contrato y realice auditorías por medio de auditores designados por el Banco, si así lo requiere el Banco. El Proveedor y los Subcontratistas deberán prestar atención a lo estipulado en la Cláusula 3 de las CGC "Prácticas Prohibidas", según la cual las actuaciones dirigidas a obstaculizar significativamente el ejercicio por parte del Banco de los derechos de inspección y auditoría consignados en ésta Subcláusula 11.1 constituye una Práctica Prohibida que podrá resultar en la terminación del contrato (al igual que en la declaración de inelegibilidad de acuerdo a los procedimientos vigentes del Banco).	De conformidad con las políticas globales de Deloitte, no nos es posible aceptar cláusulas que contemplen auditorías e inspecciones a nuestras cuentas y registros contables por parte de terceros. En consecuencia, solicitamos amablemente la eliminación del numeral 11.1 (o su ajuste correspondiente)."		No es posible modificar este apartado ya que es un estándar 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.
454	Sección II. Datos de la Licitación (DDL)	La fecha límite para presentar las ofertas es: Fecha: 14 de mayo de 2026 Hora: hasta las 10:00 am (hora legal colombiana)	Respetuosamente solicitamos una prórroga a la fecha límite para la presentación de ofertas, actualmente establecida para el 14 de mayo, en la medida en que requerimos contar con las respuestas a las observaciones presentadas a fin de estructurar y consolidar adecuadamente nuestra propuesta.	Modificar la fecha límite de presentación de ofertas del 14 de mayo al 29 de mayo (y ajustar el cronograma del proceso en consecuencia).	La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, la fecha de entrega de ofertas se modificó mediante adenda.

455	Sección VI. Requisitos de los Bienes y Servicios Conexos	A partir de la terminación de las fechas mencionadas, el contratista 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:	Agradecemos aclarar si nuestro entendimiento es el correcto. Teniendo en cuenta las definiciones de fechas para cada una de las tecnologias que requiere la entidad, solicitamos claridad respecto a que el periodo solicitado de licenciamiento debe ser de 3 años (36 meses), una vez termine el periodo mencionado del licenciamiento en curso. Esto implicaria que el licenciamiento para algunas de las tecnologias tenga una fecha de vencimiento entre el año 2030 y 2031.	Solicitamos considerar una unica fecha de finalización del licenciamiento de las distitnas tecnologias, para evitar una desalineación que represente escenarios mas complicados de renovación de las mismas.	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 item 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.
456	Sección VI. Requisitos de los Bienes y Servicios Conexos	A partir de la terminación de las fechas mencionadas, el contratista 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:	Agradecemos aclarar si nuestro entendimiento es el correcto. Teniendo en cuenta las definiciones de fechas para cada la prestación de servicios solicitamos claridad respecto a que el periodo solicitado de servicios tiene como vencimiento el 10/30/2028. Adicionalmente aclarar si los periodos de implementación deben ser igualmente considerados como parte del periodo de operación.	NA.	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 item 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. La implementación no hace parte del período de operación.
457	Sección VI. Requisitos de los Bienes y Servicios Conexos	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 CONTRATISTA deberá proveer el hardware requerido, considerando siempre el cumplimiento del anexo de características técnicas mínimas requeridas.	Solicitamos amablemente aclarar si es posible que las tecnologias ofertadas sean 100% en modalidad SAAS. De lo contrario agradecemos confirmar si la entidad será responsable del alocation (rack, puntos de red, alimentación energetica, espacio en datacenter, entre otros).	NA.	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.
458	Sección VI	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 a la entidad este criterio debería ampliarse para incluir también fabricantes clasificados como Strong Performers en Forrester o contemplar otros estudios de mercado, tal como se propuso previamente. Por lo tanto se solicita permitir contemplar estudios de Gartner tales como Exposure Assessment Platforms ya que corresponde a un complemento de la gestión de las vulnerabilidades y es solicitado dentro del pliego como parte de una plataforma de ciberexposición. Lo anterior, considerando que en la evaluación actualmente citada el único fabricante ubicado como líder es Tenable, lo que limita la libre competencia y restringe la participación de otras soluciones con capacidades igualmente competitivas.	La solución ofertada deberá ser provista por un fabricante clasificado en el cuadrante de Líderes de Gartner o Strong Performers de Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management) ó última evaluación de gartner para (Exposure Assessment Platforms).	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.
459	Sección VI	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 modificar el requisito para que la implementación y despliegue de la solución de Gestión de Vulnerabilidades pueda ser realizada por el personal certificado del proponente, acreditando que dicho personal cuenta con las certificaciones vigentes emitidas por el fabricante para tal fin.	Se debe ofrecer despliegue de fabricante o mediante personal de proponente certificado 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.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad.
460	Sección VI	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	La plataforma CNAPP propuesta integra de forma unificada los siguientes componentes: CSPM, que proporciona cumplimiento continuo con marcos como PCI DSS 4.0, HIPAA, NIST 800-53/171 y GDPR; CWPP, que ofrece priorización de riesgos basada en explotabilidad, criticidad y análisis de rutas de ataque; CIEM, que visualiza y aplica el principio de acceso de privilegio mínimo; CDR, que detecta malware sin archivos y comportamiento anómalo mediante monitoreo eBPF con playbooks de respuesta automatizada; IaC/DevSecOps y SSPM. El conjunto de capacidades requeridas en el ítem 5.11.1 se encuentra cubierto al 100%, a excepción del componente DSPM. En relación con este último, se solicita respetuosamente a la entidad considerar el cumplimiento de DSPM (Data Security Posture Management) como requisito deseable y no eliminatorio, dado que esta capacidad se encuentra actualmente en el roadmap del fabricante.	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),deseable 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	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad.
461	Sección VI	El CONTRATISTA deberá conformar y mantener un equipo de trabajo para la ejecución del contrato, compuesto por perfiles especializados ajustados al proyecto. Este equipo deberá organizarse según los roles, perfiles, componentes o soluciones a desarrollar/implementar, e integrarse por recurso humano propio y, cuando se requiera, por expertos externos.	Con respecto a la conformación del equipo de trabajo y el equipo clave mínimo, se solicita aclarar si la prestación del servicio se realizará bajo modalidad presencial, remota o híbrida. En caso de requerirse presencialidad, se solicita especificar si esta aplica para la totalidad del equipo o únicamente para el Equipo Clave Mínimo en las instalaciones de la DIAN, y si existen roles (como analistas de CTI o SOC) que puedan operar de forma remota.	No aplica	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.

462	Sección VI	Tres (03) Analistas SOC Nivel I Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 2 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: -Cédula de Ciudadanía -Tarjeta Profesional -Certificación vigente como analista o profesional o especialista o arquitecto en seguridad de operaciones o su equivalente en las soluciones ofertadas (SIEM, SOAR, caza de amenazas o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. - Certificación en Plataformas de Gestión de la Superficie de Ataque. - Certificaciones de experiencia mínima de dos (2) años en implementación y/o soporte y/o administración de soluciones de seguridad. NOTA: Estos tres perfiles (analista I) deben cumplir los ANS de 7x24x365	Se solicita amablemente a la Entidad eliminar el requisito de Certificación en Superficie de Ataque para los perfiles de Analista SOC Nivel I y Nivel II, dado que no guarda relación con las funciones operativas de dichos cargos. Esta exigencia está ligada a un grupo muy limitado de herramientas específicas en el mercado, lo que impide la participación de profesionales altamente calificados en las demás soluciones de monitoreo solicitadas y restringe injustificadamente la pluralidad de oferentes en este proceso internacional.	Tres (03) Analistas SOC Nivel I Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 2 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: -Cédula de Ciudadanía -Tarjeta Profesional -Certificación vigente como analista o profesional o especialista o arquitecto en seguridad de operaciones o su equivalente en las soluciones ofertadas (SIEM, SOAR, caza de amenazas o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. - Certificaciones de experiencia mínima de dos (2) años en implementación y/o soporte y/o administración de soluciones de seguridad. NOTA: Estos tres perfiles (analista I) deben cumplir los ANS de 7x24x365	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad.
463	Sección VI	El CONTRATISTA deberá conformar y mantener un equipo de trabajo para la ejecución del contrato, compuesto por perfiles especializados ajustados al proyecto. Este equipo deberá organizarse según los roles, perfiles, componentes o soluciones a desarrollar/implementar, e integrarse por recurso humano propio y, cuando se requiera, por expertos externos.	Respecto al requerimiento del equipo mínimo de trabajo para los tres (03) Analistas SOC Nivel I, y considerando que este proceso corresponde a una licitación internacional, se solicita respetuosamente a la entidad, permitir la participación de personal que se tiene distribuido en la región que apoya el SOC en Bogotá. Además agradecemos confirmar que tratamiento se le da frente al requerimiento de la targeta profesional.	No aplica	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad.
464	Sección VI	El CONTRATISTA deberá conformar y mantener un equipo de trabajo para la ejecución del contrato, compuesto por perfiles especializados ajustados al proyecto. Este equipo deberá organizarse según los roles, perfiles, componentes o soluciones a desarrollar/implementar, e integrarse por recurso humano propio y, cuando se requiera, por expertos externos.	Para el equipo del SOC requerido,si solicita a la entidad confirmar si se pueden anexar las hojas de vidas y demostrar que son recursos propios del oferente al momento de la firma del contrato.	No aplica	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los perfiles solicitados y sus hojas deben ser presentados por el oferente ganador cuando se adjudique el contrato.
465	Sección VI	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 a la entidad flexibilizar los requisitos de Postgrado e ITIL V3 para el perfil de Especialista IR, permitiendo su cumplimiento mediante certificaciones técnicas de ciberseguridad o experiencia adicional. Justificación: Idoneidad: Las certificaciones de seguridad validan competencias técnicas de remediación de vulnerabilidades y contención de ataques, las cuales son más pertinentes para este rol que el marco administrativo de ITIL o un postgrado académico. Equivalencia Legal: Según el Decreto 1083 de 2015, es estándar permitir la compensación de títulos de postgrado por años de experiencia relacionada. Solicitud: Solicitamos modificar los requisitos del perfil permitiendo las siguientes equivalencias: Para el Postgrado: Acreditar dos (2) años adicionales de experiencia profesional relacionada. Para el ITIL: Acreditar una (1) certificación técnica vigente en ciberseguridad, tales como: CEH (Certified Ethical Hacker), CompTIA Security+, ECIH (EC-Council Certified Incident Handler), CompTIA CySA+, CSA (Certified SOC Analyst - EC-Council)	Especialista de Respuesta a Incidentes (IR) Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Certificaciones vigentes: Acreditar una (1) certificación técnica vigente en ciberseguridad, tales como: CEH (Certified Ethical Hacker), CompTIA Security+, ECIH (EC-Council Certified Incident Handler), CompTIA CySA+, CSA (Certified SOC Analyst - EC-Council) Postgrado: Acreditar dos (2) años adicionales de experiencia profesional relacionada 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.	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.
466	Sección VI	**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 amablemente a la entidad eliminar el requisito certificación en gestión de plataformas de seguridad informática , ya que se presenta una duplicidad con el requisito de 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.	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. Certificaciones de experiencia mínima de 5 años en implementar y/o soportar y/o administrar soluciones de seguridad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
467	Sección VI	**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	Solicitamos a la entidad que, para el perfil de Líder / Coordinador SOC, se acepte como equivalente a la certificación PMP la presentación de: Certificación Scrum Master, en conjunto con Certificación de liderazgo o gestión en ciberseguridad tipo LCSP (Lead Cybersecurity Professional) o similares Adicional que se permita como equivalente al postrado en gerencia de proyectos el posgrado en seguridad informática ya que ratifica las habilidades que se deben tener para ser un líder o coordinador SOC.	**Líder /Coordinador SOC** Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Gerencia de proyectos ó posgrado en seguridad informática o similares Certificaciones vigentes: •Certificación Scrum Master, en conjunto con Certificación de liderazgo o gestión en ciberseguridad tipo LCSP (Lead Cybersecurity Professional) o similares 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	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.

468	Sección VI	**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 ampliar el requisito de posgrado para el perfil de Threat Hunter / Analista de Ciber Inteligencia, incluyendo denominaciones equivalentes reconocidas por el Ministerio de Educación Nacional, tales como Especialización o Maestría en Seguridad de las Tecnologías de la Información y las Comunicaciones, Ciberseguridad o Seguridad Digital, dado que estas forman profesionales con competencias iguales o superiores a las requeridas para las funciones del perfil, garantizando así la pluralidad de oferentes sin reducir el nivel académico exigido.	**Threat Hunter / Analista de Ciber inteligencia** Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado:Especialización o Maestría en Seguridad de las Tecnologías de la Información y las Comunicaciones, Ciberseguridad o Seguridad Digital 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	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.
469	SECCION III	d. Metodología para el cálculo de ROSI (Retorno a la inversión en seguridad de la Información).	El criterio de calificación para obtener los 12 puntos exige "precisión en la estimación" y "facilidad de comunicación ante la alta dirección". Bajo este estándar, ¿Estaría dispuesta la entidad a aceptar y valorar con el máximo puntaje metodologías que operen mediante modelado dinámico en tiempo real (basado en FAIR) e integradas a las plataformas de seguridad, permitiendo generar reportes de ROSI y ALE actualizados permanentemente para la Alta Dirección, en lugar de reportes estáticos trimestrales o a demanda?	Teniendo en cuenta el inventario relacionado en el anexo técnico y los compontes de ciberseguridad con los que cuenta y que involucran el proyecto en asunto, sumando que los riesgos de cinerseguridad son cada vez mas. dinamicos y cada vez el riesgo es mas alto, es recomendable incluya reportes y tableros ejecutivos en tiempo real	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.
470	SECCION III	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.	Tratandose de un proyecto que abarca varias capacidades y servicios, es importante que estos esten cubiertos en los procesos de la ISO27001.	Sugerencia: Asignar puntaje a la ISO 27001 que cubra el mayor numero de capacidades, Ejemplo: Gestion Vulnerabildiades, Gestion Amenzas, Gestion Plataformas etc Esto permitira garantizar: Alineación Técnica: Si los procesos, datos y activos involucrados en estos servicios se encuentran plenamente cubiertos por los controles vigentes del SGSI. Identificación de Brechas (Gaps): Detectar si existen componentes de los servicios que queden fuera del perímetro certificado, lo que podría representar un riesgo no mitigado para la entidad. Optimización del Cubrimiento: Evaluar las acciones necesarias para extender o ajustar el alcance, asegurando que la protección de la certificación sea integral y no parcial. Considero que esta evaluación es un paso preventivo indispensable para evitar silos de información no protegidos y para asegurar que la inversión en estos servicios esté respaldada por nuestros estándares internacionales de seguridad.	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.
471	Sección IV	El SIEM deberá ser implementado a partir de septiembre 1 de 2027 con licenciamiento soporte, garantía y derecho a uso hasta septiembre de 2030. • La protección de bases de datos (Firewall de bases de datos) 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. • 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	Entendiendo que los requisitos de ciberseguridad y cumplimiento regulatorio pueden evolucionar en los próximos años: ¿Se permitirá un proceso de 'actualizacion de cotizacion' sin penalización para ajustar la arquitectura técnica a los estándares vigentes en el momento de la activación efectiva? ¿Permitirá un ajuste de costo basado en índices de mercado o variaciones de fabricante, con un tope máximo de protección del [15-20%]?	No aplica	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.
472	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 solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
473	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 deben estar vigentes para la puntuación y mantenerse vigentes durante la operación del SOC.
474	7,3	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 solicitada es por 25000, las cantidades se corrigieron mediante adenda.

475	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 solicitada es por 25000, los documentos fueron ajustados mediante adenda.
476	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 al observante que, la operación será hasta octubre 31 de 2028, quedó modificado mediante adenda.
477	Seccion VI	Forma de pago El valor del contrato será pagado de la siguiente manera:.....	Se solicita aclarar el esquema de pagos del contrato, incluyendo periodicidad, condiciones de facturación y tiempos estimados de pago, con el fin de evaluar adecuadamente la estructuración financiera de la oferta	NA	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los pagos se realizarán a medida de que el futuro proveedor de SOC vaya realizando la implementación y puesta en operación de cada uno de los servicios y capacidades SOC requeridas por la Entidad.
478	Seccion VI	Si bien el documento técnico describe el alcance del proyecto, no se evidencia con total claridad la distribución del plazo contractual entre las fases de implementación y operación, ni los hitos asociados a cada una de ellas. Esta definición resulta clave para la estructuración técnica, operativa y financiera de la oferta, en la medida en que los costos, recursos y riesgos asociados difieren significativamente entre dichas fases. Por lo anterior, respetuosamente solicitamos a la Entidad: Precisar el plazo total del contrato, Detallar la duración de cada fase (implementación y operación), y Indicar los hitos de inicio de operación y aplicación de niveles de servicio (SLA). Lo anterior con el fin de permitir una adecuada planificación y estructuración de la propuesta.	NA		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la operación, seguimiento, gestión, monitoreo y administración por parte del futuro proveedor de todos los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho a uso, licenciamiento, suscripciones, actualizaciones, soporte y garantía irá por tres (3) años y sus periodos se contabilizarán a partir de la puesta en operación de cada uno de los servicios requeridos, incluyendo lo siguiente: Tener en cuenta que desde el inicio del contrato se deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, una vez esto ocurra, se deberá implementar, administrar y operar a partir del 1 de septiembre de 2027 nuevo SIEM (solicitado en el item 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. El tiempo máximo de implementación es de cuatro (4) meses para el proyecto.
479	Anexo Técnico Proyecto SOC DIAN (Equipo Mínimo de Trabajo) NOTA 2:	**NOTA 2:**Todo el personal del SOC requerido para la implementación, operación, gestión, monitoreo, soporte, garantía, entre otros, deberá ser propio evitando figuras de tercerización, sin embargo se aclara que el CONTRATISTA se podrá apoyar con recursos (personal) directamente del fabricante para la etapa de implementación.	Se solicita amablemente a la entidad modificar el presente requerimiento, permitiendo el uso de esquemas de tercerización o prestación de servicios, toda vez que estos modelos son ampliamente utilizados en el territorio colombiano y se encuentran permitidos dentro del marco legal vigente. La restricción de exigir personal exclusivamente propio puede limitar la pluralidad de oferentes y la libre competencia, al excluir modelos operativos válidos que garantizan calidad, especialización y cumplimiento de los niveles de servicio requeridos. En este sentido, se propone permitir la participación de oferentes que integren esquemas de tercerización, siempre que se garantice el cumplimiento de los requisitos técnicos, operativos y de seguridad exigidos por la entidad.		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.
480	8,21	El CONTRATISTA 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 desbordas que muestre la respectiva herramienta. El CONTRATISTA debe poner a disposición el recurso humano para generar planes de acción sobre la información reportada en la herramienta.	Se solicita amablemente a la entidad aclarar el alcance del requerimiento establecido en el ítem 8.21, particularmente en lo relacionado con la gestión y remediación de vulnerabilidades, toda vez que puede interpretarse como una obligación directa del CONTRATISTA sobre la ejecución de dichas actividades. Lo anterior, considerando que en el ítem 8.17 se establece que el CONTRATISTA brindará acompañamiento, apoyo y experticia, siendo el personal de la DIAN quien estará al frente de las actividades de remediación. En este sentido, se evidencia una posible ambigüedad entre ambos ítems, por lo que se solicita precisar que el alcance del CONTRATISTA en las actividades de remediación corresponde a un rol de acompañamiento, asesoría y generación de planes de acción, y no a la ejecución directa de las acciones de remediación. Lo anterior con el fin de garantizar una correcta delimitación de responsabilidades y una adecuada estructuración de la oferta.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor deberá realizar el acompañamiento desde el inicio y hasta la solución de las acciones de remediación, tal como se indica en el anexo técnico, así mismo generar los planes de acción correspondientes para la ejecución de las acciones de remediación, el equipo de seguridad de la Entidad será el responsable de llevar a cabo las labores propias de intervención en las plataformas tecnológicas de la Entidad.

481	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.	Se solicita amablemente a la entidad aclarar el alcance del servicio de gestión y remediación indicado en el presente ítem, en particular respecto al rol del CONTRATISTA dentro de las actividades de remediación de vulnerabilidades. Lo anterior, considerando que el texto menciona el apoyo para "resolver todos los casos a remediar", lo cual podría interpretarse como ejecución directa; sin embargo, en otros apartados del documento se establece que estas actividades son lideradas por los equipos internos de la entidad. En este sentido, se entiende que el alcance del CONTRATISTA corresponde a la generación de planes de acción, análisis, priorización y acompañamiento técnico durante el proceso de remediación, siendo la ejecución de las actividades responsabilidad de los equipos designados por la entidad. Se solicita confirmar si esta interpretación es correcta, con el fin de asegurar una adecuada delimitación del alcance del servicio y una correcta estructuración de la propuesta.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara el observante que, el futuro proveedor deberá realizar el acompañamiento desde el inicio y hasta la solución de las acciones de remediación, tal como se indica en el anexo técnico, así mismo generar los planes de acción correspondientes para la ejecución de las acciones de remediación, el equipo de seguridad de la Entidad será el responsable de llevar a cabo las labores propias de intervención en las plataformas tecnológicas de la Entidad.
482	410-Solicitud-de-Oferta-VSD-SdO-SOC Pagina 123	6.1. Procedimiento de Cambio de Perfiles 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: • 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 • 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. • El contratista deberá garantizar la transferencia de conocimiento entre la persona remplazada y quien lo remplaza. • La DIAN se reserva el derecho a solicitar por escrito el remplazo motivado de profesionales que no se acoplen al equipo de trabajo o que sus condiciones técnicas, profesionales, gerenciales o de resultados no satisfagan las necesidades del proyecto. Esta solicitud podrá realizarla la Supervisión del contrato. • El contratista tendrá máximo diez (10) días hábiles para presentar por escrito el remplazo, el cual deberá tener un perfil igual o superior al del profesional que fue presentado para la ejecución del contrato. • Reporte de Cambio: El CONTRATISTA deberá documentar el cambio en un reporte que incluya las razones del reemplazo, detalles del perfil de reemplazo, y las acciones tomadas para garantizar la continuidad del servicio. Este reporte será entregado a la DIAN para su archivo y seguimiento.	Se solicita amablemente a la entidad ajustar el plazo establecido para la presentación de reemplazos de personal, ampliándolo hasta sesenta (60) días calendario, teniendo en cuenta que los perfiles requeridos corresponden a cargos de alta responsabilidad y especialización. Lo anterior, considerando que, ante situaciones de fuerza mayor no atribuibles al CONTRATISTA, los procesos de selección, validación y contratación de este tipo de perfiles pueden implicar tiempos superiores, debido a la necesidad de realizar estudios previos, verificaciones de antecedentes, evaluaciones técnicas y procesos de seguridad de la información, con el fin de garantizar la idoneidad del recurso y la confidencialidad de la información de la entidad. Adicionalmente, se precisa que el servicio SOC se presta bajo un esquema continuo 7x24, soportado por un equipo de trabajo estructurado, lo cual garantiza la continuidad operativa del servicio mientras se surte el proceso de reemplazo del personal requerido. En este sentido, el plazo actualmente establecido podría resultar insuficiente y afectar la adecuada gestión del recurso humano especializado. Por lo anterior, se solicita considerar un plazo de hasta sesenta (60) días calendario para la presentación del reemplazo, garantizando así un proceso riguroso y alineado con las buenas prácticas de seguridad y gestión del talento humano.		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.
483	1,3	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.	Se solicita amablemente a la entidad revisar el esquema de implementación y pagos de las plataformas SIEM, Firewall de bases de datos y NDR, considerando que el modelo actual, con adquisiciones diferidas en el tiempo, genera impactos financieros que pueden trasladarse a la oferta económica. Lo anterior, debido a que el proponente debe asumir riesgos asociados a proyecciones futuras, tales como variación de precios, tasas de cambio y condiciones de licenciamiento, lo cual puede derivar en sobrecostos para la entidad o en riesgos durante la ejecución del contrato. Por lo anterior, se sugiere considerar que el pago de estas plataformas se realice desde las fases iniciales del proyecto, permitiendo una mejor estructuración financiera y optimización de los recursos.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los pagos se realizarán a medida de que el futuro proveedor de SOC vaya realizando la implementación y puesta en operación de cada uno de los servicios y capacidades SOC requeridas por la Entidad.
484	7	Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas	En el Anexo Técnico se describen las capacidades y alcances funcionales de la solución NDR; sin embargo, no se especifica de manera explícita la cantidad de Datacenters (principales, alternos o de contingencia) que deberán ser cubiertos por dicha solución, ni si su alcance debe incluir todos los Datacenters de la Entidad de forma simultánea o únicamente aquellos definidos como críticos. Solicitamos amablemente nos indiquen en que Datacenter se instalaría la solución de NDR		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los servicios deben prestarse para la infraestructura tecnológica de la Entidad, si algunos de sus ofrecimientos serán onpremise y requieren instalarse en las instalaciones de la Entidad, deberán estar en el datacenter principal, recordando que dicha infraestructura quedará a nombre de la Entidad.

485	7	Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas	Si bien en el Anexo Técnico se solicita una solución NDR (Network Detection and Response) y se describen ampliamente las capacidades asociadas a la detección, análisis y visibilidad del tráfico de red, no se evidencia de manera clara y explícita el alcance correspondiente a la fase de respuesta y contención, propia de este tipo de soluciones. En particular, no se especifica: •Qué tipo de acciones de respuesta se espera que realice la solución NDR ante la detección de una amenaza. •Si la respuesta y contención debe realizarse: oa través de integración con la infraestructura de seguridad existente de la DIAN omediante bloqueos o acciones directas ejecutadas por el propio componente NDR, o ouna combinación de ambos mecanismos. Se solicita respetuosamente a la Entidad aclarar y precisar el alcance de la funcionalidad de respuesta y contención requerida para la solución NDR, indicando como mínimo: •Qué tipos de acciones de respuesta y/o contención deben ser soportadas. •Si dichas acciones deben realizarse exclusivamente mediante integración con la infraestructura de seguridad de la DIAN, directamente desde la solución NDR, o mediante ambos esquemas. •El nivel de automatización esperado en dichas respuestas (manual, semiautomática o automática).		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las especificaciones de la solución NDR están detalladas en el anexo técnico.
486	7	Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas	En el mercado actual existen múltiples fabricantes y soluciones de ciberseguridad que intentan incorporar o emular funcionalidades asociadas a NDR (Network Detection and Response); sin embargo, no todas estas soluciones corresponden realmente a una tecnología NDR madura, ni cuentan con el reconocimiento del mercado o el aval de firmas de análisis especializadas como una solución NDR propiamente dicha. Si bien en el Anexo Técnico se detallan múltiples capacidades asociadas al monitoreo, detección y análisis del tráfico de red, no se establece un criterio claro que permita garantizar que la solución ofertada sea efectivamente una plataforma NDR reconocida, y no una funcionalidad parcial incluida dentro de otro tipo de tecnología (por ejemplo, IDS, NetFlow, NPM, SIEM extendido u otras aproximaciones). Esta situación puede generar el riesgo de que la Entidad no adquiera una solución NDR real, tal como lo solicita expresamente en las fichas técnicas, afectando los objetivos de detección avanzada, análisis basado en comportamiento e inteligencia artificial, y respuesta ante amenazas en la red. Se solicita respetuosamente a la Entidad establecer como criterio de validación que la solución NDR ofertada corresponda a una tecnología reconocida en el mercado, solicitando que: •La solución NDR se encuentre posicionada en al menos uno de los cuadrantes de Gartner en NDR. •O, en su defecto, que se trate de una solución NDR líder en Gartner, lo cual deberá ser soportado mediante documentación		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.
487	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.	Se solicita amablemente a la entidad considerar el presente requerimiento, en el sentido de que el costo asociado al soporte actualizado por un (1) año de las licencias entregadas a perpetuidad para los casos donde aplique sea asumido por el nuevo contratista que entre a operar el servicio. Lo anterior, considerando que dicho soporte estará directamente relacionado con la operación, administración y continuidad del servicio bajo la responsabilidad del nuevo operador, por lo que no resultaría proporcional trasladar este costo al contratista saliente. En este sentido, se sugiere que el contratista actual realice la entrega de las licencias a perpetuidad en correcto estado operativo, y que el soporte posterior sea gestionado y asumido por el nuevo contratista, garantizando así una adecuada distribución de responsabilidades y optimización de costos para la entidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se deberá licenciar por un (1) año más, sólo se contemplan tres (3) años, 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.
488	Sección III. Criterios de Evaluación y Calificación	b. 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.	Solicitamos a la entidad permitir que se avalen las membresías de los productos, servicios o plataformas en al menos los tres niveles más altos, ya que los fabricantes poseen diferentes mecanismos de categorías. Por ejemplo existen fabricantes que categorizan el nivel de mebresía en Expert, Advanced, etc y otros en Platinum, Silver, etc, lo cual no es uniforme en todos los fabricantes.	b. El oferente deberá acreditar su pertenencia a los dos niveles más altos de membresía por parte de las fabricantes de los productos, servicios, plataformas o licenciamientos ofrecidos y requeridos por la DIAN, para tal efecto, el oferente deberá informar los mecanismos suficientes para corroborar dicha información.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta su sugerencia, sin embargo se aclara que el ítem fue modificado mediante adenda, quedando de la siguiente manera: b. El oferente, para poder acceder a esta puntuación, deberá acreditar que se encuentra en la membresía más alta concedida por el o los fabricantes de los productos, servicios, plataformas o licenciamientos que ofrece y que son requeridos por la DIAN. A tal efecto, el oferente deberá indicar los mecanismos suficientes para corroborar dicha información.
489	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 evaluar cúales son los fabricante en el cual debera entregarse el TAM durante la vigencia del contrato, teniendo en cuenta que el servicio a ofertar contempla varios productos y fabricantes, alguno no poseen este servicio.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, literal c en mención es un puntuable, no es obligatorio, el interesado deberá acreditar lo solicitado para puntuar, de acuerdo a los fabricantes ofrecidos.
490	Sección III. Criterios de Evaluación y Calificación	b. Nivel de partner más alto en las capacidades ofertadas (ítems 2 al 9 del anexo técnico).	Solicitamos a la entidad **modificar** el esquema de ponderación de los puntos asociados a este ítem, debido a que se solicitó que se permitieran los tres niveles más altos de membresía de las soluciones incluidas en el servicio. Agradecemos a la entidad, confirmar como espera la entidad ponderar esta categoría debido a que los fabricantes no tienen una mecanismo estandard de categorías y capacidades.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, es un ítem puntuable, el ítem fue modificado mediante adenda quedando de la siguiente manera: b. El oferente, para poder acceder a esta puntuación, deberá acreditar que se encuentra en la membresía más alta concedida por el o los fabricantes de los productos, servicios, plataformas o licenciamientos que ofrece y que son requeridos por la DIAN. A tal efecto, el oferente deberá indicar los mecanismos suficientes para corroborar dicha información.

491	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, literal c en mención es un puntuable, no es obligatorio, el interesado deberá acreditar lo solicitado para puntuar.
492	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 en la sesión de aclaraciones, se evidenció un esquema en donde la operación finaliza en Octtubre de 2028 (Mes 10).		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la operación, seguimiento, gestión, monitoreo y administración por parte del futuro proveedor de los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho de 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, conforme a lo establecido en los documentos del proceso.
493	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Como parte de este proceso, el contratista deberá suministrar el licenciamiento para las nuevas herramientas por un período de tres años, a partir de la fecha de su implementación y acorde a las características solicitadas en el anexo de características mínimas	Solicitamos a la entidad **aclarar** quien realizara las actividades de operación del SIEM, en el periodo de 1 Septiembre 2027 a 31 Agosto de 2030, ya que en este periodo el contrato de la operación a finalizado. Se espera que el oferente entregue la solucion con derecho a uso de este item.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el futuro contratista deberá recibir, gestionar, administrar y operar el SIEM actual de propiedad de la DIAN hasta el 31 de agosto de 2027. A partir del 1 de septiembre de 2027 deberá implementar, administrar y operar el nuevo SIEM requerido en el proceso durante el periodo de operación del contrato. El licenciamiento, soporte, garantía y derecho de uso del nuevo SIEM deberá mantenerse por tres (3) años contados a partir de su puesta en operación, conforme a lo establecido en los documentos del proceso. Una vez finalizada la operación contractual, la solución será entregada a la DIAN en el marco del proceso de devolución del servicio.
494	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Como parte de este proceso, el contratista deberá suministrar el licenciamiento para las nuevas herramientas por un período de tres años, a partir de la fecha de su implementación y acorde a las características solicitadas en el anexo de características mínimas	Solicitamos a la entidad **aclarar** quien realizara las actividades de operación del Firewall de Proteccion de bases de datos, en el periodo de 1 Nov 2028 a Enero de 2031, ya que en este periodo el contrato de la operación a finalizado. Se espera que el oferente entregue la solucion con derecho a uso de este item.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el futuro contratista deberá recibir, gestionar, administrar y operar la solución actual de protección de bases de datos de propiedad de la DIAN hasta el 31 de diciembre de 2027. Posteriormente, deberá implementar, administrar y operar la nueva capacidad de protección de bases de datos requerida en el proceso durante el periodo de operación contractual. El licenciamiento, soporte, garantía y derecho de uso deberá mantenerse por tres (3) años contados a partir de su puesta en operación, conforme a lo establecido en los documentos del proceso. Una vez finalizada la operación contractual, la solución será entregada a la DIAN en el marco del proceso de devolución del servicio.
495	410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf	Como parte de este proceso, el contratista deberá suministrar el licenciamiento para las nuevas herramientas por un período de tres años, a partir de la fecha de su implementación y acorde a las características solicitadas en el anexo de características mínimas	Solicitamos a la entidad **aclarar** quien realizara las actividades de operación del NDR, en el periodo de 1 Ene 2028 a Enero de 2031, ya que en este periodo el contrato de la operación a finalizado. Se espera que el oferente entregue la solucion con derecho a uso de este item. En el anexo tecnico se menciona este parrafo "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." Agradecmos claridad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la capacidad NDR deberá iniciar operación conforme a las fechas establecidas en los documentos del proceso, previa autorización de la Entidad. El contratista deberá implementar, administrar, operar, soportar y garantizar el servicio durante el periodo de operación contractual aplicable, y entregar el licenciamiento, soporte, garantía y derecho de uso por tres (3) años contados a partir de su puesta en operación. Una vez finalizada la operación contractual, la solución será entregada a la DIAN en el marco del proceso de devolución del servicio.
496	Especificaciones Técnicas herramienta de protección de Bases de Datos	Anexo Técnico ItemsVerificables 4,4	Se solicita a la entidad aclarar el inventario de servidores de bases de datos que deberán ser cubiertos por la solución de protección de bases de datos, ya que la información incluida en el inventario de infraestructura no resulta clara al respecto. En el archivo ""410-Solicitud-de-Oferta-VSD-SdO-SOC.pdf"" pagina 98, se mencionan 224 core virtuales de Bases de Datos pero en el Anexo tecnico No mencionan niguna referencia. Por favor acalarar		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el número de servidores de bases de datos que deberán ser cubiertos por el servicio de firewall de bases de datos es de 60 servidores.
497	Sección I. Instrucciones a los Oferentes (IAO)	10. Idioma de la Oferta	Solicitamos a la entidad permitir la traduccion simple del idioma ingles al español en la entrega de especificaciones, fichas técnicas y/o catálogos que están en idioma inglés por parte del fabricante. 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.
498	Sección VIII. Condiciones Especiales de Contrato (CEC)	CGC 16.1 Forma de pago	La forma de pago prevista, condicionada exclusivamente a la entrega y aceptación de entregables concluidos al término de cada capacidad, sin reconocer entregas parciales ni actividades técnicas complementarias, genera un riesgo jurídico y financiero para el contratista, pues limita el flujo económico en proyectos donde el valor se produce de manera progresiva y en fases interdependientes. Al supeditar el pago únicamente al recibo a satisfacción de informes finales, manuales y protocolos, se desconoce la relevancia de tareas como análisis, diseño, pruebas y documentación, que constituyen parte integral del desarrollo y cuya ejecución implica costos reales para el proveedor. Asimismo, la ausencia de plazos máximos para la validación del supervisor puede ocasionar demoras indefinidas en la facturación, afectando la sostenibilidad operativa. En consecuencia, se recomienda ajustar la cláusula para permitir pagos por entregables parciales funcionales debidamente validados, reconocer actividades técnicas complementarias como susceptibles de pago, establecer tiempos definidos para la aceptación de entregables y prever mecanismos de conciliación técnica en caso de desacuerdo, garantizando así un equilibrio contractual y la continuidad del proyecto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, la forma de pago es clara en el sentido que solo se pagaría a la puesta en producción de cada uno de los servicios requeridos, por lo tanto no se acepta su sugerencia.

499	Sección III. Criterios de Evaluación y Calificación	b. 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 observa que el requisito previsto en el literal b, consistente en exigir que el oferente acredite el nivel máximo de membresía respecto de todos los fabricantes de las tecnologías ofertadas, resulta desproporcionado y contrario a los principios de pluralidad de oferentes y libre concurrencia. Dicha exigencia, aplicada de manera acumulativa, restringe de forma significativa la participación en el proceso, en tanto que en el mercado son escasos los integradores que ostentan simultáneamente el más alto nivel de certificación con múltiples fabricantes. En consecuencia, esta condición genera un efecto excluyente que reduce injustificadamente el universo de proponentes, pudiendo comprometer la selección objetiva, sin que ello implique necesariamente una mejor ejecución contractual, al no estar directamente relacionada con la capacidad técnica del oferente. En virtud de lo anterior, y en aplicación de los principios de proporcionalidad, transparencia y economía, se solicita a la entidad ajustar el requisito, permitiendo que el oferente acredite el nivel máximo de membresía respecto de al menos una de las tecnologías principales, y para las demás, se acepten mecanismos alternativos como certificaciones de partner autorizado o cartas de respaldo del fabricante.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta su sugerencia, sin embargo se aclara que el ítem fue modificado mediante adenda, quedando de la siguiente manera: b. El oferente, para poder acceder a esta puntuación, deberá acreditar que se encuentra en la membresía más alta concedida por el o los fabricantes de los productos, servicios, plataformas o licenciamientos que ofrece y que son requeridos por la DIAN. A tal efecto, el oferente deberá indicar los mecanismos suficientes para corroborar dicha información. 
500	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 al observante que el futuro contratista deberá recibir, gestionar, administrar y operar las soluciones IBM QRadar e IBM Guardium actualmente en operación, conforme a las fechas y condiciones definidas en los documentos del proceso. En particular, QRadar deberá ser operado hasta el 31 de agosto de 2027 y Guardium hasta el 31 de diciembre de 2027, momento a partir del cual deberán implementarse y operarse las nuevas capacidades correspondientes, sin afectar la continuidad del servicio.
501	Sección III. Criterios de Evaluación y Calificación	b. 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 evidencia que la exigencia de contar con el nivel máximo de membresía del fabricante constituye una restricción a la libre concurrencia, en la medida en que condiciona la participación a una habilitación comercial otorgada por un tercero. Esta situación implica que la capacidad de participar no depende exclusivamente de la idoneidad técnica o experiencia del proponente, sino de criterios definidos por fabricantes, lo cual configura una barrera de acceso que puede afectar los principios de transparencia y selección objetiva. En consecuencia, se solicita eliminar la exigencia del nivel máximo de membresía y, en su lugar, permitir la acreditación mediante cartas de respaldo del fabricante para cada tecnología ofertada, garantizando así el soporte técnico y comercial durante la ejecución contractual.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta su sugerencia, por cuanto es un ítem puntuable, sin embargo se aclara que el ítem fue modificado mediante adenda, quedando de la siguiente manera: b. El oferente, para poder acceder a esta puntuación, deberá acreditar que se encuentra en la membresía más alta concedida por el o los fabricantes de los productos, servicios, plataformas o licenciamientos que ofrece y que son requeridos por la DIAN. A tal efecto, el oferente deberá indicar los mecanismos suficientes para corroborar dicha información. 
502	Sección III. Criterios de Evaluación y Calificación	b. 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 a la entidad aclarar los criterios y metodología de ponderación que serán aplicados para la evaluación de la experiencia exigida dentro del proceso.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el literal b fue modificado mediante adenda, quedando de la siguiente manera: b. El oferente, para poder acceder a esta puntuación, deberá acreditar que se encuentra en la membresía más alta concedida por el o los fabricantes de los productos, servicios, plataformas o licenciamientos que ofrece y que son requeridos por la DIAN. A tal efecto, el oferente deberá indicar los mecanismos suficientes para corroborar dicha información.
503	Especificaciones Técnicas Solución de análisis de código estático y dinámico para aplicaciones	En el ciclo de desarrollo las herramientas del CONTRATISTA 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 solicita a la entidad establecer la cantidad de usuarios para los cuales se debe considerar el licenciamiento SASE.		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.
504	Anexo-Tecnico-Proyecto-SOC-DIAN	Especialista de Respuesta a Incidentes (IR)	Se agradece a la entidad ampliar por pluralidad de oferentes ampliar la base para este perfil de la siguiente Manera: Especialista de Respuesta a Incidentes (IR) Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Seguridad Informática o Seguridad de la Información o Afines 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 En cuanto al requisito de posgrado, se propone aceptar no solo "Seguridad Informática" , sino también programas relacionados tales como Ciberseguridad, Seguridad Digital, Gestión de la Seguridad de la Información, Seguridad de la Información, Seguridad de Tecnologías de la Información, Riesgos y Seguridad de la Información, entre otros afines. En el contexto actual, estos programas comparten fundamentos, metodologías y enfoques prácticos orientados a la protección de activos digitales y la gestión de incidentes, por lo que limitar la exigencia a una denominación específica restringe la participación de profesionales con formación equivalente.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los requisitos de formación, certificación y experiencia establecidos para el Especialista de Respuesta a Incidentes - IR obedecen a la criticidad del servicio, al alcance de las actividades de análisis, acompañamiento, remediación y respuesta, y a las necesidades puntuales de la Entidad. Por lo anterior, no se acepta la solicitud.

505	Equipo Mínimo de Trabajo	Gerente de Proyecto	Se agradece a la entidad ampliar por pluralidad de oferentes ampliar la base para este perfil de la siguiente Manera: Gerente de Proyecto Profesional en Ingeniería de sistemas, telemática, electrónica, telecomunicaciones o áreas afines. Con posgrado en Gerencia de Proyectos o en áreas relacionadas tales como: Dirección de Proyectos, Gestión de Proyectos, Administración de Proyectos, Project Management, Gerencia de Tecnologías de la Información (TI), Gerencia de Ingeniería, MBA o programas afines que incluyan formación en gestión de proyectos • PMP Mínimo cinco (5) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales cinco (3) años en Gerencia de proyectos de seguridad de la información , Lo anterior se fundamenta en la necesidad de garantizar el principio de pluralidad de oferentes, promoviendo la participación de un mayor número de proponentes idóneos en el proceso. En el mercado actual, existen múltiples programas de posgrado con enfoques equivalentes en gestión de proyectos, cuyos contenidos académicos desarrollan competencias similares en planificación, ejecución, control y cierre de proyectos, bajo estándares internacionales. Limitar el requisito exclusivamente a una		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los requisitos de formación, certificación y experiencia definidos para el Gerente de Proyecto responden a la complejidad, criticidad, alcance y duración del proyecto SOC. En consecuencia, se mantienen las condiciones establecidas en los documentos del proceso. Por lo anterior, no se acepta la solicitud.
506	Equipo Mínimo de Trabajo	Threat Hunter / Analista de Ciber inteligencia	Se agradece a la entidad ampliar por pluralidad de oferentes ampliar la base para este perfil de la siguiente Manera: Threat Hunter / Analista de Ciber inteligencia Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Gerencia de proyectos o Seguridad Informatica, Ciberseguridad, Seguridad Digital, Gestión de la Seguridad de la Información, Seguridad de la Información, Seguridad de Tecnologías de la Información, Riesgos y Seguridad de la Información, entre otros afines Certificaciones vigentes: • Licensed Penetration Tester (LPT) o similares 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 En cuanto al requisito de posgrado, se propone aceptar no solo "Seguridad Informática" , sino también programas relacionados tales como Ciberseguridad, Seguridad Digital, Gestión de la Seguridad de la Información, Seguridad de la Información, Seguridad de Tecnologías de la Información, Riesgos y Seguridad de la Información, entre otros afines. En el contexto actual, estos		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 solicitud.
507	Equipo Mínimo de Trabajo	QA / Analista de Calidad SOC.	QA / Analista de Calidad SOC. Ingeniería industrial , de sistemas o, telemática o, electrónica o, telecomunicaciones. Postgrado en Gerencia de proyectos o Especialización o Maestría en Gerencia de Proyectos, Gestión de Proyectos, Dirección de Proyectos, Project Management, Gerencia de Programas, Gerencia de Ingeniería, Gerencia de Tecnologías de la Información (TI), Administración de Proyectos, e incluso programas en Gerencia Estratégica o Administración (MBA) con énfasis en proyectos. Certificaciones vigentes: • ISO 9001 o similar 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 Lo anterior se fundamenta en la necesidad de garantizar el principio de pluralidad de oferentes, promoviendo la participación de un mayor número de proponentes idóneos en el proceso. En el mercado actual, existen múltiples programas de posgrado con enfoques equivalentes en gestión de proyectos, cuyos contenidos académicos desarrollan competencias similares en planificación, ejecución, control y cierre de proyectos, bajo estándares internacionales. Limitar el requisito exclusivamente a una denominación específica puede restringir injustificadamente la		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los requisitos establecidos para el perfil QA / Analista de Calidad SOC obedecen a las necesidades de aseguramiento de calidad, seguimiento, control, mejora continua y verificación de los servicios del SOC. Por lo anterior, no se acepta la solicitud.

508	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	El CONTRATISTA 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 desbordas que muestre la respectiva herramienta. El CONTRATISTA debe poner a disposición el recurso humano para generar planes de acción sobre la información reportada en la herramienta.	Se solicita a la entidad aclarar si es correcto entender que las actividades de remediación derivadas de los hallazgos identificados por la herramienta estarán a cargo de los equipos de desarrollo y/o de las áreas responsables de la entidad, siendo el CONTRATISTA un apoyo en la gestión, priorización y seguimiento de dichas actividades. En caso contrario, se agradece especificar si el CONTRATISTA deberá asumir directamente la ejecución de las remediaciones dentro del ciclo de DevSecOps, detallando el alcance, responsabilidades, perfiles requeridos, niveles de acceso y recursos necesarios para su ejecución, con el fin de dimensionar adecuadamente la prestación del servicio. Es importante precisar que la ejecución de actividades de remediación implica capacidades propias de equipos de desarrollo de software, incluyendo análisis, desarrollo, pruebas, gestión de ambientes (laboratorios) y despliegue de aplicaciones, aspectos que no se encuentran definidos dentro del alcance actual. En este sentido, la ausencia de dicha definición puede generar ambigüedades en la asignación de responsabilidades. Adicionalmente, se solicita a la entidad aclarar la posible inconsistencia de este requerimiento frente a lo establecido en el numeral 12.78 del Anexo Técnico Administrativo, con el fin de asegurar coherencia en el alcance contractual		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el acompañamiento en la remediación de vulnerabilidades hace parte del alcance del servicio durante la vigencia contractual. El contratista deberá disponer los recursos necesarios para apoyar la priorización, análisis, generación de planes de acción, seguimiento, soporte y acompañamiento técnico, sin que ello implique la intervención directa sobre plataformas, aplicaciones o servicios de la Entidad. Las acciones de contención, erradicación o remediación sobre activos institucionales las realizará el personal de la Entidad.
509	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	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.	Según lo establecido en el presente numeral, y conforme a lo indicado en el numeral 12.78 – 4. Respuestas, donde se señala que "se deberá reportar de manera oportuna al equipo de seguridad de la Entidad para que pueda contener, erradicar y remediar", entendemos que la ejecución de las acciones de remediación será gestionada ante el equipo de seguridad de la Entidad, quien será el responsable de llevarlas a cabo dichas labores generando los planes de acción correspondiente. Se agradece confirmar, luego una remediación puede la generara la entidad acompañado del SOC del contratista.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que su entendimiento es correcto en cuanto a que la ejecución directa de acciones de contención, erradicación o remediación sobre plataformas, aplicaciones o activos de la Entidad corresponderá a las áreas responsables de la DIAN. No obstante, el contratista deberá apoyar la priorización, análisis, generación de planes de acción, seguimiento, soporte técnico y acompañamiento durante la remediación de las vulnerabilidades identificadas en la prestación del servicio.
510	Formulario 1 lista de precios VSD	Monitoreo a la Gestión de Vulnerabilidades (Ver características en el ítem 5 del anexo).	Se agradece a la entidad aclarar la cantidad de activos luego para el Formulario 1 lista de precios VSD solo indican 18000		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la cantidad definitiva para el licenciamiento de la solución de Gestión de Vulnerabilidades corresponde a veinticinco mil (25.000) activos, conforme a los ajustes realizados mediante adenda. El oferente deberá estructurar su propuesta con base en dicha cantidad y en las condiciones definidas en los documentos del proceso.
511	Formulario 1 lista de precios VSD	NDR - Detección y respuesta en red e Inteligencia de amenazas (Ver características en el ítem 7 del anexo).	Se agradece a la entidad aclarar la cantidad de activos luego para el Formulario 1 lista de precios VSD solo indican 18000		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la cantidad definitiva para el licenciamiento de la capacidad NDR corresponde a veinticinco mil (25.000) dispositivos, conforme a los ajustes realizados mediante adenda. El oferente deberá estructurar su propuesta con base en dicha cantidad y en las condiciones definidas en los documentos del proceso.
512	Formulario 1 lista de precios VSD	Servicios de Monitoreo y operación de SOC con el personal mínimo requerido (Ver características en el ítem 12 del anexo).	Se agradece a la entidad indicar si para todo los 36 meses de servicio se facturaran 30 meses, se agradece aclarar luego esto esta estimado en el Formulario 1 lista de precios VSD		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la operación, seguimiento, gestión, monitoreo y administración por parte del futuro proveedor de los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho de 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, conforme a lo establecido en los documentos del proceso y en el Formulario de Lista de Precios aplicable.
513	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	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.	Se agradece a la entidad especificar si la facturación podrá realizarse una vez implementados los equipos, aun cuando el licenciamiento no se encuentre activado o los equipos no estén en operación. Lo anterior es relevante, en la medida en que esta condición impacta directamente los flujos de caja de los oferentes, incrementando el riesgo financiero asociado al contrato. Adicionalmente el incremento de los componentes como memorias y procesadores que pueden impactar el costo de los mismos en el tiempo.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, la facturación iniciará una vez los servicios sean puestos en operación.
514	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	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.	Teniendo en cuenta las fechas establecidas, se solicita a la entidad aclarar que, una vez finalizado el contrato de servicios, se defina expresamente quién será responsable de gestionar los procesos de RMA en caso de requerirse. Asimismo, se agradece precisar si, en el evento de existir un nuevo proveedor, este asumirá la gestión de dichos RMA o si la entidad reconocerá económicamente los costos asociados a cambios de partes o procesos de RMA correspondientes a equipos suministrados por el proveedor anterior.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el contratista deberá garantizar el soporte, garantía y derecho de uso de las capacidades suministradas por el periodo establecido en los documentos del proceso. Una vez finalizada la operación contractual, las capacidades serán entregadas a la DIAN en el marco del proceso de devolución del servicio, incluyendo la información, soportes, garantías y mecanismos de escalamiento aplicables. La gestión posterior de garantías o RMA se realizará conforme a las condiciones de soporte y garantía contratadas y a los procedimientos que defina la Entidad.
515	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	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.	Se agradece a la entidad especificar el momento exacto en que deberá activarse el incremento adicional de licenciamiento, indicando si este corresponde a la fecha de implementación, puesta en operación, acta de recibo a satisfacción u otro hito contractual definido		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el licenciamiento mínimo requerido para la capacidad SIEM corresponde a dos mil cuatrocientos sesenta y siete (2.467) dispositivos, incluyendo el incremento previsto en los documentos del proceso. Dicho licenciamiento deberá estar disponible desde la implementación y puesta en operación de la capacidad correspondiente, sin perjuicio de la incorporación progresiva de fuentes conforme al plan aprobado por la Entidad.
516	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	Debe tener autoaprendizaje de inventario de activos (CMDB) contando con capacidades de descubrimiento automático para alimentar y mantener actualizada la Base de Datos de Gestión de Configuración (CMDB). Esto implica que el sistema debe ser capaz de identificar, clasificar y registrar de forma dinámica los activos tecnológicos presentes en la infraestructura, incluyendo servidores, estaciones de trabajo, dispositivos de red, aplicaciones y servicios, sin intervención manual constante. Para tal efecto se informa que actualmente la Entidad cuenta con un ITSM del fabricante ARANDA.	Se agradece a la entidad especificar las labores administrativas de integración y Gestión con Aranda ITSM quien sera el encargado. Luego la integracion se realizara por API,	Debe tener autoaprendizaje de inventario de activos (CMDB) contando con capacidades de descubrimiento automático para alimentar y mantener actualizada la Base de Datos de Gestión de Configuración (CMDB). Esto implica que el sistema debe ser capaz de identificar, clasificar y registrar de forma dinámica los activos tecnológicos presentes en la infraestructura, incluyendo servidores, estaciones de trabajo, dispositivos de red, aplicaciones y servicios, sin intervención manual constante. Para tal efecto se informa que actualmente la Entidad cuenta con un ITSM.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la integración con el ITSM institucional podrá realizarse mediante API, conectores, capacidades nativas o desarrollos requeridos por el contratista, siempre que se cumpla la funcionalidad solicitada. El contratista será responsable de implementar, configurar y dejar operativa la integración correspondiente, con el acompañamiento y suministro de la información técnica disponible por parte de la Entidad, bajo los controles de seguridad y confidencialidad aplicables.

517	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	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 agradece a la entidad aclarar si los veinte (20) casos de uso adicionales deberán desarrollarse a lo largo de toda la ejecución del contrato o si corresponden a casos de uso ya existentes y personalizados en el SIEM actual, los cuales deberán ser migrados durante el plazo contractual.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que para la fase de implementación se deberán desarrollar y ejecutar veinte (20) casos de uso, los cuales podrán ser propuestos por el contratista y deberán ser revisados, priorizados y validados por la Entidad. Estos no se entienden como una simple migración automática de casos existentes del SIEM actual. Durante la operación se deberán desarrollar los casos de uso adicionales que sean requeridos por la DIAN, conforme a las necesidades del servicio.
518	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	Debe tener métricas de base y detección de desviaciones (comportamientos anómalos).	Se agradece a la entidad indicar el número total de activos que serán objeto de verificación de comportamiento anómalo, así como el alcance de dicha verificación (por ejemplo, endpoints, servidores, aplicaciones, entre otros), con el fin de dimensionar adecuadamente la solución requerida.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, para el servicio SIEM son los 2467 dispositivos de las que trata el servicio.
519	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	Contexto del dispositivo y de la aplicación, como mínimo debe incluir los siguientes elementos: - Dispositivos de red incluyendo switches, routers, WLAN. - Dispositivos de seguridad - Firewalls, IPS de red, gateways Web/Mail, protección contra malware, escáneres de vulnerabilidades. - Servidores, incluyendo Windows, Linux, AIX, HP UX. - Servicios de infraestructura incluyendo DNS, DHCP, DFS, AAA, controladores de dominio. - Aplicaciones orientadas al usuario, incluidos servidores Web, servidores de aplicaciones, correo, bases de datos. - Dispositivos de almacenamiento como (revisar contra inventario) - Cloud Apps, incluyendo AWS, Azure. - Infraestructura de la nube incluyendo AWS. - Dispositivos ambientales como UPS, HVAC, hardware del dispositivo. - Infraestructura de virtualización incluyendo VMware ESX, Microsoft HyperVScalable .	Se agradece a la entidad aclarar si, para los dispositivos alojados en entornos de nube como Azure y AWS, es correcto entender que la entidad dispondrá de los recursos necesarios para su monitoreo (tales como infraestructura para la instalación de colectores, sondas, entre otros).		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, es un contrato llave en mano, por lo tanto el futuro proveedor del SOC deberá disponer de todos los elementos necesarios para realizar todas las implementaciones del proyecto SOC.
520	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	Recolección de logs escalable y flexible, como mínimo 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.	Se agradece a la entidad indicar la cantidad total de activos que requerirán capacidades de FIM (File Integrity Monitoring), así como su tipología (servidores, endpoints, bases de datos, entre otros), con el fin de dimensionar adecuadamente la solución.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem respectivo no habla de FIM.
521	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	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 agradece a la entidad confirmar que el alcance se limita a la integración de la herramienta de ITSM mediante API, y que no incluye actividades de administración, implementación, configuración o provisión de una nueva herramienta de ITSM.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem respectivo exige solamente integración más no administración del ITSM o provisión de alguna herramienta de este tipo.
522	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	Escalabilidad - Escalabilidad de recolección de datos mediante la implementación de máquinas virtuales con la función de recolección (colectores virtuales). - Los recolectores deben poder almacenar en búfer eventos cuando la conexión no esté disponible. - Escalado del análisis mediante la implementación de nuevas máquinas virtuales. - Arquitectura de balanceo integrada para recoger eventos desde sitios remotos usando recolectores	Se agradece a la entidad aclarar si, en caso de requerirse colectores o workers adicionales, esta será responsable de suministrar los recursos de infraestructura necesarios (máquinas virtuales, almacenamiento, red, entre otros) para su implementación y operación		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, es un contrato llave en mano, por lo tanto el futuro proveedor del SOC deberá disponer de todos los elementos necesarios para realizar todas las implementaciones del proyecto SOC.
523	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	Se solicita a la entidad validar y actualizar la nomenclatura de los cuadrantes definidos, considerando que estos han sido modificados en versiones recientes de la metodología o herramienta de referencia, con el fin de evitar ambigüedades en la interpretación y asegurar la correcta alineación con los estándares vigentes.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto no se acepta su sugerencia.
524	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	La solución debe realizar el escaneo para la detección de vulnerabilidades locales y remotas sin la necesidad de un agente en el dispositivo de destino.	Se solicita a la entidad confirmar si, dentro de su infraestructura on-premise y/o en entornos de nube, se permitirá el despliegue de sondas necesarias para la ejecución de las tareas de escaneo, así como precisar las condiciones, restricciones o requisitos técnicos asociados a su implementación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro proveedor del SOC deberá disponer de los elementos necesarios para la puesta en operación de los servicios, es un contrato llave en mano, por lo tanto se deberá cumplir con todas las características solicitadas.
525	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	La solución se debe integrar como mínimos con los siguientes elementos: - Sistema de control de acceso a la red (NAC) - Herramienta de Sandbox - Solución SIEM - Solución de respuesta automática (SOAR) - BitDefender - Solución de detección y respuesta en el endpoint (EDR)	Se solicita a la entidad suministrar el inventario detallado de soluciones NAC, Sandbox u otros dispositivos de seguridad que deban ser integrados, toda vez que estos no se encuentran reflejados en el inventario actualmente proporcionado, lo cual puede generar vacíos en la definición del alcance e integración de la solución.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el inventario fue actualizado mediante adenda, favor revisar la publicación.
526	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	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 agradece a la entidad Confirmar la cantidad de activos, luego esta cantidad difiere del anexo economico : Formulario 1 lista de precios VSD		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el inventario fue actualizado mediante adenda, favor revisar la publicación, donde se especifican que son 25000 activos.
527	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	Determinar automáticamente los scanner de código a utilizar en función del lenguaje, atributos y configuración de la aplicación.	Se agradece a la entidad cual es el tipo de información requiere que muestre el escaneo (o Solo mostrar la información sin importar la tecnologia)		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características y requerimientos solicitados se encuentran en detalle en el anexo técnico.
528	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	Debe tener la funcionalidad de visualizar en detalle las vulnerabilidades de una aplicación, en el cual se muestre: - Archivo asociado - Número de líneas (SAST) o URL(DAST) - Severidad de la vulnerabilidad - Descripción. - CWE asociado, si existe. - El número de instancias en las que se encuentra - Historia de la vulnerabilidad que incluye el tiempo de su primera y última aparición. - Estado de la Vulnerabilidad (Activa o Cerrada).	Se agradece aclarar a la entidad, cuando hablan de "El número de instancias en las que se encuentra" entendemos que hablan las aplicaciones a evaluar.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, al mencionar instancias se refiere a cada ocurrencia individual/localizada de la vulnerabilidad que el escaneo fue capaz de identificar.
529	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	Se debe licenciar como mínimo para 260 activos públicos o equivalente o similar de acuerdo con la tecnologia ofrecida.	Se solicita a la entidad definir la cantidad estimada de *takedowns* requeridos por año, con el fin de dimensionar adecuadamente la capacidad operativa y los recursos necesarios para la prestación del servicio.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante, que de acuerdo sugerencia se adiciona un ítem en gestión de incidentes (19.1.10), cambio que se publicará en los próximos días mediante adenda, quedando de la siguiente manera: 19.1.10 Para protección de marca deberá realizar el acompañamiento desde el inicio de la detección del incidente hasta la verificación de su cierre (takedown), para lo cual se informa que estas solicitudes se harán bajo demanda.
530		Detección de Amenazas	Solicitamos a la entidad aclarar cuantos endpoints se encuentran definidos en el alcance que debe tener en cuenta el oferente para el dimensionamiento del servicio.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el detalle del inventario de la infraestructura tecnológica se encuentra especificado en los documentos del proyecto.

531		Detección de Amenazas	Solicitamos a la entidad aclarar si la entidad cuenta con una solución EDR para servidores y equipos de computo, por favor informar el fabricante, la version del producto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se cuenta con la plataforma bitdefender.
532		Detección de Amenazas	Solicitamos a la entidad informar cual es el inventario de fuentes a integrar en la solución SIEM y donde se ubican las fuentes en el alcance?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el detalle del inventario de la infraestructura tecnológica se encuentra especificado en los documentos del proyecto, su cantidad mínima es de 2467 fuentes.
533		Detección de Amenazas	Solicitamos a la entidad aclarar si se espera una solucion SaaS (Cloud) o On-premise de la entidad o instalaciones del oferente.		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.
534		SIEM	Solicitamos a la entidad aclarar cual es la volumetria de la solucion actual de los ultimos 12 meses en la plataforma actual IBM y cuantas alertas (mensuales o diarias) se generan actualmente?		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.
535		Code Review	Solicitamos a la entidad suministrar detalles de los códigos a revisar en el alcance, confirmar su son desarollos propios y si se cuentan con la documentacion de los codigos fuentes, necesarios para entender el tema de remediación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se deben analizar como mínimo 50 aplicaciones, son desarrollos propios y se cuenta con el código fuente.
536		Code Review	Solicitamos a la entidad informar cuantas líneas de código se deben revisar en el alcance dle proyecto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se debe dimensionar con la cantidad de 50 aplicaciones.
537		Code Review	Solicitamos a la entidad informar si es posible hacer escaneos SAST en caso de ser un numero muy grande de líneas de codigo que tengan que revisarse en el alcance del proyecto.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, se pueden hacer escaneos SAST.
538		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.	Se solicita a la entidad aclarar que no se realizaran cambios sobre la platafroma actual IBM QRADAR durante el inicio de contrato. En caso de requerirse actualización y/o cambio de versión deberá asumirlo la entidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el futuro proveedor del SOC, deberá recibir, gestionar, administrar y operar el SIEM propiedad de la DIAN del fabricante IBM Referencia QRADAR hasta agosto 31 de 2027, por lo tanto, deberá realizar las respectivos cambios (de versión), actualizaciones y demás actividades a las que haya lugar, para lo cual, la Entidad informa que se cuenta con el respectivo soporte de fabricante.
539	20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	NOTA 2:Todo el personal del SOC requerido para la implementación, operación, gestión, monitoreo, soporte, garantía, entre otros, deberá ser propio evitando figuras de tercerización, sin embargo se aclara que el CONTRATISTA se podrá apoyar con recursos (personal) directamente del fabricante para la etapa de implementación.	Se solicita amablemente a la entidad revisar y ajustar el presente requerimiento, con el fin de permitir el uso de esquemas de tercerización o prestación de servicios. En este sentido, se propone permitir la participación de oferentes que integren esquemas de tercerización, siempre que se asegure el cumplimiento integral de los requisitos técnicos, operativos y de seguridad establecidos por la entidad.Estos modelos son ampliamente utilizados en el entorno colombiano y se encuentran debidamente habilitados dentro del marco legal vigente.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el proveedor del SOC deberá entregar el equipo de trabajo mínimo requerido por la Entidad para realizar las labores propias de implementación, gestión y operación, por lo tanto, no se acepta su solicitud.
540	Sección III. Criterios de Evaluación y Calificación	Sesión de Aclaraciones	Se solicita a la entidad especificar la profundidad y duración de la transferencia de conocimiento requerida para su equipo interno? ¿Hay certificaciones o niveles de habilidad específicos que esperan que su equipo alcance después de la transferencia?		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, no se exigen certificaciones para los asistentes.
541	Sección VI - SDP Fase 1, punto 7 / Anexo Técnico Ítems 2.13, 2.32, 2.35	SDP punto 7: "En el caso de on-premises, el CONTRATISTA deberá proveer el hardware requerido." Ítem 2.32: colectores virtuales. Ítem 2.35: "Se podrán desplegar tantos colectores virtuales en ambientes híbridos como se quiera sin coste adicional."	¿La DIAN proveerá recursos de cómputo (CPU, RAM, almacenamiento) en sus hipervisores (Hyper-V, VMware ESXi 7.0.3) y en sus nubes (Azure, AWS) para alojar los colectores virtuales del SIEM? ¿O el contratista debe provisionar infraestructura de cómputo independiente, incluyendo VMs en Azure/AWS, para desplegar los colectores?		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, es un contrato llave en mano, por lo tanto, el contratista debe provisionar la infraestructura de cómputo independiente, incluyendo VMs en Azure/AWS, para desplegar los colectores
542	Anexo Técnico Sección 12 / Especificaciones Técnicas Servicios de Monitoreo	Prestar el servicio desde un centro de operaciones de seguridad (SOC) ubicado en la ciudad de Bogotá D.C. (Colombia), cuya comunicación con la infraestructura de la Dian, se hará utilizando los canales de la Entidad.	Agradecemos a la entidad indicar si se cuenta con puertos disponibles en su infraestructura de red y perímetros (SWs y FWs) para instalar canales de comunicación vía Internet con el SOC del oferente		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. Es un contrato llave en mano, el futuro proveedor del SOC deberá disponer de todos los elementos necesarios para la puesta en operación de los nuevos servicios.
543	Sección VI - SDP Tabla 1, nota / Anexo Técnico Ítem 2.4	SDP: "Las proyecciones de crecimiento ya están inmersas dentro de las cantidades." Ítem 2.4 incluye 20% adicional.	Si durante la vigencia del contrato la cantidad de activos supera los 2,467 dispositivos o los 25,000 EPS licenciados (debido a la modernización y migración a multinube), ¿el contratista debe absorber ese crecimiento dentro del precio ofertado, o se reconoce mediante adición contractual? ¿Cuál es el mecanismo de ajuste previsto?		La Dirección de Impuestos y Aduanas Nacionales (DIAN) informa al observante que, las proyecciones ya están incorporadas en las cantidades mínimas requeridas. Por tanto, la entidad solo exigirá el cumplimiento de estos topes y no se contemplan adiciones.
544	Anexo Técnico Administrativos Ítem 12.80	Ítem 12.80: "El servicio del SOC deberá contar con mínimos dos (2) centros de datos geográficamente ubicados en diferentes lugares."	¿El datacenter de contingencia debe tener réplica completa de todas las plataformas del SOC (SIEM, SOAR, NDR, etc.) en esquema activo-activo, o se acepta un esquema activo-pasivo donde la contingencia se activa solo ante caída del principal? ¿Las 8 capacidades tecnológicas deben estar replicadas en contingencia, o solo las críticas (SIEM, SOAR, monitoreo)?		La Dirección de Impuestos y Aduanas Nacionales (DIAN) informa al observante que, se exige contingencia con dos centros de datos, pero el esquema de replica o de contingencia estará a cargo del futuro proveedor del SOC, aclarando que se deben cumplir con los ANS requeridos.
545	Anexo Técnico Ítem 8.20	Ítem 8.20: "Las herramientas del CONTRATISTA deben utilizar SASE (Secure Access Services Edge)."	¿Se requiere que el contratista provea una solución SASE completa como parte del proyecto, o se refiere a que las herramientas de análisis de código deben ser compatibles con entornos protegidos por SASE? ¿La DIAN cuenta actualmente con una solución SASE desplegada?		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 si una funcionalidad del servicio o capacidad a adquirir.
546	Sección VI - Requisitos de los Bienes y Servicios Conexos / Anexo Técnico Ítem 2.5	Ítem 2.5: "Debe tener la capacidad de manejar como mínimo 25000 EPS o unidad de medida equivalente o superior."	Los 25,000 EPS mínimos, ¿corresponden a EPS promedio sostenido o a EPS pico? ¿Cuál es el EPS promedio actual del QRadar en producción y cuál es el pico máximo registrado?		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, las características de la plataforma SIEM de la Entidad son: 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" Aclarando que se debe cumplir con lo solicitado 25000 EPS.
547	Anexo Técnico Ítem 2.25	Ítem 2.25: "Búsqueda de eventos en real - sin necesidad de indexación."	¿La "búsqueda sin necesidad de indexación" se refiere a la capacidad de buscar en el flujo de eventos en tiempo real (streaming search) antes de que se persistan, o se requiere que el sistema no use indexación para búsquedas históricas?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem 2.25 fue ajustado mediante adenda.

548	Anexo Técnico Ítem 1.1	Ítem 1.1 : "NOTA 1: Se entiende que es un contrato llave en mano."	Agradecemos a la entidad considerar que la infraestructura que será instalada por el proponente, destinada a la implementación de las soluciones de seguridad, pueda hacer uso de la alimentación eléctrica regulada disponible en el Data Center de la entidad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, futuro proveedor del SOC podrá utilizar la alimentación regulada en el datacenter en caso de ser requerida.
549	Sección VI. Requisitos de los Bienes y Servicios Conexos	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, por ello, el CONTRATISTA deberá prever que el diseño propuesto permita el monitoreo, detección y respuesta de eventos en ambiente hibrido y deberá ser resiliente ante cambios de medio, estado inclusión de nuevas herramientas o supresión de existentes en alguno de los ambientes. Luego, el diseño y la metodología debe responder a este ambiente adaptativo, dinámico y evolutivo.	Agradecemos a la entidad considerar que los colectores de eventos requeridos para las soluciones SIEM y NDR sean provistos directamente por la entidad, haciendo uso de sus suscripciones de servicios en la nube, tanto en Microsoft Azure como en Amazon Web Services.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, futuro proveedor del SOC deberá disponer de todos los elementos necesarios para la implementación de los servicios, es un contrato llave en mano.
550	Anexo Técnico Adm. Ítem 12.49 / Protección energética	Ítem 12.49: Protección contra fallas en el suministro de energía.	a) ¿Los cuartos de cómputo cuentan con UPS? ¿De qué capacidad (kVA)? ¿Cuánta capacidad libre tienen para soportar carga adicional de los equipos del contratista?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la Entidad cuenta con la capacidad necesaria de UPS para los nuevos equipos.
551	Sección IV	Alcance	Agradecemos a la entidad aclarar ¿Cuál es el modelo de toma de decisiones operativas entre el SOC y la OSI (qué decide el SOC autónomamente y qué requiere validación)? ¿La OSI define y aprueba: casos de uso, reglas de correlación, playbooks, métricas e indicadores?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que la OSI aprueba: casos de uso, reglas de correlación, playbooks, métricas e indicadores, la definición, confección, pruebas, implementación y puesta en operación lo debe realizar el futuro proveedor del SOC.
552	Sección IV	Objetivo general	Agradecemos a la entidad aclarar si el monitoreo incluye solo eventos de seguridad o también: disponibilidad, integridad, desempeño de servidores, monitoreo tipo NOC?		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el monitoreo es sólo para eventos de seguridad y actividades propias de un cento de operaciones de seguridad SOC.
553	Sección IV	Objetivo general	Agradecemos a la entidad indicarnos, ¿Cuál es el estado de madurez de: QRadar, Guardium, gestión de vulnerabilidades hoy? ¿Se cuenta con: inventario actualizado de fuentes conectadas a QRadar, reglas/casos de uso existentes, playbooks actuales?		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, las características de la plataforma SIEM de la Entidad son: 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" Aclarando que se debe cumplir con lo solicitado 25000 EPS
554	5.4.9	La solución ofertada permitirá proveer métricas de evaluación de los programas de evaluación y remediación de la Entidad.	Se solicita amablemente aclarar bajo qué marcos de referencia (framework) desean medir sus programas?		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, los marcos de referencia los proporcionará el futuro proveedor del SOC, de acuerdo a las mejores practicas, y cumpliendo los lineamientos de la Entidad y los requerimientos descritos en el proyecto SOC.
555	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.	se solicita amablemente aclarar si el cliente está planeando o ya tiene una red bajo el nuevo estándar de direccionamiento IPv6? Que porcentaje de su infraestructura ya esta operando en IPv6		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, la infraestructura tecnológica de la Entidad cumple con IPV6.
556	5.5.2	Debe proporcionar una API integral o solución similar de iguales o superiores características para la automatización de procesos e integración con aplicaciones de terceros.	se solicita amablemente aclarar qué aplicaciones de terceros y procesos críticos requieren integrarse mediante una API integral para garantizar la automatización total del flujo de trabajo y la sincronización de datos?		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, se deben realizar las integraciones necesarias y suficientes consideradas en el proyecto SOC de acuerdo a la infraestructura tecnológica detallada en los documentos del proceso.
557		VACIA	VACIA	VACIA	
558	5.5.5	Debe soportar integración con Centro de Operaciones de Seguridad (SOC) mediante alertas automatizadas nativas en el producto. También deberá tener la capacidad de integrarse a soluciones tipo SIEM y de Orquestación de seguridad (SOAR), la solución deberá estar en capacidad de generar alertas cuando se detecten nuevas vulnerabilidades críticas en sistemas relevantes, nuevas vulnerabilidades asociadas a una amenaza conocida y otras reglas personalizables.	se solicita amablemente aclarar con qué soluciones SIEM, SOAR se integrarán nativamente?		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, la solución SIEM de la Entidad es QRADAR, y actualmente no se cuenta con un SOAR en la DIAN.
559	5.7.9	La solución debe poder realizar búsquedas de datos confidenciales en los endpoint o equipos de usuario final. La aplicación deberá contar con una biblioteca o similar que permita la identificación y parametrización de los datos a identificar.	Se solicita amablemente aclarar que tipos de datos se desean identificar y bajo que estándar o marco normativo		La Dirección de Impuestos y Aduanas Nacionales - DIAN indica al observante que, se debe buscar como mínimo sin limitarse a datos PII/PCI/PHI + credenciales principalmente bajo Ley 1581 de 2012 (Colombia) y estándares internacionales como PCI DSS, para prevenir fugas en endpoints comprometidos
560	5.10.1	La solución debe poder escanear aplicaciones web internas y externas (hasta copar el licenciamiento requerido para 260 aplicaciones) y debe permitir la definición de secciones criticas de la aplicación que sean seguras para escanear y de otras partes que nunca deberían escanearse, para evitar latencias de rendimiento e interrupciones.	Se solicita amablemente aclarar, en relación con el requerimiento asociado al escaneo de hasta 260 aplicaciones web, se solicita a la entidad aclarar si las 260 aplicaciones web se encuentran definidas en términos de FQDN/URL únicos o corresponden a aplicaciones lógicas que pueden incluir múltiples dominios y subdominios?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las doscientas sesenta (260) aplicaciones corresponden a aplicaciones definidas por la Entidad para efectos del alcance del servicio. Durante la fase de implementación se precisará el detalle técnico aplicable, incluyendo URL, FQDN, dominios, subdominios o componentes asociados, conforme a la arquitectura, priorización y lineamientos de seguridad de la Entidad.
561	5.10.17	"La solución debe estar en capacidad de detectar vulnerabilidades de las siguientes familias, entre otras: - Access Restriction Bypass via Origin Spoof - Basic Authentication without HTTPS - Password field with auto-complete - Session Fixation - Unencrypted Password Form - Code Injection - Code Injection (php://input wrapper) - Code Injection (timing attack) - Operating System Command Injection - Operating System Command Injection (timing attack) - Component Vulnerability: Angular, Apache, Apache Solr, Apache Struts, Apache Tomcat, Atlassian, Bootstrap, Drupal, Wordpress, Joomla, jQuery, Kentico, Kibana, Knockout.js, lighttpd, Magento, MediaElement.js, Modernizar, Moment.js, nginx, PHP, Sitefinity, vBulletin, Webmin, YUI. - Cross Site Request Forgery - Cross-Site Scripting (XSS): In event tag of HTML element, in HTML tag, in path, in script context, in script src, DOM based, Response Splitting. - Data Exposure: Backup file/directory, Credit Card number disclosure, CVS Entries Detected, CVS Repository Detected, CVS/SVN user disclosure, Disclosed US Social Security Number, E-mail address Disclosure, Error Message, Full Path Disclosure, Git Repository Detected, Gitignore File Detected, Private IP address Disclosure, Source Code Disclosure, Source Code Leakage, SVN Repository Detected, Web.config File Information Disclosure, WS_FTP.Log File Detected. - Local or Remote File Inclusion - SSL/TLS: SSL Insecure Protocols, Certificate Expired, Certificate Common Name Mismatch, Certificate RSA Keys less than 2048 bits, Weak Hashing Algorithm, Insecure/Null Cipher Suites Supported, HTTP to HTTPS redirect not enabled. - HTTP Security Header: Deprecated Content Security Policy, Disabled X-XXS-Protection Header, HTTP Header Information Disclosure, Insecure ´Access-control-allow-origin´ Header, Insecure Cross-Origin Resource Sharing Configuration, Insecure Cross-Origin Resource Sharing Configuration, Missing Header (Cache-control, Content-type, Expect-CT, X-Content-Type-Options, X-Frame-Options, X-XSS-Protection), Missing Content Security Policy, Missing Feature Policy, Missing HTTP Strict Transport Security Policy, Missing Referrer	Se solicita amablemente aclarar si el alcance del análisis de seguridad de aplicaciones se limita a pruebas dinámicas DAST sobre aplicaciones en ejecución		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el análisis de seguridad de aplicaciones deberá cumplir con las capacidades definidas en los documentos del proceso. El alcance no se limita únicamente a pruebas dinámicas DAST cuando los requerimientos técnicos exijan capacidades adicionales o complementarias para la identificación, análisis y gestión de vulnerabilidades en aplicaciones.
562	5.10.19	Tener la capacidad para ser desplegada como un contenedor de Docker, permitiendo el escaneo de sitios públicos y privados.	Se solicita amablemente aclarar, considerando que el documento especifica una solución de análisis de vulnerabilidades 100% SaaS, cuál es el propósito del uso de Docker: si está orientado al despliegue de la solución o si corresponde a un mecanismo para automatizar los escaneos cada vez que los desarrolladores publiquen nuevas versiones de sus aplicaciones.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la capacidad de despliegue como contenedor Docker debe entenderse como un mecanismo técnico que permite facilitar la ejecución, automatización o integración de escaneos sobre sitios públicos y privados, conforme a las necesidades de la Entidad y a la arquitectura definida durante la implementación. Lo anterior no modifica la obligación de cumplir integralmente con las capacidades requeridas para la solución ofertada.

563	5.10.24	El fabricante de la solución deberá poner a disposición acceso a una API que permita crear conectores, importar/exportar datos y automatizar procesos.	Se Solicita amablemente aclarar qué tipos de integraciones y automatizaciones espera la entidad implementar mediante la API?		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las APIs deberán permitir, entre otros usos, la creación de conectores, importación y exportación de información, automatización de procesos, integración con herramientas del SOC, intercambio de hallazgos, generación de reportes y articulación con plataformas institucionales cuando aplique. El detalle de integraciones será definido durante la fase de diseño e implementación, conforme a las capacidades de la solución y los lineamientos de la Entidad.
564	5.11.3	La solución ofertada deberá poseer capacidades de auto remediación.	Se solicita amablemente aclarar el alcance esperado de las capacidades de remediación		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las capacidades de remediación deberán permitir la generación de recomendaciones, priorización de hallazgos, propuestas de corrección, automatización o asistencia controlada cuando aplique, y seguimiento a las acciones de tratamiento. Cualquier acción que pueda modificar configuraciones, cargas de trabajo, identidades, activos o servicios de la Entidad deberá ser previamente autorizada y coordinada con la DIAN.
565	5.12.2	La solución debe proporcionar puntos de referencia de auditoría de seguridad y configuración para estándares de cumplimiento normativo así como otros estándares de mejores prácticas de la industria.	se solicita amablemente aclarar cuáles son los estándares de cumplimiento normativo y marcos de mejores prácticas que deben ser considerados por la solución		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la solución deberá considerar estándares de cumplimiento normativo, marcos de referencia y buenas prácticas de la industria aplicables a seguridad de la información, ciberseguridad, gestión de vulnerabilidades, configuración segura, protección de datos y entornos tecnológicos, conforme a los requerimientos definidos en los documentos del proceso.
566	5.12.3	Debe permitir el monitoreo continuo de la seguridad del directorio activo identificando y alertando frente a ataques como Ramsonware, Golden Ticket entre otros, dando recomendaciones de remediación y evidenciando la ruta de los atacantes para llegar a objetos o grupos críticos para la DIAN.	Se solicita amablemente aclarar el alcance funcional requerido para el monitoreo de seguridad del directorio activo, especificando el tipo de análisis esperado		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el monitoreo de seguridad del Directorio Activo deberá permitir identificar, analizar, alertar y recomendar acciones frente a configuraciones inseguras, rutas de ataque, privilegios excesivos, movimientos laterales, técnicas asociadas a ransomware, Golden Ticket u otros escenarios de compromiso que puedan afectar objetos, usuarios, grupos o activos críticos de la Entidad.
567	4,39	Deberá ser capaz de monitorear al menos las siguientes plataformas de bases de datos: - Oracle (Including NDE/ASO, SSL) - Oracle Exadata - Microsoft SQL Server - IBM DB2 para Linux, z/OS y DB2/400 - IBM IMS para z/OS - IBM Informix - IBM Netezza - SAP Sybase (ASE, IQ, SQL Anywhere) - SAP-HANA - Teradata - MySQL - PostgreSQL - Progress OpenEdge - Maria DB	se solicita a la entidad, confirmar el alcance que requiere con Oracle NDE/ASO y que es un componente ofrecido por Oracle para nivel base de protección de datos; en caso de que la entidad confirme que no se debe tener en cuenta, solicitamos retirarlo		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.
568	4		Agradecemos a la entidad indicar la cantidad de usuarios que operaran la plataforma		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la operación de la plataforma deberá contemplar los usuarios, roles y perfiles que resulten necesarios para la adecuada administración, gestión, monitoreo, auditoría y supervisión del servicio, conforme al modelo operativo aprobado durante la fase de implementación. El oferente deberá dimensionar su propuesta con base en el alcance y equipo mínimo requerido en los documentos del proceso.
569	410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	**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	De manera atenta solicitamos a la Entidad revisar el enfoque del perfil, teniendo en cuenta que los requisitos actuales incluyen certificaciones como PMP y Scrum, así como formación en gerencia de proyectos, los cuales están más alineados con un rol de gestión y no con funciones técnicas propias del cargo. En este sentido, sugerimos que el perfil se oriente a competencias técnicas en ciberseguridad y seguridad de la información, evitando la exigencia de certificaciones como PMP o Scrum Master, y en su lugar considerar posgrados en áreas afines a ciberseguridad y seguridad de la información. Lo anterior permitirá una mejor alineación del perfil con las funciones esperadas y una adecuada diferenciación frente al rol de Gerente de Proyecto		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que los requisitos definidos para el perfil Líder / Coordinador SOC corresponden a las necesidades de coordinación, planeación, seguimiento, control operativo y articulación del servicio SOC. En consecuencia, se mantienen las condiciones de formación, certificación y experiencia establecidas en los documentos del proceso. Por lo anterior, no se acepta la solicitud.
570	410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	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	De manera atenta nos permitimos presentar la siguiente observación respecto al perfil de Threat Hunter / Analista de Ciberinteligencia, especificamente en relación con la certificación requerida Licensed Penetration Tester (LPT). Si bien dicha certificación está orientada a pruebas de penetración avanzadas, consideramos que su exigencia como requisito único y excluyente puede resultar restrictiva frente a las competencias reales requeridas para un rol de Threat Hunting y ciberinteligencia, el cual involucra también análisis de amenazas, investigación de indicadores de compromiso, correlación de eventos, inteligencia de amenazas (Threat Intelligence) y respuesta proactiva ante ataques. En el mercado existen certificaciones equivalentes en áreas de ethical hacking, threat intelligence, SIEM/SOAR y detección de amenazas que son igualmente válidas para garantizar la idoneidad del perfil. Por lo anterior, solicitamos permitir certificaciones equivalentes en seguridad ofensiva, ciberinteligencia o threat hunting emitidas por fabricantes o entidades reconocidas. Ejemplo: Certified Ethical Hacker (CEH), Certified Penetration Testing Engineer (CPTE)...		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.

571	410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN	**NOTA1 :** Cada uno de los anteriores perfiles deberá presentarse por separado donde ninguno podrá repetir rol o perfil o cargo, para lo cual se deberá aportar la hoja de vida actualizada a fecha del proceso, y las respectivas evidencias para el cumplimiento de cada uno de los requerimientos solicitados.	Teniendo en cuenta la naturaleza del servicio y el nivel de especialización de los perfiles solicitados los cuales, en muchos casos, cuentan con certificaciones específicas y experiencia altamente demandada en el mercado, consideramos que exigir la disponibilidad inmediata y acreditación documental del personal en esta fase del proceso puede limitar la pluralidad de oferentes y la participación efectiva. Lo anterior obedece a que este tipo de talento especializado suele encontrarse vinculado laboralmente al momento de la oferta, y su desvinculación o asignación definitiva generalmente se materializa una vez adjudicado el contrato. En ese sentido, garantizar su disponibilidad anticipada sin certeza de adjudicación implica un riesgo tanto para los profesionales como para los oferentes. Por lo anterior, respetuosamente solicitamos a la entidad evaluar la posibilidad de flexibilizar este requisito, permitiendo que, en lugar de adjuntar las hojas de vida y certificaciones en la etapa de oferta, se acepte una carta de compromiso firmada por el representante legal, en la cual el proponente se obligue a disponer del personal que cumpla con la totalidad de los requisitos exigidos, para el inicio de la ejecución del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que las hojas de vida y soportes del equipo mínimo deberán ser presentados por el oferente adjudicatario en la etapa que corresponda, conforme a lo establecido en los documentos del proceso. En la oferta deberán acreditarse las condiciones exigidas para los perfiles, roles, experiencia mínima y certificaciones requeridas.
572	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, los requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
573	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 objeto de evaluación deberán estar vigentes y verificables al momento previsto en los documentos del proceso para su acreditación. En relación con FIRST, deberá atenderse lo dispuesto en los ajustes realizados mediante adenda, según corresponda.
574	Sección VI — Anexo Técnico / Formulario Lista de Precios	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 definitiva para el licenciamiento de la capacidad NDR corresponde a veinticinco mil (25.000) dispositivos, conforme a los ajustes realizados mediante adenda.
575	Sección VI — Anexo Técnico / Formulario Lista de Precios	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 definitiva para el licenciamiento de la solución de Gestión de Vulnerabilidades corresponde a veinticinco mil (25.000) activos, conforme a los ajustes realizados mediante adenda.

576	Sección VI — Anexo Técnico / Formulario Lista de Precios	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 al observante que la operación, seguimiento, gestión, monitoreo y administración por parte del futuro proveedor de los servicios requeridos irá hasta el 31 de octubre de 2028. El derecho de 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, conforme a lo establecido en los documentos del proceso.
577	Sección VI — Anexo Técnico	Ítem 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."	El Ítem 2.4 indica que la base de licenciamiento del SIEM es de 2.056 dispositivos, señalando que dicha cifra se encuentra estipulada en el inventario anexo. Sin embargo, la hoja de Inventario de Infraestructura IT del archivo anexo no presenta ese total de manera consolidada en ninguna tabla. La suma de los activos identificables en el inventario no permite llegar directamente a la cifra de 2.056, ya que el inventario no incluye una tabla unificada que discrimine cada categoría de activo con su respectivo conteo, lo que impide a los oferentes verificar la composición de la base de licenciamiento. Esta ambigüedad genera incertidumbre sobre qué activos deben incluirse y cuáles quedan excluidos del alcance del SIEM, afectando el dimensionamiento y la comparabilidad de las ofertas.	Se solicita amablemente a la Entidad publicar el listado consolidado de los 2.056 activos que componen la base de licenciamiento del SIEM, discriminados por categoría (infraestructura on-premise, activos de seguridad, infraestructura en nube, usuarios de Directorio Activo y aplicaciones web), de manera que los oferentes puedan verificar y dimensionar correctamente el licenciamiento sin ambigüedad.	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, los inventarios fueron actualizados mediante adenda, favor revisar en el sitio de publicación.
578	Criterios de Evaluación (IAO 34.6) Evaluación Técnica:	Criterios de Evaluación (IAO 34.6) Evaluación Técnica: b. Nivel de partner más alto en las capacidades ofertadas (ítems 2 al 9 del anexo técnico).	Se solicita eliminar este método de ponderación, toda vez que limita la cantidd de oferentes que pueden obtener puntaje en el desarrollo del proceso.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta su observación, por cuanto el literal b es un ítem puntuable que le permite al futuro proveedor del SOC hacerse con una con una puntuación de acuerdo a su calidad de membresía, sin embargo el literal en cuestión fue modificado mediante adenda, por lo tanto su revisión se puede hacer en el sitio de publicación del proceso.
579	Criterios de Evaluación (IAO 34.6) Evaluación Técnica:	b. 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.	En caso que no se elimine este requerimiento, nos permitimos solicitar que para la asignación de puntaje se permita que el oferente pertenezca a las tres más altas categorías con el correspondiente fabricante		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta su observación, por cuanto el literal b es un ítem puntuable que le permite al futuro proveedor del SOC hacerse con una con una puntuación de acuerdo a su calidad de membresía, sin embargo el literal en cuestión fue modificado mediante adenda, por lo tanto su revisión se puede hacer en el sitio de publicación del proceso.
580	2. Estrategia de implementación (40 puntos)	Los oferentes deberán allegar como parte de la oferta técnica las siguientes certificaciones vigentes y que sean verificables para lograr la puntuación de la que trata este ítem: Certificación que acredite vinculación directa y activa con FIRST (Forum Incident Response and Security Teams). (como mínimo doce (12) meses de antigüedad.).	Nos permitimos solicitar que o se limite el certificado FIRST a los doce (12) meses de antigüedad.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requisito relacionado con FIRST es un ítem puntuable con doce (12) meses de antiguedad.
581	Criterios de Calificación (IAO 38.1) Capacidad Financiera	Apalancamiento a corto plazo Menor o igual a 0,5	Nos permitimos solicitar que se permita un Apalancamiento a corto plazo menor o igual a 0,8. El límite de 0,5 resulta excesivamente restrictivo y puede excluir a oferentes con estructuras financieras sanas, pero con un mayor nivel de pasivos corrientes debido a la naturaleza de su operación. Un índice de hasta 0,8 mantiene un nivel prudente de solvencia y equilibrio patrimonial, garantizando la capacidad de cumplimiento sin restringir injustificadamente la participación, en concordancia con los principios de proporcionalidad y libre concurrencia		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que el requisito relacionado con FIRST fue ajustado mediante adenda, por lo cual deberá atenderse lo allí dispuesto.
582	Criterios de Calificación (IAO 38.1) Experiencia y capacidad técnica general	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.	Nos permitimos solicitar se elimine el requerimiento de al menos un contrato ejecutado para el sector financiero		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, las características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto no es posible aceptar su sugerencia.
583		Vacia	Vacia	Vacia	
584	SDO – Sección VI / Anexo Técnico Ítems 2.4 y 2.5	El oferente debe licenciar como mínimo para 2.467 dispositivos (2.056 del inventario anexo más el 20% de incremento adicional). Debe tener la capacidad de manejar como mínimo 25.000 EPS o unidad de medida equivalente o superior.	Los pliegos establecen 25.000 EPS como capacidad mínima del SIEM; sin embargo, dado el tamaño de la infraestructura (24.284 activos, incluyendo 21.000 endpoints, 1.700 servidores virtuales y activos en nube Azure/AWS), la generación real de eventos puede superar ampliamente este umbral durante picos operativos o incidentes. Se solicita aclarar: (1) si el umbral de 25.000 EPS es el mínimo sostenido o el mínimo pico (burst), (2) si existe una medición histórica de EPS promedio y pico del SIEM IBM QRadar actual que sirva como referencia, y (3) si el licenciamiento de 2.467 dispositivos incluye los activos en nube (Azure/AWS) o únicamente los on-premise.		La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que la capacidad mínima requerida para el SIEM corresponde a veinticinco mil (25.000) EPS o unidad de medida equivalente o superior, conforme a lo establecido en los documentos del proceso. El oferente deberá dimensionar su solución considerando dicha capacidad mínima, el licenciamiento requerido para dos mil cuatrocientos sesenta y siete (2.467) dispositivos y las condiciones de crecimiento, retención, operación y continuidad definidas para el servicio.
585	SDO – Sección VI / Anexo Técnico Ítem 2.13	La solución debe estar en capacidad de instalarse en Azure, AWS, HyperV (en las versiones con que cuenta la entidad), VMware (en las versiones con que cuenta la entidad). La entidad cuenta con Windows Server 2012R2, Windows Server 2022 y VMware ESXi 7.0.3.	El pliego exige compatibilidad con VMware ESXi 7.0.3 y Windows Server 2012R2. VMware ESXi 7.0.3 alcanzó fin de soporte general en abril de 2022 y fin de soporte extendido en 2025. Operar un SIEM sobre hipervisores fuera de soporte impone riesgos de seguridad incompatibles con ISO/IEC 27001:2022. Se solicita que la DIAN aclare: (1) si la exigencia de compatibilidad con ESXi 7.0.3 es un requisito de habilitación o simplemente informativo, y (2) si el contratista podrá proponer versiones superiores del hipervisor sin que esto sea causal de rechazo, dado que el proyecto contempla la migración a multinube híbrida.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, para todas las capacidades asociadas directamente al SOC el Contratista deberá proveer toda la infraestructura relacionada.
586	SDO – Sección VI / Anexo Técnico Ítem 2.36	En la solución SIEM entregada debe integrarse al SOAR, firewalls, plataforma antivirus y las demás plataformas de seguridad de la Entidad y que sean susceptibles de integración.	El pliego menciona la integración con "las demás plataformas de seguridad de la Entidad", pero no especifica un listado cerrado ni una API de referencia para cada fuente. Dado que la DIAN opera firewalls CheckPoint, antivirus Symantec, balanceadores F5, proxy McAfee, entre otros (Tabla 2 SDO), se solicita que el Fondo DIAN publique el inventario completo y actualizado de fuentes de log que deben integrarse al SIEM, incluyendo versiones de firmware/software, para permitir al oferente dimensionar correctamente los conectores requeridos y garantizar el compromiso de integración sin costos adicionales.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.

587	SDO – Sección VI / Anexo Técnico Ítem 3.52	La solución debe tener al menos 300 playbooks preconfigurados o equivalentes, con posibilidad de expansión (sin que implique costos adicionales para la Entidad) mediante comunidad, marketplace o desarrollo propio.	El pliego exige 300 playbooks preconfigurados, pero no distingue entre playbooks genéricos de mercado y playbooks adaptados al contexto específico de la DIAN (sistemas MUISCA, NSGT, plataformas BID, etc.). Se solicita precisar: (1) si los 300 playbooks deben ser funcionales desde el día 1 de operación o si pueden incluir plantillas que se ajusten durante la Fase 1 (Diseño), (2) si el desarrollo de playbooks a medida para los sistemas misionales DIAN estará dentro del alcance del contrato sin costo adicional, y (3) el mecanismo de aprobación de nuevos playbooks durante la operación (¿OSI valida cada playbook antes de activarlo en producción?).		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 a cerca de la operación del mismo, adicionalmente, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
588	SDO – Sección VI / Anexo Técnico Ítem 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).	El pliego menciona 'Firewall de Nueva Generación' pero la DIAN opera actualmente firewalls CheckPoint (no NGFW de fabricantes como Fortinet, Palo Alto o Cisco). Se solicita confirmar si el requisito de conector NGFW aplica a CheckPoint específicamente, o si la DIAN prevé migrar a otra plataforma de firewall durante la vigencia del contrato. Esta aclaración es indispensable para garantizar que los conectores SOAR ofertados sean operativos desde el inicio del contrato.		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 a cerca de la operación del mismo, adicionalmente, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
589	SDO – Sección VI / Ítem 1.3 (Consideraciones herramientas)	La protección de bases de datos (Firewall de bases de datos) 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 pliego establece que el contratista administrará IBM Guardium hasta diciembre 2027 y luego implementará el nuevo DB Firewall desde enero 2028. Se solicita aclarar: (1) si durante el período de transición (diciembre 2027 – enero 2028) el contratista debe garantizar continuidad absoluta del servicio sin brecha de cobertura, (2) cuál es el proceso de migración de las políticas, reglas y configuraciones de IBM Guardium hacia la nueva herramienta, y si este proceso tiene un entregable formal de aprobación por parte de la OSI, y (3) si la nueva solución de DB Firewall debe cubrir las bases de datos en Azure (Microsoft SQL Azure, indicadas en Tabla 5 SDO) además de las on-premise.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que: 1) El Contratista debe asumir la operación completa de la herramienta, que implica todas las gestiones relacionadas (no limitadas) como son: gestión del sistema operativo de los componentes (gestión de parches y actualizaciones, cambios de configuración, corrección de errores, afinamiento, control de tareas administrativas, generación de scripts, etc.), gestión de la configuración de los componentes (Despliegue de políticas, afinamiento, creación de exclusiones, evaluación de desempeño, ajustes de umbrales, etc.), gestión del ciclo de monitoreo (análisis, alertamiento, clasificación, generación de informes, verificación de cierre de brechas, etc.) 2) El contratista deberá migrar toda la configuración compatible y entregar un informe del proceso al finalizar la tarea. 3) Efectivamente.
590	SDO – Sección VI / Anexo Técnico Ítem 5 (Caza de amenazas)	Caza de amenazas (Ver características en el ítem 6). NDR - Detección y respuesta en red e Inteligencia de amenazas (Ver características en el ítem 7).	El pliego agrupa 'Caza de amenazas' e 'Inteligencia de amenazas' en el ítem 6, y el NDR en el ítem 7, pero no define con precisión si el Threat Hunting debe ser proactivo (búsqueda continua de IOC/TTPs) o reactivo (solo a demanda de la OSI). Se solicita que el Fondo DIAN especifique: (1) el número mínimo de ejercicios de Threat Hunting proactivo por mes o trimestre, (2) si el monitoreo de Dark Web y Deep Web para protección de marca DIAN es parte del alcance del ítem 6 o corresponde al ítem 9 (Protección de marca), y (3) si la Inteligencia de Amenazas actual que administra la DIAN hasta diciembre 2027 puede ser accedida por el contratista SOC desde el inicio del contrato para enriquecer los casos de uso del SIEM.		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 a cerca de la operación del mismo, adicionalmente, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
591	SDO – Sección VI / Hoja Administrativos Ítem 10	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 pliego exige autorización formal de la OSI para cada ejercicio de Ethical Hacking, pero no establece plazos de respuesta para dichas autorizaciones ni un procedimiento de aprobación estandarizado. Se solicita que los pliegos definan: (1) el tiempo máximo de respuesta de la OSI para aprobar o rechazar una solicitud de Ethical Hacking (sugerimos máximo 5 días hábiles), (2) el alcance permitido de las pruebas (¿incluye sistemas en producción como MUISCA y el Sistema de Facturación Electrónica, declarados infraestructura crítica?), y (3) si los resultados de los ejercicios de Ethical Hacking son entregables formales que afectan el indicador de ANS del contrato.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el Contratista deberá ceñirse a la información y asignación de recursos disponible que entregue la Entidad.
592	SDO – Sección VI / Ítem 6 Equipo Mínimo de Trabajo	El contratista deberá conformar y mantener un equipo de trabajo para la ejecución del contrato, compuesto por perfiles especializados ajustados al proyecto. El equipo mínimo de trabajo debe estar conformado por: Gerente de Proyecto (1), Líder/Coordinador SOC (1), Threat Hunter (1), QA (1), Especialista IR (1), Analista N3 (1), Analista N2 (1), Analistas N1 (3).	El pliego define 10 perfiles mínimos, pero no establece si estos perfiles deben ser exclusivos del contrato DIAN o si pueden ser compartidos con otros proyectos del contratista. Se solicita aclarar: (1) si la exclusividad (dedicación 100%) es requisito obligatorio para todos los perfiles o solo para los Analistas N1 (que deben cumplir el ANS 7×24×365), (2) si los perfiles del equipo mínimo deben estar certificados individualmente (ej. CEH, OSCP, SANS FOR508) o si las certificaciones institucionales del oferente son suficientes, y (3) si se aceptan subcontratistas para cubrir perfiles especializados como Threat Hunter o Especialista IR, dado que estos perfiles tienen alta escasez en el mercado colombiano.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los perfiles solicitados son de uso exclusivo para la Entidad.
593	SDO – Sección III / Criterio 2c – Certificaciones	Los oferentes deberán allegar las siguientes certificaciones vigentes y verificables: ISO 27001:2022, ISO 22301:2019 o superior, FIRST (vinculación directa y activa, mínimo 12 meses de antigüedad). Otras certificaciones internacionales y reconocidas de SOC relevantes para el proyecto.	El criterio de certificaciones otorga hasta 20 puntos pero no especifica qué 'otras certificaciones internacionales de SOC' son consideradas equivalentes para efectos de puntaje. Se solicita que el Fondo DIAN publique una lista indicativa (no taxativa) de certificaciones adicionales aceptadas, por ejemplo: SOC 2 Type II, CREST, PCI DSS QSA, CSA STAR, NIST CSF Tier 3+, o certificaciones de fabricante (FortiGuard SOC Certification, Tenable Certified Security Engineer), con el fin de que todos los oferentes compitan en igualdad de condiciones y puedan planificar las certificaciones requeridas con suficiente antelación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem en mención es puntuable, y es bien claro al puntuar "otras certificaciones internacionales y reconocidas de SOC relevantes para el proyecto", por lo tanto, no se acepta su sugerencia.

594	SDO – Sección III / Criterio 1d – Metodología ROSI	El interesado deberá generar una metodología que permita calcular el retorno a la inversión en seguridad de la información (ROSI) que contenga como mínimo: identificar los riesgos, estimar ARO, calcular ALE, estimar reducción de ALE, calcular el beneficio, aplicar la fórmula de ROSI.	La metodología ROSI es presentada en la oferta técnica, pero el pliego no define los datos de entrada que la DIAN pondrá a disposición del contratista (ej. historial de incidentes, valoración de activos, costos operativos por incidente). Sin esta información base, la metodología ROSI propuesta será teórica y no podrá generar reportes confiables para la alta dirección de la DIAN. Se solicita que el Fondo DIAN confirme: (1) si compartirá con el contratista el registro histórico de incidentes de seguridad y la valoración de activos críticos para alimentar el modelo ROSI, (2) si el reporte ROSI trimestral es un entregable formal sujeto a aprobación de la OSI, y (3) si una metodología ROSI que incluya herramienta/dashboard automatizado para comunicación ante la alta dirección recibirá la calificación 'Muy Bueno' (máximo puntaje) independientemente de los datos históricos disponibles.		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.
595	SDO – Sección VI / Fase 4 – Devolución del servicio	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, con las mismas capacidades de operación del SOC en el momento de la devolución del servicio, con soporte actualizado por mínimo un año.	El pliego exige licencias a perpetuidad al finalizar el contrato, pero las soluciones SaaS (SIEM en nube, Vulnerability Management SaaS) no disponen de modelo de licenciamiento perpetuo por su naturaleza de suscripción. Se solicita que el Fondo DIAN aclare: (1) cómo aplica el requisito de 'licencias a perpetuidad' para soluciones SaaS: ¿es suficiente con transferir la suscripción activa con saldo de tiempo restante, o la DIAN exige exclusivamente soluciones on-premise con licencia perpetua?, y (2) si una solución SaaS que incluya exportación completa de datos, reglas, configuraciones y casos de uso en formato estándar al finalizar el contrato es equivalente a una licencia perpetua para efectos de cumplimiento del ítem.		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, si el esquema de licenciamiento no cumple con los requisitos mínimos no será tenido en cuenta para la evaluación.
596	Sección III. Criterios de Evaluación y Calificación	Al menos uno (1) debe haber sido ejecutado para el sector Financiero.	En relación con el requisito establecido en los términos del proceso, según el cual "al menos uno (1) de los contratos presentados debe haber sido ejecutado para el sector financiero", respetuosamente solicitamos a la entidad se sirva aclarar el alcance de dicho criterio. Lo anterior, en el entendido de que, en el contexto colombiano, existen entidades que se encuentran sometidas a la inspección, vigilancia y control de la Superintendencia Financiera de Colombia, lo que implica el cumplimiento de estándares rigurosos en materia de gestión de riesgos, seguridad de la información, ciberseguridad, control interno y continuidad del negocio. Bajo este marco, entendemos que la experiencia adquirida mediante la ejecución de contratos para entidades que se encuentren vigiladas por la Superintendencia Financiera de Colombia será considerada como válida para acreditar experiencia en el sector financiero, en la medida en que dichas entidades operan bajo exigencias regulatorias equivalentes en términos de control, supervisión y gestión de riesgos. En ese sentido, agradecemos a la entidad confirmar si este entendimiento es correcto, con el fin de garantizar una adecuada estructuración de la propuesta y la correcta acreditación de la experiencia requerida o en su defecto indicar el criterio que se utilizará para la validar del sector financiero	Al menos uno (1) debe haber sido ejecutado para el sector Financiero (Para validar que se ejecutó en el sector financiero, se tendrán en cuenta las entidades vigiladas por la Superintendencia Financiera	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, por sector financiero debe entenderse bancos, corporaciones financieras, otras entidades con actividades financieras, tales como cooperativas, fintech, entidades de economía solidaria o empresas con operaciones financieras internas, etc., siempre y cuando pertenezca al sector mencionado.
597	Sección III. Criterios de Evaluación y Calificación	Al menos uno (1) debe haber sido ejecutado para el sector Financiero.	En relación con el requisito establecido en los términos del proceso, según el cual "al menos uno (1) de los contratos presentados debe haber sido ejecutado para el sector financiero", respetuosamente solicitamos a la entidad se sirva aclarar el alcance de dicho criterio. Lo anterior, en el entendido de que, en el contexto colombiano, existen entidades que se encuentran sometidas a la inspección, vigilancia y control de la Superintendencia Financiera de Colombia, lo que implica el cumplimiento de estándares rigurosos en materia de gestión de riesgos, seguridad de la información, ciberseguridad, control interno y continuidad del negocio. Bajo este marco, entendemos que la experiencia adquirida mediante la ejecución de contratos para entidades que se encuentren vigiladas por la Superintendencia Financiera de Colombia será considerada como válida para acreditar experiencia en el sector financiero, en la medida en que dichas entidades operan bajo exigencias regulatorias equivalentes en términos de control, supervisión y gestión de riesgos. En ese sentido, agradecemos a la entidad confirmar si este entendimiento es correcto, con el fin de garantizar una adecuada estructuración de la propuesta y la correcta acreditación de la experiencia requerida o en su defecto indicar el criterio que se utilizará para la validar del sector financiero	Al menos uno (1) debe haber sido ejecutado para el sector Financiero (Para validar que se ejecutó en el sector financiero, se tendrán en cuenta las entidades vigiladas por la Superintendencia Financiera	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, por sector financiero debe entenderse bancos, corporaciones financieras, otras entidades con actividades financieras, tales como cooperativas, fintech, entidades de economía solidaria o empresas con operaciones financieras internas, etc., siempre y cuando pertenezca al sector mencionado.
598	Sección III. Criterios de Evaluación y Calificación	Al menos uno (1) incluya actividades de prestación de servicios de SOC, por un valor mayor a un (1) millón de dólares.	Agradecemos confirmar en el caso de contratos en monedas diferente al USD, que TRM se tendrá en cuenta para la conversión, si la fecha de inicio o terminación del contrato o la de presentación de la oferta		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 se hará el análisis de las certificaciones de acuerdo a lo expuesto en el mismo ítem, no se permite pesos constantes o ajustados.
599	Sección III. Criterios de Evaluación y Calificación	Nota: Si el contrato presentado corresponde a una APCA: asociación en participación, consorcio, unión temporal, asociación o cualquier otra figura asociativa en la que se responda solidariamente por la ejecución del contrato, se tendrá como válido el valor del total del contrato multiplicado por el porcentaje de participación del interesado, para el efecto, las certificaciones allegadas deben especificar el porcentaje de participación y que esta sea verificable.	Agradecemos confirmar si en caso que la experiencia sea un APCA, y los mismos integrantes sean proponentes en este proceso mediante APCA, se tendrá en cuenta el valor total del contrato		El texto es explicito "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." solo se tendrá en cuenta el valor del contrato multiplicado por el porcentaje de participación.
600	Sección II. Datos de la Licitación (DDL)	La fecha límite para presentar las ofertas es: Fecha: 14 de mayo de 2026 Hora: hasta las 10:00 am (hora legal colombiana)	Agradecemos prorrogar la entrega de las proupuestas hasta el 29 de mayo		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.

601	Anexo técnico Administrativos	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. En el caso de un Incidente se seguridad se debe seguir el Modelo de Operación requerido para el SOC DIAN, y por lo tanto el procedimiento de escalamiento de incidentes sea de la siguiente manera: Nivel del Incidente: Es una herramienta estratégica la respuesta a incidentes dada la criticidad de la información y sus activos, el SOC debe estar en capacidad de dar respuesta efectiva y oportuna a los incidentes de seguridad, así mismo detectar, evaluar, gestionar vulnerabilidades y disparar la remediación al área de TI encargada, en todos los activos de información y en los sistemas de información de la DIAN. Severidad del incidente: Alto Impacto: Es un incidente de Seguridad que afecta a activos de información que tengan asociados los impactos catastrófico y mayor, que además de esto se relacionan directamente a los objetivos misionales y el Core de los sistemas de la DIAN, así como también son la reputación, el buen nombre y que involucren aspectos legales. Tipo de respuesta: Inmediata. Medio Impacto: Es un incidente de seguridad que afecta a activos de información que tengan asociados los impactos moderados que influyen directamente a los objetivos de un proceso. Tipo de respuesta: Media.	Solicitamos amablemente a la entidad, relacionar el ticket promedio para los incidentes con categoria Alto, Medio, Bajo de los ultimos 12 meses.		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.
602	Sección VI. Requisitos de los Bienes y Servicios Conexos	6. NDR - Detección y respuesta en red e Inteligencia de amenazas	Si bien el Anexo Técnico establece el requerimiento de una solución NDR (Network Detection and Response) y detalla ampliamente capacidades relacionadas con la detección, el análisis y la visibilidad del tráfico de red, no se evidencia de forma clara el alcance asociado a la fase de respuesta y contención, componente esencial de este tipo de tecnologías. De manera específica, no se precisa: •El tipo de acciones de respuesta que deberá ejecutar la solución ante la identificación de una amenaza. •El mecanismo mediante el cual deberá llevarse a cabo la respuesta y contención, ya sea: oa través de integración con la infraestructura de seguridad existente de la DIAN, omediante acciones directas ejecutadas por la propia solución NDR, oo a través de un esquema combinado de ambos enfoques. Por lo anterior, solicitamos de manera respetuosa a la Entidad aclarar y delimitar el alcance de las funcionalidades de respuesta y contención esperadas, indicando como mínimo: •Los tipos de acciones de respuesta y/o contención que deberá soportar la solución. •El esquema de ejecución de dichas acciones (integración, ejecución directa o ambos). •El nivel de automatización esperado para dichas respuestas (manual, semiautomático o automático).		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el numeral es claro en cuanto a funcionalidades y características por lo tanto no se acepta su sugerencia, por cuanto los alcances están claramente definidos.
603	Sección VI. Requisitos de los Bienes y Servicios Conexos	6. NDR - Detección y respuesta en red e Inteligencia de amenazas	En el Anexo Técnico se describen de forma general las capacidades y funcionalidades asociadas a la solución NDR requerida; sin embargo, no se identifica de manera precisa el alcance respecto a la infraestructura que deberá ser cubierta. En particular, no se determina la cantidad de Datacenters de la Entidad (principales, alternos o de contingencia) que deberán ser protegidos, ni si la solución deberá operar de forma simultánea en todos ellos o únicamente en aquellos catalogados como críticos. En este sentido, solicitamos respetuosamente a la Entidad aclarar en cuál o cuáles Datacenters se prevé la instalación de la solución NDR, así como el alcance esperado de dicha implementación.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, en el respectivo numeral se definen las características que debe tener este servicio, así mismo, en el anexo se hace claridad que los servicios deben cubrir la infraestructura tecnológica de la Entidad, que esta detallada en los respectivos cuadros de inventario mostrados en los documentos del proyecto, se aclara que la información es amplia y suficiente para que el futuro proveedor pueda dimensionar su ofrecimiento.
604	Sección VI. Requisitos de los Bienes y Servicios Conexos	6. NDR - Detección y respuesta en red e Inteligencia de amenazas	Actualmente, el mercado de ciberseguridad ofrece múltiples soluciones que incorporan funcionalidades relacionadas con la visibilidad y detección de eventos en red; no obstante, no todas ellas corresponden a plataformas NDR (Network Detection and Response) propiamente dichas, ni cuentan con un nivel de madurez, reconocimiento o validación por parte de firmas especializadas de análisis del mercado. Si bien el Anexo Técnico contempla diversas capacidades asociadas al monitoreo, detección y análisis del tráfico de red, no se establece un criterio objetivo que permita asegurar que la solución ofertada corresponda realmente a una plataforma NDR reconocida, y no a una funcionalidad parcial integrada dentro de otro tipo de tecnología, tales como IDS, NetFlow, NPM, SIEM extendido u otras aproximaciones similares. Esta falta de definición puede derivar en el riesgo de que la Entidad adquiera una solución distinta a una NDR real, lo cual podría afectar los objetivos esperados de detección avanzada, análisis basado en comportamiento, uso de inteligencia artificial y capacidades de respuesta ante amenazas en la red. En consecuencia, solicitamos respetuosamente que la Entidad considere establecer como criterio de validación que la solución NDR ofertada corresponda a una tecnología reconocida en el mercado, solicitando para ello que: •La solución se encuentre posicionada en al menos uno de los cuadrantes de Gartner para NDR, o		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
605	410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN 8.20	En el ciclo de desarrollo las herramientas del CONTRATISTA deben utilizar SASE (Secure Access Services Edge), buscando seguridad en dispositivos móviles, Internet de la cosas y migración de aplicaciones on-premise hacia Cloud.	Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que la plataforma SASE sera dispuesta por parte 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.

606	410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN 8.30	Determinar automáticamente los scanner de código a utilizar en función del lenguaje, atributos y configuración de la aplicación.	Agradecemos a la entidad confirmar si el escaneo realizado debe contener los atributos relacionados.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem referido menciona y es razonable que el escaneo (análisis estático y/o dinámico) deba contener o tener en cuenta los atributos relacionados con la aplicación, en la medida en que dichos atributos sirvan para seleccionar los escáneres y configurar el análisis.
607	410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN 8.45	Debe tener la funcionalidad de visualizar en detalle las vulnerabilidades de una aplicación, en el cual se muestre: - Archivo asociado - Número de líneas (SAST) o URL(DAST) - Severidad de la vulnerabilidad - Descripción. - CWE asociado, si existe. - El número de instancias en las que se encuentra - Historia de la vulnerabilidad que incluye el tiempo de su primera y última aparición. - Estado de la Vulnerabilidad (Activa o Cerrada).	Agradecemos a la entidad confirmar si al mencionar instancias se esta haciendo referencia a Aplicaciones. En caso de no ser si por favor confirmar a que se refiere con instancias.		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, al mencionar instancias se refiere a cada ocurrencia individual/localizada de la vulnerabilidad que el escaneo fue capaz de identificar.
608	410-20260220-Anexo-Tecnico-Proyecto-SOC-DIAN 8.48	Debe permitir filtrado en función de los directorios específicos.	Es de nuestro entender que la funcion de filtrado especifico debe contener: * Ámbito * Categoría * Con archivos adjuntos * Con comentarios * CWE * CWE Top 25 2023 * DISA STIG 5.1 * DISA STIG 5.2 * DISA STIG 5.3 * DISA STIG 6.1 * Error enviado * Estado * Estado del auditor * Estado del desarrollador * FISMA * Herramienta de análisis * Microservicio * NIST SP 800-53 Rev. 5 * Origen * OWASP 2014 Mobile * OWASP 2017 * OWASP 2021 * OWASP API Top 10 2023		La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem refiere a la capacidad de seleccionar qué carpetas del código se analizan y/o de ver los hallazgos agrupados o filtrados por esas mismas carpetas.
609	Sección VII	Requisito actual: La solución debe estar en capacidad de instalarse en Azure, AWS, HyperV, VMware (en las versiones con que cuenta la entidad).	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 informa al observante que, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
610	Sección VII	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 informa al observante que, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
611	Sección VII	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, los ítems 2.12 y 2.33 fueron eliminados del anexo técnico mediante adenda a publicar en los próximos días.
612	Sección VII	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 informa al observante que, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
613	Sección VII	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, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.

614	Sección VII	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, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
615	Sección VII	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 inyección 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, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
616	Sección VII	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, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
617	Sección VII	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 informa al observante que, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
618	Sección VII	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.
619	Sección VII	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.	Justificación: 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 informa al observante que, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
620	Vacio	Vacio	Vacio	Vacio	
621	Vacio	Vacio	Vacio	Vacio	
622	Vacio	Vacio	Vacio	Vacio	
623	Vacio	Vacio	Vacio	Vacio	
624	Vacio	Vacio	Vacio	Vacio	
625	Sección III. Criterios de Evaluación y Calificación	b. Nivel de partner más alto en las capacidades ofertadas (ítems 2 al 9 del anexo técnico).	los criterios de evaluación deben ser objetivos. Los niveles de "Partner" son métricas comerciales privadas que varían entre fabricantes, en la que algunos no cuentan con dichos niveles. Evaluar la calidad mediante este indicador genera una ventaja competitiva artificial basada en la capacidad de venta y no en la pericia técnica.	Sustituir el nivel de partner por la acreditación de al menos dos (2) ingenieros con certificación nivel 'Expert' o equivalente en las herramientas propuestas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, no se acepta su sugerencia, por cuanto el ítem es puntuable
626	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 informa al observante que, el SOC del futuro proveedor debe estar en la ciudad de Bogotá, es un requerimiento obligatorio.
627	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 informa al observante que, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
628	Anexo técnico: Especificaciones Técnicas Solución de análisis de código estático y dinámico para aplicaciones	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.
629	Anexo técnico: Descripción General y Requerimientos para la DIAN	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.
630	Anexo técnico: Especificaciones Técnicas Protección de Marca (Deep&Dark Web)	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 de acuerdo sugerencia se adiciona un ítem en gestión de incidentes (19.1.10), cambio que se publicará en los próximos días mediante adenda, quedando de la siguiente manera: 19.1.10 Para protección de marca deberá realizar el acompañamiento desde el inicio de la detección del incidente hasta la verificación de su cierre (takedown), para lo cual se informa que estas solicitudes se harán bajo demanda.
631	Anexo técnico: Especificaciones Técnicas Protección de Marca (Deep&Dark Web)	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, el futuro proveedor del SOC deberá integrar todos los servicios adquiridos entre sí, monitoreando toda la infraestructura tecnológica de la Entidad, definida en los documentos del proceso.
632	Anexo técnico: Especificaciones Técnicas Protección de Marca (Deep&Dark Web)	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, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.

633	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, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
634	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, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
635	Anexo técnico	La solución ofertada deberá ser provista por un fabricante en el cuadrante de líderes de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).	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, los requerimientos y características solicitadas obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
636	Anexo técnico: Especificaciones Técnicas - SIEM	Se aclara que la Entidad cuenta con Windows Server 2012R2, Windows Server 2022 y VMware ESXi, 7.0.3	La entidad tiene un plan de actualización durante el tiempo del servicio?, por favor indicar el tiempo aproximado.	Precisar fecha de cubrimiento necesario para estos S.O.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el futuro proveedor del SOC deberá integrar la infraestructura tecnológica mencionada en el proyecto.
637	Anexo técnico: Especificaciones Técnicas - SIEM	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.	Es posible tener un valor aproximado de acuerdo con la operación actual?	Indicar un promedio de casos de uso requeridos en la operación	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los 20 casos de uso solicitados son requerimientos mínimos, los demás se harán bajo demanda, no se maneja un promedio para este servicio.
638	Anexo técnico: Especificaciones Técnicas - SIEM	Contexto en tiempo real para análisis de seguridad	Por favor confirmar si se requiere suministrar herramientas que permitan estas acciones como monitoreo de estado de salud de equipos, inventario de software, monitoreo de red, nube, actualización de parches, etc. O cual es el alcance esperado en esta capacidad, con que origen de logs se puede medir?	Aclarar el suministro de herramienta o el alcance esperado	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la solución requerida para este servicio debe estar en capacidad de realizar lo solicitado para este ítem.
639	Anexo técnico: Especificaciones Técnicas - SIEM	Contexto del dispositivo y de la aplicación	Por favor confirmar si se requiere suministrar herramientas que permitan estas acciones como monitoreo de estado de salud de equipos, inventario de software, monitoreo de red, nube, actualización de parches, etc. O cual es el alcance esperado en esta capacidad, con que origen de logs se puede medir?	Aclarar el suministro de herramienta o el alcance esperado	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la solución requerida para este servicio debe estar en capacidad de realizar lo solicitado para este ítem.
640	Anexo técnico: Especificaciones Técnicas - SIEM	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.	Por favor confirmar si todos estos reportes son utilizados actualmente por la DIAN y si algunos de estos como GPG13 y NERC son mandatorios?, dado que pertenecen a norma del reino unido o del sector eléctrico y no tiene valor limitar la capacidad con esta inclusión, en lugar de esto es posible mencionar únicamente los más importantes y valorar capacidades de creación de reportes personalizables dentro del servicio que permita cubrir las necesidades de la entidad	Acotar a reportes necesarios en el servicio por default y personalizados	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
641	Anexo técnico: Especificaciones Técnicas - SIEM	Búsqueda de eventos en real - sin necesidad de indexación.	Se aceptarán soluciones líderes en el mercado que utilicen arquitecturas de indexación optimizada, siempre que cumplan con los tiempos de respuesta exigidos para búsquedas en tiempo real y análisis forense?	Permitir arquitecturas de indexación	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
642	Anexo técnico: Especificaciones Técnicas - SIEM	Supervisión de disponibilidad	Por favor confirmar si debe cubrirse estas capacidades que son para herramientas de disponibilidad y gestión de activos y no de un SIEM.	Retirar del alcance de SIEM o establecer el monitoreo desde logs de eventos o con una herramienta de propósito específico	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el ítem en mención fue retirado mediante adenda.
643	Anexo técnico: Especificaciones Técnicas - SIEM	Licenciamiento	Es posible permitir modelos de licenciamiento de UEBA basados en otros parámetros (como cantidad de usuarios o entidades), siempre que la propuesta económica sea global y no se penalice técnicamente al oferente por la métrica de consumo de su solución?	No restringir la forma de licenciar UEBA de la fábrica a proponer	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
644	Anexo técnico: Especificaciones Técnicas - SIEM	Debe tener autoaprendizaje de inventario de activos (CMDB) contando con capacidades de descubrimiento automático para alimentar y mantener actualizada la Base de Datos de Gestión de Configuración (CMDB).	La actualización de la CMDB debe realizarse con una solución de gestión de inventario y no un SIEM, es posible retirar este requerimiento?	Retirar del alcance de SIEM	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
645	Anexo técnico: Especificaciones Técnicas - SIEM	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)	El escaneo activo de la red debe realizarse con soluciones de propósito específico para esto.	Retirar del alcance de SIEM	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
646	Anexo técnico: Especificaciones Técnicas - SOAR	La solución debe proporcionar como mínimo un marco de desarrollo de tablero basado en HTML / JSON / JS	Al parecereste detalle de creación de tableros aplica para un único fabricante, podría retirarse esta limitante que permita al SOAR crear los taleros en cualquier marco de desarrollo, los cuales muchas veces son propietarios.	Permitir otras formas de desarrollo de tableros.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
647	Anexo técnico: Especificaciones Técnicas - SOAR	La solución debe tener al menos 300 playbooks preconfigurados o equivalentes	¿Podría la entidad basar este requerimiento en la cobertura funcional de las tecnologías e inventario actual de la DIAN en lugar de un número estático de 300, permitiendo que soluciones con librerías dinámicas o modulares puedan competir en igualdad de condiciones?"	Retirar este mínimo y permitir mencionarlo en la propuesta sin que esto limite las capacidades en la operación de la solución ofertada	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
648	Anexo técnico: Especificaciones Técnicas - SOAR	El administrador debe tener la capacidad de exportar Playbook, incluidas todas sus versiones guardadas (similar a SVN / GIT).	Mantener diferentes versiones o exportarlas de manera adecuada va a ser ejecución dentro del servicio, esta capacidad GIT limita los fabricantes que puedan presentarse, dado que es muy especifico de uno o dos de estos.	No involucrar el export de versiones.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
649	Anexo técnico: Especificaciones Técnicas - SOAR	La solución debe incluir al menos 300 conectores de integración preconfigurados	¿Podría la entidad basar este requerimiento en la cobertura funcional de las tecnologías e inventario actual de la DIAN en lugar de un número estático de 300, permitiendo que soluciones con librerías dinámicas o modulares puedan competir en igualdad de condiciones?"	Retirar este mínimo y permitir mencionarlo en la propuesta sin que esto limite las capacidades en la operación de la solución ofertada	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
650	Anexo técnico: Especificaciones Técnicas - Protección Base de Datos	Deberá ser capaz de monitorear al menos las siguientes plataformas de bases de datos: ... - IBM DB2 para Linux, z/OS y DB2/400 - IBM IMS para z/OS - IBM Informix - IBM Netezza	Por favor confirmar las plataformas de BBDD con las cuales cuenta la entidad y son parte del alcance de este requerimiento, para no cerrar a un cubrimiento que no será necesario tener y ampliar la opción de participación de fabricantes.	Retirar motores no utilizados por la entidad del alcance de capacidades de la solución a ofertar	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
651	Anexo técnico: Especificaciones Técnicas - Gestión y Monitoreo de Vulnerabilidades	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.	Se permitirá el cumplimiento de este ítem mediante la demostración de cobertura del 100% de las vulnerabilidades críticas y altas reportadas en el NVD (National Vulnerability Database), independientemente del conteo total de IDs históricos del fabricante?".	Retirar requerimiento de numeros especificos y generalizar el requerimiento	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.

652	Anexo técnico: Especificaciones Técnicas - Caza de Amenazas	El appliance, o solución, plataforma o servicio de decepción debe estar en capacidad de crear al menos 400 señuelos, en hasta 20 máquinas virtuales y desplegarse en mínimo 120 VLANs. o características similares o superiores en las tecnologías ofrecidas.	Se aceptarán arquitecturas de decepción basadas en otros elementos como por ejemplo agentes ligeros, nubes distribuidas, optimización de número de VMs, u otro que logren la misma capacidad de visibilidad de ataques, sin estar limitadas por un número específico de máquinas virtuales (VMs), dado que al parecer este alcance puntual pertenece a Fortinet?	Retirar requerimiento de numeros específicos y generalizar el requerimiento	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
653	Anexo técnico: Especificaciones Técnicas - Caza de Amenazas	La solución debe poder crear señuelos para ambientes OT	Es posible confirmar que tipo de dispositivos OT y redes cuentan con la entidad para acotar el alcance de la Caza de Amenazas a estos dispositivos y no contar con capacidades que no sean requeridas por la entidad, las cuales cierran la oportunidad de fabricantes para proponer.	Confirmar dispositivos utilizados en la red OT	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la característica se requiere para futuras implementaciones en la Entidad.
654	Anexo técnico: Especificaciones Técnicas - NDR	La herramienta debe soportar los siguientes modos de implementación: Port mirror (SPAN PORT)	Considerando que port mirror debe ser una opción, pero teniendo en cuenta diferentes necesidades de despliegue en las diferentes redes o vlans, es posible considerar despliegues en línea como complemento de la solución?	Ampliar métodos de despliegue	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
655	Anexo técnico: Especificaciones Técnicas - NDR	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.	Con el objetivo de optimizar costos, por favor considerar reducir el tiempo de retención, dado que la inspección de tráfico puede contener una enorme cantidad de datos para almacenar y no son muy necesarios en el tiempo dentro del hardware, dado que se genera envío de logs y/o reportes que mantienen los eventos históricos y sus datos requeridos en el futuro lejano para revisión de incidentes (posterior a 1 mes)	Reducción de retención a 1 mes.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
656	Anexo técnico: Especificaciones Técnicas - NDR	El CONTRATISTA deberá entregar un servicio con licenciamiento total de la solución para 17727 dispositivos por (3) años.	Es posible contar con datos de tráfico en Gbps en lugar de dispositivos?	Ampliar la información de licenciamiento	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la cantidad solicitada es por 25000 dispositivos, el ítem en mención se corrige mediante adenda, así mismo, se aclara que la cantidad requerida es suficiente para que el futuro proveedor de SOC pueda dimensionar su ofrecimiento.
657	Anexo técnico: Especificaciones Técnicas - Análisis de código estático y dinámico	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	Al parecer WEB Inspect es un componente nombrado en Fortify de esta manera, es posible confirmar que capacidad es la que busca la entidad, quizá se refiera a DAST y busca una correlación dinámica (IAST/DAST), la cual de esta manera puede darse el cumplimiento con otro fabricante diferente a Fortify.	Aclarar el alcance de WEB Inspect	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.
658	Anexo técnico:Administrativos - Certificaciones	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.	Por favor retirar requerimiento dado que la entidad solicita 8 soluciones o fabricantes diferentes, en los cuales es posible que no se tenga cubrimiento en todos del nivel requerido, pero si es posible garantizar una correcta implementación y administración, basado en servicios profesionales y experiencia en servicios.	Validar requerimiento de certificaciones y experiencia	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
659	SECCIÓN III	(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	Solicitamos respetuosamente a la entidad precisar la TRM aplicable para la conversión del requisito de experiencia establecido en USD (1.000.000), con el fin de garantizar una evaluación objetiva y en condiciones de igualdad. Lo anterior, considerando que el requisito permite acreditar experiencia dentro de los últimos 7 años, periodo en el cual la TRM ha tenido variaciones relevantes que impactan directamente el valor equivalente en pesos colombianos. A manera de ejemplo concreto: Hace aproximadamente 7 años, la TRM era de $3.177,94 COP/USD, por lo que USD 1.000.000 equivalían a $3.177.940.000 COP. Actualmente, con una TRM de $3.650,62 COP/USD, USD 1.000.000 equivalen a $3.650.620.000 COP. Esto representa una diferencia cercana a $472.680.000 COP, lo que evidencia que el mismo requisito en dólares no es equivalente en términos reales, generando una carga distinta para los proponentes dependiendo del momento en que ejecutaron sus contratos. En ese sentido, la ausencia de una regla clara de conversión puede afectar los principios de igualdad, proporcionalidad y selección objetiva, establecidos en la Ley 80 de 1993, la Ley 1150 de 2007 y el	Por lo anterior, se solicita: i) Definir expresamente la TRM aplicable para la conversión (por ejemplo, la TRM del año de ejecución, de suscripción o de liquidación del contrato), o en su defecto, ii) Permitir la acreditación del requisito en pesos constantes o ajustados, de manera que se garantice una comparación homogénea, objetiva y equitativa de la experiencia. Lo anterior, con el fin de evitar distorsiones en la evaluación y asegurar que el requisito mida efectivamente la capacidad del proponente, sin generar barreras indirectas a la participación.	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 se hará el análisis de las certificaciones de acuerdo a lo expuesto en el mismo ítem, no se permite pesos constantes o ajustados.
660	SECCIÓN III	Entre los contratos presentados se debe cumplir que: Al menos uno (1) debe haber sido ejecutado para el sector Financiero	Respecto al requisito que establece que "al menos uno (1) de los contratos debe haber sido ejecutado para el sector financiero", solicitamos respetuosamente a la entidad precisar el alcance y los criterios de verificación de dicha condición. Lo anterior, en la medida en que el término "sector financiero" resulta ambiguo y puede dar lugar a interpretaciones subjetivas durante la etapa de evaluación	En particular, se solicita aclarar: Si se entenderá por "sector financiero" exclusivamente a entidades vigiladas por la Superintendencia Financiera de Colombia (como bancos, aseguradoras, fiduciarias, etc.), O si se incluirán otras entidades con actividades financieras, tales como cooperativas, fintech, entidades de economía solidaria o empresas con operaciones financieras internas. Adicionalmente, es necesario definir qué tipo de soporte será válido para acreditar dicha condición (certificación contractual, objeto del contrato, actividad económica del contratante, entre otros), con el fin de garantizar una verificación objetiva	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, por sector financiero debe entenderse bancos, corporaciones financieras, otras entidades con actividades financieras, tales como cooperativas, fintech, entidades de economía solidaria o empresas con operaciones financieras internas, etc., siempre y cuando pertenezca al sector mencionado.

661	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.	Respecto al requisito que exige certificación de vinculación directa y activa con FIRST (Forum of Incident Response and Security Teams) con una antigüedad mínima de doce (12) meses, solicitamos respetuosamente a la entidad su revisión, en los siguientes términos: La exigencia de una antigüedad mínima específica no guarda una relación directa con la capacidad técnica actual del proponente, en tanto que la membresía activa vigente en FIRST ya acredita el cumplimiento de estándares técnicos y buenas prácticas en la gestión de incidentes de seguridad. En consecuencia, dicho condicionamiento puede constituir una restricción desproporcionada a la participación, en contravía de los principios de pluralidad de oferentes, igualdad y selección objetiva (Ley 80 de 1993, Ley 1150 de 2007 y Decreto 1082 de 2015), así como de los lineamientos de competencia efectiva en procesos financiados por el BID. Adicionalmente, frente a la participación mediante Asociaciones en Participación, Consorcio o Asociación (APCA), limitar este requisito a todos los integrantes desconoce la naturaleza de estas figuras, en las cuales las capacidades se integran de manera complementaria, tal como lo reconoce el propio esquema del proceso.	i) Eliminar la exigencia de antigüedad mínima de doce (12) meses en la certificación de vinculación a FIRST, manteniendo únicamente la condición de membresía activa; ii) Permitir que, en caso de participación mediante APCA, al menos uno de sus integrantes acredite el cumplimiento de dicho requisito. Lo anterior, con el fin de garantizar condiciones de participación amplias y proporcionales, sin afectar la idoneidad técnica requerida para la ejecución del contrato.	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 antiguedad de doce (12) meses lo que es amplio y suficiente a consideración de la Entidad, así mismo se indica que en caso de APCA, para optar por dicha puntuación al menos uno de los integrantes la deberá acreditar.
662	VI	El requerimiento contempla la adquisición de una solución catalogada como NDR (Network Detection and Response); sin embargo, a partir de los criterios técnicos establecidos, no se identifican elementos objetivos que permitan diferenciar una plataforma NDR propiamente dicha frente a otras tecnologías que incorporan únicamente funciones parciales de monitoreo o análisis de tráfico de red.	Lo anterior podría impactar el cumplimiento de los objetivos esperados en términos de detección avanzada, análisis basado en comportamiento, uso de inteligencia artificial y capacidad de respuesta ante amenazas en la red. En ese sentido, se solicita respetuosamente a la Entidad definir un criterio técnico que garantice que la solución ofertada corresponda efectivamente a una plataforma NDR reconocida en el mercado, soportada mediante documentación verificable emitida por firmas especializadas de análisis del sector, como Gartner.	Dado que en el mercado existen soluciones de distinta naturaleza tecnológica (IDS, NetFlow, NPM, SIEM con capacidades extendidas, entre otras) que podrían cumplir parcialmente los requisitos descritos, la ausencia de un criterio de validación explícito puede dar lugar a interpretaciones disímiles sobre lo que la Entidad entiende como una solución NDR.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
663	VI	De la revisión del Anexo Técnico no resulta claro el alcance de la solución NDR en relación con la infraestructura de Datacenters de la Entidad. En particular, no se especifica si la implementación deberá considerar uno o varios Datacenters, ni si su cobertura deberá extenderse a todos los ambientes (principales, alternos o de contingencia), o únicamente a aquellos considerados críticos.	Esta falta de precisión impide dimensionar adecuadamente la solución, tanto desde el punto de vista técnico como operativo, y puede generar interpretaciones distintas entre los oferentes. Por lo anterior, se solicita a la Entidad indicar de manera expresa el Datacenter o Datacenters en los cuales se prevé el despliegue de la solución NDR, así como el alcance esperado de dicha cobertura.	Se solicita aclaración	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el alcance especificado para el servicio en cuestión esta claramente detallado en los inventarios referenciados en los documentos del proceso, y debe cubrir toda la infraestructura tecnológica de la Entidad en las cantidades solicitadas.
664	VI	Si bien los requisitos técnicos desarrollan ampliamente las capacidades asociadas a la detección y análisis del tráfico de red, no se encuentra definido de forma concreta el alcance de las funcionalidades relacionadas con la respuesta y contención ante incidentes de seguridad, las cuales forman parte integral del enfoque NDR. En particular, no se establece si la solución deberá limitarse a la generación de alertas y evidencias, o si se espera que ejecute acciones de respuesta, ni el mecanismo mediante el cual dichas acciones serían implementadas, ya sea mediante integración con las herramientas de seguridad existentes de la DIAN, acciones directas desde la plataforma NDR, o un esquema mixto. Adicionalmente, no se precisa el nivel de automatización requerido para dichas respuestas, lo cual resulta relevante para la correcta alineación de la solución con los procesos operativos de la Entidad. En consecuencia, se solicita aclarar el alcance funcional esperado en materia de respuesta y contención, indicando los tipos de acciones requeridas, el modelo de ejecución y el grado de automatización esperado.		Se solicita aclarar	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, el alcance especificado para el servicio en cuestión esta claramente detallado en los documentos del proceso, y debe cubrir toda la infraestructura tecnológica de la Entidad en las cantidades solicitadas.
665	VI	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.		Gerente de Proyecto Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Gerencia de proyectos y Especialización en seguridad de la información con mínimo 2 de las siguientes certificaciones vigentes•PMP •Scrum Master -Scrum fundamental - Auditor Líder Mínimo CINCO (5) 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 y/o ciberseguridad , plan de recuperación de desastres o continuidad de negocio, demostrados con al menos dos (2) proyectos	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
666	VI	**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		**Líder /Coordinador SOC** Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines. Posgrado en Gerencia de proyectos Certificaciones vigentes: PMP o Auditor Líder 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 y /o gerente o coordinador de SOC demostrados en al menos dos(2) proyectos de esta naturaleza	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.

667	VI	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.		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 dos (2) años de experiencia profesional en proyectos de tecnologías de la información de los cuales dos (2) 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.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
668	VI	**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		**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 Alguna de las siguientes Certificaciones vigentes: • Licensed Penetration Tester (LPT) o Certifed Ethical Hacker (CHE) Mínimo tres (3) años de experiencia profesional en proyectos de tecnologías de la información dentro de los cuales dos (2) 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	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
669	VI	**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		QA / Analista de Calidad SOC. Ingeniería industrial , de sistemas o, telemática o, electrónica o, telecomunicaciones. Alguna de las siguientes Certificaciones vigentes: • ISO 9001 - Auditor Lider - Auditor Interno 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	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
670		**Tres (03) Analistas SOC Nivel I** Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 2 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: -Cédula de Ciudadanía -Tarjeta Profesional -Certificación vigente como analista o profesional o especialista o arquitecto en seguridad de operaciones o su equivalente en las soluciones ofertadas (SIEM, SOAR, caza de amenazas o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. - Certificación en Plataformas de Gestión de la Superficie de Ataque. - Certificaciones de experiencia mínima de dos (2) años en implementación y/o soporte y/o administración de soluciones de seguridad. **NOTA: Estos tres perfiles (analista I) deben cumplir los ANS de 7x24x365**		**Dos (02) Analistas SOC Nivel I** Profesional en Ingeniería de sistemas o, telemática o, electrónica o, telecomunicaciones o, afines, con experiencia mínima de 2 años a partir de la emisión de la Tarjeta Profesional y para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986: -Cédula de Ciudadanía -Tarjeta Profesional -Certificación vigente como analista o profesional o especialista o arquitecto en seguridad de operaciones o su equivalente en las soluciones ofertadas (SIEM, SOAR, caza de amenazas o Protección de Marca) emitida por el fabricante con el cual se presenta el oferente. - Certificación en Plataformas de Gestión de la Superficie de Ataque. - Certificaciones de experiencia mínima de dos (2) años en implementación y/o soporte y/o administración de soluciones de seguridad. **NOTA: Estos tres perfiles (analista I) deben cumplir los ANS de 7x24x365**	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
671	410-Formulario-1-lista-de-precios-VSD	NOTA 2: Todos los elementos adquiridos y entregados, producto del presente proceso contractual serán de propiedad de la DIAN, para los casos donde aplique.	¿Puede la DIAN confirmar que la exigencia de que "todos los elementos adquiridos y entregados sean de propiedad de la DIAN, para los casos donde aplique" se entenderá aplicable únicamente a bienes o licencias transferibles (on-premise), y que para capacidades prestadas bajo modalidad SaaS/suscripción se aceptará el derecho de uso durante la vigencia del contrato (y, de ser necesario, un periodo de transición), sin requerir que dichas licencias/servicios sean de propiedad de la DIAN?	No aplica	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, su entendimiento es correcto.
672	410-Formulario-1-lista-de-precios-VSD	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.	¿Podría la DIAN confirmar si en el documento existe un error de redacción al indicar "Inteligencia de Amenazas (NDR)"? En términos técnicos, NDR corresponde a "Network Detection and Response" (Detección y Respuesta en Red), mientras que "Inteligencia de Amenazas" suele referirse a Threat Intelligence (TI). Agradecemos precisar el concepto correcto, con el fin de interpretar adecuadamente el alcance de la exigencia y las certificaciones asociadas.	Sugerimos corregir la denominación para evitar ambigüedades, conforme aplique: (i) "Network Detection and Response (NDR)", o (ii) "Inteligencia de Amenazas (Threat Intelligence – TI)".	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, la denominación refiere a inteligencia de amenazas y NDR.
673	8.1	Marca (Especificar la marca ofrecida)	Se identifica que no hay una tecnología única que cumpla con el requisito para ambos análisis estático y dinámico.	Se solicita amablemente que se permita el uso de múltiples herramientas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
674	4		Se identifica que en los numerales 4.15, 4.20, 4.24, 4.27, 4.33, 4.36, 4.39, 4.40, 4.43, 4.51, 4.52, 4.54.4, 4.54.5, 4.54.6, 4.54.6, 4.54.10 hacen referencia a una tecnología única o muy específica como es IBM Guardium.	Solicitamos amablemente quitar estos requisitos o abrirlos a múltiples fabricantes.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.

675	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 tos hallazgos identificados por la inteligencia Artificial. - Se deberá poder integrar el proceso de Threat Hunting automatizado para que otros servicios via 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.	Se identifica que el numeral 7.23 no hace relación a tecnología NDR sino a threat hunting, contemplado en la sección 6 de Caza de Amenazas.	Solicitamos amablemente quitar este requisito o permitir cubrirlo con múltiples herramientas de caza de amenazas.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
676	18.2	Certificaciones	Se identifica que la sección 18.2 relativa a las certificaciones hace relación a herramientas físicas y no a tecnologías SaaS.	Solicitamos amablemente quitar estos requisitos o especificar su cumplimiento únicamente en caso de ofrecerse en modalidad hardware físico.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
677	Inventario Infraestructura IT		Se solicita amablemente el detalle de los fabricantes de tecnologías cloud usadas en DIAN.	NA	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los fabricantes de la nubes utilizadas por la DIAN, son MICROSOFT y AMAZON.
678	2.7	Debe manejar tasa de retención de doce (12) meses en línea y doce (12) meses fuera de línea.	En atención al requerimiento de retención definido por la Entidad (12 meses en línea y 24 meses fuera de línea), y con base en prácticas operativas habituales para SIEM/SOC, consideramos que dicho esquema puede resultar desproporcionado para el objetivo principal de operación (detección, análisis, respuesta y hunting) y generar sobrecostos y afectación de desempeño sin un incremento equivalente en valor. Desde una perspectiva técnica, la retención "en línea" implica datos indexados y consultables en tiempo casi real (hot/warm), lo cual es el componente más costoso en términos de almacenamiento, licenciamiento (EPS/GB/día), cómputo de indexación y tiempos de búsqueda. Incrementar la ventana en línea de 3 a 12 meses suele multiplicar el volumen indexado y los costos asociados, además de degradar el rendimiento de consultas y correlación (mayor latencia, mayor tiempo de reindexación y ventanas de mantenimiento más extensas), afectando la oportunidad de la operación del SOC. Adicionalmente, en la práctica la gran mayoría de investigaciones operativas y de threat hunting se concentran en ventanas recientes (30–90 días), ya que las detecciones, movimientos laterales y persistencia suelen identificarse y tratarse dentro de ese horizonte cuando existe monitoreo continuo. Por ello, proponemos un modelo escalonado: (i) 3 meses en línea (indexado y consultable) para operación diaria y hunting; y (ii) 9 meses fuera de línea o en	¿Puede la DIAN confirmar si la exigencia de 12 meses en línea y 24 meses fuera de línea obedece a una disposición normativa, lineamiento de auditoría o requerimiento específico de investigación (por tipo de fuente de log)? En caso de no existir una obligación expresa, solicitamos considerar un esquema escalonado que mantenga el valor operativo y optimice costos/desempeño, por ejemplo: - 3 meses en línea (indexado y consultable en SIEM) para operación y hunting; - 9 meses fuera de línea o en repositorio de bajo costo, recuperable/consultable bajo demanda con tiempos definidos; - y, si se requiere 24 meses, retención como archivo inmutable (evidencia) sin indexación permanente, garantizando exportación/consulta cuando sea necesario.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
679	8.20	En el ciclo de desarrollo las herramientas del CONTRATISTA 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 identifica que SASE no es un requisito natural de SAST/DAST, sino un modelo/arquitectura de acceso y seguridad perimetral, no una propiedad intrínseca del análisis de código.	Se solicita amablemente quitar este requisito.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
680	6.3.1	Para el monitoreo y alertamiento temprano sobre nuevas vulnerabilidades, ataques. amenazas externas y del ciberespacio que puedan afectar a la infraestructura interna de la entidad el CONTRATISTA debe adelantar el despliegue, configuración y afinamiento de herramientas para cacería de amenazas, las cuales permitan tener una visual horizontal y vertical en el caso de incidentes de seguridad de la información. Debe tener por lo menos las siguientes componentes: Herramientas de caza de amenazas: herramienta para buscar e interceptar ataques ocultos de una manera proactiva. Se puede desplegar una sola herramienta siempre y cuando tanto la inteligencia como la caza sean completamente identificables y a nivel de mercado sea aceptada como tal. Hay que tener en cuenta que el despliegue de herramientas que no tengan las capacidades de cacería de amenazas completas, no serán evaluadas. Parametrizar y/o configurar la herramienta adquirida, a partir de las mejores prácticas definidas por el fabricante y las exigencias de la entidad.	Se identifica que se solicita una herramienta dedicada a caza de amenazas. La caza de amenazas se realiza mediante múltiples tecnologías no necesariamente exclusivas para ello, con el enriquecimiento de la inteligencia de amenazas.	Se solicita formalmente el uso de múltiples herramientas para ofrecer servicio de caza de amenazas y que no sean exclusivamente para este fin.	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.
681	Inventario Infraestructura IT		Se solicita amablemente la confirmación de las nubes en las cuales la DIAN posee infraestructura tecnológica	NA	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los fabricantes de la nubes utilizadas por la DIAN, son MICROSOFT y AMAZON.
682	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	De manera respetuosa, solicitamos a la Entidad ajustar el perfil descrito en la celda Observaciones!G55 para que, en lugar de exigir la certificación ISO 9001, se requiera la certificación ISO/IEC 27001 (o equivalente), por ser el estándar internacional de referencia para la implementación y gestión de un Sistema de Gestión de Seguridad de la Información, alineado con la naturaleza y criticidad de los servicios de ciberseguridad objeto del proyecto.	NA	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, las características y requerimientos solicitados obedecen a necesidades puntuales de la Entidad, por lo tanto, no se acepta su sugerencia.

683	Equipo Mínimo de trabajo	El Numeral 5 de los requisitos financieros, que define el indicador de apalancamiento a corto plazo Pasivo Corriente/Patrimonio, debera ser Menor o igual a 0,5	Se solicita a la Entidad informar de manera expresa los criterios técnicos, financieros y la fuente metodológica utilizada para la definición de los indicadores de capacidad financiera exigidos, en especial el indicador de apalancamiento a corto plazo (Pasivo Corriente / Patrimonio ≤ 0,5). Lo anterior, toda vez que dicho umbral resulta desproporcionado y restrictivo frente a las prácticas financieras del mercado, incluso para empresas con adecuada solidez patrimonial y capacidad operativa. Este nivel de exigencia limita injustificadamente la pluralidad de oferentes, en contravía de los principios de selección objetiva y libre concurrencia. Adicionalmente, el indicador de apalancamiento a corto plazo, en los términos planteados, no constituye por sí mismo un criterio determinante de riesgo contractual, ya que puede reflejar dinámicas normales de operación, gestión de flujo de caja o estrategias financieras propias del giro ordinario del negocio, sin que ello comprometa la liquidez, la estabilidad financiera ni la capacidad de ejecución del contrato.	Se sugiere a la Entidad evaluar el ajuste del indicador de apalancamiento a corto plazo (Pasivo Corriente / Patrimonio), estableciendo un umbral que refleje de manera más adecuada las condiciones del mercado, tales como un valor menor o igual a uno punto ocho (≤ 1,8), o alternativamente, adoptar parámetros sustentados en promedios sectoriales o metodologías financieras reconocidas. Este ajuste permitiría fortalecer la pluralidad de oferentes, promover la competencia efectiva y garantizar la participación de empresas con capacidad técnica y operativa suficiente, sin comprometer la adecuada ejecución del contrato ni incrementar el nivel de riesgo para la Entidad.	En atención a la observación no se acepta la solicitud, el indicador se mantiene en las mismas condiciones debido a la envergadura del proyecto.
684	7.7.10	(i) El Oferente deberá proporcionar prueba documental que demuestre que cumple los siguientes requisitos financieros:	El indicador de apalancamiento a corto plazo (Pasivo Corriente / Patrimonio) fijado en ≤ 0,5 introduce una restricción que no refleja de manera integral la solvencia ni la capacidad financiera real del oferente, toda vez que este ratio, analizado de forma aislada, no incorpora variables clave como liquidez corriente, flujo de caja operativo o cobertura de obligaciones, ampliamente utilizadas en análisis financiero bajo estándares internacionales (NIIF/IFRS)	Se solicita ajustar el umbral del indicador a un valor ≤ 1,2, en concordancia con prácticas financieras del mercado y análisis integral de estados financieros, permitiendo una evaluación más objetiva de la capacidad de endeudamiento de corto plazo. Lo anterior en aplicación de los principios de pluralidad de oferentes y selección objetiva establecidos en la Ley 80 de 1993 (art. 24 y 29) y la Ley 1150 de 2007, evitando restricciones que limiten la participación sin una justificación técnica suficiente.	En atención a la observación. no se acepta la solicitud, el indicador se mantiene en las mismas condiciones debido a la envergadura del proyecto.
685	18.2	(i) El Oferente deberá proporcionar prueba documental que demuestre que cumple los siguientes requisitos financieros:	El indicador de apalancamiento a corto plazo (Pasivo Corriente / Patrimonio), establecido en un valor ≤ 0,5, se considera restrictivo frente a las prácticas financieras del mercado.	Se recomienda ajustar el indicador de apalancamiento a corto plazo (Pasivo Corriente / Patrimonio), actualmente ≤ 0,5, a un valor ≤ 1,15, por considerarse un umbral más acorde con las prácticas financieras del mercado.	En atención a la observación no se acepta la solicitud, el indicador se mantiene en las mismas condiciones debido a la envergadura del proyecto.
686	X	• 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 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.	Modificar el formato de presentacion de los balances y estados de resultados, ya que al ser una oferta internacional no necesariamente todos los reportes van en el formato solicitado	Modificar el formato de presentacion de los balances y estados de resultados, ya que al ser una oferta internacional no necesariamente todos los reportes van en el formato solicitado	Se precisa al observante que los estados financieros requeridos en el documento de solicitud corresponden a la información financiera mínima necesaria para verificar la capacidad financiera de los oferentes dentro del proceso. En el caso de oferentes extranjeros, el mismo documento establece expresamente que podrán presentar "los documentos o sus equivalentes de acuerdo con las normas del país de origen", permitiendo así que la información financiera sea aportada conforme a los estándares contables y formatos aplicables en cada jurisdicción. En consecuencia, no se considera necesario modificar el formato de presentación solicitado, toda vez que el requerimiento no pretende imponer un modelo contable específico, sino garantizar que la información financiera presentada permita realizar una verificación objetiva, comparable y suficiente de la situación financiera del oferente.
687		Monedas de la Oferta y de los Pagos . 15.2 El Oferente podrá expresar el Precio de su Oferta en cualquier moneda. Si el Oferente desea recibir el pago en una combinación de montos en diferentes monedas, podrá cotizar su precio en las monedas que correspondan. Sin embargo, no podrá incluir más de tres monedas extranjeras además de la del País del Comprador.	Se identifica que el Anexo 410 – Formulario 1 Lista de Precios VSD, el cual es de diligenciamiento obligatorio y no permite modificaciones, no contempla campos ni opciones para la selección, combinación o discriminación de precios en diferentes monedas, permitiendo únicamente el registro de valores en una única moneda. Solicitamos modificar el anexo indicando la opción de la composición de la oferta económica en múltiples monedas,		Se aclara que se podrá incluir la moneda de la preferencia dentro de la lista de precios, no obstante, se precisa que no se podrá modificar el formulario de lista de precios ni los otros formularios incluidos en la Solicitud de Oferta.
688	2.13	Fecha limite para presentar ofertas	Observación: Solicitamos a la DIAN ampliar unos dias más la entrega de la licitación asociada al presente proceso.		Mediante Adenda No. 1 de amplió el plazo de presentación de ofertas hasta el 9 de junio de 2026 hasta las 10:00 a.m. (hora legal colombiana)
689	Financiera		Respecto al indicador de Apalancamiento a corto plazo, agradecemos considerar la naturaleza de las entidades del sector económico al que pertenecen los potenciales Ofertantes se caracteriza por financiamientos altos, esto es endeudamientos altos que permiten constantes renovaciones, adquisiciones y actualizaciones de infraestructura (a través de financiamiento). En ese sentido, agradecemos modificar el indicador aceptable de Apalancamiento de corto plazo de menor o igual a 0.5, a menor o igual a 1,2.		En atención a la observación no se acepta la solicitud, el indicador se mantiene en las mismas condiciones debido a la envergadura del proyecto.
690	IAO 11.1		En la medida en que los indicadores considerados para el cumplimiento de capacidad financiera implican una evaluación integral a la situación financiera de los oferentes, y al menos tres indicadores tienen a consideración el endeudamiento o pasivos de los oferentes (a saber, índice de liquidez, razón de endeudamiento y Apalancamiento de corto plazo), agradecemos modificar el criterio de habilitación permitiendo que los oferentes que cumplan con dos de tres criterios asociados con pasivos o endeudamientos esto es, dos o tres criterios ente el índice de liquidez, razón de endeudamiento y apalancamiento de corto plazo.		En atención a la observación no se acepta la solicitud, los indicadores se mantiene en las mismas condiciones debido a la envergadura del proyecto.

691	Financiera		En cuanto a la acreditación de requisitos habilitantes como existencia, capacidad financiera y experiencia técnica, agradecemos confirmar que los oferentes extranjeros con origen en un País Elegible, que aporten documentación obtenida en el extranjero podrán presentar los documentos i) en sus monedas de origen sin necesidad de conversión, ii) sin necesidad de apostillas o legalizaciones, y iii) no será necesario otra solemnidad para acreditar la condición o calidad del firmante. Lo anterior teniendo en cuenta que las disposiciones de la IAO 11.1.j, establecen que "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 precisa al observante que, de conformidad con lo establecido en el documento de solicitud, los oferentes extranjeros provenientes de países elegibles podrán presentar los documentos o sus equivalentes conforme a las normas aplicables en su país de origen. En este sentido, para la acreditación de requisitos habilitantes financieros, jurídicos y técnicos, se aceptarán documentos expedidos en el extranjero que permitan verificar de manera suficiente las condiciones requeridas dentro del proceso. Los estados financieros para verificar los requisitos financieros corresponderán al último año fiscal cerrado. Para el caso de las firmas con residencia fiscal en Colombia, se tomarán los estados financieros con corte al 31 de diciembre de 2025. En el caso de países cuyos cierres fiscales correspondan a meses diferentes, se deberá aportar el último estado financiero aprobado por la Junta Directiva o quien haga sus veces, adjuntando la normatividad que sustente dicha fecha de cierre. Para efectos de la verificación financiera, se aplicará la Tasa Representativa del Mercado (TRM) vigente publicada por la Superintendencia Financiera de Colombia al cierre de la vigencia fiscal de los estados financieros. Así mismo, en el caso de oferentes extranjeros, se podrán presentar documentos equivalentes a los certificados de existencia y representación legal o registro mercantil, expedidos por la autoridad competente del país de origen, siempre que estos permitan verificar, como mínimo, la constitución de la firma, su vigencia, el objeto social y las facultades de representación del firmante. Frente a las formalidades documentales, se aclara que los documentos emitidos en el extranjero que acompañen la oferta no requerirán apostilla o legalización para su presentación dentro del proceso. Igualmente, cuando dichos documentos se encuentren en un idioma distinto al español, podrán ser aportados con traducción simple. No obstante, en caso de adjudicación, la entidad podrá solicitar la presentación de documentos debidamente apostillados o legalizados, según corresponda.
692	Financiera		En cuanto a la forma de presentación de la Oferta, agradecemos limitar las alternativas (actualmente presentación presencial y digital) exclusivamente a la alternativa de radicación digital para garantizar igualdad en la forma de presentación de la Oferta a todos los interesados, en particular teniendo en cuenta el interés de oferentes del extranjero.		No se acepta la observación. La entidad considera pertinente mantener las alternativas de presentación de ofertas previstas en el documento de solicitud, esto es, tanto la presentación física como la digital, con el fin de garantizar la pluralidad de oferentes y permitir mecanismos amplios de participación dentro del proceso. En consecuencia, no se considera procedente limitar la presentación de ofertas exclusivamente al mecanismo digital, toda vez que ambas modalidades previstas en el proceso garantizan condiciones de acceso, transparencia e igualdad para todos los interesados.
693	Financiera		Respecto a la Garantía de Mantenimiento de la Oferta, agradecemos su confirmación respecto a que será suficiente con la presentación de la Declaración de Mantenimiento de la Oferta y no requerirán una garantía adicional (póliza, carta bancaria u otra).		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.
694	Procesal / Procedimental		Apalancamiento a corto plazo	Solicitamos a la entidad que ajuste del indicador "apalancamiento a corto plazo" a 1,0.	En atención a la observación no se acepta la solicitud, el indicador se mantiene en las mismas condiciones debido a la envergadura del proyecto.

Original firmado
CARLOS JAVIER OSORIO BELTRÁN
Gestor III - OSI

Original firmado
JAVIER EDGARDO SOTO ARGEL
Consultor Fondo DIAN

Original firmado
DIEGO FERNANDO PALACIOS SÁNCHEZ
Especialista de Adquisiciones - UCP