PROGRAMA APOYO A LA MODERNIZACIÓN DE LA DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES -DIAN
CONTRATO DE PRÉSTAMO BID 5148/OC-CO

PREGUNTAS Y RESPUESTAS A RFI SOC V.2

No.	Pregunta	Respuesta
1	1. Por favor compartimos los documentos adjuntos, ya que estaban incrustados como link de accesos pero pide permisos de Microsoft para descargarlos: Anexo Técnico Proyecto SOC DIAN 24 de Abril de 2024.xlsx PropuestaValoresEconomicaSOC.xlsx	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que, en los adjunto del SECOP se encuentran dicho archivos publicados para ser bajados. Darle Click en Detalle.
2	2. Agradecemos si pueden extender el plazo de las preguntas al miércoles 16 de Octubre entendiendo que el lunes es un día festivo. Con el fin de tener el tiempo de la respuesta por parte de ustedes a los documentos solicitados, analizarlos y poder lanzar las preguntas.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que, en atención a su solicitud se extiende el plazo, para que puedan realizar las consultas necesarias, así mismo alleguen la respectiva oferta de las capacidades requeridas por la DIAN para implementar un Centro de Operaciones de Seguridad SOC.
3	OBSERVACION No. 1: Estimados, Nos gustaría plantear algunas preguntas relacionadas con el estudio de mercado en curso, con el fin de aclarar ciertos aspectos antes de la presentación de nuestra oferta: ¿Es posible presentar la oferta en USD?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que la oferta allegada debe venir expresada en pesos colombianos, con el ánimo de poder realizar un análisis normalizado de las posibles ofertas.
4	OBSERVACIÓN No. 2: ¿Sería posible contar con una extensión del plazo para la presentación de la oferta?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que, en atención a su solicitud se extiende el plazo, para que puedan realizar las consultas necesarias, así mismo alleguen la respectiva oferta de las capacidades requeridas por la DIAN para implementar un Centro de Operaciones de Seguridad SOC.
5	OBSERVACIÓN No. 3: Respecto a los logs (2.12): 2.12 El contratista 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. En ningún caso la	La Dirección de Impuestos y Aduanas Nacionales – DIAN manifiesta al observante que, los futuros proponentes deben poseer capacidad instalada de Centro de Operaciones de Seguridad en Colombia, por lo tanto, su entendimiento NO ES CORRECTO.

6	OBSERVACIÓN No. 4: ¿Es necesario completar todo el anexo técnico para responder a la RFI?	La Dirección de Impuestos y Aduanas Nacionales – DIAN indica al observante que, el anexo técnico es un compendio de todas las características requeridas por la DIAN para el proyecto SOC, para efectos de que los futuros oferentes tengan el conocimiento especifico de lo requerido, por lo tanto, para la etapa de RFI su diligenciamiento es obligatorio, ya que de antemano el equipo a cargo de la DIAN conocería de primera mano cual sería el ofrecimiento de los posibles oferentes, especificando el cumplimiento de todas y cada una de las especificaciones consignadas allí.
7	Agradecemos la ayuda para aclarar los siguientes puntos que forman parte del RFI-SOC 2024. Respecto al item de Base de Datos, por favor suministrar - Inventario de BD o Numero de instancias o Fabricante(s) o Versiones de cada fabricante o Ubicacion (on-premise / Cloud) ▪ Cuales proveedores cloud estan en el alcance? ▪ Cuales proveedores On-Premise están en el alcance?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, manifiesta al observante que, la información referente a las bases de datos y demás características de estas, se encuentra en el inventario anexo a este proceso.
8	Respecto al Item Gestion de Vulnerabilidades, por favor aclarar lo siguiente: - Gestion de vulerabilidades: o Puede ofrecerse un servicio administrado en lugar de una solución? ▪ Cual es el alcance requerido para Scan de aplicaciones? ▪ Cual es el alcance para Scan de redes? - Escaneo de aplicaciones o Puede ofrecerse un servicio en lugar de un producto para ejecutar escaneos? ▪ En caso afirmativo, vamos a precisar mas detalles acerca de las aplicaciones a escanea	La Dirección de Impuestos y Aduanas Nacionales – DIAN, indica al observante lo siguiente: La solución de gestión de vulnerabilidades se solicita SaaS - Software como servicio, precisando el fabricante y el modelo de la solución a proveer. El alcance de la gestión de vulnerabilidades está definido en el ítem 5.3.2 que a la letra menciona lo siguiente: Licenciamiento para 17727 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web). Las licencias podrán ser reasginadas entre activos, sin generar costos adicionales para la Entidad. Los detalles de los activos de infraestructura los encuentran en el inventario anexo a este proyecto.

9	Respecto al Item Detección de Amenazas, por favor aclarar lo siguiente: - Deteccion de amenazas: o Cuantos endpoints se encuentran en el alcance? o Se cuenta ya con una solución EDR para servidores y equipos de computo? o Cual es el inventario de fuentes a integrar en la solución SIEM? o Donde se ubican las fuentes en el alcance? ▪ Cloud? ▪ On-premise? - SIEM o Cuantas alertas (mensuales o diarias) se generan actualmente? o Cual es la plataforma SIEM actual? - Code Review o Por favor suministrar detalles de los códigos a revisar en el alcance o Cuantas líneas de código se deben revisar? o Es posible hacer escaneos SAST en caso de ser un numero muy grande de líneas de codigo	La Dirección de Impuestos y Aduanas Nacionales – DIAN, precisa al observante lo siguiente: La cantidad de endpoints la pueden revisar en el inventario de infraestructura anexo a este proceso. Actualmente en la Entidad existe una solución EDR cuyo fabricante es BITDEFENDER. La cantidad de fuentes a integrar en el SIEM y su ubicación se encuentran en el inventario anexo. La plataforma SIEM actual es Q-RADAR de IBM. Dentro de las características solicitadas para el Item 8 de análisis de código se contempla el escáneo SAST, por lo tanto es posible, acorde a su consulta.
10	Ingenieria Social o Se incluirá phishing? ▪ En caso afirmativo, vamos a requerir detalles del alcance de la prueba. Este formato de dimensionamiento lo podemos suministrar/revisar una vez sea confirmado este punto o Se incluirá Vishing? ▪ En caso afirmativo, vamos a requerir detalles del alcance de la prueba. Este formato de dimensionamiento lo podemos suministrar/revisar una vez sea confirmado este punto o Se incluirá Physical Revew? ▪ En caso afirmativo, vamos a requerir detalles del alcance de la prueba. Este formato de dimensionamiento lo podemos suministrar/revisar una vez sea confirmado este punto.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, lo solicitado en el punto 10, son dos ejercicios de ethical hacking por año, donde el futuro proponente podrá incluir las técnicas que considere pertinentes y serán acordadas en su momento con la Entidad a razón de poder llevar dichos ejercicios a feliz término.
11	2.4. Se debe licenciar como mínimo para 1600 dispositivos (1340 que están estipulados en el inventario anexo más el 20% de incremento adicional). Observación No. 1: Se solicita a la entidad confirmar la cantidad de EPS para dimensionar este servicio. De igual forma confirmar la cantidad de retención de data en el mes.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, indica al observante que la cantidad de EPS requeridos es de 25000 EPS con una tasa de retención al mes es de 600 Gb mensual.

12	2.10. La solución debe estar en capacidad de instalarse en Azure, AWS, HyperV (en la versiones con que cuenta la entidad), Vmware (en la versiones con que cuenta la entidad). (Revisar archivo anexo inventarios). Observación No. 2: Se solicita a la entidad confirmar la catidad de equipos/servidores/servicios que se encuentra por cada plataforma (AWS/HyperV/Azure).	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que las cantidades de equipos y demás temas requeridos para dimensionamiento se encuentran en el anexo técnico e inventario que hace parte de este proceso, favor revisar.
13	Observación No. 3: Se solicita a le entidad confirmar si los servidores de recolección de datos, serán provisto por la entidad	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
14	2.36. En la solución SIEM entregada se debe integrar al SOAR, 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. Observación No. 4: Se solicita a la entidad confirmar la solución de firewall, antivirus y demás plataformas de seguridad que cuenta la entidad	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que los datos solicitados se encuentran detallados en el inventario anexo a este proyecto.
15	4.38. Contar con políticas de vulnerabilidades para bases de datos y descubrir vulnerabilidades conocidas para las siguientes bases de datos: • DB/2 • Informix • MSSQL • MySQL • Oracle • Sybase Observación No. 5: Se solicita a la entidad confirmar la cantidad de bases de datos como motores a realizar protección de bases de datos.	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, la información requerida en cuanto a características y cantidades de bases de datos de la Entidad, se encuentran referidas en el inventario anexo que hace parte de este proyecto.
16	4.54.9. La solución deberá ser capaz de poder desplegarse en nubes públicas como Amazon Web Services o Microsoft Azure. Observación No. 6: Se solicita a la entidad confirmar la cantidad de motores que cuentan en Amazon y Azure	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la solución requerida debe poseer la característica de desplegarse en nubes para cuando la Entidad lo requiera, la cantidad de motores en nube puede ser consultada en el inventario anexo que hace parte de este proyecto.
17	5.2. Referencia o Modelo o Versión (Especificar el modelo ofrecido). Observación No. 7: Se solicita amablemente a la entidad confirmar el periodo de ejecución de gestión de vulnerabilidades (Mensual, trimestral, anual) etc.	La Dirección de Impuestos y Aduanas Nacionales – DIAN manifiesta al observante que, la solución requerida en este punto debe realizar gestión de vulnerabilidades de manera proactiva las 24 horas del días por el tiempo que dure el proyecto.

18	7.1. Marca (Especificar la marca de la herramienta del servicio ofrecido). Observación No. 8: Se solicita amablemente a la entidad confirmar el throughput dentro de la red de DIAN, de igual forma confirmar la cantidad de sedes y appliances solicitados.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la cantidad de elementos a monitorear, supervisar y hacer seguimiento mediante los capacidades requeridas en este proyecto, se encuentran en el inventario anexo, así como las ubicaciones de estos, respecto a la cantidad de apliances solicitados, lo determina el oferente en su propuesta de acuerdo al estudio realizado por este a las necesidades establecidas por la Entidad en el anexo técnico.
19	Clarificaciones sobre el Alcance del Servicio y Requisitos Límite del Servicio: El RFI menciona infraestructuras tanto on-premise como en la nube. Pregunta: ¿Podría la DIAN proporcionar más detalles sobre los servicios en la nube actualmente en uso y el volumen de datos, aplicaciones o sistemas que el SOC monitoreará tanto en la nube como en las instalaciones locales? Volumen de Eventos y Amenazas: Comprender el volumen actual de eventos de seguridad/incidentes que enfrenta la DIAN es crucial para dimensionar la solución. Pregunta: ¿Podrían compartir el número promedio de eventos de seguridad, incidentes o alertas que la DIAN maneja actualmente en una base diaria/semanal y si se espera que aumenten con el tiempo?	La Dirección de Impuestos y Aduanas Nacionales – DIAN manifiesta al observante que, la cantidad de EPS en la Entidad según la infraestrura monitoreada es de 25000 EPS, los elementos a monitorear se encuentran en el inventario de activos anexo a este proyecto.
20	Clarificaciones sobre Costos y Licencias Preferencias sobre el Modelo de Costos: Aunque la DIAN solicita estimaciones de costos, no menciona cómo preferirían estructurar los costos (por ejemplo, fijo, basado en suscripción, basado en uso). Pregunta: ¿Podría aclarar su estructura de costos preferida? ¿Preferiría la DIAN una tarifa anual fija, pago por uso, o un modelo híbrido dependiendo del uso del servicio y los volúmenes de incidentes? Modelos de Licenciamiento: Si la DIAN requiere software y herramientas como parte del SOC (por ejemplo, SIEM, SOAR), no está claro si hay preferencias sobre el licenciamiento. Pregunta: Para herramientas como SIEM y SOAR, ¿preferiría la DIAN un licenciamiento de propiedad (licencias perpetuas) o basado en suscripción? ¿Deberían estas herramientas ser alojadas en la infraestructura de la DIAN o proporcionadas como un servicio gestionado?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, para efectos de tener un acercamiento real al mercado de las capacidades requeridas, la Entidad no tiene una estructura de costos preferida, por el contrario se espera que los posibles oferentes presenten una propuesta acorde a lo requerido por la Entidad y según sea su modelo de prestación de este tipo de servicios. Referente al licenciamiento de herramientas, la Entidad espera un licenciamiento a perpetuidad de las capacidades como SIEM, SOAR entre otras, y una entrega de los dispositivos a que haya lugar a la DIAN una vez se termine el contrato. Las soluciones, servicios, infraestructura y demás elementos que hacen parte de este proyecto, deberán ser administradas y gestionadas por el futuro contratista en el SOC del mismo, y una vez concluya el proyecto deberán ser retornadas (para las que aplique) a la Entidad para que queden bajo su inventario y administración.

21	Clarificaciones sobre Implementación del Proyecto Cronograma de Implementación: El RFI solicita un cronograma típico para la implementación del SOC, pero no aclara fechas de inicio o fin esperadas. Pregunta: ¿Puede proporcionar más orientación sobre la fecha de inicio esperada del proyecto y si hay fechas límite importantes para los hitos clave del proyecto? Transferencia de Conocimiento: Aunque el RFI menciona la necesidad de capacitación y transferencia de conocimiento, no se detalla el alcance de este requisito. Pregunta: ¿Podría 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 informa al observante que, si bien es cierto que no se estipula una fecha inicial esperada, el futuro contratista debe estar en la capacidad de dimensionar el proyecto, así como confeccionar un cronograma basado en las capacidades y características solicitadas por la Entidad. La transferencia del conocimiento, es una característica que se contempla en este tipo de proyectos tecnológicos y su alcance esta limitado a las herramientas, soluciones, plataformas y servicios entregados, en su administración y gestión. Respecto a los niveles mencionados en la transferencia de conocimiento, se espera que se apropie la administración y gestión de lo implementado, los demás niveles se esperan en la capacitación.
22	Clarificaciones sobre Cumplimiento y Certificaciones Marcos de Cumplimiento: El RFI menciona cumplimiento con regulaciones de ciberseguridad colombianas, pero no detalla marcos específicos (por ejemplo, ISO, NIST). Pregunta: ¿Podría aclarar los marcos de cumplimiento y certificaciones específicas (por ejemplo, ISO 27001, NIST, GDPR) que el SOC y sus operaciones deben cumplir, además de las regulaciones locales de Colombia?	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, las certificaciones de SOC, están contempladas en el anexo técnico de este proceso, items 12.78, 12.8, 12.22 entre otros.
23	Clarificaciones sobre Medidas de Seguridad Recuperación ante Desastres y Redundancia: Aunque se menciona el DRP (Plan de Recuperación ante Desastres), no hay detalles sobre los tiempos de recuperación esperados o las medidas de redundancia. Pregunta: ¿Podrían proporcionar más detalles sobre los requisitos de recuperación ante desastres y continuidad del negocio, incluyendo los Objetivos de Tiempo de Recuperación (RTO) y los Objetivos de Punto de Recuperación (RPO)?	La Dirección de Impuestos y Aduanas Nacionales – DIAN indica al observante que, el DRP se menciona como referencia en alguno de los apartes del RFI, y la infraestructura que hace parte de este. Dentro del inventario anexo se encuentra dicha infraestructura para que los posibles contratistas puedan revisar y calcular su oferta, se solicita que el futuro contratista cuente con capacidad instalada de SOC en Bogotá, y cuente con su respectiva contingencia ya sea en la misma ciudad u en otra, por lo tanto, los datos de RTO y RPO no son relevantes para hacer dichos cálculos.

24	Clarificaciones sobre Inteligencia de Amenazas Fuentes de Inteligencia de Amenazas: La DIAN menciona la necesidad de inteligencia de amenazas, pero no proporciona detalles específicos sobre las fuentes o tipos de inteligencia de amenazas requeridas. Pregunta: ¿Prefiere la DIAN fuentes específicas de inteligencia de amenazas (comerciales, gubernamentales, de código abierto)? ¿El SOC debe incluir integraciones con los feeds de inteligencia de amenazas que la DIAN ya utiliza?	La Dirección de Impuestos y Aduanas Nacionales – DIAN manifiesta al observante que, la solución requerida en este punto debe realizar gestión de vulnerabilidades en todo contexto que tenga la entidad, de modo que minimice el riesgo general en la infraestructura tecnologica, y debe realizar integración con las capacidades adquiridas en este proyecto.
25	Pregunta sobre impuestos: Incluir Impuestos: En el RFI no se menciona explícitamente si los valores estimados deben incluir impuestos. ¿Podrían confirmar si los costos propuestos por los proveedores deben incluir impuestos, como el IVA (Impuesto sobre el Valor Añadido) u otros impuestos aplicables en Colombia?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, todos los posibles oferentes que deseen participar deben presentar sus ofertas en pesos colombianos, discriminando el IVA y los valores según el formado destinado para tal fin.
26	Pregunta sobre la duración del proyecto: Duración del Proyecto: El RFI no especifica la duración esperada del proyecto de implementación del SOC. ¿Podrían proporcionar una estimación del tiempo total para la ejecución del proyecto, desde la fase de diagnóstico hasta la operación continua? ¿Existen plazos clave o hitos importantes que debamos tener en cuenta?	La Dirección de Impuestos y Aduanas Nacionales – DIAN manifiesta al observante que, la duración del proyecto, en un principio se tiene contemplada para tres (3) años, pudiendo ser más, o menos según las disposiciones presupuestales y conveniencia de la Entidad, en el tema de la implementación se tienen contemplados tiempos de dos a tres meses como máximo para poner el proyecto a punto. Es de entender que el posible contratista debe contar con capacidad instalada y funcionando de un centro de operaciones de seguridad - SOC, por lo tanto la implementación de las capacidades requeridas por la Entidad en el anexo técnico, no demanda tiempos que se puedan considerar altos o extensivos en el tiempo
27	Pregunta sobre el uso de USD en la oferta: Moneda de la Oferta: ¿Se puede presentar la propuesta en dólares estadounidenses (USD) o existe una preferencia por utilizar pesos colombianos (COP)? Si es posible utilizar USD, ¿hay algún requisito específico para convertir los valores a la moneda local para el proceso de evaluación?	La Dirección de Impuestos y Aduanas Nacionales – DIAN manifiesta al observante que, la propuesta debe ser presentanda en pesos colombianos, tal como lo indica el formato propuesta de valores que hace parte de este proceso RFI SOC
28	"Se debe licenciar como mínimo para 1600 dispositivos (1340 que están estipulados en el inventario anexo más el 20% de incremento adicional)." **Pregunta: Agradecemos a la entidad confirmar la cantidad de EPS o GB/dia que deben ser procesados en la solución SIEM.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la cantidad de EPS estipulada para este proyecto es de 25000.

29	"En caso de implementarse mediante máquina virtual, los recursos de computo serán entregados por la entidad." **Pregunta: Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que entregara todos los recursos solicitados para la implementación de la solución propuesta.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, el ítem en cuestión presenta un error involuntario en su publicación por ende se procedió a su eliminación, aclarando que, 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
30	" Se deberá disponer de paquetes de licencia de agentes de UEBA para equipos Windows. Dichas licencias de UEBA no deberán conllevar consumo asociado ni de licencia de dispositivos ni de EPS." **Pregunta: Agradecemos a la entidad confirmar la cantidad de agente de UEBA requeridos.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, los paquetes de licencias de agentes de UEBA solicitados en este ítem son para los servidores windows que tiene actualmente la Entidad, y su número y cantidades pueden ser consultados en el inventario anexo de este proceso.
31	"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)." **Pregunta: Agradecemos a la entidad confirmar la cantidad de agentes avanzados requeridos.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN indica al observante que, los paquetes de licencias de agentes avanzados requeridos son para los servidores windows y linux que tiene actualmente la Entidad, y su número y cantidades pueden ser consultados en el inventario anexo de este proceso.
32	"Especificaciones Técnicas SIEM" **Pregunta: Agradecemos a la entidad confirmar los tiempos de retención de logs requeridos, (en linea y fuera de linea).**	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el SIEM a adquirir debe manejar tasa de retención de tres (3) meses en línea y seis (6) meses fuera de línea.
33	"Debe tener correlación cruzada de analítica de SOC y NOC" **Pregunta: Agradecemos a la entidad confirmar si aunque la solución soporte analitica de SOC y NOC, para la ejecución del servicio solicitado (SIEM) unicamente se deberan tener en cuenta alertamientos de seguridad.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN indica al observante que, si para la correlación cruzada requerida en este punto de SOC y NOC, surgen alertamientos de otro tipo que no sean de seguridad y que sean relevantes para el monitoreo de SOC se deben tener en cuenta.
34	"El contratista 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. En ningún caso la información de log deberá salir de 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." **Pregunta: Agradecemos a la entidad confirmar si se debe tener en cuenta migración de casos de uso con los que cuenta actualmente, de ser afirmativo, solicitamos indicar la cantidad y tipo.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN manifiesta al observante que, para la implementación de este proyecto no se deben migrar casos de uso.

35	"Licenciamiento para 16600 activos que incluyen (15000 pc´s, más 1340 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web). Las licencias podrán ser reasginadas entre activos, sin generar costos adicionales para la Entidad." **Pregunta: Agradecemos a la entidad considerar que si bien es cierto que las licencias se puede reasignar, en la mayoria de soluciones depende de x tiempo para realizar este proceso, por lo cual se deberia definir entre las partes el tiempo para la reasignación de la licencia.**	La Dirección de impuestos y Aduanas Nacionales - DIAN informa al observante que, los tiempos para la reasignación de licencias serán acordados en su momento con el contratista ganador, normalmente estos tiempos oscilan entre uno y quince días dependiendo de la cantidad y el grado de complejidad de la actividad.
36	"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." **Pregunta: Agradecemos a la entidad confirmar si puede proporcionar los sensores requeridos en formato de VM tanto en el onpremise como en las nubes.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
37	"Especificaciones Técnicas Plataforma SOAR" **Pregunta: Agradecemos a la entidad confirmar si de ser requeridas VM para la implementación del servicio las puede proporcionar.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
38	"El licenciamiento de la solución debe ser como mínimo ciento veinte (120) vlans." **Pregunta: Agradecemos a la entidad confirmar la cantidad maxima de vlan a tener en cuenta.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la cantidad mínima solicitada es de ciento veinte (120) vlans, y dentro de esta cantidad se encuentra la proyección de crecimiento realizada por la Entidad.
39	"Especificaciones Técnicas Caza de Amenazas" **pregunta: Agradecemos a la entidad confirmar si puede proveer MV para la implementación del servicio de ser requerido.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
40	"La solución ofertada debe incorporar paquetes de tokens para las máquinas señuelo o VM decoy." **Pregunta: Agradecemos a la entidad confirmar la cantidad de tokens/decoy requeridos.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la cantidad se deja a la experiencia del proponente aclarando que se deben cubrir la cantidad de vlans solicitadas, que son 120.
41	"La solución debe contar con soporte de fábrica 7x24, garantía y actualizaciones de inteligencia de amenazas por un período de XXX año. " **Pregunta: Agradecemos a la entidad confirmar el tiempo en años que se debe tener en cuenta.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el tiempo estipulado en este ítem de tres (3) años.

42	"La cantidad mínima de activos tecnológicos de información por ejercicio de ethical hacking sera de cien (100) activos, de acuerdo a los inventarios de activos entregado en este mismo archivo en sus hojas adyacentes." **Pregunta: Agradecemos a la entidad confirmar la cantidad maxima de activos a tener en cuenta por cada prueba de ethical hacking.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que en relación con el Ethical HAcking se aclara que el objetivo de esta acción es la infraestructura indicada en el Inventario de dispositivos y elementos que hacen parte del Proyecto. Se aclara que la cantidad mínima de activos para el ejercicio es de cien (100)
43	"Prestar el servicio desde un centro de monitoreo ubicado en la ciudad de Bogotá D.C. (Colombia). " **Pregunta: Agradecemos a la entidad confirmar si para la comunicación entre el SOC y la entidad, se hara uso de sus canales de internet o se debe proveer un canal de internet para este fin.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, para la comunicación del SOC del futuro contratista y la DIAN se hará uso de los canales de la Entidad.
44	"El servicio del SOC deberá contar con mínimos dos (2) centro de datos geográficamente ubicados en diferentes lugares dentro de Bogotá D.C., siendo uno ellos para contingencia o alta disponibilidad. El proponente debe especificar la cantidad de Centro de Datos de los que dispone para el SOC, su ubicación y el rol de cada uno de ellos." **Pregunta: Agradecemos a la entidad considerar que los DC se encuentren dentro o fuera de la ciudad de Bogotá.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, para un mejor entendimiento el Item en mención se ajusta de la siguiente manera: El servicio del SOC deberá contar con mínimos dos (2) centro de datos geográficamente ubicados en diferentes lugares dentro de Bogotá D.C o uno de estos puede estar fuera de Bogotá, siendo este para contingencia o alta disponibilidad, aclarando que el datacenter principal de donde se prestará el servicio de SOC y las capacidades contratadas, debe encontrarse en la ciudad de Bogotá. El proponente debe especificar la cantidad de Centro de Datos de los que dispone para el SOC, su ubicación y el rol de cada uno de ellos.
45	"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 por parte del fabricante de las soluciones y plataformas entregadas, durante la vigencia del contrato de soporte y garantía." **Pregunta: Agradecemos a la entidad confirmar la cantidad de integrantes.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que, para un mejor entendimiento el Item en mención se ajusta de la siguiente manera: 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 de soporte y garantía.
46	"Debe ser mínima de cuarenta (40) horas para veinte (20) personas, cuyo contenido debe contemplar uso y administración, además de conocer la instalación, configuración, monitoreo, administración y resolución de problemas de todas la plataformas, soluciones, servicios y dispositivos entregados, entre otros" **Pregunta: Agradecemos a la entidad confirmar nuestro entendimiento en el sentido que la transferencia de conocimiento solicitada sera entregada por el oferente del servicio.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que, la transferencia de conocimiento y capacitaciones deben ser entregadas por el oferente de servicio.

47	"Debe ser mínima de cuarenta (40) horas para veinte (20) personas, cuyo contenido debe contemplar uso y administración, además de conocer la instalación, configuración, monitoreo, administración y resolución de problemas de todas la plataformas, soluciones, servicios y dispositivos entregados, entre otros" **Pregunta: Agradecemos a la entidad confirmar si la transferencia de conocimiento puede ser entregada de forma virtual.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que, la transferencia de conocimiento y capacitaciones deben ser entregadas por el oferente del servicio y pueden darse de manera virtual, sobre la aplicacion de mensajeria definida por la DIAN. MS Teams.
48	"Realizar el análisis Forense para incidentes críticos, y determinar el origen y el vector de inicio del incidente. " **Pregunta: Agradecemos a la entidad confirmar la cantidad de analisis forense ejecutados en los ultimos 12 meses.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que, no se cuenta con esta estadística, ya que el servicio, característica o capacidad solicitada es nueva para la Entidad.
49	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 "Cifras Infraestructura IT". **Pregunta: Agradecemos a entidad confirmar si es necesario desplegar un sensor en nube de azure para monitorear las bases de datos, la entidad no suministraria la VM.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
50	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.**Pregunta: Agradecemos a la entidad indicarnos si la solución puede ser una solucion en nube o debe ser on-premise.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN inforrma al observante que, en atención a lo solicitado en el anexo técnico la solución requerida para la protección de bases de datos puede ser en nube, física o como servicio.
51	Incluir una consola de reportería basada en big data, que retenga los datos siempre en tiempo real y permita generar búsquedas y analítica forense. **Pregunta: Agradecemos a la entidad indicarnos cual es el periodo de retencion de los datos que se debe contemplar para la solución.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, como mínimo se contempla una retención de datos por seis (6) meses.
52	La solución podrá ser desplegada dentro de ambientes virtuales VMWare como dispositivo virtual. **Pregunta: Agradecemos confirmar si nuestro entendimiento es correcto, la DIAN siministraria los recuros de VM para el despliegue de la solución de monitoreo de base de datos.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
53	La solución deberá soportar el volumen de tráfico y deberá tener una latencia menor a 5ms, para no impactar el desempeño de las aplicaciones. **Consideración: Agradecemos a la entidad reconsiderar eliminar este item, ya que la latencia depende de la solución sino del estado de la conectividad de la red de la entidad.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la Entidad requiere mínimo de un tiempo de 5 ms, lo que garantiza que se tenga tiempos cercanos al tiempo real para auditoría y monitoreo de las bases de datos.

54	Capacidad de realizar consultas a los datos capturados y almacenados en el hardware de uso específico (appliance) sin conectarse a la nube. **Pregunta: Agradecemos la entidad indicarnos el tiempo de retencion de los logs por parte de la solucion de NDR.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el tiempo de retención para la solución NDR es de seis (6) meses como mínimo.
55	El oferente y/o contratista deberá entregar un servicio con licenciamiento total de la solución para 1600 dispositivos por (3) años. **Pregunta: Agradecemos a la entidad indicarnos el Throughput que pueda estar generando lod 16000 dispositivos.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la información de throughput solicitada la pueden calcular los futuros oferentes de acuerdo al inventario anexo a este proyecto.
56	El servicio debe basarse en un sistema de seguridad que reciba todo el tráfico de la red desde uno o varios switches, lo analice e identifique las amenazas o incidentes que están ocurriendo en la red. **Pregunta: Agradecemos a la entidad indicarnos para dimesionar la arquitectura de la solución, indicarnos si los switch core cuentan con puertos de fibra.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el switch core de la Entidad cuentan con puertos de fibra.
57	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: o La línea base de la red debe ser lo suficientemente adaptable y dinámica para adaptarse a cualquier cambio en el comportamiento del entorno o Debe funcionar completamente en función del comportamiento, donde no se permitan las tecnologías que	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la solución NDR requerida por la Entidad debe contar con las funciones de detección y respuesta entre otras.
58	Se debe licenciar como mínimo para 16000 dispositivos. **Pregunta: Agradecemos a la entidad indicarnos si las cantidad de dispositivos hacen parte del ambiente IT ó tambien se tiene contemplado ambiente OT.** **En caso de tener dispositivos OT, indicanos si se desea que la solucion NDR modele eventos de este tipo de ambiente. indicarnos cuantos dispositivos con su posible crecimiento.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, los dispositivos mencionados en este punto son IT.
59	La herramienta/servicio debe rastrear y monitorear continuamente la presencia en línea de la marca en sitios web, redes sociales, foros, blogs y otros espacios digitales relevantes para identificar cualquier uso no autorizado o infracción de la marca. **Pregunta: Agradecemos a la entidad indicarnos la siguiente información:** **No de dominios a monitorear** **No de IP a monitorear** **No de APKs** **No de redes sociales** **Cuales redes sociales se deben monitorear (Facebook, X, Tiktok, etc.)** **Cuales son los dominios de correo electronico.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, dentro de la cantidad de activos públicos estipulada en este punto se encuentran IPs públicas y dominios. El monitoreo solicitado en este punto, se debe realizar a las principales redes sociales (twitter, facebook, tik tok, instagram, entre otros), la información adicional se proporcionará en su momento al oferente ganador.
60	Generar informes detallados sobre actividades de protección de marca, incluidas estadísticas de monitoreo, acciones tomadas y resultados obtenidos. **Pregunta: Agradecemos a la entidad indicarnos la periodicidad de la generacion de los informes.**	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante que, los informes solicitados en este punto se deben realizar mensualmente o bajo demanda cuando la Entidad así lo requiera

61	Referencia o Modelo (Especificar el modelo ofrecido). **Pregunta: Agradecemos a la entidad aclarar la espectativa que se tiene respecto al item (sensores, software, entre otros)**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, en este ítem se requiere un servicio de SaaS (software como servicio) que monitoree los activos públicos de la Entidad (dominio de correo, dominios públicos, ip´s públicas, certificados SSL, entre otros).
62	Se debe licenciar para 260 activos públicos. **Pregunta: Agradecemos a la entidad aclarar la espectativa la cantidad de activos publicos, si entre ellos se encuentran dominios, APKs ó solo se encuentran IPs publicas a monitorear.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, dentro de la cantidad de activos públicos estipulada en este punto se encuentran IPs públicas y dominios.
63	La herramienta/servicio debe realizar la creación y gestión de casos para seguir el progreso de las acciones tomadas contra infractores, incluidas las comunicaciones legales, las medidas de cumplimiento y las soluciones. **Considerar: agradecemos a la entidad considerar que el item sea gestionano desde el servicio, más no por la herramienta.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la característica solicitada en este ítem debe ser realizada por la herramienta proporcionada.
64	Realizar análisis retrospectivos y comparativos para evaluar la efectividad de las estrategias de protección de marca y ajustarlas según sea necesario. **Pregunta: Agradecemos a la entidad aclarar la espectativa de cumplimiento y la periodicidad de los entregables.**	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, los entregables tendrán que estar adjunto a los tiempos solicitados en el servicio del monitoreo del SOC o por demanda si asi lo determina la Entidad.
65	Respetuosamente solicitamos a la entidad ampliar el plazo para realizar preguntas y/o aclaraciones para el 22 de Octubre dado que la entidad solicita mas de +1200 requerimientos y toma tiempo analizar cada requerimiento para poder realizar las aclaraciones necesarias.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, los plazos estipulados podrán ser ampliados de acuerdo a las necesidades de la Entidad, y según las solicitudes realizadas una vez analizada su pertinencia, aclarando que es optativo de la Dian realizar cualquier concesión al respecto.
66	Respetuosamente solicitamos a la entidad ampliar el plazo para el envío de respuesta por parte de los proveedores para el 15 de noviembre, teniendo en cuenta el alto volumen de fabricantes que se deben incluir y la cantidad de requerimientos que solicita la entidad.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, los plazos estipulados podrán ser ampliados de acuerdo a las necesidades de la Entidad, y según las solicitudes realizadas una vez analizada su pertinencia, aclarando que es optativo de la Dian realizar cualquier concesión al respecto.
67	Por favor aclarar las líneas que se deben cotizar porque no están servicios y soluciones solicitadas en el Anexo técnico, no hay concordancia con el listado del anexo económico y el numeral 1.1 del Anexo técnico, por ejemplo no esta la línea para Solución de análisis de código estático y dinámico para aplicaciones, Capacitación o Gestión de Incidentes	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que en el anexo economico se realizaron ajustes en concordancia con el anexo tecnico.
68	Por favor aclarar si la Dian pretende entregar todas las soluciones a un solo proponente o estas serán asignadas por Lotes individuales.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que todas las capacidades, plataformas, soluciones, servicios, adminsitración, monitoreo y demás requerimientos solicitados por la Entidad deberán ser prestados por el futuro contratista ganador, es un solo lote, no se discriminan lotes individuales.

69	Por favor aclarar la propiedad de los servicios y soluciones en el caso que sean consumos de nube o servicios profesionales solicitados	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante, que se ajusta la nota 2 del Anexo Propuesta de valores, quedando asi: NOTA 2: Todos los elementos adquiridos y entregados, producto del presente proceso contractual serán de propiedad de la DIAN, para los casos donde aplique.
70	Por favor indicar si es posible ofertar las soluciones en dólares americanos, lo cual permitirá a la Dian poder realizar una adecuada comparación de los precios de las distintas soluciones ofertadas por los diferentes proponentes.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que todas las soluciones deberan ser entregadas en pesos colombianos COP.
71	Por favor indicar la solución actual de SIEM con la que cuenta la DIAN	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la solución de SIEM con la que cuenta actualmente la Entidad es QRADAR.
72	Por favor aclarar la cantidad de EPS esperada o el consumo en GB de los logs ya que no todas las soluciones de SIEM del mercado se licencias por el numero de dispositivos	La Dirección de Impuestos y Aduanas Nacionales – DIAN indica observante que, la cantidad de EPS requeridos es de 25000.
73	Por favor aclarar que significa una "Transacción Sintética" ¿A que se hace referencia?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el monitoreo de transacciones sintéticas hace referencia a una característica eficaz que permite monitorizar aplicaciones desde la perspectiva del usuario, donde se simula las interacciones de los usuarios generando solicitudes o transacciones artificiales que imitan el comportamiento real del usuario.
74	Por favor indicar las versiones de hyper V y Vmware ya que no se encuentran en el inventario	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, las versiones de Vmware y Hyper V con las que cuenta la Entidad se encuentran en el inventario anexo, pero se aclara que la Entidad cuenta con Windows Server 2012R2, Windows Server 2022 y VMware ESXi, 7.0.3
75	Por favor confirmar que la administración de la solución SIEM será del oferente y no de la DIAN, es decir se deben brindar servicios profesionales de administración y operación adicionales al soporte y garantía	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la administración, operación, gestión de los servicios y demás actividades de las plataformas, soluciones, software, hardware, entre otros, que hacen parte de las capacidades requeridas por la Entidad en este proyecto, debe ser realizadas por el futuro oferente, tal como se indica en el anexo de caracterítiscas técnicas que hace parte de este proceso.

76	por favor confirmar el alcance del numeral, es de nuestro entendimiento que todos los cambios en plataformas productivas de la DIAN serán realizadas por la DIAN y el oferente solo entregará los procedimiento y acompañamiento en esas configuraciones. ¿Es correcto nuestro entendimiento?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, todos los cambios, remediaciones, configuraciones y demás actividades que haya que realizar en las plataformas productivas de la DIAN serán llevados a cabo por la Entidad, con el acompañamiento, experticia, soluciones, apoyo y soporte del futuro contratista de este proyecto, por el tiempo que dure la garantía y el soporte contratados.
77	Por favor indicar cuantos usuarios finales serán monitoreados	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la cantidad de usuarios a monitorear es la estipulada en el anexo técnico, 17727 usuarios.
78	Por favor aclarar el requerimiento, cuando se solicita contexto a que se hace referencia?	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la palabra contexto en este ítem se refiere al entorno o escenario, el cual debe ser en tiempo real y debe incluir las características solicitadas en este mismo ítem.
79	Por favor aclarar el requerimiento, cuando se solicita contexto a que se hace referencia? ¿Qué se debe hacer con estos dispositivos?	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la palabra contexto en este ítem se refiere al entorno o escenario, el cual debe ser en tiempo real y debe incluir las características solicitadas en este mismo ítem.
80	Por favor confirmar que la DIAN requiere servicios de NOC donde se monitoreará la salud de los dispositivos de la hoja "Cifras Infraestructura IT" y que ese será el alcance	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el alcance del proyecto y lo que se requiere en cuanto a servicios, capacidades, plataformas y soluciones, se encuentra estipulado en cada uno de los apartes del anexo técnico
81	Por favor aclarar cuantas aplicaciones serán monitoreadas	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, como minimo se deben monitorear 260 aplicaciones.
82	Por favor dar mas detalle de la infraestructura VoIP con el fin d epoder dimensionar adecuadamente el servicio	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, actualmente no existe infraestructura en las instalaciones de la Dian, el cliente softphone que se utiliza en los PCs y dispositivos móviles es el que ofrece Teams y los teléfonos que se utilizan, principalmente en las porterías, corresponden a dispositivos Polycom VVX 400, VVX 300 y VVX 201, los cuales se aprovisionan en la nube de Microsoft, el ítem en mención se expresa de mejora manera para evitar equivocos.

83	Por favor aclarar el requerimiento, una solución SIEM no recopila archivos de configuración ni mantiene un inventario de versiones de software	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el SIEM requerido debe entregar la característica de recopilar archivos de configuración y mantener un inventario de versiones de software.
84	Por favor confirmar que la DIAN entregará las soluciones que realizan el monitoreo y que el requerimiento se limita a traer los logs y procesarlos al SIEM propuesto	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el SIEM propuesto deberá cumplir con la totalidad de las características solicitadas en este ítem y el anexo técnico.
85	Por favor confirmar que adicional al SIEM se requiere una solución de FIM - File Integrity Monitoring	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, dentro de las capacidades y características solicitadas para el SIEM este debe contar con la funcionalidad FIM.
86	Por favor indicar las políticas de retención de logs esperadas, tanto en línea (caliente) como en archivo (almacenamiento en frio), ¿Cuánto tiempo?	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el SIEM a adquirir debe manejar tasa de retención de tres (3) meses en línea y seis (6) meses fuera de línea.
87	Por favor cambiar el requerimiento, no todas las soluciones de SIEM ofrecen todas las modalidades solicitadas, si los requerimientos técnicos son cumplidos no debería ser un decisor el modo de licenciamiento	La Dirección de Impuestos y Aduanas Nacionales – DIAN indica al observante que, las características descritas en este ítem obedecen a especificaciones requeridas por la Entidad, por lo tanto su cambio no es posible.
88	Por favor indicar la solución actual de SOAR con la que cuenta la DIAN	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, actualmente la Entidad no cuenta con una solución SOAR.
89	Por favor aclarar si las licencias de SOAR no se manejan por usuarios, este será un descalificante para la solución de SOAR	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, las capacidades requeridas en el anexo técnico junto con sus características son de obligatorio cumplimiento.
90	Por favor indicar la solución actual de protección de Bases de Datos con la que cuenta la DIAN	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la solución de protección de bases de datos con la que cuenta actualmente la Entidad es Guardium.

91	Por favor confirmar que son 100 bases de datos Oracle y 20 MSSQL	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, las cantidades requeridas de bases de datos las encuentra en el inventario que hace parte de este proyecto.
92	Por favor indicar la solución actual de Monitoreo Gestión de Vulnerabilidades con la que cuenta la DIAN	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, actualmente no cuenta con una solución de gestión de vulnerabilidades que cuente con las características descritas en el anexo técnico.
93	Por favor confirmar que la DIAN espera escanear 15.000 PC o si la solución debe estar circunscrita al ambiente productivo de 1340 Activos de información.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la solución requerida debe realizar gestión de vulnerabilidades a los 17727 activos descritos en el ítem 5.3.2
94	Por favor aclarar cuales nubes son el alcance del requerimiento	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, las nubes con las que cuenta la Entidad son Azure y AWS.
95	Por favor ampliar el requerimiento de que infraestructura deberá estar cubierta por la solución	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el ítem al indicar "La solución ofertada permitirá la protección de la infraestructura en la nube", y las cantidades y características de dicha infraestructura la pueden consultar en el archivo de inventario, anexo a este proyecto.
96	Por favor indicar la solución actual de Caza de Amenazas con la que cuenta la DIAN	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, actualmente la Entidad no cuenta con una solución de Caza de Amenazas de las características y capacidades requeridas en el anexo técnico de este proyecto.
97	Por favor indicar la solución actual de NDR - Detección y respuesta en red e Inteligencia de amenazas con la que cuenta la DIAN	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, actualmente la Entidad no cuenta con una solución NDR de las características y capacidades requeridas en el anexo técnico de este proyecto.
98	Por favor indicar la solución actual de análisis de código estático y dinámico para aplicaciones con la que cuenta la DIAN	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, actualmente la entidad no cuenta con herramientas de analisis de código estático y dinámico.

99	Por favor confirmar que se requiere 50 licencias de solución SAST y 50 licencias de solución DAST	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que en la etapa de operación se definirá el tipo de análisis requerido (SAST o DAST), de acuerdo con las necesidades específicas de cada aplicación. Sin embargo, se debe garantizar que la solución ofertada permita realizar análisis estático y dinámico en un total de cincuenta (50) aplicaciones.
100	Por favor aclarar el alcance de dar soporte a las fabricas de desarrollo en el proceso de desarrollo seguro, ¿Qué significa dar soporte en este caso? ¿Se requiere consultoría especializada en desarrollo seguro adicional a la solución solicitada?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que el alcance de dar soporte a las fábricas de desarrollo en el proceso de desarrollo seguro, consiste en proporcionar orientación y asistencia técnica para el uso adecuado de la herramienta de análisis de código, con el fin de asegurar que se cumplan las prácticas de desarrollo seguro definidas por la DIAN. Esto incluye el apoyo en la ejecución de pruebas y la interpretación de los resultados generados por la herramienta, pero no implica una consultoría especializada en desarrollo seguro adicional a la solución solicitada.
101	¿Requiere la Dian servicios profesionales de consultoría para la solución de vulnerabilidades en código?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que no se requiere un servicio de consultoría adicional para la solución de vulnerabilidades en el código. El alcance solicitado incluye el análisis de vulnerabilidades, la generación de recomendaciones para su remediación, el acompañamiento en las solución de remediaciones y el soporte necesario para llevar la solución a feliz término, en ningún caso se habla de una consultoría aparte para dicha solución.
102	¿La identificación la realizarán los desarrolladores? Ó ¿deberá ser ejecución de análisis por parte del proveedor?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que, según el punto 8.11, la identificación de deficiencias en la programación de funciones de autenticación, registro, cifrado, manejo de errores y procesamiento de datos debe realizarse mediante la ejecución de análisis por parte del proveedor, utilizando la solución contratada. El proveedor será responsable de ejecutar estos análisis y de reportar los hallazgos a las áreas correspondientes para su revisión y remediación.
103	Por favor confirmar que el administrador de la solución será la DIGIT y que el oferente solo brindará soporte y mantenimiento	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que el futuro contratista deberá administrar, operar, gestionar, configurar, mantener y realizar todas las actividades propias del día a día con la solución de análisis de código estático y dinámico para aplicaciones. Asimismo con los demás dispositivos, plataformas, soluciones y servicios adquiridos en este proyecto

104	Por favor indicar la solución actual de Protección de Marca (Deep&Dark Web)con la que cuenta la DIAN	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, actualmente la Entidad no cuenta con una solución de Protección de marca (Deep&Dark Web) de las características y capacidades requeridas en el anexo técnico de este proyecto.
105	Por favor confirmar que esta solución puede ser un servicio y no una herramienta, en cuyo caso no se entrega propiedad a la DIAN	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la capacidad solicitada en este ítem puede ser una herramienta o sofware como servicio (Saas).
106	Por favor aclarar que cuando se menciona 260 activos públicos son URLS o son indicadores que deberán ser monitoreados.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, dentro de la cantidad de activos públicos estipulada en este punto se encuentran IPs públicas y dominios.
107	Por favor aclarar si las pruebas son internas o externas	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que, conforme al punto 10.2, los ejercicios de ethical hacking a realizar serán de tipo caja gris, lo cual implica que pueden involucrar tanto pruebas internas como externas, según lo definido en cada caso. La modalidad específica de cada prueba se determinará en conjunto con la entidad, de acuerdo con los objetivos de seguridad establecidos para cada ejercicio.
108	con el fin de realizar un adecuado dimensionamiento de los servicios solicitados por favor confirmar que cada prueba será de máximo 100 objetivos	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que en relación con el Ethical HAcking se aclara que el objetivo de esta acción es la infraestructura indicada en el Inventario de dispositivos y elementos que hacen parte del Proyecto. Se aclara que la cantidad mínima de activos para el ejercicio es de cien (100)
109	¿Qué espera la DIAN como respuesta a incidentes en este caso si la responsabilidad de los activos escaneados no es del proponente?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que, conforme al punto 10.5, el contratista debe preparar un plan de respuesta a incidentes que contemple las acciones a seguir en caso de descubrir vulnerabilidades graves durante los ejercicios de ethical hacking. Aunque la responsabilidad de los activos escaneados recae sobre la DIAN, se espera que el contratista colabore con el reporte detallado de los hallazgos, recomendaciones para la mitigación de riesgos y el soporte técnico necesario para que la DIAN pueda tomar las medidas de remediación correspondientes de manera oportuna.

110	por favor aclarar si hay ubicaciones fuera de la ciudad de Bogotá donde se deberán entregar equipos o brindar servicios	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, para un mejor entendimiento el Item en mención se ajusta de la siguiente manera: Ubicaciones para implementación y configuración: El oferente contará con un Centro de Operaciones de Seguridad SOC en la ciudad de Bogotá, donde se implementarán todos y cada uno de los servicios, dispositivos, plataformas, soluciones y demás productos que hagan parte de los requerimientos de la Entidad en este proyecto.
111	En el caso que los equipos sean Hardware y deban ser instalados en los centros de datos de la Dian, por favor confirmar que la DIAN Proveerá Todo el cableado eléctrico, lógico, patchs cords, conectores, patch panels.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que el contratista deberá proveer todos los elementos necesarios para la instalación, incluidos el cableado eléctrico, lógico, patch cords, conectores, y patch panels. Esto está en concordancia con las condiciones del contrato en modalidad "llave en mano" establecidas en el numeral 11.11 de las especificaciones técnicas, el cual define que todos los componentes y accesorios necesarios para la correcta instalación de las soluciones son responsabilidad del contratista.
112	Por favor confirmar que la DIAN solo requiere servicios de soporte y NO de administración y/o operación de las plataformas. El oferente entregará las soluciones implementadas a la DIAN, realizará transferencia de conocimientos y capacitación y la DIAN tomará control de todas las soluciones, es decir la DIAN operará y administrará las soluciones y solo en caso de falla o incidentes abrirá tickets de soporte al oferente.	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que el futuro contratista deberá administrar, operar, gestionar, configurar, mantener y realizar todas las actividades propias del día a día con las plataformas y soluciones implementadas. Esto se extiende a todos los dispositivos, plataformas, soluciones y servicios adquiridos en el marco de este proyecto.
113	Por favor confirmar si este requerimiento es el mismo reflejado en el capitulo 5.1	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que lo referente a este punto debe realirse con la herramienta de gestión de vulnerabilidades entregada por el oferente.
114	Por favor confirmar el entendimiento que la DIAN requiere 5 capacitaciones certificadas por cada una de las soluciones certificadas para un total de 40 entrenamientos con sus respectivos vouchers	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que son 5 capacitaciones para 5 Integrantes con capacidad minima de 40 Horas, con vouchers respectivos.
115	Por favor aclarar que ocurre si el fabricante no ofrece entrenamiento gratuito ¿Se descalifica la solución?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que si no se ofrece, no sera tenida en cuenta.
116	Por favor confirmar que la transferencia se dará una única vez para todas las plataformas implementadas	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que se debera dar por parte del contratista, la transferencia de conocimiento para todas las plataformas, servicios, soluciones y capacidades requeridas, una única vez dentro de la ejecución del proyecto.

117	En aras de la pluralidad de los oferentes respetuosamente solicitamos ala entidad eliminar el requerimiento de contar con alguno de los tres niveles de membresía mas alto con cada uno de los fabricantes. Este requerimiento limita significativamente los posibles oferentes al proceso	La Dirección de Impuestos y Aduanas Nacionales – DIAN agradece la observación presentada. Sin embargo, se considera que el requisito de contar con alguno de los tres niveles de membresía más altos ante cada uno de los fabricantes es fundamental para asegurar que los oferentes tengan el respaldo técnico y la capacidad adecuada para proporcionar la calidad de servicio y soporte requeridos para las soluciones ofertadas. Este nivel de certificación garantiza que los proveedores tienen acceso a recursos y conocimientos técnicos actualizados, lo que es crucial para el éxito de la implementación y el mantenimiento de las plataformas y soluciones de seguridad. Se mantiene, por lo tanto, el requerimiento
118	Por favor confirmar que los servicios de atención de incidente solo tienen alcance sobre las plataformas ofertadas por el proponente, cualquier incidente de seguridad de la información es responsabilidad de la DIAN	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la atencion de incidentes incluyen cualquier incidente de seguridad de la informacion, dado que el SOC centraliza este manejo para incrementar la postura en general de seguridad de la DIAN, también se aclara que los servicios y demás capacidades adquiridas deben monitorear toda la infraestructura tecnológica descrita en el inventario de activos que hace parte de este proyecto.
119	Por favor aclarar el alcance de los servicios de análisis forense, ¿requiere la DIAN servicios profesionales especializados de análisis forense? ¿Se agregaría una línea en el anexo económico?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, dentro de los requerimientos solicitados, el futuro contratista deberá realizar el análisis Forense para incidentes críticos, y determinar el origen y el vector de inicio del incidente como parte de su pull de servicios SOC, en ningún momento se habla de un servicio adicional o anexo a este proyecto.
120	Por favor confirmar que el requerimiento solo aplica para las plataformas ofertadas por el proponente	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, este y todos los requerimientos que tenga que ver con incidentes, monitoreo y demás actividades que se solicitan dentro del alcance del anexo técnico de este proyecto, aplica para toda la infraestructura relacionada en el inventario anexo que son aprox 17727. El futuro contratista debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá, que le permita realizar todas las actividades solicitadas por la DIAN en el anexo técnico, cobijando toda la infraestructura tecnológica de la Entidad. Aclarando que no se debe limitar unicamente a las plataformas, servicios, soluciones, servicios y dispositivos ofertados por el posible proponente.

121	Por favor confirmar que el requerimiento solo aplica para las plataformas ofertadas por el proponente	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, este y todos los requerimientos que tenga que ver con incidentes, monitoreo y demás actividades que se solicitan dentro del alcance del anexo técnico de este proyecto, aplica para toda la infraestructura relacionada en el inventario anexo que son aprox 17727. El futuro contratista debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá, que le permita realizar todas las actividades solicitadas por la DIAN en el anexo técnico, cobijando toda la infraestructura tecnológica de la Entidad. Aclarando que no se debe limitar unicamente a las plataformas, servicios, soluciones, servicios y dispositivos ofertados por el posible proponente.
122	Por favor confirmar que el requerimiento solo aplica para las plataformas ofertadas por el proponente	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, este y todos los requerimientos que tenga que ver con incidentes, monitoreo y demás actividades que se solicitan dentro del alcance del anexo técnico de este proyecto, aplica para toda la infraestructura relacionada en el inventario anexo que son aprox 17727. El futuro contratista debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá, que le permita realizar todas las actividades solicitadas por la DIAN en el anexo técnico, cobijando toda la infraestructura tecnológica de la Entidad. Aclarando que no se debe limitar unicamente a las plataformas, servicios, soluciones, servicios y dispositivos ofertados por el posible proponente.
123	Por favor confirmar que el requerimiento solo aplica para las plataformas ofertadas por el proponente	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, este y todos los requerimientos que tenga que ver con incidentes, monitoreo y demás actividades que se solicitan dentro del alcance del anexo técnico de este proyecto, aplica para toda la infraestructura relacionada en el inventario anexo que son aprox 17727. El futuro contratista debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá, que le permita realizar todas las actividades solicitadas por la DIAN en el anexo técnico, cobijando toda la infraestructura tecnológica de la Entidad. Aclarando que no se debe limitar unicamente a las plataformas, servicios, soluciones, servicios y dispositivos ofertados por el posible proponente.
124	con el fin de realizar un adecuado dimensionamiento de los servicios solicitados por favor confirmar que la DIAN requiere servicios adicionales de Atención de Incidentes al soporte normal de las plataformas solicitadas	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el futuro contratista debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá, que le permita realizar todas las actividades solicitadas por la DIAN en el anexo técnico, cobijando toda la infraestructura tecnológica de la Entidad. Para el efecto debe tener la capacidad de detectar, escalar, informar, acompañar apoyar y soportar a la DIAN en la resolución de cada uno de los incidentes encontrados durante el tiempo que dure el proyecto en mención.

125	por favor aclarar el requerimiento, ¿La DIAN va incluir activos y consumos adicionales al SOC? ¿Qué alcance tendrá?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el futuro contratista debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá, que le permita realizar todas las actividades solicitadas por la DIAN en el anexo técnico, cobijando toda la infraestructura tecnológica de la Entidad. Para el efecto debe tener la capacidad de detectar, escalar, informar, acompañar apoyar y soportar a la DIAN en la resolución de cada uno de los incidentes encontrados durante el tiempo que dure el proyecto en mención. Los activos y demás características de estos se encuentran detallados en el apartado de inventarios y las especificaciones de cada una de las soluciones, plataformas, capacidades, servicios, soporte y garantía se encuentran en el anexo técnico.
126	Sin contar con las herramientas que entreguen la información necesaria no podrá realizarse un monitoreo, por favor confirmar que la DIAN proveerá toda solución requerida para poder monitorear los controles tecnológicos que relacionan	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el futuro contratista debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá, que le permita realizar todas las actividades solicitadas por la DIAN en el anexo técnico, cobijando toda la infraestructura tecnológica de la Entidad. Para el efecto debe tener la capacidad de detectar, escalar, informar, acompañar apoyar y soportar a la DIAN en la resolución de cada uno de los incidentes encontrados durante el tiempo que dure el proyecto en mención. Por ende debe contar con la capacidad necesaria para monitorear los controles requeridos en este ítem.
127	Como espera la DIAN que el oferente "garantice" la disponibilidad, confidencialidad, integridad, no repudio, auditoria y privacidad de los datos y servicios soportados	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el futuro contratista esta obligado contractualmente y mediante las respectivas clausulas y seguros a preservar las propiedades de la información tratada durante el proyecto, la supervisión y los mecánimos propios con los que cuenta la Entidad le permitirán realizar las actividades necesarias para verificar el cumplimiento de lo solicitado en el anexo técnico de proyecto.
128	Solicitamos por favor aclarar si el alcance incluye la administración de las plataformas y/o servicios solicitados, entendiendose que la administración incluye actividades de Configuración, monitoreo y mantenimiento de la plataforma y/o servicio durante el período del contrato.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la administración, operación, gestión de los servicios, mantenimiento y demás actividades de las plataformas, soluciones, software, hardware, entre otros, que hacen parte de las capacidades requeridas por la Entidad en este proyecto, debe ser realizadas por el futuro oferente, tal como se indica en el anexo de caracterítiscas técnicas que hace parte de este proceso, por lo tanto su entendimiento es correcto.

129	Solicitamos por favor aclarar si el alcance incluye la Operación de las plataformas y/o servicios solicitados, entendiendose que la Operación incluye actividades de día a día a nivel funcional como el monitoreo de eventos, análisis y atención de incidentes.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la administración, operación, gestión de los servicios, mantenimiento y demás actividades de las plataformas, soluciones, software, hardware, entre otros, que hacen parte de las capacidades requeridas por la Entidad en este proyecto, debe ser realizadas por el futuro oferente, tal como se indica en el anexo de caracterítiscas técnicas que hace parte de este proceso, por lo tanto su entendimiento es correcto.
130	Solicitamos por favor aclarar si la para la prestación de los servicios del SOC, se deberan considerar actividades llevadas a cabo por equipos o funcionarios de la DIAN o equipos de terceros prestadores de servicios para la DIAN. En caso de ser afirmativo, solicitamos por favor describir estas actividades o delimitar el alcance frente a los diferentes involucrados.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la administración, operación, gestión de los servicios, mantenimiento y demás actividades de las plataformas, soluciones, software, hardware, entre otros, que hacen parte de las capacidades requeridas por la Entidad en este proyecto, debe ser realizadas por el futuro oferente, tal como se indica en el anexo de caracterítiscas técnicas que hace parte de este proceso, aclarando que la intervención en las plataformas productivas con las que cuenta actualmente la Entidad será realizada por personal de la DIAN.
131	OBSERVACIÓN No. 1 Solicitamos amablemente enviar el Anexo 1. Anexo Técnicos SOC, toda vez que no es posible acceder al link.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que el anexo tecnico se encontraba en el link de la publicacion como archivos adjuntos o detalle.
132	OBSERVACIÓN No. 2 En el numeral 1 del literal 3.3 condiciones generales dispuesto en el documento RFI, la entidad solicita: “El CONSULTOR estará obligado a conocer, observar, cumplir e implementar la normativa interna y externa aplicable en la DIAN, así como incorporarla y tenerla en cuenta durante la ejecución del presente contrato (SOC).” Para el presente contrato, solicitamos amablemente aclarar y detallar que normativa interna y externa de la DIAN será aplicable.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la normativa referida trata del SGSPI de la Entidad así como a conocer el manual de políticas de la Entidad en lo que respecta a la información y su tratamiento.
133	OBSERVACIÓN No. 3 Respecto al numeral 6. del literal 3.3 condiciones generales dispuesto en el documento RFI: “Se deberá definir el contenido de los productos finales requeridos para el desarrollo del contrato de manera conjunta entre el equipo de gobierno del proyecto del CONSULTOR y los funcionarios “pares” de la DIAN en la fase inicial del proyecto y/o cuando se requiera”. Solicitamos amablemente aclarar su alcance, toda vez que los oferentes elaboran sus propuestas con base a los productos y servicios especificados en el Anexo 1. Dichas especificaciones no deberían ser modificadas posteriormente, so pena de que el costo del negocio incremente.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el alcance del proyecto se encuentra especificado en los productos, capacidades, plataformas, soluciones, servicios y demás actividades que están estipuladas en el anexo técnico de este proceso, incluyendo toda la gestión, monitoreo, administración, acompañamiento, soporte y grarantía por parte del futuro contratista, por lo tanto su modificación en etapas de ejecución del proyecto no está contemplada, los ajustes en razón a actualizaciones, soporte , garantía y demás actividades deberán realizarse previo acuerdo entre las partes (DIAN y Contratista).

134	OBSERVACIÓN No. 4 Con relación al numeral 18 del literal 3.3 condiciones generales dispuesto en el documento RFI: “El CONSULTOR deberá considerar dentro de su propuesta económica todos los valores asociados al desarrollo del proyecto incluyendo los derivados de herramientas, desarrollos e integraciones con sistemas ya existentes o similares, personal, infraestructura, recursos ofimáticos y administrativos, entre otros” Solicitamos se aclare y precise el alcance de la citada obligación, específicamente, se detallen los componentes y alcances esperados para cada uno de los conceptos mencionados (herramientas, desarrollos, integraciones, etc.), con el fin de que todos los oferentes puedan realizar una propuesta económica alineada con las expectativas del proyecto y evitar futuras interpretaciones ambiguas que puedan afectar la ejecución contractual.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que, el ítem refiere a todas las consideraciones que debe tener en cuenta el futuro contratista para poner en producción todos los los productos, capacidades, plataformas, soluciones, servicios y demás actividades que están estipuladas en el anexo técnico de este proceso, incluyendo toda la gestión, monitoreo, administración, acompañamiento, soporte y grarantía por parte del futuro contratista.
135	OBSERVACIÓN No. 5 Con relación al numeral 3.1 alcance en el documento RFI: la entidad menciona el alcance general, se solicita confirmar si requieren un servicio o requieren la instalación de todas las herramientas en la infraestructura de la entidad para que se gestione por especialistas del proponente.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el futuro contratista debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá, donde instalará todos los los productos, capacidades, plataformas, soluciones y servicios, requeridos por la Entidad y que se encuentran en el anexo técnico y que le permitan realizar todas las actividades solicitadas en este por la DIAN. Entendiendose que el contratista realizará toda la gestión, monitoreo, administración, acompañamiento, soporte y grarantía de los mismos, cobijando toda la infraestructura tecnológica de la Entidad. Para el efecto debe tener la capacidad de detectar, escalar, informar, acompañar apoyar y soportar a la DIAN en la resolución de cada uno de los incidentes encontrados por el futuro SOC durante el tiempo que dure el proyecto en mención. Los activos y demás características de estos se encuentran detallados en el apartado de inventarios y las especificaciones de cada una de las soluciones, plataformas, capacidades, servicios, soporte y garantía se encuentran en el anexo técnico
136	OBSERVACIÓN No. 6 Con relación al numeral 9 Especificaciones Técnicas Protección de Marca (Deep&Dark Web) en el documento Anexo Tecnico Proyecto SOC, se solicita entregar el listado con la cantidad de redes sociales a monitorear, correos electrónicos y demás puntos de control en el monitoreo de marca.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que, el monitoreo solicitado en este punto, se debe realizar a las principales redes sociales (twitter, facebook, tik tok, instagram, entre otros), la información adicional se proporcionará en su momento al oferente ganador.
137	OBSERVACIÓN No. 7 Con relación al numeral 3.1 alcance en el documento RFI: la entidad menciona el alcance general, se solicita confirmar si el actual proveedor entregara copia de la configuración del esquema actual, para realizar una transición liviana en la prestación del servicio o se debe hacer una configuración completa de los servicios solicitados	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el futuro contratista deberá realizar una configuración completa de todo lo solicitado en el Anexo Técnico.

138	OBSERVACIÓN No. 8 Con relación al numeral 10 Especificaciones Técnicas Ethical Hacking en el documento Anexo Tecnico Proyecto SOC, se solicita entregar el listado con la cantidad de redes de páginas web a revisar junto con el listado de la infraestructura de la entidad.	La Dirección de Impuestos y Aduanas Nacionales – DIAN indica al observante que, en relación con el Ethical HAcking se aclara que el objetivo de esta acción es la infraestructura indicada en el Inventario de dispositivos y elementos que hacen parte del proyecto SOC en mención.
139	OBSERVACIÓN No. 9 Con relación al numeral 13 Garantía y Soporte Técnico por tres (3) años en el documento Anexo Tecnico Proyecto SOC, se solicita a la entidad confirmar si se debe instalar la infraestructura mencionada en los datacenter de la entidad	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el futuro contratista debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá, donde instalará todos los los productos, capacidades, plataformas, soluciones y servicios, requeridos por la Entidad y que se encuentran en el anexo técnico y que le permitan realizar todas las actividades solicitadas en este por la DIAN. Entendiendose que el contratista realizará toda la gestión, monitoreo, administración, acompañamiento, soporte y grarantía de los mismos, cobijando toda la infraestructura tecnológica de la Entidad. Para el efecto debe tener la capacidad de detectar, escalar, informar, acompañar apoyar y soportar a la DIAN en la resolución de cada uno de los incidentes encontrados por el futuro SOC durante el tiempo que dure el proyecto en mención. Los activos y demás características de estos se encuentran detallados en el apartado de inventarios y las especificaciones de cada una de las soluciones, plataformas, capacidades, servicios, soporte y garantía se encuentran en el anexo técnico
140	OBSERVACIÓN No. 10 Con relación al numeral 13 Garantía y Soporte Técnico por tres (3) años en el documento Anexo Tecnico Proyecto SOC, si la respuesta anterior es afirmativa se solicita a la entidad confirmar que disponibilidad de espacio tiene en el data center para la instalación de los equipos, o se debe informar con antelación a la entidad que espacio y características de consumo se requieren para que confirmen que disponibilidad tienen. Si la entidad no cuenta con disponibilidad de espacio en el datacenter, aceptaría la instalación de los equipos en otra ubicación.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el futuro contratista debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá, donde instalará todos los los productos, capacidades, plataformas, soluciones y servicios, requeridos por la Entidad y que se encuentran en el anexo técnico y que le permitan realizar todas las actividades solicitadas en este por la DIAN. Entendiendose que el contratista realizará toda la gestión, monitoreo, administración, acompañamiento, soporte y grarantía de los mismos, cobijando toda la infraestructura tecnológica de la Entidad. Para el efecto debe tener la capacidad de detectar, escalar, informar, acompañar apoyar y soportar a la DIAN en la resolución de cada uno de los incidentes encontrados por el futuro SOC durante el tiempo que dure el proyecto en mención. Los activos y demás características de estos se encuentran detallados en el apartado de inventarios y las especificaciones de cada una de las soluciones, plataformas, capacidades, servicios, soporte y garantía se encuentran en el anexo técnico
141	OBSERVACIÓN No. 11 Con relación al numeral 18,2 Certificaciones en el documento Anexo Tecnico Proyecto SOC, se solicita a la entidad confirmar si la certificación de garantía sobre los equipos se debe entregar con la propuesta o se debe entregar al momento de la entrega de los equipos en el datacenter.	La Dirección de Impuestos y Aduanas Nacionales DIAN informa que la certificaciones de las que trata el anexo técnico deben ser entregadas junto con la propuesta.

142	OBSERVACIÓN No. 12 Con relación al Anexo Tecnico Proyecto SOC, se solicita a la entidad confirmar si cuenta con un listado de ANS a tener en cuenta en la ejecución del proceso.	La Dirección de Impuestos y Aduanas Nacionales – DIAN indica al observante que, los acuerdos de nivel de servicio (ANS) están claramente definidos en el anexo técnico, los cuales deben ser cumplidos durante todas las etapas del proyecto.
143	OBSERVACIÓN No. 13 Con relación al Anexo Tecnico Proyecto SOC, se solicita a la entidad confirmar si cuenta con un listado de sanciones por el no cumplimiento de los ANS establecidos por la entidad	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, para el proyecto se contempla una disponibilidad cercana al 99.9%, que para el efecto se solicita al contratista contar con esquema de continuidad para la prestación de los servicios contratados, por lo tanto, no se contemplan sanciones por la interrupción del servicio.
144	Respetuosamente nos permitimos solicitar a la DIAN una extensión en el plazo de envío de dudas y aclaraciones hasta el martes 22 de octubre dado que: 1. La complejidad del proceso y la interacción con los fabricantes de las soluciones solicitadas demanda de cuidados especiales. 2. No fue enviado el archivo "inventarios" mencionado en varias partes del anexo técnico por lo que es posible que no estemos considerando todas las variables para ofertar responsablemente.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, los tiempos se extendieron acorde a lo solicitado y al análisis realizado por el equipo técnico de la Entidad.
145	Respetuosamente nos permitimos solicitar a la DIAN una prórroga en la fecha límite para el envío a la respuesta al RFI hasta el 22 de noviembre de 2024 dado que la complejidad del requerimiento demanda de análisis profundos de arquitectura de soluciones y servicios.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, los tiempos se extendieron acorde a lo solicitado y al análisis realizado por el equipo técnico de la Entidad.
146	Atentamente agradecemos a la DIAN aclarar si el alcance del RFI incluye la gestión de las herramientas incluidas en el requerimiento.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el alcance del proyecto se encuentra especificado en los productos, capacidades, plataformas, soluciones, servicios y demás actividades que están estipuladas en el anexo técnico de este proceso, incluyendo toda la gestión, monitoreo, administración, acompañamiento, soporte y grarantía por parte del futuro contratista.
147	Por favor aclarar el punto mencionado sobre los planes de choque. En que casos se hace necesario aplicarlos?	La Dirección de Impuestos y Aduanas Nacionales – DIAN indica al observante que, en los casos donde se generen retrasos o contratiempos en el cronograma pactado, el contratista deberá generar planes de choque que le permitan adelantar las actividades atrasadas.
148	Agradecemos a la DIAN que comparta los modelos de acuerdo de confidencialidad requeridos.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que esta informacion se entregara en la etapa de implementacion del proyecto

149	Agradecemos a la DIAN compartir los manuales mencionados.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que esta informacion se entregara en la etapa de implementacion del proyecto
150	Solicitamos sean aclaradas las ubicaciones físicas donde se encuentras los componentes de infraestructura de la DIAN.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, las ubicaciones de la infraestructura tecnológica de la DIAN se encuentra estipulada en el inventario que hace parte de este proyecto.
151	La DIAN ya posee metodologías, herramientas y métricas que hayan sido aplicadas en el pasado para medir servicios de monitoreos previamente contratados? En caso de que la respuesta sea afirmativa, agradecemos que los compartan.	La Dirección de Impuestos y Aduanas Nacionales – DIAN indica al observante que, no se cuentan con metricas o herramientas del tipo en mención, ya que la Entidad hasta ahora va a contratar los servicios de un Centro de Operaciones de Seguridad SOC.
152	Agradecemos aclarar que tipo de evidencias digitales desea la DIAN que sean cargadas.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que evidencia digital corresponde a todo documento, archivo o artefacto que se considera como entregable o registro de la operación de los servicios solicitados en cada una de las capacidades del SOC, segun el anexo tecnico
153	Agradecemos aclarar cual es la expectativa de la DIAN con respecto a la áreas involucradas en la gestión de cambios, así como la cantidad de funcionarios que deberían ser tenidos en cuenta para cumplir con este requerimiento.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que en la gestion de cambios se ve involucrada el Area de DGIT junto con la OSI, y las areas misionales que deban entender el cambio con el SOC para temas de seguridad.
154	Qué tipo de servicio tiene contratado la DIAN en este momento?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, actualmente no se tiene contratado ningún servicio que tenga que ver con la continuidad del SOC.
155	De acuerdo a los 1600 dispositivos mencionados que deben entrar dentro de las capacidades de monitoreo del servicio. ¿Se tiene conocimiento o ya un estimado de cuántas EPS promedio se estan generando o requieren para hacer la ingesta de logs en el SIEM?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la cantidad de EPS estipulada para este proyecto es de 25000.
156	En cuánto tiempo se estima el crecimiento mencionado?	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, el crecimiento proyectado es para los tres (3) años de duración del proyecto.

157	Es clara la expectativa de la entidad de que el análisis de logs se realice en tiempo real. Quisieramos saber cuáles son los tiempos de retención de logs en caliente y en frío requeridos por la DIAN.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el SIEM a adquirir debe manejar tasa de retención de tres (3) meses en línea y seis (6) meses fuera de línea.
158	Agradecemos a la DIAN aclarar que tipo dispositivos ICS posee y que deban ser monitoreados por el servicio del SOC.	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, la característica es requerida para proyectos a futuro, que se van a desarrollar en las próximas vigencias.
159	Agradecemos a la DIAN compartir el archivo "Inventarios" mencionado en el numeral 2.10. con el fin de conocer las versiones de HiperV y VMware.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, en el inventario de infraestructura anexo a este proyecto pueden encontrar las versiones de Vmware y Hyper V.
160	Agradecemos aclarar de que infraestructura de cómputo podría disponerse.	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, el ítem en cuestión presenta un error involuntario en su publicación por ende se procedió a su eliminación, además se aclara que, 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
161	Que solución de SIEM posee la entidad en este momento? Sería necesario llevar a cabo la migración de casos de uso aplicados en esta plataforma o deben ser construidos de cero? Al indicar que "En ningún caso la información de log deberá salir de la Entidad" implica que el almacenamiento de logs debe hacerse localmente en la infraestructura física de la DIAN?	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, la solución SIEM con la que cuenta la Entidad es QRADAR, y los casos de uso deberán contruirse de cero, no se va a realizar migración de casos, sin embargo , aclarar que se debe realizar la implementación de por lo menos veinte casos de uso durante la etapa de implementación, y después dentro del transcurso del contrato, se deberán implementar los que sean requeridos por la Entidad.
162	Agradecemos a la DIAN proporcionar el archivo "Inventarios".	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, se procede a publicar nuevamente los archivos necesarios para este proyecto, dentro de los cuales se encuentra el de inventarios.

163	De acuerdo a los eventos mencionados que se deben monitorear con la herramienta de correlación, agradecemos nos aclararen ¿si tienen un esperado por año de nuevas reglas de correlación?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, no se tiene un estimado de nuevas reglas, las que se realicen se harán por demanda y de acuerdo a mejores prácticas y a las necesidades puntuales de la Entidad.
164	Agradecemos a la DIAN ser más específica en la descripción de dispositivos y aplicaciones. Con esta información podemos tener un panorama claro de las integraciones que deberán realizarse entre la infraestructura y la herramienta SIEM.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, todos los dispositivos y su descripción se encuentran en el archivo de inventarios que hace parte de este proyecto, favor revisar.
165	Agradecemos especificar que normativas debe cumplir la DIAN con el fin de entender que tipo de reportes personalizados, adicionales a los que vienen Out of the Box en la solución SIEM.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, los informes solicitados, son predefinidos que vienen con la herramienta SIEM implementada, y están descritos en el ítem 2.21, que a la letra dice: Informes de Cumplimiento Out-of-the-Box · 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.
166	Agradecemos aclarar que tipo de directorio de usuarios posee la DIAN.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la Entidad utiliza active directory.
167	¿Dentro de la integración y correlación de eventos en la plataforma SIEM se tiene algun sistema de servidores AS400?	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, no se tiene dentro del inventario sistemas AS400.
168	Solicitamos nos indiquen que ticketing system posee la DIAN en este momento así como aclarar por que razón es necesario que la solución SIEM posea uno incorporado.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la característica en mención hace referencia a que la solución SIEM debe tener un sistema de ticketing y obedece a necesidades puntuales de la Entidad, y ademas debe estar en la capacidad de integrarse a sistemas externos de ticketing como ARANDA, SERVICENOW entre otros.
169	Framework de notificación de incidentes basado en políticas. ¿Actualmente que frameworks o estándares se estan utlizando o cuáles desea incluir por parte del proveedor? NIST SP 800-61, SO/IEC 27035, SANS Institute, FIRST -CSIRT Services Framework, COBIT.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la solución SIEM debe tener la capacidad de framework de notificación basado en políticas, durante la implementación se decidirá cuales se van a utilizar.

170	Agradecemos especificar el alcance del UEBA mencionado en este punto. La naturaleza del análisis de comportamiento de usuarios y entidades puede requerir de infraestructuras adicionales independientes de una solución SIEM por lo que serían necesarios licenciamientos extra.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, los paquetes de licencias de agentes de UEBA solicitados en este ítem son para los servidores windows que tiene actualmente la Entidad, y su número y cantidades pueden ser consultados en el inventario anexo de este proceso, y tal como lo indica este ítem Dichas licencias de UEBA no deberán conllevar consumo asociado ni de licencia de dispositivos ni de EPS.
171	El CONTRATISTA deberá gestionar la herramienta SOAR?	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, el futuro contratista deberá administrar, operar, gestionar, configurar, mantener y realizar las demás actividades propias del día a día con el SOAR, así mismo con los demás dispositivos, plataformas, soluciones y servicios adquiridos en este proyecto.
172	¿el alcance de la herramienta SOAR incluye el 100% de la integración al SIEM, implementación, y administración y soporte nivel 3 o de fabricante de la herramienta?	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, el futuro contratista deberá administrar, operar, gestionar, configurar, mantener y realizar las demás actividades propias del día a día con el SOAR, así mismo con los demás dispositivos, plataformas, soluciones y servicios adquiridos en este proyecto.
173	¿Cuántos usuarios con rol de administrador se deben considerar para el dimensionamiento de la herramienta?	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, se solicitan en el anexo de características licenciamiento para tres (3) analistas.
174	En caso de que la solución pueda ser instalada en entornos virtuales, la DIAN proporcionará la infraestructura para este fin?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
175	Agradecemos a la DIAN aclarar si la entidad ya tiene playbooks caracterizados y desarrollados.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, actualmente no se tienen playbooks caracterizados.
176	Favor aclarar cuántos playbooks se espera implementar en promedio al mes/año	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, no se tiene un estimado, ni promedio de playbooks al año, los que se realicen se harán por demanda y de acuerdo a mejores prácticas y a las necesidades puntuales de la Entidad.

177	La solución SOAR deberá integrarse con plataformas cuyo desarrollo haya sido hecho o contratado por la DIAN? En caso de ser así, por favor especificar las características técnicas de estas plataformas.	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, en el anexo técnico en ningún caso se solicitan integraciones con desarrollos in house de la Entidad, se habla de integraciones con software de terceros standar en la industria.
178	La DIAN cuenta en este momento con alguna herramienta de protección de bases de datos?	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, se cuenta con la herramienta Guardium para bases de datos.
179	¿Cuántas DDBB críticas de negocio se tienen planificadas en total?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, el número de bases de datos y sus características las puede consultar en el archivo de inventario que hace parte de este proyecto.
180	Solicitamos confirmar Cantidad de segmentos de red por las que pasa el tráfico hacia las Bases de datos. Esto es para definir la cantidad de interfaces que se requieren.	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, se debe tener presente el punto desde donde se pretende realizar la métrica. desde sedes en nivel central para llegar a bases de datos podemos tener hasta 7 vlans, desde sedes remotas con Mpls podemos tener hasta 9 Vlans, para bases de datos central son hasta 4 vlans.
181	En caso de que la solución pueda ser instalada en entornos virtuales, la DIAN proporcionará la infraestructura para este fin?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
182	Posee la DIAN infraestrutura en nube a ser monitoreada? IaaS? PaaS? En caso de que así sea, agradecemos indicar las caracterísitcas de estas bases de datos.	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, a la fecha, la Entidad cuenta con recursos en nube con aproximadamente 400 Máquinas virtuales (260 Windows y 140 Linux), asi como 50 SQL databases
183	Agradecemos especificar la distribución de manejadores de base de datos Oracle, sus versiones específicas y la cantidad de cores que tiene cada uno. En general y con el fin de dimensionar a futuro, se espera un crecimiento de bases de datos a ser monitoreadas en la entidad? Cual sería la proporción de este crecimiento en el tiempo y que manejadores de bases de datos se usarían? Cómo sería la infraestructura de estos crecimientos?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, el número de bases de datos y sus características las puede consultar en el archivo de inventario que hace parte de este proyecto.
184	En que casos se espera la instalación de agentes?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, la solución debe poder instalarse sin requerir agentes, la cual será la opción primordial, en el caso de que por temas de configuración o temas asociados a las características propias de las bases de datos se procederá a utilizar agente.

185	¿el alcance de la herramienta **herramienta de protección de Bases de Datos** incluye el 100% de la integración al SIEM, implementación, y administración y soporte nivel 3 o de fabricante de la herramienta?	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, el futuro contratista deberá administrar, operar, gestionar, configurar, mantener y realizar las demás actividades propias del día a día con la protección de bases de datos, así mismo con los demás dispositivos, plataformas, soluciones y servicios adquiridos en este proyecto.
186	Agradecemos especificar cuantos servidores, switches, routers y plataformas de virtualización posee la entidad así como los volúmenes de crecimiento en el tiempo de duración del contrato.	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, el número de servidores, switches, routers, plataformas de virtualización y demás dispositivos las puede consultar en el archivo de inventario que hace parte de este proyecto, en cuanto al crecimiento está estipulado hasta llegar a los 2467 dispositivos.
187	La utilización de una solución de gestión de vulnerabilidades desemboca en un servicio completo de aseguramiento y remediación. Agradecemos a la DIAN aclarar lo siguiente: 1. Cantidad de servidores, estaciones y dispositivos de telecomunicaciones por sistema operativo. 2. Porcentaje de obsolescencia de la infraestructura. 3. Cantidad de vulnerabilidades detectadas y de vulnerabilidades pendientes clasificadas por severidad en el escaneo más reciente: Vulnerabilidades detectadas (Crítica, Alta, Media, Baja), Vulnerabilidades pendientes (Crítica, Alta, Media, Baja). 4. Fecha de ejecución del escaneo más reciente y frecuencia de esta actividad. 5. Herramienta utilizada para ejecución de escaneos y tipo de escaneo (por red / Autenticado / Con agentes) 6. Cantidad de infraestructura detectada. 7. La DIAN cuenta con herramienta para despliegue de parches en servidores y estaciones? En caso afirmativo especificar el nombre. 8. Frecuencia de realización de despliegue de parches. 9. Frecuencia de remediación en servidores, estaciones y dispositivos de telecomunicaciones. 10. Por favor describir la infraestructura en nube que deberá ser escaneada.	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, de acuerdo a su inquietud se permite precisar lo siguiente: Cantidad de dispositivos de telecomunicaciones: (router (120), switches 700, AP 120, controladoras (2), entre otros). La Entidad cuenta con una infraestructura tecnológica que tiene una vida útil de 5 años con garantías de fábrica y contratos de mantenimiento y soporte Si, Windows Update Services En servidores Windows, mensualmente La remediación de equipos está ligada al ciclo de mantenimiento de la infraestructura y durante el mismo se ejecuta con la última liberación de parches de los fabricantes (Switches Hp, HP_Aruba), (Routers Cisco y Huawei) Vulnerabilidades detectadas (Crítica: 1, Alta: 5, Media: 4 y Baja: 1), Vulnerabilidades pendientes (Alta:3, Media: 4, Baja: 1). La última ejecución de escaneo se realizó el 28 de mayo de 2024 Host Penetration, Intranet Penetration, Weak Credential Exploit
188	¿El alcance de la herramienta para el Monitoreo a la Gestión de Vulnerabilidades incluye el 100% de la integración al SIEM, implementación, y administración y soporte nivel 3 o de fabricante de la herramienta?	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, el futuro contratista deberá administrar, operar, gestionar, configurar, mantener y realizar las demás actividades propias del día a día con la gestión de vulnerabilidade, así mismo con los demás dispositivos, plataformas, soluciones y servicios adquiridos en este proyecto.
189	Para la Postura de Seguridad infraestructura Cloud especificar que tipo y cantidad de activos en las nubes de Azure, AWS entre otras	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, a la fecha, la Entidad cuenta con recursos en nube con aproximadamente 400 Máquinas virtuales (260 Windows y 140 Linux)

190	¿El alcance de la herramienta para el Caza de amenazas incluye el 100% de la integración al SIEM por parte del proveedor, administración y soporte nivel 3 o de fabricante de la herramienta?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, todas las herramientas, soluciones, servicios, plataformas y demas componentes que sean solicitados en el anexo técnico de este proyecto y que sean susceptibles a ello, deben ser integradas al SIEM. En cuanto al soporte y garantía de los niveles que se requiera (nivel 1, 2 y 3) deben ser prestados por el futuro oferente y acorde a los fabricantes de las soluciones entregadas.
191	¿El alcance de la herramienta NDR incluye el 100% de la integración al SIEM por parte del proveedor, administración y soporte nivel 3 o de fabricante de la herramienta?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, todas las herramientas, soluciones, servicios, plataformas y demas componentes que sean solicitados en el anexo técnico de este proyecto y que sean susceptibles a ello, deben ser integradas al SIEM. En cuanto al soporte y garantía de los niveles que se requiera (nivel 1, 2 y 3) deben ser prestados por el futuro oferente y acorde a los fabricantes de las soluciones entregadas.
192	La DIAN solicita en este apartado una solución de Protección de Marca. Dadas las implicaciones de los resultados obtenidos por una solución de este tipo, la DIAN estaría en disposición de contratar un servicio de protección de marca donde la herramienta sea propiedad del CONSULTOR? En caso afirmativo agradecemos aclarar lo siguiente: 1. Cuantos dominios/marcas se desea monitorear? Por favor indicar cuales. 2. Cuantos subdominios se desea monitorear? Por favor indicar cuales. 3. Con cuantas redes sociales cuenta la DIAN? Por favor indicar cuales. 4. Se desea monitorear usuarios VIP? Indicar la cantidad de usuarios VIP. 5. Por favor indicar el número de incidentes por suplantación de marca, dominios, subdominios y usuarios VIP ocurridos en el último año.	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, las herramientas, plataformas, soluciones y servicios requeridos por la DIAN serán de propiedad de la DIAN, por lo tanto su entendimiento no es correcto.

193	Agradecemos detallar los activos que serán incluidos en el ejercicio de Ethical Hacking: Servidores: Cantidad, Sistema operativo, Externo/interno/Nube (IaaS, PaaS, SaaS), Tipo de servidor (propósito general, Servidor Web, servidor de base de datos, servidor de directorio activo, servidor de anti-virus, etc.). Aplicaciones: Cantidad, Tipo de Aplicación - WEB - Consultas o cliente - servidor, Móvil: Android o IOS, Interno/Externo, Cantidad de Usuarios Recurrentes, Cantidad de URLs/IPs. Otros Activos: Cantidad, Tipo de Activo (Switch, Router, Firewall, Estación de Trabajo, IoT), Interno/Externo, Cantidad de URLs/IPs 1. La DIAN desea incluir retest? 2. La DIAN requiere alinear las pruebas bajo una metodología específica? (SANS Top 25, OWASP, OS, ISSAF, OSSTMM, otra?) 4. Que tipo de prueba espera la DIAN que sea realizada? (orientadas a un objetivo, interna, externa, a ciegas y dobleciegas?)	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa lo siguiente: Inventario de dispositivos y elementos se encuentra disponible en el anexo que hace parte de éste proyecto Inclusión de Retest: La DIAN considera la posibilidad de realizar retests, de acuerdo con los hallazgos y el impacto de las vulnerabilidades detectadas en el ejercicio inicial. Los detalles específicos se acordarán con el contratista en la planeación de cada prueba. Metodología de Pruebas: La DIAN requiere alinear las pruebas con metodologías de referencia como OWASP, SANS Top 25 o similares, adaptando las pruebas a las mejores prácticas en desarrollo seguro. La metodología específica será concertada con el contratista para asegurar el cumplimiento de los objetivos de cada ejercicio. Tipo de Pruebas Esperadas: La DIAN espera que las pruebas sean de tipo caja gris, pudiendo incluir tanto pruebas internas como externas. La orientación específica de cada ejercicio (pruebas orientadas a objetivos, ciegas, doble ciegas, entre otras) se definirá en coordinación con el contratista, atendiendo a los requisitos de seguridad de la entidad para el ejercicio correspondiente.
194	1. Agradecemos indicar el tiempo total de duración del servicio de monitoreo contratado. 2. Agradecemos indicar número de datacenters o sitios en los cuales se encuentra la infraestructura a monitorear. Por favor indicar si la DIAN cuenta con dispositivos a monitorear ubicados en nubes públicas como AWS, Azure u otro. 3. Por favor confirmar si la DIAN desea almacenar los logs en su infraestructura propia o si desea que el CONSULTOR lo haga. En todo caso agradecemos confirmar los tiempos de retención: Almancenamiento en línea, Almacenamiento en reposo. 4. Por favor confirmar si la DIAN desea que la solucion SIEM esté instalada en su infraestructura interna o en las premisas del CONSULTOR (o en la nube). 5. Agradecemos especialmente a la DIAN confirmar los activos que harán parte del servicio de monitoreo y gestión de incidentes de ciberseguridad de acuerdo con las siguientes especificaciones:	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, en cuanto a sus consideraciones se hacen las siguientes precisiones: 1.El monitoreo y todas las actividades de administración, gestión, operación, garantía y soporte se harán por el término de duración del contrato, tres años (3). 2.Las ubicaciones y locación de la infraestructura TI de la Entidad que hace parte de este proceso se encuentra en el anexo de inventarios. 3. El SIEM a adquirir debe manejar tasa de retención de tres (3) meses en línea y seis (6) meses fuera de línea. 4.el futuro contratista debe contar con un Centro de Operaciones de Seguridad - SOC ubicado en una locación física en la ciudad de Bogotá, donde instalará todos los los productos, capacidades, plataformas, soluciones y servicios, requeridos por la Entidad y que se encuentran en el anexo técnico y que le permitan realizar todas las actividades solicitadas en este por la DIAN. Entendiendose que el contratista realizará toda la gestión, monitoreo, administración, acompañamiento, soporte y grarantía de los mismos, cobijando toda la infraestructura tecnológica de la Entidad especificada en el inventario anexo. 5. Los activos y demás características de estos se encuentran detallados en el apartado de inventarios y las especificaciones de cada una de las soluciones, plataformas, capacidades, servicios, soporte y garantía se encuentran en el anexo técnico.

195	Por mejores prácticas y especificaciones de continuidad de negocios, se recomienda dispersión geográfica de los centros de datos de al menos 100 kilómetros. Respetuosamente solicitamos a la DIAN que considere que los centros de datos y centros de monitoreo observen esta recomendación para efectos de asegurar la continuidad del servicio en situaciones de desastre.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el servicio del SOC deberá contar con mínimos dos (2) centro de datos geográficamente ubicados en diferentes lugares dentro de Bogotá D.C o uno de estos puede estar fuera de Bogotá, siendo este para contingencia o alta disponibilidad, aclarando que el datacenter principal de donde se prestará el servicio de SOC y las capacidades contratadas, debe encontrarse en la ciudad de Bogotá. El proponente debe especificar la cantidad de Centro de Datos de los que dispone para el SOC, su ubicación y el rol de cada uno de ellos, por lo tanto no se acepta su sugerencia.
196	El punto mencionado solicita "Certificación vigente como arquitecto de seguridad de redes o analista de seguridad de redes o su equivalente en la solución ofertada. Emitida por el fabricante". A cual de las soluciones ofertadas se refiere la solicitud?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que la referencia se hace a las soluciones SIEM, SOAR o monitoreo de marca según el anexo técnico.
197	Agradecemos a la DIAN aclarar cuantos analistas nivel I son el mínimo para cumplir con el requerimieto.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, son tres (3) analistas nivel I, tal como lo indica el anexo técnico.
198	En 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. ¿Se puede proponer la atención de acuerdo a estos niveles de atención especializada como bolsa de horas prepagada?	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la atención, servicio o soporte es 7x24x365 a cualquier nivel de escalamiento, la cual en ningún momento está supeditada a bolsa de horas prepagada, las solicitudes deben ser bajo demanda y de acuerdo a las necesidades propias de la Entidad y de acuerdo a la presentación de problemas, inconvenientes o incidentes durante la ejecución del proyecto SOC.
199	Realizar el análisis Forense para incidentes críticos, y determinar el origen y el vector de inicio del incidente. ¿Se puede proponer la atención de análisis forense como bolsa de horas prepagada?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, dentro de los requerimientos solicitados, el futuro contratista deberá realizar el análisis Forense para incidentes críticos, y determinar el origen y el vector de inicio del incidente como parte de su pull de servicios SOC, en ningún momento se habla de un servicio adicional o anexo a este proyecto, por lo cual se aclara que no está solicitando un servicio de horas prepagada. Todas las solicitudes deben ser bajo demanda y de acuerdo a las necesidades propias de la Entidad y de acuerdo a la presentación de problemas, inconvenientes o incidentes durante la ejecución del proyecto SOC.

200	Agradecemos a la DIAN detallar el requerimiento mencionado en este punto, de integración y cacería de amenazas.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la integración de la que se menciona en este ítem es la caceria de amenazas del punto 6 y la gestión de incidentes de seguridad.
201	Favor aclarar cuántos casos de uso se espera implementar en promedio al año	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, referente al item en mención la Dian no cuenta con una proyección o estadística a futuro de casos de uso para este caso en particular, ya que al servicio nuevo no propone un estimado, se deben realizar bajo demanda y de acuerdo a las necesidades propias de la Entidad y al tiempo de ejecución del proyecto.
202	De acuerdo a la tabla de tiempos de atención/solución para incidentes aclarar si: - ¿Si la tabla de ANS hace referencia a la atención de incidentes relacionados con las herramientas o al servicio de incidentes de seguridad? - ¿Si el nivel máximo de atención hace referencia al tiempo maximo para noticar al cliente debido a la detección de un incidente?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, de acuerdo a sus inquietudes se permite hacer las siguientes precisiones: -Hace referencia al servicio de incidentes de seguridad. -Los tiempos referidos son claros y determinan desde la atención a la solución, favor revisar.
203	Agradecemos a la DIAN aclarar por cuanto tiempo será contratado el servicio objeto del presente RFI. Entendemos que el soporte de fabricante de las soluciones será contratado por un año, pero no se especifica el tiempo de los servicios que deberá proveer el CONSULTOR.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la administración, operación, gestión de los servicios y demás actividades de las plataformas, soluciones, software, hardware, entre otros, que hacen parte de las capacidades requeridas por la Entidad en este proyecto, debe ser realizadas por el futuro oferente, tal como se indica en el anexo de caracterítiscas técnicas que hace parte de este proceso, y deben ser prestada por el tiempo de ejecución del proyecto que es de tres (3) años.
204	Agradecemos a la DIAN indicar cuales serían los crecimientos de la infraestructura que deberá cubrirse durante el tiempo de duración del contrato.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el crecimiento proyectado está incluido dentro de los 2467 dispositivos, y debe ser puesto para uso de la Entidad desde el inicio del proyecto.
205	Por favor especificar si lo mencionado en la página 7 párrafo 5 en relación con "Por lo anterior, la DIAN requiere una Solución de Identidades centralizada.", hace referencia al contexto de la entidad? o a parte de la solución requerida?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que hace parte del contexto de la Entidad, dado que en el alcance del anexo tecnico adjunto la solucion de identidades no es requerida. La DIAN surtio otro proceso para tal fin.
206	¿Se contempla como punto de partida la información actual sistema SIEM o es un proceso con totalmente nuevo?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, es un proceso totalmente nuevo.

207	¿Las cifras proporcionadas en este punto son únicamente infraestructura DIAN o esta mezclada con componentes de terceros y cadena de suministro?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, el inventarioo anexo comprende todos los elementos de la infraestructura tecnológica de la DIAN.
208	¿Cuales servicios se requiere que se realice monitoreo de transacciones sintéticas, a nivel general, o para algún tipo de transacción especifica (Aduanas, impuestos,etc)?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, el monitoreo de transacciones sintéticas debe ser general, aclarando que en caso de requerirse por parte de la Entidad, se deberá hacer más especifico y exhaustivo.
209	¿Se contemplan sistemas de información legados o que estén fuera de soporte por parte del proveedor?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, en el inventario anexo encontrará las características y cantidades de las aplicaciones a las cuales hay que realizar monitoreo.
210	Especifique las actividades de cuentas de usuario que se desea monitorear	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, corresponde a todo tipo de actividades administrativas que se pueden realizar sobre cuentas de usuario como por ejemplo: Crear cuentas,Creación de grupos,Asignar permisos, Asignar usuarios autorizados, Eliminar cuentas de usuario.
211	¿Se solicita ampliar el detalle de los elementos que se indican "revisar contra inventario" tales como el versionamiento, el fabricante entre otras características?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, los elementos de almacenamiento y demás dispositivos pueden ser revisados en cantidad y características en el inventario anexo a este proceso.
212	Se solicita la lista exacta de los elementos de seguridad que serán incluidos en el SIEM	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, los elementos y dispositivos a ser incluidos en el monitoreo del SIEM pueden ser revisados en cantidad y características en el inventario anexo a este proceso, aclarando que el alcance es de 2467 dispositivos como m{aximo.
213	¿Se contempla que dentro de la propuesta se incluyan elementos tecnológicos que se están implementando en otros proyectos o se van a implementar durante el proyecto?	La Dirección de Impuestos y Aduanas Nacionales - DIAN informa al observante, que el alcance del proyecto está detallado en el anexo técnico, es claro que a futuro el contratista deberá implementar monitoreo y soporte a nuevos dispositivos hasta copar el licenciamiento solicitado.
214	¿Se conoce algún tipo de restricción de compatibilidad de los componentes tecnológicos relacionados que deba tenerse en cuenta y que pueda afectar la implementación de algún tipo de servicio?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, no existe ninguna restriccion

215	¿Se cuenta con las autorizaciones y viabilidad para realizar la conexión a toda la infraestructura solicitada en el RFI?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, se cuenta con la viabilidad para conectar toda la infraestructura.
216	¿Todos los dispositivos referenciados cuentan con soporte vigente por parte del fabricante?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, toda la infraestructura tecnológica de la Entidad cuenta con soporte y garantía con vigencias entre 2026 y 2028.
217	¿Se cuenta con topologías de RED actualizados y hace cuanto tiempo fueron actualizados?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, si, las topologías se consideran como documento vivo, por lo que son actualizadas cada vez que se presentan cambios en la infraestructura.
218	¿Dentro de estos componentes se contemplan componentes de terceros o cadena de suministro?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, el inventario anexo a este proceso no contempla equipos de terceros.
219	¿Los elementos que deben ser incluidos en el análisis son los 1.608 referenciados?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, para efectos del presente proceso son 2467 dispositivos, incluyendo su crecimiento, dichos elementos se encuentran en el inventario anexo.
220	¿Se tienen KPI´S previamente definidos o se pueden considerar libremente por parte del proveedor?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, los kpi's a los que se refiere este punto son los que vienen con la herramienta, así mismo durante la implementación y el transcuso del contrato se definiran y solicitarán varios por parte de la Entidad, y el contratista podrá realizar las recomendaciones pertienentes frente a este tema y otros referentes a las actividades e implementación de las capacidades del proyecto en mención.
221	¿Existen análisis de capacidad actuales que midan el crecimiento de la infraestructura tecnológica de la DIAN?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, tal como lo indica el anexo técnico de este proyecto, la proyección para el crecimiento de dispositivos esta dada hasta para 2467 incluyendo crecimiento, por lo tanto el futuro contratista no requiere conocer analisis de capacidades de la Entidad para hacer sus respectivos estimativos.

222	¿Qué tipo de usuarios y cuántos usuarios se requiere auditar?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, la auditoria es completa a la actividad de usuarios, debe realizarse a todos los usuarios internos , inicialmente se requiere a 17727
223	¿Como se relaciona este punto con el punto 2.4?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que,los dos ítems están relacionados al hablar de licenciamiento y dar un alcance de hasta 2467 dispositivos para el SIEM, y que dichas licencias no deben ser afectadas agregando características como las que se solicitan en el 2.35.
224	¿Existe un sistema pre definido o pre determinado de referencia para la gestión del SOAR?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, la Entidad no cuenta con plataforma SOAR actualmente.
225	¿A qué se refiere con "Cantidad (Especificar la cantidad ofrecida)" se refiere al número de licencias, usuarios o algo adicional?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, se refiere a la cantidad de aplliances o dispositivos de proposito especifico SOAR ofrecidos.
226	¿A qué tipo de usuario se hace referencia?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, se refiere a los usuarios con roles en el SOC que tendran funciones como analisitas o usarios de la solucion SOAR
227	¿A qué tipo de usuario se hace referencia?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, se refiere a los usuarios con roles en el SOC que tendran funciones como analisitas o usarios de la solucion SOAR
228	¿Este requerimiento hace referencia al sistema de solicitud de servicios o a que hace referencia?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, se refiere al sistema de escalamiento con el cual debe contar el SOAR ofertado.
229	Especificar si se requiere que la herramienta cuente con una funcionalidad para generar y gestionar tickets adicional a la herramienta de gestión de requerimientos de la entidad	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, el SOAR ofertado debe venir con la funcionalidad de generar sus propios tickets y poder hacer escalamiento de requerimientos entre analistas, además debe poseer la posibilidad de integrarse con la mesa de ayuda ARANDA de la Entidad.

230	¿Todos los dispositivos referenciados cuentan con soporte vigente por parte del fabricante?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, toda la infraestructura tecnológica de la Entidad cuenta con soporte y garantía con vigencias entre 2026 y 2028.
231	¿Se cuenta con las autorizaciones y viabilidad para realizar la conexión a toda la infraestructura solicitada en el RFI?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, en el momento que sea requerido se podrá realizar la conexión a toda la infraestructura por parte del futuro contratista.
232	¿Todos las bases de datos referenciadas cuentan con soporte vigente por parte del fabricante?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, la Entidad cuenta con un contrato vigente de soporte y actualización de licencias con Oracle Colombia, mediante la Orden de compra número 120059. Igualmente se cuenta con soporte para las bases de datos de Microsoft SQL
233	¿Se cuenta con las autorizaciones y viabilidad para realizar la conexión a todas las bases de datos solicitadas en el RFI?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, en el momento que sea requerido se podrá realizar la conexión a todas las bases de datos que hacen parte de este proyecto por parte del futuro contratista.
234	Se requiere contar con el listado de las cantidades (16.600) discriminado por Tipo de Activo, Sistema Operativo, Versión, Modelo y Fabricante	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, en el inventario anexo encontrará las características y cantidades de dispositivos mencionadas en el anexo técnico.
235	¿Se cuenta con las autorizaciones y viabilidad para realizar la conexión a todos los activos relacionados en el RFI?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, en el momento que sea requerido se podrá realizar la conexión a todos los dispositivos que hacen parte de este proyecto por parte del futuro contratista.
236	¿Este ítem hace referencia a que serán más de 16.600 dispositivos que se requerirán analizar en el escaneo de vulnerabilidades? ¿Se cuenta con un límite máximo de dispositivos?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, el alcance está estipulado en el anexo técnico y será para 17727 dispositivos.
237	¿Estas 260 aplicaciones son adicionales a los 16.600 dispositivos mencionados en el 5.3.2?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, las aplicaciones están incluidos en el alcance de los 17727 dispositivos.

238	¿Se cuenta con las autorizaciones y viabilidad para realizar la conexión a las 260 aplicaciones solicitadas en el RFI?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, en el momento que sea requerido se podrá realizar la conexión a todoas las aplicaciones que hacen parte de este proyecto por parte del futuro contratista.
239	¿Por favor especifique a qué hace referencia este requerimiento?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, corresponde a la capacidad para reutilizar plantillas predefinidas que revisen la configuracion de la aplicación web escaneada y que muestre vulnerabilidades a ser explotadas por atacantes.
240	¿Se cuenta con las autorizaciones y viabilidad para realizar el escaneo a los sitios públicos y privados solicitados en el RFI?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, en el momento que sea requerido se podrá realizar la conexión a todoas las aplicaciones que hacen parte de este proyecto por parte del futuro contratista.
241	Por favor especificar el periodo solicitado para la solución	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, la solución debe contar con soporte de fábrica 7x24X365, garantía y actualizaciones de inteligencia de amenazas por un período de 3 años.
242	Se requiere contar con el listado de las cantidades (16.000) discriminado por Tipo de Activo, Sistema Operativo, Versión, Modelo y Fabricante	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, el listado y las cantidades solicitadas se encuentran en el inventario anexo a este proyecto.
243	Por favor aclarar si es para 16.000 dispositivos o para 1.600 dispositivos	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, son 17727 dispositivos, los mismos referenciados en el numeral 5.3.2
244	¿Se cuenta con las autorizaciones y viabilidad para realizar la conexión de la solución con las 50 aplicaciones solicitadas en el RFI?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, en el momento que sea requerido se podrá realizar la conexión a toda la infraestructura por parte del futuro contratista, que hace parte del inventario y del anexo técnico de este proyecto.

245	¿Se cuenta con las autorizaciones y viabilidad para realizar la conexión de la solución con los 260 activos públicos solicitados en el RFI?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, en el momento que sea requerido se podrá realizar la conexión a toda la infraestructura por parte del futuro contratista, que hace parte del inventario y del anexo técnico de este proyecto.
246	¿Cuál es el alcance de las pruebas técnicas a activos críticos o a toda la infraestructura de la entidad?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que en relación con el Ethical HAcking se aclara que el objetivo de esta acción es la infraestructura indicada en el Inventario de dispositivos y elementos que hacen parte del Proyecto. Se aclara que la cantidad mínima de activos para el ejercicio es de cien (100)
247	¿Por favor especificar si se tiene un procedimiento de gestión de incidentes que se deba seguir en caso de identificar vulnerabilidades graves?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa que, se tiene un procedimiento que sera proporcionado en su momento al futuro contratista ganador.
248	¿Por favor indicar cuántas personas estarán habilitadas para la realización de las actividades del proyecto y confirmar a que áreas pertenecen?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa que, este punto se refiere a que "el personal destinado por el contratista para realizar estos ejercicios debe ser completamente diferente al personal destinado por el contratista para la implementación y operación del SOC". La Oficina a cargo por parte de la DIAN para liderar este proyecto es la Oficina de Seguridad de la Información, por lo tanto, el futuro contratista tendrá que entenderse con esta Oficina.
249	¿Por favor especificar en donde se encuentran las sedes de las que se refiere el punto si es Bogotá, otras ciudades o inclusive en algún país en el exterior?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el punto en mención hace referencia a lo siguiente: Ubicaciones para implementación y configuración: El oferente contará con un Centro de Operaciones de Seguridad SOC en la ciudad de Bogotá, donde se implementarán todos y cada uno de los servicios, dispositivos, plataformas, soluciones y demás productos que hagan parte de los requerimientos de la Entidad en este proyecto.
250	¿Por favor aclarar a que tipo de actividades se refiere este numeral?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, este numeral hace referencia a que el proveedor debe entregar un plan de trabajo detallado de las actividades a realizar, el cual será validado por la Entidad para iniciar la ejecucion de estas actividades.

251	¿Por favor confirmar que esto hace referencia a las herramientas adquiridas durante el proyecto? Las herramientas y software que se encuentra en la entidad ¿Deben tener soporte por parte del fabricante bajo la responsabilidad de la DIAN? ¿Por favor confirmar que se tendrá apoyo por parte del fabricante en la realización de las pruebas y la estabilización de las plataformas de las herramientas o software que no hacen parte de la ejecución del proyecto?	La Dirección de Impuestos y Aduanas Nacionales - Dian indica al observante que, el ítem en mención hace referencia a las herramientas, plataformas, soluciones y demás servicios entregados por el contratista. Se aclara que la infraestructura a monitorear cuenta con soporte del fabricante. Las pruebas para realizar la implementación y puesta en producción de todo lo entregado durante el proyecto las debe realizar el futuro contratista, en caso de requerirse apoyo por parte de los fabricantes de la infraestructura de la Entidad será coordinado en su momento.
252	¿Por favor confirmar quien debe realizar la gestión los acercamientos con el parthner de la nube contratada para coordinar los despliegues e implementaciones que se deben realizar?	La Dirección de Impuestos y Aduanas Nacionales - Dian indica al observante que, la supervisión y el seguimiento del presente proyecto estará en cabeza de la Oficina de Seguridad de la Dian, por lo tanto, cualquier actividad como acercamientos con terceros (fabricantes o contratistas) de la infraestructura tecnológica de la DIAN será realizada a través de este canal.
253	¿Por favor confirmar esta información dado que existen puntos en donde se hablan de PC´S y sitios WEB?	La Dirección de Impuestos y Aduanas Nacionales - Dian indica al observante que, los servicios de monitoreo, correlación, administración, gestiión, automatización y los demás que hagan parte del centro de operaciones de seguridad - SOC, deberán hacerse sobre toda la infraestructura tecnológica (appliance, plataformas, pc`s, endpoints, aplicaciones, bases de datos, servidores, entre otros) estipulada en el archivo de inventarios que hace hace parte de este anexo técnico, y hasta copar las capacidades de licenciamiento solicitadas en este proyecto.
254	¿Confirmar que el alcance sean dispositivos de propiedad de la DIAN sin incluir terceros o cadena de suministro?	La Dirección de Impuestos y Aduanas Nacionales - Dian indica al observante que, toda la infraestructura tecnológica estipulada en el archivo de inventarios de este proyecto, es propiedad de la Entidad.
255	¿Confirmar si los controles tecnológicos que se relacionan en este numeral están relacionados o se incluyen dentro de los activos de información relacionados en este anexo?	La Dirección de Impuestos y Aduanas Nacionales - Dian indica al observante que, los controles tecnologicos estan realacionados con los activos de informacion e inventario de este anexo tecnico.
256	¿Confirmar que el alcance esta limitado solamente a la conexión más no a realizar algún tipo de configuración, pruebas o estabilización en la herramienta GRC?	La Dirección de Impuestos y Aduanas Nacionales - Dian indica al observante que, tal como se estipula en este ítem se debe realizar la integración con la herramienta GRC propiedad de la Entidad, dejando la automatización totalmente funcional, para lo cual el futuro contratista se podrá apoyar con el fabricante de la herramienta en mención.

257	¿Por favor confirmar en que versión de la norma 27001 debe estar certificado si en la versión 2013 o en la versión 2022?	La Dirección de Impuestos y Aduanas Nacionales - Dian comunica al observante que, para evitar interpretaciones, el ítem en mención se ajusta de la siguiente manera: Los procesos de gestión y operación deben estar basados en las mejores prácticas establecidas por los modelos de procesos ITIL, CSIRT, ISO 27001:2013 o 27001:2022, NIST (CSF) o CERT. Nota: El contratista debe estar certificado en estas mejores prácticas de ISO 27001 en las versiones mencionadas, para su proceso de SOC.
258	¿Por favor confirmar si se puede presentar otro tipo de certificaciones que soporten o reemplacen la ISO 27001?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, como mínimo según lo solicitado en este ítem el contratista debe estar certificado en la norma ISO 27001.
259	¿Por favor confirmar sise debe tener una alineación con un proceso de gestión de incidentes vigente o debe crearse?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro contratista debe alinearse a la metodología existente en la Entidad para la gestión de incidentes.
260	¿Por favor confirmar si todos los servicios del SOC entran dentro de esta consideración o solo aplica para los servicios de monitoreo?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, todos los servicios, plataformas, soluciones y capacidades deben instalarse, implementarse, operarse, administrarse y prestarse desde la instalaciones del Proveedor SOC (contratista) en la ciudad de Bogota.
261	¿Por favor confirmar si los servidores de sincronización de relojes van a estar conectados a los que tiene la entidad en este momento o si se requiere una implementación nueva?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, para fines de correlacion es requerido que la sincronizacion de relojes esten conectados a los que tienen la Entidad
262	¿Por favor verificar el nivel de implementación que tiene la entidad de los ítems relacionados y su nivel de madurez?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem refiere a los incidentes y a su forma de gestión.
263	¿Por favor confirmar si se puede presentar otro tipo de certificaciones que soporten o reemplacen la ISO 27001?	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, como mínimo según lo solicitado en este ítem el contratista debe estar certificado en la norma ISO 27001, por lo tanto, su solicitud no procede.

264	Especificar si se requiere que el contratista suministre una solución para generar y gestionar tickets adicional a la herramienta de gestión de requerimientos de la entidad	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el ítem referido no hace mención alguna de una solicitud de una herramienta adicional, por lo tanto, su entendimiento no es acertado.
265	Las capacitaciones solicitadas podrán ser seleccionadas por el contratista o ya se tienen identificadas las capacitaciones requeridas?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que las capacitaciones pueden seleccionadas por el contratista, cumpliendo con los parámetros mínimos solicitados, cuarenta (40) horas, en temas de SIEM, SOAR, y las demás soluciones, tecnologías y servicios adquiridos.
266	Los váuchers son solo de capacitación? o también se requieren váuchers de certificación? si es así especificar el número	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que los vouchers solicitados son de certificación, tal como se indica en el ítem en mención.
267	¿Se requiere que el Gerente de Proyecto cuente con la Maestría solicitada y la Certificación en PMP o puede ser alguna de las dos?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que, tal como se indica en este ítem, debe tener los dos estudios (maestría y certifidado PMP).
268	¿Se requiere que el Gerente de Proyecto cuente con la Maestría en Gerencia de Proyectos? o puede ser Especialización en Gerencia de Proyectos?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, debe ser Maestria en Gerencia de Proyectos.
269	¿Por favor confirmar si existen una metodología para la gestión de incidentes implementada en la entidad y cual	La Dirección de Impuestos y Aduanas Nacionales - DIAN aclara al observante que, el futuro contratista debe alinearse a la metodología existente en la Entidad para la gestión de incidentes, su estado es funcional y se aplica para todos los incidentes.
270	¿Especificar si el numero de años de soporte requerido para las soluciones contratadas es de 3 o de 4 años?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, el alcance para monitoreo, soporte, garantía y demás actividades que hacen parte integral de este proyecto es de tres (3) años.
271	Solicitamos por favor poder suprimir el ítem "Debe tener autoaprendizaje de inventario de activos (CMDB)" de las caracteristicas presentes por el SIEM a fin de poder obtener pluralidad de ofertas	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, la característica solicitada en este ítem esta estructurada con base en las necesidades puntuales de la Entidad, por lo tanto su supresión no es posible.

272	Agradecemos por favor informar a mas detalle los activos que van a ser parte de la solución SOC	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que el futuro contratista deberá administrar, operar, gestionar, configurar, mantener y realizar todas las actividades propias del día a día con las plataformas y soluciones implementadas. Esto se extiende a todos los dispositivos, plataformas, soluciones y servicios adquiridos en el marco de este proyecto, el detalle de todos los activos se encuentra especificado en el inventario anexo a este proyecto.
273	Agradecemos por favor confirmar la ubicación de los activos para poder estimar la cantidad de colectores necesarios para la implementación del servicio SOC	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la ubicación de toda la infraestructura tecnológica de la Entidad y que hace parte de este proyecto es en la ciudad de Bogotá en el datacenter principal.
274	agradecemos por favor informar en base al texto "La solución debe estar en capacidad de instalarse en Azure, AWS, HyperV (en la versiones con que cuenta la entidad), Vmware (en la versiones con que cuenta la entidad). (Revisar archivo anexo inventarios)" cuales son las versiones para HyperV y Vmware	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, las versiones de Vmware y Hyper V con las que cuenta la Entidad se encuentran en el inventario anexo.
275	agradecemos por favor aclarar segun el punto 84 "Supervisión del cambio de configuraciones en tiempo real" si estas funcionalidades pedidas deben ser nativas por la plataforma o que permitan la integracion de estas	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, estas funcionalidades deben ser nativas de la plataforma.
276	agradecemos por favor confirmar si ya se cuenta con casos de uso para la solución Siem - SOC y si podemos tener detalle de estos para poder validarlos a nivel de solucion	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, se deben implementar casos de uso nuevos, por lo tanto, no es necesaria información anterior.
277	por favor aclarar segun el item " Soporte inmediato para una amplia variedad de sistemas de seguridad y APIs de proveedores - tanto locales como en la nube." a que se hace referencua con un soporte inmediato	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la plataforma debe soportar variedad de sistemas de seguridad y APIs de proveedores tanto locales como en la nube.
278	Solicitamos por favor eliminar o dejar como opcional el cumplimiento de "Sistema incorporado de ticketing." dado que la herramienta de Siem permite la integracion con estas soluciones	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la característica en mención hace referencia a que la solución SIEM debe tener un sistema de ticketing y obedece a necesidades puntuales de la Entidad, y ademas debe estar en la capacidad de integrarse a sistemas externos de ticketing como ARANDA, SERVICENOW entre otros.

279	Solicitamos por favor segun el siguiente parrafo " Dashboards configurables en tiempo real, con desplazamiento "Slide-Show" para mostrar KPIs." poder eliminar la condicion de Slide-Show de este numeral	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la funcionalidad requerida obedece a necesidades puntuales de la Entidad, y a la facilidad de manejo y gestión de las plataformas, por lo tanto suprimir dicha característica no es posible.
280	Solicitamos por favor en el ïtem de licenciamiento segun el parrafo " Se deberá disponer de paquetes de licencia de agentes de UEBA para equipos Windows. Dichas licencias de UEBA no deberán conllevar consumo asociado ni de licencia de dispositivos ni de EPS." podar quitar de este el NO consumo de EPS dado que las soluciones SIEM al colectar estos logs lo hacen partiendo tambien de la cantidad de EPS	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la funcionalidad requerida obedece a necesidades puntuales de la Entidad, por lo tanto suprimir dicha característica no es posible.
281	Agradecemos confirmar, la cantidad de casos de usos y playbooks que se desean implementar con la Solución SOAR	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, en anexo tecnico items 3.52 se solicitan la cantidad mínima de playbooks que debe venir la solución SOAR requerida, su implementación tanto de estos como de casos de uso se hará de acuerdo a las necesidades de la Entidad.
282	Agradecemos confirmar los activos, cantidades soluciones con sus versiones de sistema operativo que serán vinculados a los playbooks	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que en el Anexo Inventario de IT, se encuentra esta informacion, por favor remitirse a este documento.
283	Agradecemos confirmar los protocolos especificos sobre los cuales serán vinculados los activos necesarios en los playbooks	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que esta informacion se entregara en la etapa de implementacion del proyecto
284	agradecemos confirmar la ubicación de los activos que serán vinculados a los playbooks del SOAR	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la ubicación de toda la infraestructura tecnológica de la Entidad y que hace parte de este proyecto es en la ciudad de Bogotá en el datacenter principal.
285	Agradecemos confirmar si el hardware e infraestrcutura requerida sea virtual/física será proporcionada por DIAN	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
286	Agradecemos confirmar si la solcuión SOAR será administrada por el equipo DIAN o si se requiere un servicio adicional	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, el futuro contratista deberá administrar, operar, gestionar, configurar, mantener y realizar las demás actividades propias del día a día con el futuro SOAR de la Entidad, así mismo con los demás dispositivos, plataformas, soluciones y servicios adquiridos en este proyecto.

287	Agradecemos confirmar si para cumplir cada uno de los alcances del documento pueden ser ofrecidas multiples soluciones y no una sola por cada ITEM	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que para cumplir cada una de las capacidades requeridas en el anexo técnico de este proyecto, se debe entregar una solución por ítem.
288	agradecemos por favor aclarar segun el texto "Realizar levantamiento de información previo a la instalación de todas las soluciones y las plataformas entregadas. La entidad dispondrá de los recursos humanos suficientes y necesarios para apoyar las labores propias de esta contratación, previo acuerdo entre las partes." al hablar de levantamiento de información a que se hace referencia, dado que se entendia que la información relevante para la puesta en marca de las soluciones se entrega por parte de la DIAN	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que el levantamiento de información al que se hace referencia en el numeral 11.7 consiste en un proceso de recolección y análisis de datos específicos necesarios para la instalación, configuración y puesta en marcha de las soluciones. Este levantamiento incluirá detalles adicionales sobre los entornos de trabajo, configuraciones específicas y cualquier ajuste requerido para que las plataformas funcionen de manera óptima. Aunque la DIAN proporcionará información inicial relevante, el contratista deberá recopilar información específica en campo y en conjunto con el personal asignado por la DIAN, para afinar la implementación según las condiciones reales de los entornos de la entidad.
289	por favor segun el siguiente texto "Ubicaciones para implementación y configuración: El oferente deberá entregar todas las soluciones / equipos en los sitios/sedes indicados por la entidad." por favor indicar cuales son las posibles ubicaciones para el despliegue de la solución e caso de que sea requerido un despiegue a nivel de infraestructura	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, Ubicaciones para implementación y configuración: El oferente contará con un Centro de Operaciones de Seguridad SOC en la ciudad de Bogotá, donde se implementarán todos y cada uno de los servicios, dispositivos, plataformas, soluciones y demás productos que hagan parte de los requerimientos de la Entidad en este proyecto.
290	Referente al punto 12,4 "Controles: El servicio de SOC ofrecido debe contemplar también el monitoreo de los siguientes controles tecnológicos pertenecientes al SGSI de la Entidad:" solicitamos por favor dar un poco mas de contexto, segun el entendimiento se deben dimensionar adicional a los activos de infraestructura el listado indicado en este numeral?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, dentro del servicio de monitoreo que debe prestar el futuro contratista, debe contemplar el monitoreo del listado de controles de este punto.
291	agradecemos por favor confirmar segun el item 12,36 "El Proponente debe demostrar algún reconocimiento del centro de gestión de seguridad propuesto (SOC), acompañado de una carta por el representante legal que consta que el SOC que propone cumple con los estándares requeridos por la DIAN." cuales son los estandares requeridos por la organización para garantizar la prestación del servicio	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, los estándares a que se hace mención es al cumplimiento de todos y cada uno de los ítems solicitados en el anexo técnico, además de ser reconocido como un prestador de servicios SOC, tener capacidad instalada en Bogotá y contar con la respectiva experiencia.

292	Con la finalidad de realizar una estimacion mas aproximada a la realidad de la entidad, agradecemos por favor entregar la informacion de bases de datos de forma individual, en lugar de totalizada. Y por cada base de datos indicar: - Ubicación (On Premise o Cloud; indicar proveedor cloud en caso de aplicar) - Cluster o Standalone - Si es cluster indicar cantidad de servidores que conforman el cluster. - Cantidad de cores por cada Base de datos. - En caso de que existan bases de datos en la nube indicar cantidad de vCPU o vCores de cada una. - Motor de Base de Datos por cada Base de datos. - S.O. de cada servidor de Base de datos.	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, las características y cantidades de las bases de datos que hacen parte de este proyecto, pueden ser consultadas en el anexo técnico que hace parte de este proyecto.
293	Agradecemos a la entidada indicar a que hacen referencia con tendencias?. Esto debe ser un reporte o algun tipo de dahborad? Por favor entregar mas informacion al respecto.	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, esta característica hace referencia a reportes que muestran variables, tendencias, problemas, anomalias, comportamientos, entre otros.
294	Teniendo en cuenta que un esquema agentless en cualquier solucion de proteccion de bases de datos limita las capacidades a nivel de captura de eventos en tiempo real, visibilidad limitada exclusivamente a los logs de las bases de datos, monitoreo parcial de actividad privilegiada, entre otras. Agradecemos a la entidad confirmar que tienen total conocimento de esto y por lo tanto permitira la instalaccion de agentes para permitir tener una mayor visibilidad en las bases de datos?	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, la solución debe poder instalarse sin requerir agentes, la cual será la opción primordial, en el caso de que por temas de configuración o temas asociados a las características propias de las bases de datos se procederá a utilizar agente, aclarando que sería para casos excepcionales, procurando siempre contar con la opcion agentless.
295	Agradecemos a la entidad confirmar si en el item se requiere solamente que la solucion pueda trabajar en esquema agentless y mas no que este seria el esquema final de implementacion de la solucion. Ya que en caso de que este fuera este el esquema final de implementacion se entraria en conflicto con los item 4.40 al 4.44 en donde se solicita explicitamente el uso de agentes. Agradecemos dar claridad al respecto.	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, la solución debe poder instalarse sin requerir agentes, la cual será la opción primordial, en el caso de que por temas de configuración o temas asociados a las características propias de las bases de datos se procederá a utilizar agente, aclarando que sería para casos excepcionales, procurando siempre contar con la opcion agentless.

296	Agradecemos a la entidad entregar mas informacion sobre la solucion de parcheo virtual: - Cual es el alcance que debe tener la solucion? - La solucion puede ser parte de una solucion diferente a la de proteccion de base de datos? - Confirmar sobre cuales y cuantas bases de datos se debe aplicar el parcheo virtual - Cada cuanto se deben realizar las tareas de parcheo? - El parcheo se debe realizar sobre las bases de datos o tambien sobre el servidor quer las hospeda? Indicar S.O. y versiones de los servidores.	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, de acuerdo a sus inquietudes se permite hacer las siguientes precisiones: *Alcance: La solución debe contar con firmas de protección contra vulnerabilidades conocidas de bases de datos standar del mercado, que permitan mitigar el riesgo generado por estas vulnerabilidades. *La solución debe ser parte de la misma herramienta de protecci{on de bases de datos. *El parcheo virtual debe alicarse sobre todas las bases de datos en el alcance de la solución de protección de bases de datos. *El término parcheo virtual hace referencia a la aplicación de reglas de mitigación de vulnerabilidades y no a la aplicación de parches de software, por lo que no debe tener periodicidad y deben estar aplicadas desde el inicio del proyecto. *El parcheo virtual se debe ejecutar sobre las bases de datos más no sobre el servidor que las hospeda.
297	Agradecemos a la entidad por favor aterrizar un poco mas el alcance de la palabra "Granular", ya que este puede abarcar alcances muy amplios, por lo cual agradecemos ser mas especificos en las capacidades de reglas y politicas que se requieren.	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, la funcionalidad requerida es clara por cuanto la Entidad puede requerir manejar reglas y políticas amplias o especificas, detalladas a granulares de acuerdo a sus necesidades, y la plataforma o soluci{on debe permitirlo.
298	Agradecemos a la entidad indicar a que otras plataformas de administracion hacen referencia. Por favor indicar Fabricante y version actualo de esas herramientas	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, la característica solicitada en este ítem es agnóstica en cuanto a marca o fabricante, ya que el protocolo SNMP lo manejan la gran mayoría o todas las marcas.
299	Agradecemos indicar cuales y cuantas bases de datos MySQL tienen. Indicar cantidad de cores, ubicación, S.O.	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, las características y cantidades de las bases de datos que hacen parte de este proyecto, pueden ser consultadas en el anexo técnico que hace parte de este proyecto.

300	Es nuesto entendimiento que al solicitar el monitoreo de las bases de datos del item 4,39 l entidad cuenta con estas bases de datos en su infraestructura, sin embargo no vemos evidenciamos informacion de estas DBs en la documentacion "Cifras Infraestructura de TI". Agradecemos entregar la siguiente informacion por cada DB: - Ubicación (On Premise o Cloud; indicar proveedor cloud en caso de aplicar) - Cluster o Standalone - Si es cluster indicar cantidad de servidores que conforman el cluster. - Cantidad de cores por cada Base de datos. - Motor de Base de Datos por cada Base de datos. - S.O. de cada servidor de Base de datos.	La Dirección de Impuestos y Aduanas Nacionales – DIAN precisa al observante que, las características y cantidades de las bases de datos que hacen parte de este proyecto, pueden ser consultadas en el anexo técnico que hace parte de este proyecto.
301	Agradecemos a la entidad confirmar si en el item se requiere solamente que la solucion pueda trabajar en esquema de agente y mas no que este seria el esquema final de implementacion de la solucion. Ya que en caso de que este fuera este el esquema final de implementacion se entraria en conflicto con el item 4.8 en donde se solicita explicitamente el esquema de trabajo agentless. Agradecemos dar claridad al respecto.	La Dirección de Impuestos y Aduanas Nacionales – DIAN especifica al observante que, la solución debe poder instalarse sin requerir agentes, la cual será la opción primordial, en el caso de que por temas de configuración o temas asociados a las características propias de las bases de datos se procederá a utilizar agente, aclarando que sería para casos excepcionales, procurando siempre contar con la opcion agentless.
302	Es nuestro entendimiento que la entidad suministrara toda la infraestructura de virtualizacion, software y comunicaciones necesaria para el despliegue de la solucion. Es esto correcto?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
303	Es nuestro entendimiento que la entidad suministrara la infraestructura de Kubernetes en la nube requerida para la gestion de agentes para monitoreo de Bases de Datos Cloud, es esto correcto?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.

304	segun el ítem. "El oferente deberá ofrecer cinco (5) capacitaciones para cinco (5) ingenieros cada una, designados por la DIAN, con sus respectivos vouchers, dictadas en un centro de capacitación certificado por el fabricante de las soluciones, con una intensidad mínima de cuarenta (40) horas, en temas de SIEM, SOAR, y las demás soluciones, tecnologías y servicios adquiridos." se deben contemplar 5 capacitaciones para cada una de las soluciones que estan dentro del RFI?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, son cinco (5) capacitaciones en total, con voucher de certificación, basadas en los temas de SIEM, SOAR y las demas soluciones, tecnologías y servicios adquiridos.
305	si las certificaciones emitidas son el linea estas aplican para dar respuesta al punto anterior, dado que se habla de que deben ser dictadas en centros de capacitaciones certificados	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, deber ser en forma presencial en centros de capacitaciones certificados
306	por favor tener presente que para el caso de algunas plataformas estas ofrecen la solución como SaaS y no aplica EOL EOS	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, tal como lo indica el ítem es para las capacidades, plataformas, appliances, software donde aplique.
307	Debe ser en modalidad software como servicio. (SaaS), con capacidad de aprovisionamiento rapido y elasticidad automática de servicios. No se aceptan soluciones de codigo abierto o similares. debe integrarse con herramientas de vulnerabilidades tal como Trend Vision One, entre otras. Se solicita amablemente extender la necesidad o caso de uso de integración con Vision One y a que otras herramientas se hace referencia.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que la integración de esta y las otras herramientas, capacidades, servicios y plataformas que hacen parte de este proyecto, se debe hacer de acuerdo a lo solicitado en el anexo técnico, y como segunda medida de acuerdo a los requerimientos que puedan surgir durante la implementación, o las etapas de administración, soporte, garantía y soporte por el tiempo que dure el proyecto, dicha integración se hará también bajo demanda y de acuerdo a las posibilidades de cada solución, previo cumplimiento de todos y cada uno de los requerimientos del anexto técnico de este proyecto.
308	Se solicita amablemente confirmar si cuentan con recursos disponibles virtuales para el despliegue de sensores sobre los diferentes ambientes y datacenters. Por favor detallar recursos disponibles.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
309	Se solicita amablemente confirmar cantidad de señuelos, carnadas o servicios falsos se estiman dentro del requerimiento.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el alcance debe cubrir como mínimo las 120 vlans requeridas en el anexo técnico.

310	Se solicita amablemente confirmar sistemas operativos sobre los cuales se requieren señuelos	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, los sistemas operativos son windows y linux en sus multiples distribuciones.
311	Se solicira amablemente confirmar cuantas VLAN se tendrán para creación de señualos o carnadas.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el número de vlans es de 120.
312	Agradecemos por favor aclarar los activos a los cuales se les van a realizar el Ethical Hacking y sus cantidades, IP’s internas, IP’s externas. APP's WEB y su respectiva cantidad de funcionalidades por APP, cantidad de API's y su respectiva cantidad de endpoints por API. Adicional ¿Cuál es el crecimiento estimado anualmente?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que en relación con el Ethical HAcking se aclara que el objetivo de esta acción es la infraestructura indicada en el Inventario de dispositivos y elementos que hacen parte del Proyecto. Se aclara que la cantidad mínima de activos para el ejercicio es de cien (100)
313	Por favor confirmar si el alcance es solo para los activos críticos de la entidad	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que el alcance de los ejercicios de ethical hacking no se limita únicamente a los activos críticos de la entidad sino también a los que hacen parte del anexo de inventarios de éste proyecto. Aunque se priorizarán activos de relevancia en cada ejercicio, la selección de activos incluirá aquellos que la DIAN considere esenciales para evaluar la postura de seguridad de la infraestructura tecnológica en general. La determinación específica de los activos a incluir se hará en la fase de planeación de cada ejercicio, en conjunto con el contratista, de acuerdo con las necesidades de seguridad identificadas.
314	agradecemos por favor informar si es viable que la ubicación del SOC sea prestado desde otro pais	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante que, el futuro contratista debe tener capacidad instalada de SOC en la ciudad de Bogotá, la ubicacion y prestación del servicio del SOC debe ser desde esta ciudad en Colombia

315	Solicitamos por favor que se cuente con presencia regional en no menos de 3 paises por parte del oferente para garantizar la prestación del servicio	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el servicio del SOC deberá contar con mínimos dos (2) centros de datos geográficamente ubicados en diferentes lugares dentro de Bogotá D.C o uno de estos puede estar fuera de Bogotá, siendo este para contingencia o alta disponibilidad, aclarando que el datacenter principal de donde se prestará el servicio de SOC y las capacidades contratadas, debe encontrarse en la ciudad de Bogotá. El proponente debe especificar la cantidad de Centro de Datos de los que dispone para el SOC, su ubicación y el rol de cada uno de ellos, por lo tanto no se acepta su sugerencia.
316	Con respecto al NUMERAL 7. 3. Se debe licenciar como mínimo para 16000 dispositivos del literal, Especificaciones Técnicas NDR - Detección y respuesta en red e Inteligencia de amenazas, a) se agradece a la entidad indicar, ¿cuál es el throughput esperado en la solución?	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el ítem en mención es bien claro al indicar que se debe licenciar como mínimo para 17727 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 ningún momento se habla de un throughput en especifico.
317	Con respecto al NUMERAL 19.1.5 del documento, Anexo-Tecnico-Proyecto-SOC-DIAN 24042024 - Realizar el análisis Forense para incidentes críticos, y determinar el origen y el vector de inicio del incidente, a) Se solicita comedidamente a la entidad especificar la modalidad de servicio, Bolsa de hora, especialista dedicado o tiempo parcial y su correspondiente alcance.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, dentro de los requerimientos solicitados, el futuro contratista deberá realizar el análisis Forense para incidentes críticos, y determinar el origen y el vector de inicio del incidente como parte de su pull de servicios SOC, en ningún momento se habla de un servicio adicional o anexo a este proyecto, por lo cual se aclara que no está solicitando un servicio de horas prepagada. Todas las solicitudes deben ser bajo demanda y de acuerdo a las necesidades propias de la Entidad y de acuerdo a la presentación de problemas, inconvenientes o incidentes durante la ejecución del proyecto SOC.
318	Con respecto al NUMERAL 18.3 Se debe allegar como máximo tres (3) certificaciones de experiencia en la que conste que la empresa prestó los servicios de centro de operaciones de seguridad (SOC) o suministro de plataformas o dispositivos o tecnologías de información y comunicaciones como (Seguridad Informática, Firewalls, SANDBOX, SIEM), y/o implementó soluciones de (Seguridad informática), y/o en servicios de soporte técnico o tecnológico de soluciones o dispositivos de seguridad informática., a) Se solicita respetuosamente a la entidad la aceptación de certificaciones de experiencia en servicios de SOC que estén actualmente en ejecución. Estos servicios, al ser recientes, han sido contratados por períodos de 12, 24 o 36 meses, y su implementación está en curso. Es importante señalar que, dada la naturaleza dinámica y en constante evolución de los servicios de seguridad operativa, la experiencia acumulada durante la fase de ejecución es crucial para garantizar la eficacia	La Dirección de Impuestos y Aduanas Nacionales – DIAN agradece la solicitud y aclara que, conforme a lo establecido en el numeral 18.3 del Anexo Técnico, se aceptarán certificaciones de contratos de: centro de operaciones de seguridad (SOC) o suministro de plataformas o dispositivos o tecnologías de información y comunicaciones como (Seguridad Informática, Firewalls, SANDBOX, SIEM), y/o implementó soluciones de (Seguridad informática), y/o en servicios de soporte técnico o tecnológico de soluciones o dispositivos de seguridad informática actualmente en ejecución, siempre y cuando estas demuestren que la empresa ha prestado los servicios requeridos de manera continua y acorde con las especificaciones.
319	Con respecto al documento, Anexo-Tecnico-Proyecto-SOC-DIAN-24042024, se solicita comedidamente especificar la modalidad de pago a para una correcta la ejecución de contrato, luego los equipos se tienen tiempos específicos de pago, se sugiere un pago inicial contra entrega del 65% de los equipo o licencias y otro pago de 12% contra entrega a satisfactorio e instalación y un ultimo pago del 45% del servicio de SOC.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, se realizará un único pago al termino de la implementación más o menos a las 2 o tres meses contados desde el inicio del proyecto, previo cumplimiento de la entrega en producción de todos los servicios, plataformas, soluciones, y capacidades requeridas en el anexo técnico.

320	Por favor indicar para los costos finales los tipos de polizas que se solicitaran para la empresa contratista y si existen algun impuesto adicional a conciderar adicional al impuesto del IVA.?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, nos encontramos en una etapa de RFI por lo tanto, la información solicitada no es relevante para esta etapa, referente a los impuestos se debe considerar los impuestos mínimos cuando se contrata con una Entidad estatal.
321	Los varoles de las herramientas el valor unitario es por el valor de los 3 años?.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante, que pueden utilizar la columna unidad de medida para colocar Anualidad y la cantidad puede ser 3 para colocar el valor unitario por año y multiplicar esto por la cantidad.
322	Los valores de "Servicios de Monitoreo, Gestion Incidentes y operación" es el valor por los 36 meses de servicio?, es correcto el entendimiento?.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante, que se realizo el ajuste en el formato de propuesta economica, de acuerdo a los numerales del anexo tecnico, adicionalmente es por 3 años.
323	En los item 6, 7y 8 que se menciona que son servicios. Se idicaria el costo de los servicios por los 36 meses? Es correcto?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante, que se realizo el ajuste en el formato de propuesta economica, de acuerdo a los numerales del anexo tecnico, adicionalmente es por 3 años.
324	En los item 9 que se mencionaes el servicio de EH. Se daria el precio de los 6 ejercicios a realizar durante los 3 años?. Es correcto?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa al observante, que se realizo el ajuste en el formato de propuesta economica, de acuerdo a los numerales del anexo tecnico, adicionalmente es por 3 años. adicionalmente pueden utilizar la unidad de medida y cantidad para especificar cuantos ejercicios durante los 3 años.

325	Solicitamos amablemente la inclusión de experiencia relacionada con diversos aspectos de la seguridad de la información. Específicamente, consideramos fundamental que se reconozcan competencias en áreas como la protección de datos, gestión de riesgos, respuesta ante incidentes, auditoría de seguridad, cifrado de información, firewall, protección contra malware, y políticas de acceso y autenticación, así como la provisión de servicios integrales de ciberseguridad. Dada la creciente sofisticación y frecuencia de las amenazas cibernéticas, resulta esencial abarcar la identificación, monitoreo, análisis y mitigación de riesgos utilizando tecnologías avanzadas. Esto incluye la gestión de vulnerabilidades, configuración y cumplimiento normativo, detección de amenazas, respuesta a incidentes y análisis de la superficie de ataque. La inclusión de estas competencias garantiza una cobertura integral en la protección de la información y la ciberseguridad, alineándose con las mejores prácticas y normativas internacionales, lo que fortalecerá la capacidad de la entidad para enfrentar desafíos cibernéticos actuales y futuros. Es fundamental ampliar y diversificar la experiencia en cada una de las tecnologías mencionadas en los requisitos del anexo técnico, que destaca la necesidad de trabajar con herramientas calificadas, que exigen la implementación de soluciones tecnológicas avanzadas para asegurar una infraestructura robusta y adaptable a las amenazas actuales. Para cumplir con estas exigencias, no solo es necesario ampliar el espectro de tecnologías a utilizar, sino también adquirir experiencia práctica en proyectos previos con herramientas específicas, lo cual permitirá un enfoque más integral y eficiente. La capacidad de manejar múltiples tecnologías y adaptarse a las dinámicas de cada una es clave para asegurar una integración fluida de las diferentes soluciones, por eso es necesario abarcar la experiencia con diferentes proyectos, clientes y tecnología. Esta diversificación tecnológica es crítica para la consolidación de un Security Operation Center (SOC) robusto, que pueda responder de manera ágil y eficaz a las amenazas emergentes, así como gestionar de forma unificada las operaciones de seguridad. Por ello, se requiere un enfoque estratégico en la selección y uso de	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la experiencia y el conocimiento requerido por la Entidad para el futuro contratista, ya se encuentra estipulado en el anexo técnico junto con su alcance, por lo tanto, no se acepta su solicitud.
326	¿Cuál es el volumen de datos (logs) anual generado por los sistemas que deberán ser monitoreados?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el dimensionamiento del SIEM se encuentra estipulado en el anexo técnico, se requiere para 25000 EPS así como una retención en línea de tres (3) meses y fuera de línea de seis (6) meses.
327	¿Cuántos endpoints (dispositivos, servidores, estaciones de trabajo, móviles) están conectados y deben ser monitoreados por el SOC?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, las cantidades y detalles de la infraestructura tecnológica de la Entidad, se encuentran estipuladas en el anexo de inventarios de este proyecto, aclarando que toda la infraestructura tecnológica mencionada allì y que hace parte de este proyecto debe ser monitoreada.

328	¿Qué sistemas críticos (aplicaciones, bases de datos, servicios en la nube) necesitan estar bajo monitoreo constante?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, toda la infraestructura tecnológica de la Entidad que hace parte del anexo técnico y del inventario de este proyecto, debe ser monitoreada por el futuro contratista 7x24x365 de forma constante, no se diferencian unos de otros.
329	¿Cuántas ubicaciones físicas y virtuales (on-premises y en la nube) estarán bajo la supervisión del SOC?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, toda la infraestructura tecnológica de la Entidad que hace parte del anexo técnico y del inventario de este proyecto, debe ser monitoreada por el futuro contratista 7x24x365 de forma constante, dicha infraestructura se encuentra ubicada en el datacenter central de la DIAN, y en la nube de AZURE, el detalle de ubicaciones y demás los encuentran en el inventario anexo.
330	¿Cuál es el nivel de integración esperado entre los sistemas on-premises y los servicios en la nube que se están utilizando (Azure, AWS, etc.)?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la integración requerida se refiere a poder incluir toda la infraestructura tecnológica de la Entidad (onpremise, nube, entre otros) que se encuentra en el anexto técnico de este proyecto e integrarlos con los servicios contratados y entregados por el contratista, así mismo poder monitorearlos.
331	¿Se requiere que el SOC administre directamente la infraestructura existente o solo supervise los eventos y alertas?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, todos los productos, capacidades, plataformas, soluciones y servicios, requeridos por la Entidad y que se encuentran en el anexo técnico de este proyecto deberán ser gestionados, administrados por el futuro contratista, en ningún caso se solicita la administración de la infraestructura tecnológica de la Entidad.
332	¿Qué nivel de automatización desean implementar en el SOC, especialmente en términos de detección y respuesta automatizada a incidentes (SOAR)?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, los detalles de automatización y características del SOAR se encuentran en el anexo técnico de este proyecto.
333	Se solicita respetuosamente habilitar que para el despliegue de las soluciones tecnológicas incluya a Google como parte del despliegue y no solo en AWS y Azure. Esto en alineación con el numeral 6.5.9 que indica que la solución “Debe poder instalarse en infraestructura de nube pública de AWS, Azure y Google Cloud”.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el despliegue solicitado se requiere en las nubes donde tiene infraestructura la Entidad por ende se habla de Azure y AWS.
334	¿Cuál es el tiempo de respuesta esperado para los diferentes tipos de incidentes (SLA)? ¿Hay categorías críticas de incidentes que necesiten tiempos de respuesta más cortos?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que en el numeral 19.2.7 del anexo tecnico, se encuentra estos tiempos.

335	¿Cuál es la política de escalamiento para incidentes? ¿Se requiere soporte avanzado de terceros como Mandiant en incidentes críticos?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, los detalles de gestión de incidentes están consignado en el anexo técnico de este proceso, no se hace referencia a algún tercero en especial.
336	¿Cuál es la frecuencia de generación de reportes de ciberseguridad que el SOC deberá entregar?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que la generacion de reportes se debe realizar al menos una vez al mes o según por demanda la entidad lo requiere.
337	¿Existen expectativas de caza de amenazas más allá del monitoreo tradicional?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que en el item 6 del anexo tecnico, se encuentra especificado las caracteristicas requeridas para la capacidad de Caza de Amenazas.
338	¿Qué herramientas específicas esperan que el SOC implemente?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el futuro contratista debe entregar e implementar todos los productos, capacidades, plataformas, soluciones y servicios, requeridos por la Entidad y que se encuentran en el anexo técnico ítem 1 y que le permitan realizar todas las actividades solicitadas en este por la DIAN. Entendiendose que el contratista realizará toda la gestión, monitoreo, administración, acompañamiento, soporte y grarantía de los mismos, cobijando toda la infraestructura tecnológica de la Entidad. Para el efecto debe tener la capacidad de detectar, escalar, informar, acompañar apoyar y soportar a la DIAN en la resolución de cada uno de los incidentes encontrados por el futuro SOC durante el tiempo que dure el proyecto en mención. Los activos y demás características de estos se encuentran detallados en el apartado de inventarios y las especificaciones de cada una de las soluciones, plataformas, capacidades, servicios, soporte y garantía se encuentran en este anexo técnico de obligatorio cumplimiento.
339	¿Se requerirá un programa continuo de remediación o este será opcional después del primer año?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el futuro contratista debe apoyar con los recursos necesarios (personal ídoneo) constantemente a la Dian realizando el respectivo acompañamiento y apoyo con su 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.
340	¿Qué crecimiento proyectado tienen para los próximos años en cuanto a volumen de usuarios, dispositivos y nuevos sistemas que requerirán ser monitoreados por el SOC?	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el crecimiento proyectado está incluido dentro 17727 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web).

341	¿Planean incorporar nuevas tecnologías o plataformas que requieran adaptaciones del SOC en el futuro?	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el alcance y crecimiento del presente proyecto está demarcado para los 17727 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web).
342	Solicitamos amablemente a la entidad indicar cuales son los fabricantes de nube con los que actualmente se tiene infraestructura Cloud.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, los proveedores de nube con los que cuenta actualmente la Entidad son AZURE y AWS.
343	Solicitamos amablemente a entidad aclarar si en caso de requirise la implementación de la solución tipo SIEM en la nube donde se encuentran alojados los servicios de la entidad, los recursos de computo serán proporcionados para tal fin?	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
344	Solicitamos amablemente a la entidad aclarar si los recursos de computo para los sensores y/o colectores a desplegar para la arquitectura del servicio, tanto en on-premise, como en las nubes, serán asumidos por la entidad.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
345	Solicitamos amablemente a la entidad indicar cuanto es el tiempo estimado de rentención de logs en frío y caliente de la data almancenada, lo anterior con la finalidad de poder dimensionar el recurso de almanecamiento para la arquitectura de la solución.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el SIEM a adquirir debe manejar tasa de retención de tres (3) meses en línea y seis (6) meses fuera de línea.
346	Solicitamos amablemente a la entidad aclarar si los dispositivos mencionados en el punto 2.4 son los totales para la ejecución del proyecto por los 3 años, lo anterior, teniendo en cuenta que en el punto 2.35 solicitan que el licenciamiento sea escalable tanto por número de dispositivos como por eventos por segundo (EPS).	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la cantidad de dispositivos a licenciar para el SIEM se encuentra especifica en el ítem 2.4 y es de 2467 incluyendo crecimiento, se aclara que las características y demás requerimientos hechos en el ítem 2.35 no debe afectar o consumir licenciamiento del solicitado en el 2.4
347	"Solicitamos amablemente a la entidad aclarar si habrá algún stopper en la cantidad de licenciamiento por EPS requerido, lo anterior teniendo en cuenta que el licencimiento adquirido se costearía al inicio del proyecto y no en las fases de ejecución del mismo, posibilitando la inviabilidad económica del proyecto. Para lo cual se sugiere a la entidad realizar la estimación total de dispositivos y eventos por segundo (EPS) requeridos."	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la cantidad de EPS estipulada para este proyecto es de 25000.
348	Solicitamos amablemente a la entidad indicar si para la solución tipo SOAR la entidad otorgará los recursos de computo para la implementación de la máquina.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que,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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.

349	Solicitamos amablemente a la entidad nos pueda indicar la solución de monitoreo de bases de datos para cuantas transacciones por segundo requiere soportar, con este insumo se podra dimensionar la cantidad de throughput a soportar por la solución a ofertar y así mismo dimensionar la capacidad de computo.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, las variables a tener en cuenta para el dimensionamiento de la solución del monitoreo de bases de datos en este proyecto se encuentran en el inventario anexo, la cual es una informacióin amplia y suficiente para que los futuros proponentes puedan realizar sus estimaciones y costos.
350	Solicitamos amablemente a la entidad aclarar cuales de las bases de datos son en nube y cuales son en on-premise, de igual forma, solicitamos nos permitan conocer cuales son las capacidades de máquina virtual que se tienen en la nube para las bases de datos.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, las variables a tener en cuenta para el dimensionamiento de la solución del monitoreo de bases de datos en este proyecto se encuentran en el inventario anexo, la cual es una informacióin amplia y suficiente para que los futuros proponentes puedan realizar sus estimaciones y costos.
351	"Solicitamos amablemente a la entidad aclarar si dentro del licenciamiento de las 120 VLAN's cotempladas para el servicio de caza de amenazas, están incluidos los servicios en las nubes gestionadas por la entidad. En caso que no estén cotempladas, solicitamos amablemente nos aclaren la cantidad de sueñuelos o decoys requeridos para modelar el servicio."	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el alcance del licenciamiento es para 120 VLAN`S.
352	Solicitamos amablemente a la entidad aclarar la cantidad de dispositivos a licenciar con la solución tipo NDR, lo anterior teniendo en cuenta que en el ítem 7.18 habla de mil seiscientos (1600) dipositivos y para el ítem 7.3 habla de dieciséis mil (16000) dispositivos.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el alcance y crecimiento del presente proyecto está demarcado para los 17727 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web).
353	"Solicitamos amablemente a la entidad publicar el listado de activos a los cuales se les deberá realizar el ethical hacking teniendo en cuenta que no es lo mismo realizar un test a una aplicación que a un dispositivo de red, ejemplo de listado de activos a tener en cuenta para el ETH: - Servidor de aplicaciones web Windows IIS - 1 IP - Servidor de DNS Windows Server 2019 - 1 IP"	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que en relación con el Ethical HAcking se aclara que el objetivo de esta acción es la infraestructura indicada en el Inventario de dispositivos y elementos que hacen parte del Proyecto. Se aclara que la cantidad mínima de activos para el ejercicio es de cien (100)
354	"Solicitamos amablemente a la entidad no incluir para los perfiles de ethical hacking que se deban tener conocimiento en programación, teniendo en cuenta que este no es el area de experticia de un ingeniero que realiza pruebas de pentesting, sino especificamente certificado en ethical hacking. Por otra parte solicitamos amablemente que el oferente dimensione la cantidad ingenieros para realizar las pruebas de penetración, teniendo en cuenta que es un servicio bajo demanda semestral y no concurrente."	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, los detalles del ethical hacking se encuentran estipulados en el anexo técnico y obedecen a necesidades puntuales de la Entidad, por lo tanto no se aceptan sus observaciones al respecto.
355	Solicitamos amablemente a la entidad indicar cuales son los tiempo para la implementación de los servicios y a partir de que fecha se deberá empezar a operar con el servicio del SOC, lo anterior teniendo en cuenta que no se hablan de tiempos de ejecución.	La Dirección de Impuestos y Aduanas Nacionales – DIAN manifiesta al observante que, la duración del proyecto, en un principio se tiene contemplada para tres (3) años, pudiendo ser más, o menos según las disposiciones presupuestales y conveniencia de la Entidad, en el tema de la implementación se tienen contemplados tiempos de dos a tres meses como máximo para poner el proyecto a punto. Es de entender que el posible contratista debe contar con capacidad instalada y funcionando de un centro de operaciones de seguridad - SOC, por lo tanto la implementación de las capacidades requeridas por la Entidad en el anexo técnico, no demanda tiempos que se puedan considerar altos o extensivos en el tiempo

356	"Solicitamos amablemente a la entidad evaluar e incluir que en caso de uniones temporales o consorcios cada uno de los miembros deberá aportar las respectivas certificaciones de ISO27001 y pertenecer o ser miembro avalado de FIRST. (Incluyendo los ítems 12.76 y 12.78) Lo anterior con aras de garantizar que los proponentes que se presentan en unión temporal posean la experiencia y/o experticie en la calidad del objeto del proyecto, evitando figuras de posicionamiento en experiencia y/o tercerización."	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, en caso de ser uniones temporales, los integrantes de dicha unión deben ser certificados en ISO 27001 y deben ser miembros avalados de FIRST cada uno.
357	Solicitamos amablemente a la entidad evaluar y/o incluir que el oferente debera contar con certificaciones basadas en estándares internacionales, las cuales deberan ser vigentes al momento de la presentación, en servicios de las tecnologias de información y continuidad de negocio; lo anterior garantiza la experiencia del proponente en este tipo de proyectos y mejora la calidad técnica de los servicios a prestar.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el oferente debe además estar certificado en ISO 22301 Continuidad del Negocio.
358	"Solicitamos amablemente a la entidad evaluar e incluir dentro del perfil de gerente de servicio SOC lo siguiente, quedando de la siguiente forma: Un (01) Gerente de Servicio SOC: 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 de la Información. - Certificación en SCRUM Foundations - Certifiación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018 -Certificación vigente como arquitecto de seguridad de redes o analista de seguridad de redes o especialista en soluciones de seguridad de operaciones o su equivalente en la solución ofertada. Emitida por el fabricante. Certificaciones de experiencia mínima 5 años en implementación y/o soporte y/o administración de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional. Lo anterior garantiza que la persona que desarrollará este rol, posea los conocimientos en la operatividad del servicio a prestar y en metodologias agiles para la prestación del mismo."	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, para el ítem en cuestión se requiere lo siguiente: Un (01) Gerente de Servicio SOC: 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 de la Información. - Certificación en SCRUM Foundations o superior - Certificación AUDITOR INTERNO -Certificación vigente como arquitecto de seguridad de redes o analista de seguridad de redes o su equivalente en la soluciones ofertadas (SIEM, SOAR o Protección de Marca) emitida por el fabricante. Certificaciones de experiencia mínima 5 años en implementación y/o soporte y/o administración de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.

359	"Solicitamos amablemente a la entidad evaluar e incluir dentro del perfil de analista SOC nivel III lo siguiente, quedando de la siguiente forma: 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 o especialista en seguridad informática y/o de la información. -Certificación vigente como profesional y/o analista y/o arquitecto de seguridad de redes o su equivalente en la solución ofertada. Emitida por el fabricante. -Certificación en gestión o administración de plataformas de seguridad informática. - Certificaciones de experiencia mínima de 5 años en implementación y/o soporte y/o administración de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional. Lo anterior garantiza que la persona que desarrollará este rol, posea los conocimientos en la operatividad del servicio a prestar, con experencia y expertiz en la operación de servicios SOC."	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, para el ítem en cuestión se requiere lo siguiente: 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 o especialista en seguridad informática. -Certificación vigente como profesional, analista y/o arquitecto de seguridad de redes o su equivalente en las soluciones ofertadas (SIEM, SOAR o Protección de Marca) emitida por el fabricante. -Certificación en gestión o administración de plataformas de seguridad informática. Certificaciones de experiencia mínima de 5 años en implementación y/o soporte y/o administración de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.

360	"Solicitamos amablemente a la entidad evaluar e incluir dentro del perfil de analista SOC nivel II lo siguiente, quedando de la siguiente forma: Un (02) 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 profesional en operaciones de seguridad o profesional en seguridad de redes y especialista y/o arquitecto de seguridad en nube publica y/o especialista y/o arquitecto de seguridad en seguridad de redes o su equivalente en la solución ofertada. Emitida por el fabricante. - 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. La experiencia se cuenta a partir de la expedición de la tarjeta profesional. Lo anterior garantiza que la persona que desarrollará este rol, posea los conocimientos en la operatividad del servicio a prestar, con experencia y expertiz en la operación de servicios SOC y en nube pública."	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, para el ítem en cuestión se requiere lo siguiente: 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 profesional, analista, especialista y arquitecto de seguridad de redes o su equivalente en las soluciones ofertadas (SIEM, SOAR o Protección de Marca) emitida por el fabricante. - 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. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.

361	"Solicitamos amablemente a la entidad evaluar e incluir dentro del perfil de los analistas SOC nivel II lo siguiente, quedando de la siguiente forma: Dos (02) Analistas SOC Nivel I 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 profesional y/o especialista y/o arquitecto de seguridad de redes y/o operaciones de seguridad o su equivalente en la solución ofertada. Emitida por el fabricante. - Certificación en Plataformas Gestión de la Superficie de Ataque. - Certificaciones de experiencia mínima de dos (2) años en implementación y/o soporte y/o administración de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional. NOTA: Estos dos perfiles (analista I) deben cumplir los ANS de 7x24x365."	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, para el ítem en cuestión se requiere lo siguiente: Tres (03) Analistas SOC Nivel I 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 profesional, analista, especialista y arquitecto de seguridad de redes o su equivalente en las soluciones ofertadas (SIEM, SOAR o Protección de Marca) emitida por el fabricante. - Certificación en Plataformas Gestión de la Superficie de Ataque. - Certificaciones de experiencia mínima de dos (2) años en implementación y/o soporte y/o administración de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional. NOTA: Estos tres perfiles (analista I) deben cumplir los ANS de 7x24x365.
362	"Solicitamos amablemente a la entidad evaluar y/o modificar que para las soluciones de SIEM, SOAR, Protección de marca y Caza de amanezas se exija a los proponentes lo siguiente: Certificación de fabricante donde se evidencia que el proponenete cuenta con el máximo nivel de membresía en la solución ofertada, donde el oferente deberá ser especialista en al menos tres (03) categorias y donde una de estas corresponda a seguridad de operaciones. Esta membresía garantiza que el proveedor tiene las competencias técnicas más avanzadas y el acceso directo a recursos especializados del fabricante, lo cual redunda en la calidad del servicio, la actualización constante de las soluciones y la capacidad de respuesta oportuna ante cualquier eventualidad. El contar con este nivel de membresía asegura la alineación con los estándares internacionales de seguridad y permite la implementación eficiente de las soluciones ofertadas, protegiendo los intereses de la entidad. En caso de uniones temporales y/o consorcios todos los proponentes que conforman la UT deberán presentar las certificaciones del fabricante evidenciando el máximo nivel de membresia y las tres (03) especialidades	La Dirección de Impuestos y Aduanas Nacionales DIAN informa que no se acepta la sugerencia toda vez que lo definido en este punto obedece a las necesidades establecidas por le entidad
363	Solicitamos amablemente a la entidad no incluir nivel de membresia para las soluciones de protección de bases de datos y NDR - detección y respuesta en red e inteligencia de amanezas, lo anterior, teniendo en cuenta que para estas soluciones soluciones en especifico existen fabricantes que no cuentan con acreditaciones a nivel de canal y por lo tanto su esquema de venta no contempla membresias.	La Dirección de Impuestos y Aduanas Nacionales DIAN informa al observante que, se revisa su sugerencia y se ajusta el ítem.

364	"Solicitamos amablemente a la entidad permitir certificaciones de experencia de contratos en ejecución de servicios SOC, teniendo en cuenta que muchos de los proyectos ejecutados con entidades públicas y/o privadas son a 36 o 60 meses, siendo servicios con menos de 5 años en la industria colombiana. Lo anterior no impide que los proponentes cuenten con la experiencia técnica en la prestación del servicio y por otra parte mejora la participación de los oferentes."	La Dirección de Impuestos y Aduanas Nacionales – DIAN agradece la solicitud y aclara que, conforme a lo establecido en el numeral 18.3 del Anexo Técnico, se aceptarán certificaciones de contratos de: centro de operaciones de seguridad (SOC) o suministro de plataformas o dispositivos o tecnologías de información y comunicaciones como (Seguridad Informática, Firewalls, SANDBOX, SIEM), y/o implementó soluciones de (Seguridad informática), y/o en servicios de soporte técnico o tecnológico de soluciones o dispositivos de seguridad informática actualmente en ejecución, siempre y cuando estas demuestren que la empresa ha prestado los servicios requeridos de manera continua y acorde con las especificaciones.
365	Solicitamos amablemente a la entidad que el proponente pueda aportar máximo cinco (05) certificaciones de experiencia en servicios de centro de operaciones de seguridad (SOC) o suministro de plataformas o dispositivos o tecnologías de información y comunicaciones como (Seguridad Informática, Firewalls, SANDBOX, SIEM), y/o implementó soluciones de (Seguridad informática), y/o en servicios de soporte técnico o tecnológico de soluciones o dispositivos de seguridad informática.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa que se acoge la observación presentada lo cual se verá reflejado en el anexo técnico
366	Solicitamos amablemente a la entidad aclarar la totalidad del tiempo de los licenciemiento, plataformas y/o servicios requeridos, teniendo en cuenta que sobre los ítem 13 (Garantía y Soporte Técnico por tres (3) años) solicitan el licenciamiento por un tiempo determinado y en este apartado es de nuestro entendimiento que se requiere un año adicional a la entrega de los productos a la DIAN como parte de la devolución del servicio.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el tiempo total de servicios, soporte, garantia, gestion se debe prestar por 3 años.
367	Solicitamos amablemente a la entidad y con el entendimiento que los equipos y/o licencias quedaran a nombre de la misma, agradecemos nos aclaren la modalidad de pago para la ejecución del proyecto, teniendo en cuenta que las compras realizadas a los fabricantes se facturan en un tiempo especifico, sugerimos que se haga un primer pago del 60% contra entrega de equipos y/o licencias, un segundo pago 10% contra entrega a satisfacción e implementación de las plataformas y un último pago del 30% en el servicio de SOC.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, se realiza un pago del 100% al termino de implementacion y puesta en produccion de todas las capacidades, plataforma , soluciones, servicios y demas requerimientos contenidos en el anexo tecnico.
368	Solicitamos amablemente a la entidad aclarar si se requiere un perfil de consultor, teniendo en cuenta que el desarrollo del proyecto se llevara a cabo como una prestación de servicios. Lo anterior teniendo en cuenta que sobre el documento RFI-SOC-2024-v1 se detallan unas actividades que debe cumplir un consultor, sin embargo, solicitamos nos aclaren si estas actividades se deben cumplir por parte del gerente del proyecto o gerente de SOC. Es correcto nuestro entendimiento?	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, en el documento la palabra CONSULTOR hace referencia al mismo contratista.

369	Argadecemos a la entidad confirmar nuestro entendimiento, que todos los servicios asociados con la gestion de accesos e identidade,s gobierno de identidad y gestion de usuarios privilegiados, hace parte del proceso de Multinube hibrida y que no hace parte del prcoeso de Ciberseguridad objeto de este RFI	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, las capacidades y caracteristicas se encuentran en el anexo tecnico que se adjunto en el proceso de RFI
370	En el anexo 2 punto 11.6 se indica que la fase operativa es de 36 meses, agradecemos a la entidad indicar el tiempo estimado para la implementacion del servicio, y si el licenciamiento necesario para esa fase de implementacion esta contemplado en los 36 meses de soporte o si se debe considerar mas tiempo de licenciamiento para cubrir el periodo de implementacion	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el tiempo total de servicios, soporte, garantia, gestion se debe prestar por 3 años.
371	Agradecemos a la entidad indicar que servicios de los solicitados en este RFI se encuentran operativos y sobre cuales se debe hacer un proceso de migracion, tambien confirmar si la entidad pondra a dipsosicion a los equipos de operaciones de los servicios existentes con el objetivo de hacer los procesos de migracion de las soluciones actuales a las nuevas soluciones solicitadas en el RFI	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, los productos, servicios, plataformas y demás soluciones requeridas en el anexo técnico, son nuevos, por lo tanto, no es requerido realizar migraciones de plataformas antiguas, sin embargo, se especifica que se tiene que integrar y monitorear toda la plataforma tecnológica que se encuentra en el inventario anexo a este proyecto.
372	Agradecemos a la entidad confirmar nuestro entendimiento, que todas las funciones y procesos descritos en el grafico 2 - Modelo de operación hacen parte del alcance de este RFI	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que el grafico muestra las capacidades del SOC a contratar, sin embargo el detalle tecnico y todas las capacidades estan descritas en el anexo tecnico correspondiente.
373	Agradecemos a la entidad confirmar nuestra interpertacion con base en el anexo tecnico, que todo el licenciamiento debe ser adquirido a perpetuidad a excepcion de las herramientas que unicamente sean provistas en modelo suscripcion (servicios SaaS por ejemplo), y que tofdas las licencias deben quedar activas un año adicional a la finalizacion del contrato	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que en anexo tecnico, item 20.2, se encuentra detallado esta confirmacion
374	Agradcemos a la entidad indicar de forma explicita cuales son las normas y marcos legales que aplica actualmente a la DIAN, ademas indicar si sobre algun de estas normativas hay algun compromiso legal que implique alguna certificacion	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, las normativas a las que hace referencia este punto son las que debe cumplir todo contratista cuando vende o presta servicios a una empresa estatal.
375	Teniendo en cuenta que lo solicitado a nivel de implementaciones un cronograma generico, agradecemos a la entdiad confirmar nuestro entendimiento, que estos planes de choque no deben describirse uun y que haran parte de un entregable ya sea en etapa RFP o en planeacion para el contratista	La Dirección de Impuestos y Aduanas Nacionales – DIAN indica al observante que, en los casos donde se generen retrasos o contratiempos en el cronograma pactado, el contratista deberá generar planes de choque que le permitan adelantar las actividades atrasadas.
376	Agradcemos a la entidad confirmar nuestro entendimiento, que las capacidades de confidencialidad, integridad y privacidad de la informacion generaada a partis de los servicios de esta oferta, estaran delimitados por las capacicades y caracteristicas tecnologicas de las plataformas descritas en el anexo tecnico y no supone la integracion de soluciones complementarias para cifrado de informacion en reposo ni en movimiento	La Dirección de Impuestos y Aduanas Nacionales – DIAN indica al observante que, su entendimiento es correcto, sin embargo se aclara que todas y cada una de las características que hacen parte del anexo técnico son de obligatorio cumplimiento.

377	Agradecemos a la entidad indicar confirmar que, teniendo en cuenta que el proceso es solicitado para 36 meses, los valores de cada servicio se deben facturara en 36 mensualidades, por lo que la columna CANTIDAD deberia quedar en 36; en caso de ser incorrecta nuestra interpretacion, agradecemos a la entidad indicar la cantidad de pagos en los uqe se debe segmentar cada servicio	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, se realiza un pago del 100% al termino de implementacion y puesta en produccion de todas las capacidades, plataforma , soluciones, servicios y demas requerimientos contenidos en el anexo tecnico.
378	Agradecemos a la entidad indicar si todos los servicios de operación de cada una de las tecnologias solicitadas en el modelo economico deben englobarse en un solo gran valor dentro del item 11 (servicios de monitoreo, gestion de incidentes y operación)	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que se realizo la modificacion en el formato de Anexo Economico, de forma tal que no se deben englobar valores, se deben discriminar segun cada una de las capaciadades expresadas en el anexo tecnico.
379	Agradecemos a la entidad indicar si este crecimiento del 20% se debe incluir desde el inicio del contrato o si se debe considerar en algun punto de la operación, de ser asi agradecemos indicar en que momento la entidad espera disponibilidad de este crecimiento en licencias	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el crecimiento proyectado está incluido dentro de los 17727 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web). y debe ser puesto para uso de la Entidad desde el inicio del proyecto.
380	Agradecemos a la entidad indicar la estimacion del licenciamiento en funcion de EPS entendiendo que este servicio actualmente se encuentra operacional, esto con el fin de dimensionar las herramientas con todos sus numeros de parte	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la cantidad de EPS estipulada para este proyecto es de 25000.
381	Agradecemos a la entidad indicar si esta consigna aplica solo para el SIEM, o para todas las herramientas del servicio que sean virtuales, adicional indicar si el DRP para estas herramientas al quedar en el ambiente virtual de la entidad estaran cubiertas por los procesos internos de DRP de la DIAN	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, el ítem en cuestión presenta un error involuntario en su publicación por ende se procedió a su eliminación, además se aclara que, 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
382	Agradecemos a la entidad confirmar nuestro entendimiento, que no es necesario migrar los casos de uso de la herramienta actual a la nueva herramienta	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, no es necesario migrar casos de uso de la plataforma de SIEM actual.
383	Agradecemos a la entidad indicar las cantidades de de activios objeto de File Integrity Monitoring	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, dentro de las capacidades y características solicitadas para el SIEM este debe contar con la funcionalidad FIM.

384	Agradecemos a la entidad indicar si esta necesidad de integrar es debido a que se manejaran todosl os tickets con la herramietna de ITSM propiedad de la entidad, o si se debe incluir dentro del servicio una herramienta de ITSM	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la integración se debe hacer con la herramienta ITSM de la Entidad, que es del fabricante ARANDA.
385	Agradecemos a la entidad indicar la cantidad de licencias de agentes avanzados requeridos, asi como la cantidad de licencias de UEBA para comportamiento de identidades; adicional a esto indicar si el valor de estos paquetes debe ir implicito en el valor del item 1 de la propuesta de valores economicos, o si se debe agregar una linea adicional al anexo tecnico para indicar los valores base de los paquetes solicitados	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, los paquetes de licencias de agentes de UEBA solicitados en este ítem son para los servidores windows que tiene actualmente la Entidad, y su número y cantidades pueden ser consultados en el inventario anexo de este proceso.
386	Agradecemos a la entidad indciar la cantidad de aplicaciones web sobre las que se debe realizar la gestion de vulnerabilidades	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, son 260 aplicaciones web a monitorear por el servicio de gestión de vulnerabilidades.
387	Agradecemos a la entidad indicar si las 260 aplicaciones mencionadas son de diferntes dominios, o si se tratan de aplicaciones con subdominios de un mismo dominio, de ser asi agradecemos sea indicado la cantidad de dominios principales	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, las aplicaciones y sus características se encuentran detalladas en el anexo tecnico.
388	Agradecemos a la entidad indicar que solucion de Sandbox tiene, asi como la solucion de NAC y de EDR, toda vez que estos datos no se evidencian en el inventario adjunto	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el EDR de la Entidad es BITDEFENDER y el SANDBOX es BLACK HAT ARCHETYPE S.A.S/net-sn
389	Agradecemos a la entidad confirmar la cantidad de licencias, toda vez que en el punto 7.18 se mencionan 1.600 licencias para 3 años	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, se debe licenciar como mínimo para 17727 activos que incluyen (15000 pc´s, más 2467 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web).
390	Agradecemos a la entidad indicar si se pueden presentar modelos de licenciamiento alternativos que no sean basados en usuarios tales como throughput, esto teniendo en cuenta que la forma solicitada para la recoleccion de la data es por medio de span ports	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, los licenciamientos requeridos por la Entidad son basados en activos (15000 pc´s, más 1340 activos de infraestructura entre servidores, switches, routers, plataformas de virtualización, entre otros y 260 aplicaciones web), no se aceptan otros tipos de licenciamiento.
391	Agradecemos a la entidad confirmar nuestra interpretacion, que la solucion de NDR solicitada debe ser tipo hardware con un appliance en tierra desplegado en el DC del cliente, en caso que la interpretacion sea erronea agradecemos aclarar si se permiten soluciones basadaes en nube	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la solución NDR requerida es de tipo appliance de proposito especifico, la instalación de todos los servicios, productos, soluciones, plataformas, y demás capacidades requeridas en el anexo técnico deben ser instalados en el SOC del contratista.

392	Agradecemos a la entidad indicar el alance del apoyo solicitado, toda vez que mas alla de entregar recomendaciones acerca de los hallasgoz, quien realiza estos ajustes sobre el codigo son los desarrolladores, ya sean propios o tercerizados	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que el alcance del apoyo solicitado en el ítem 8.10 se refiere a la colaboración del contratista en la identificación y remediación de bugs o fallos de codificación en el software analizado. Aunque los desarrolladores, ya sean internos o tercerizados, son responsables de realizar los ajustes sobre el código, el contratista debe proporcionar recomendaciones claras y asesoría técnica para facilitar la remediación de los hallazgos. Este apoyo puede incluir la interpretación de los resultados del análisis y la validación de las soluciones propuestas, asegurando así que se sigan las buenas prácticas de desarrollo seguro establecidas por la DIAN.
393	Agradecemos a la entidad indicar la cantidad estimada de ejecicios de takedown que se podrian llegar a ralizar durante el servicio	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, como mínimo se pueden realizar cincuenta (50) takedown.
394	Agradecemos a la entidad indicar si este soporte y garantia debe ser contado desde el momento de habilitacion de las tecnologias para su implementacion y configuracion, o si debe ser contado desde el momento de entrada en operación	La Dirección de Impuestos y Aduanas Nacionales – DIAN, informa que el soporte y garantía de las tecnologías deberá contar a partir del momento de entrada en operación, es decir, una vez finalizada la implementación, configuración, pruebas y puesta en producción de las plataformas y soluciones adquiridas. Este esquema busca garantizar que el periodo de soporte cubra el tiempo en que las tecnologías están plenamente operativas y en uso por la entidad.
395	Agradecemos a la entidad confirmar nuestro entendimiento, que el monitoreo requerido en este item sera entregado a traves del modulo NOC solicitado para el SIEM en la oferta	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el monitoreo entregado debe ser a nivel de disponibilidad y seguridad.
396	Agradecemos a la entidad confirmar nuestro entendimiento, que al solicitar reconocimientos se hace referencia a certificaciones y/o membresias que respalden la experiencia del proponente, tales como certificacion ISO 20000, ISO 27000, membresia FIRST, etc	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, su entendimiento es correcto.
397	Agradecemos a la entidad confirmar nuestra interpertacion, que se requiere de recurso humano que genere los planes de remediacion según lo reportado por las herramientas de analisis de vulnerabilidade,s sin embargo, la ejecucion de estos planes estara a cargo de los administadores de los activos en cuestion y no del SOC	La Dirección de Impuestos y Aduanas Nacionales – DIAN confirma que es correcto interpretar que se requiere recurso humano dedicado a la generación de planes de remediación basados en los informes proporcionados por las herramientas de análisis de vulnerabilidades. Sin embargo, es importante aclarar que la ejecución de estos planes de remediación será responsabilidad de los administradores de los activos en cuestión y no del Centro de Operaciones de Seguridad (SOC).
398	Agradecemos a la entidad permitir la entrega de las hojas de vida para etapas posteriores como el RFP, esto teniendo en cuenta que con la oferta se debe entregar la carta firmada del representante legal del oferente garantizando que todos los puntos del anexo tecnico son cumplidos	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, para la presente etapa RFI no es necesaria la presentación de hojas de vida, ni certificaciones empresariales, se les recuerda que el anexo debe ser diligenciado en su totalidad, en los ìtems de modelos, fabricantes, cantidades se debe especificar el ofrecimiento.

399	Agradecemos a la entidad aclarar que el personal propio es el personal de operación de los servicios, esto devbido a que durante la implementacion de las tecnologias es posible requerir de especialistas de parte de las fabricas o de aliados especialistas que garanticen la idoneidad de la implementacion, lo que implica una tercerizacion de servicios	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, todo el personal del SOC requerido para la implementación, operación, gestión, monitoreo, soporte, grarantía, entre otros, deberá ser propio del canal o contratista 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.
400	Agradecemos a la entidad confirmar nuestro entendimiento, que se debe incluir adicional a los 3 años solicitados 1 año adicional de soporte	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el tiempo de ejecución para el presente proyecto es de tres (3) años.
401	Se solicita a la DIAN describir los activos a integrar dentro del servicio, por ejemplo: Numero de servidores y tipo de S.O, numero de firewalls y fabricante, nubes a integrar y fabricante, etc. Esto con el objeto de relizar un correcto dimensionamiento y validación que todas las fuentes sean integrables al servicio.	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, la información requerida en cuanto a características y cantidades de la infraestructura tecnológica de la Entidad, se encuentran en el inventario anexo que hace parte de este proyecto.
402	Por favor en el pliego incluir el tipo de activo y cantidad con el fin de cuantificar costos.	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, la información requerida en cuanto a características y cantidades de la infraestructura tecnológica de la Entidad, se encuentran en el inventario anexo que hace parte de este proyecto.
403	Se solicita a la DIAN informar el tiempo de almacenamiento en linea y fuera de Linea.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el SIEM a adquirir debe manejar tasa de retención de tres (3) meses en línea y seis (6) meses fuera de línea.
404	Se solicita a la DIAN informar el numero de sitios web donde se monitorearan las transacciones sinteticas	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, son 260 aplicaciones web a monitorear por el servicio de gestión de vulnerabilidades.
405	Se solicita la DIAN confirmar si el entendimiento es correcto, si es necesario deplegar alguna maquina vitual o servidor para disponer de la solución esta sera provista por la DIAN ?	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que,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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
406	Se solicita a la DIAN informar numero total de activos con los que cuenta la organización, incluidos, servdiores, estaciones de trabajo, equipos de red, soluciones de ciberseguridad, etc	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, la información requerida en cuanto a características y cantidades de la infraestructura tecnológica de la Entidad, se encuentran en el inventario anexo que hace parte de este proyecto.

407	Se solicita a la DIAN modificar el requerimiento de la siguinete forma: 2.21 · Permitir la creación de informes, que soporten una amplia gama de necesidades de auditoría y cumplimiento normativo, incluyendo: NIST, PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13 y SANS Critical Controls.	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, la funcionalidad requerida en este ítem obedece a necesidades de la Entidad, por lo tanto su modificación no es posible.
408	Las caracteristicas mencionadas en este punto hacen referencia a funcionalidades tipo FIM, este tipo de monitoreo por buenas practicas, se realiza unicamente sobre servidores criticos ya que puede generar un alto numero de falsos positivos, por tanto se solicita a la DIAN informar, si este monitorero se relizara sobre toda la infraestructura o se relizara sobre servidores criticos, de ser así informar la cantidad.	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, la característica solicitada se debe realizar sobre toda la infraestructura y acorde a la que permita o sea susceptible de llevar a cabo esta funcionalidad.
409	La solución SIEM descrita en el documento cuenta con funcionalidades, no propias de un sistema tipo SIEM, como lo son ASM (Attack surface management), File integrity Monitoring (FIM), Gestion de de inventario de activos (CMDB). Dado que estas NO son tecnologias nativas de un NG-SIEM se solicita a la DIAN informar si es posible participar con tecnologias diferentes a SIEM, que cumplen con las caracteristiacs de ASM, FIM y CMDB, esto teniendo en cuenta que en el numeral 11.17 se especifica que "Todas las plataformas y soluciones entregadas deberán ser de propósito específico, no se aceptan soluciones genéricas."	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, los futuros oferentes que deseen participar deben cumplicar todos y cada una de las especificaciones solicitadas en el anexo técnico que hace parte de este proyecto.
410	Con objeto de contar con pluraridad de oferentes y soluciones y en pro de que la herramienta este orientada a solucionar las necesidades de la entidad, se solicita a la DIAN modificar el requerimiento de la sigiente forma "La solución debe tener al menos playbooks que incluyan casos de uso que cubran la infraestructura tecnologica con la que cuenta la DIAN y los conectores necesarios para relizar las automatizaciones"	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, la característica requerida en este ítem obedece a necesidades y especificaciones de la Entidad, por lo tanto el ajuste solicitado no es posible.
411	Con objeto de contar con pluraridad de oferentes y soluciones y en pro de que la herramienta este orientada a solucionar las necesidades de la entidad, se solicita a la DIAN modificar el requerimiento de la sigiente forma "La solución debe tener al menos conectores suficientes para integrar al servicio el inventario de activos de la entidad"	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, la característica requerida en este ítem obedece a necesidades y especificaciones de la Entidad, por lo tanto el ajuste solicitado no es posible.
412	Para tener mayor pluralidad de fabricantes, se solicita a la DIAN cambiar el texto por: Monitorear toda la actividad de las bases de datos y registrar las transacciones SQL generadas por usuarios o aplicaciones, incluyendo comandos de gestión, modificación o control de datos.	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, la característica requerida en este ítem obedece a necesidades y especificaciones de la Entidad, por lo tanto el ajuste solicitado no es posible.
413	Se solicita a la DIAN informar si son equipos appliance se tiene el espacio de unidades disponible en sus rack de Centro de datos o si son equipos virtuales se tiene la capacidad de que la DIAN proporcione el ambiente virtual para poder instalar las Virtual Machine.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que,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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.

414	Se solicita a la DIAN se confirme en caso que el dispositivo sea físico disponga de un espacio disponible en sus rack de Centro de datos, o si son equipos virtuales se tenga la capacidad de un ambiente virtual para poder instalar las Virtual Machine.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que,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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
415	Se solicita a la DIAN proporcionar la cantidad de FQDN para el escaneo de aplicaciones.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la cantidad de aplicaciones a monitorear es de 260, tal como se indica en el ítem 5.10.1
416	Se solicita a la DIAN proporcionar el numero de cargas de trabajo en la nube, numero de identidades utilizadas en nube, cantidad de lineas de codigo, Cantidad de Equipos virtuales a utilizar.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, las cantidades de licenciamiento están estipuladas y su alcance llega a las 17727 licencias, donde están incluidos dispositivos, aplicaciones y todo aquello que consuma licencia, por lo tanto la información solicitada no es necesaria para que los futuros contratistas puedan realizar sus costeos.
417	Se solicita a la DIAN proporcionar si la unica forma de captura del tráfico de red sera por SPAN port o se requiere verificar si tambien requerira TAPs? Se solicita a la DIAN proporcionar la cantidad de Puertos I/O que se requieren que tenga el NDR, cantidad de conexiones maxima y la cantidad de Throughput solicitado?	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, la captura de tráfico se hará por SPAN port (port mirror) por de acuerdo a las características solicitadas.
418	Se solicita a la DIAN la consulta si es posible incluir no solo OPEN API, sino también API RESTFUL esto con el fin de garantizar una integración con los dispositivos para generar un mayor contexto.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, se incluye su sugerencia en el ítem en menci{on.
419	Se solicita a la DIAN la consulta si se puede exponer otros documentos de Gartner u otro consultor para poder evaluar este punto, ya que algunos cuadrantes no se encuentran actualizados por Gartner hace unos años.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, no es posible realizar el ajuste solicitado, ya que las características solicitadas en este punto se basan en las necesidades propias de la Entidad.
420	Se solicita a la DIAN informar cual es la plataforma de reporteria y SD-WAN con la que cuenta la entidad	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, debido a un error involuntario en la publicación el ítem quedó mal elaborado por lo tanto se procede a su eliminación.

421	Se solicita a la DIAN informar el tiempo minimo esperado para la implementación de las soluciones, entendiento que se relizaran cada una de las fases solicitadas	La Dirección de Impuestos y Aduanas Nacionales – DIAN manifiesta al observante que, la duración del proyecto, en un principio se tiene contemplada para tres (3) años, pudiendo ser más, o menos según las disposiciones presupuestales y conveniencia de la Entidad, en el tema de la implementación se tienen contemplados tiempos de dos a tres meses como máximo para poner el proyecto a punto. Es de entender que el posible contratista debe contar con capacidad instalada y funcionando de un centro de operaciones de seguridad - SOC, por lo tanto la implementación de las capacidades requeridas por la Entidad en el anexo técnico, no demanda tiempos que se puedan considerar altos o extensivos en el tiempo
422	Entendiendo que se suministraran todos los elementos necesarios para la prestación de los servicios, se solicita a la DIAN informar cual es el numero de datacenter´s con los que cuenta y el numero de sedes sobre los cuales se deplegaran las soluciones a ofertar, si es posible entregar digrama de distribución de activos.	La Dirección de Impuestos y Aduanas Nacionales – DIAN, aclara al observante que 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las actividades propias del presente proyecto.
423	Se solicita a la DIAN un espacio para realizar un Site Survey en el Datacenter o donde se pueda verificar lo requerido para la implementación.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, para las futuras etapas del presente proyecto se estudiará la viabilidad de realizar un site survey al datacenter principal de la Entidad, actividad que será comunicada con antelación, una vez sea positiva su inclusión.
424	Se solicita a la DIAN informar que tipo de tecnologia OTque tiene la organización, esto teniendo en cuenta que en el inventario no se menciona que tipo de infraestructura se debe cubrir en este ambito.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, se solicita que esta capacidad tenga la posibilidad de implementarse en activos OT, pero para esta etapa inicial del proyecto no se implementará.
425	Se solicita a la DIAN informar que plataforma ITSM de tickets usan.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, en la actualidad se utiliza Aranda.
426	Para contar con un referencial de la capacidad operativa a cubrir, se solicita a la DIAN informar la cantidad de tickets o atenciones generadas para este tipo de servicios en el ultimo año.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, los servicios de SOC que se quieren contratar en el presente proyecto son completamente nuevos, por lo tanto, no se tienen estadísticas anteriores de dichos servicios.

427	De forma respetuosa, se solicita a DIAN modificar el requerimiento de la siguiente manera: El servicio del SOC deberá contar con al menos dos (2) centros de datos geográficamente ubicados en diferentes ciudades, con al menos uno de ellos en la ciudad de Bogotá, siendo uno destinado para contingencia o alta disponibilidad' Este ajuste tiene en cuenta las mejores prácticas internacionales, como las indicadas en ANSI/TIA-942, donde se recomienda que los centros de datos estén lo suficientemente alejados para evitar que eventos como terremotos, inundaciones o cortes de energía afecten ambos sitios simultáneamente. "La norma ANSI/TIA-942-B es un estándar de calidad que define los requisitos de diseño de los centros de datos. Fue creada por el American National Standards Institute (ANSI) y el Telecommunications Industry Association (TIA)".	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el servicio del SOC deberá contar como mínimo con dos (2) centros de datos geográficamente ubicados en diferentes lugares dentro de Bogotá D.C o uno de estos puede estar fuera de Bogotá, siendo este para contingencia o alta disponibilidad, aclarando que el datacenter principal de donde se prestará el servicio de SOC y las capacidades contratadas, debe encontrarse en la ciudad de Bogotá. El proponente debe especificar la cantidad de Centro de Datos de los que dispone para el SOC, su ubicación y el rol de cada uno de ellos, por lo tanto no se acepta su sugerencia.
428	Se solicita a la DIAN informar si la atención de los requerimiento y seguimiento de los mismos se debe realizar mendiante la mesa de servicios de la DIAN o desde la mesa de servicios del oferente.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el futuro contratista del servicio SOC adquirido debe atender todos los eventos e incidentes presentados durante la operación y ejecución del presente proyecto, entendiendose que ademas se deben crear lla integración con la mesa de servicios propiedad de la Entidad.
429	Se solicicta a la DIAN informar si el entendimiento es correcto "la solución de gestión de vulnerabilidades debe contar con un modulo de parchado, para ejecutar parches desde la herramienta y sin hacer uso de otro sofware adicional"	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara que el entendimiento no es correcto. El numeral 13.17 establece que el contratista debe gestionar y remediar vulnerabilidades según lo reportado por la herramienta de gestión de vulnerabilidades, las características que se requieren para la herramienta de gestión de vulnerabilidades se especifican el punto 5 del anexo técnico.
430	Entendiendo que se suministrara capacitación en la gestión de las herramientas a personal de la DIAN, es posible entender que la gestión de las herramientas sera compartida? Recomendamos que esta gestión no sea compartida, con el fin de cumplir con los principios de segregación de roles y responsabilidades.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la gestion no es compartida, el futuro contratista debe realizar la administración, gestión y operación de todas las capacidades, plataformas, soluciones y servicios contratados en este proyecto.
431	Si la gestión de las herramientas será compartida, cual seria el esquema de operación esperado por la DIAN y como se garantizarian los SLA´s propuestos?	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, la gestion no es compartida, el futuro contratista debe realizar la administración, gestión y operación de todas las capacidades, plataformas, soluciones y servicios contratados en este proyecto.

432	Se solicita a la DIAN informar si el equipo minimo de trabajo es personal asignado dedicado a la DIAN o hace referencia al personal que prestará los servicios.	La Dirección de Impuestos y Aduanas Nacionales – DIAN informa al observante que, el equpo de trabajo solicitado es el personal que estará en toda la ejecución del proyecto.
433	De forma respetuosa se sugiere a la DIAN agregar en este ITEM que el oferente del servicio cuente certificacion SOC tipo 3 esto teniendo en cuenta que esta certificación se centra en controles críticos de seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad de la información. Estos controles son fundamentales y directamente relevantes para la operación segura y eficiente de un SOC de nueva generación, tal como lo requiere el alcance del contrato.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, los detalles de las certificaciones solicitadas se encuentran estipulados en el anexo técnico y obedecen a necesidades puntuales de la Entidad, por lo tanto no se aceptan sus observaciones al respecto.
434	Con el fin de contar con pluralidad de ofrentes y soluciones para participar, se solicita a DIAN ajustar el pliego de condiciones tecnicas para que el requerimiento sea: · Soporte de archivado de logs tanto para HDFS y/o NFS · Creación de políticas de retención de logs tanto por espacio como por periodos de tiempo.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, no es posible realizar el ajuste solicitado, ya que las características solicitadas en este punto se basan en las necesidades propias de la Entidad.
435	Se solicita a la DIAN aclarar el siguiente punto: En el numeral 2.11 mencionan que En caso de implementarse mediante máquina virtual, los recursos de computo serán entregados por la entidad, sin embargo en el numeral 11. 16 mencionan que 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. Por favor confirmar si la DIAN suministrara o no algun tipo de infraestructura.	La Dirección de Impuestos y Aduanas Nacionales – DIAN comunica al observante que, el ítem en cuestión presenta un error involuntario en su publicación por ende se procedió a su eliminación, además se aclara que, 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, entendiendose que es un contrato llave en mano, la Entidad no proporcionara ningún recurso requerido para realizar las futuras implementaciones.
436	Entendiendo las ncesidades y capacidades a nivel de monitoreo en en el anexo tecnico, Se suguire a la DIAN que en pliego de condiciones, se solicite que las solución SIEM a ofertar este incluida en el cuadrante de Gartner como lider, esto teniendo en cuenta que en esto dos rubros se considera la capacidad de ejecución y la visión integral. Estas herramientas son reconocidas por su capacidad para adaptarse a las tendencias emergentes y ofrecer un desempeño robusto.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, no es posible realizar el ajuste solicitado, ya que las características solicitadas en este punto se basan en las necesidades propias de la Entidad.
437	Se recomienda independizar el tema de FIM del SIEM por las siguientes razones: - Dada la importancia de la tecnologia del FIM para identificar posibles brechas de integridad en la informacion de la entidad, sugerimos que se considere una herramienta de seguridad especializada para cumplir esta caracteristica. · La organización podría contar con herramientas especializadas en FIM que ofrecen un nivel de detalle y	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el SIEM solicitado debe venir con características de FIM, por lo tanto, no se acepta su observación.

438	De forma respetuosa, se sugiere modificar el requerimiento de la certificación ITIL Foundation v3 o superior, para que sea opcional y no obligatoria, considerando que la certificación PMP ya incluye una gestión de proyectos sólida y abarca diversas disciplinas de TI y seguridad informática. Además, la certificación PMP es reconocida internacionalmente como una de las más robustas para la gestión de proyectos, lo cual garantiza que el Gerente de Proyecto propuesto posea las competencias necesarias para liderar exitosamente proyectos de TI y seguridad sin necesidad de una certificación adicional como ITIL.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, no es posible realizar el ajuste solicitado, ya que las características solicitadas en este punto se basan en las necesidades propias de la Entidad.
439	El requerimiento solicita mínimo dos (2) analistas, sin embargo, en la NOTA de éste ITEM se indica que estos dos perfiles (analista I) deben prestar el servicio 7X24 lo que implicaría turnos de 12 horas, por lo que se sugiere de forma respetuosa modificar el requerimiento mínimo ampliando a tres (3) el número de analistas para tener turnos de 8 horas.	La Dirección de Impuestos y Aduanas Nacionales – DIAN aclara al observante que, el item en cuestion se ajusta para que sean tres (3) analistas nivel I.