PROGRAMA DE APOYO A LA MODERNIZACIÓN DE LA DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES - DIAN

CONTRATO DE PRÉSTAMO BID 5148/OC-CO

SOLICITUD DE INFORMACIÓN (RFI)

SOC - MSSP

OCTUBRE DE 2024

Contenido

1. INTRODUCCIÓN

1.1 Objetivo y propósito

En el marco de la Modernización de la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales – DIAN, y de acuerdo con las necesidades de la Entidad, se hace relevante contar con un centro de operación en seguridad SOC - MSSP (Security Operation Center – Managed Security Service Provider) y los servicios de gestión de seguridad por parte de un proveedor, que permitan realizar el monitoreo, gestión de eventos e incidentes de seguridad de acuerdo al MSPI (Modelo de Seguridad y Privacidad de la Información) de MINTIC, cacería de amenazas, inteligencia de amenazas, automatización de servicios y otras capacidades asociadas para el ecosistema tecnológico (propio y de terceros) de la DIAN que soporta los procesos,. Basado en herramientas tecnológicas (hardware y software), técnicas, procesos y servicios de ciberinteligencia.

La Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales - DIAN está interesada en realizar un estudio de mercado con el fin de determinar la mejor alternativa de solución para el servicio de SOC-MSSP en las especificaciones y anexos plasmados en este documento, la DIAN envía a los interesados en participar en el eventual proceso de contratación, el siguiente documento de solicitud de información (RFI por sus siglas en inglés- Request for Information) para recibir documentación que facilite el análisis de las soluciones disponibles en el mercado para el monitoreo, gestión de eventos e incidentes de seguridad de la información, cacería de amenazas, inteligencia de amenazas, automatización de servicios y otras capacidades asociadas para el ecosistema tecnológico de la DIAN (propio y de terceros). Aunque se recomienda a los interesados en participar en el eventual proceso de contratación de la solución(es) que respondan a las preguntas de los capítulos incorporadas en este documento y en los anexos de este RFI con el mayor detalle posible, se aclara que las respuestas recibidas no tendrán ningún tipo de relación o vínculo con el proceso de contratación.

1.2 Cronograma

Las fechas previstas para la presentación del RFI son:

Actividad	Fecha
Publicación y lanzamiento del RFI	8 de octubre de 2024
Plazo para realizar preguntas y/o aclaraciones por parte del proveedor	15 de octubre de 2024
Plazo para responder preguntas y/o aclaraciones por parte de la DIAN	25 de octubre de 2024
Fecha y hora límite para envío de respuestas al RFI por parte de los proveedores	1 de noviembre de 2024 - 11:59 p.m.

La DIAN se reserva el derecho de analizar las respuestas de los interesados al RFI y de solicitar las aclaraciones que a su juicio se requieran.

1.3 Forma de presentación

El RFI se remitirá a través del correo electrónico *adquisiciones@fondodian.gov.co* que es gestionado por la Unidad de Coordinación del Programa de Apoyo a la Modernización de la DIAN, de tal manera que se centralice la información. Todas las interacciones entre la DIAN y los interesados en participar en este requerimiento se deben realizar utilizando el correo mencionado. No se aceptarán respuestas al RFI que se entreguen por un medio diferente o que se entreguen en papel en las dependencias de la DIAN.

Para efectos de cualquier comunicación, se debe relacionar el texto: Respuesta RFI-SOC 2024, la respuesta debe darse en idioma español, la documentación a remitir deberá ser en formato PDF y Word adjuntos al correo, sin que éste supere los 20MB.

2. ANTECEDENTES

La Dirección de Impuestos y Aduanas Nacionales es una Unidad Administrativa Especial del orden nacional, de carácter eminentemente técnico y especializado, con personería jurídica, autonomía administrativa y presupuestal y con patrimonio propio, adscrita al Ministerio de Hacienda y Crédito Público. Tiene a su cargo un servicio público esencial (parágrafo artículo 53 de la Ley 633 de 2000), su objetivo es coadyuvar a garantizar la seguridad fiscal del Estado colombiano y la protección del orden público económico nacional, mediante la administración y control al debido cumplimiento de las obligaciones tributarias, aduaneras y cambiarias, y la facilitación de las operaciones de comercio exterior en condiciones de equidad, transparencia y legalidad.

La Ley 1819 de 2016 facultó a la DIAN para adelantar un proceso de modernización y el Plan Nacional de Desarrollo 2018-2022 incluyó dentro de sus objetivos fortalecer la capacidad técnica e institucional de la DIAN, y en ese marco se ha estructurado el Programa de Apoyo a la Modernización de la DIAN que tiene el propósito de mejorar la eficacia y la eficiencia de la gestión tributaria y aduanera de la Entidad y así incrementar la recaudación del Gobierno Nacional.

En ese sentido, en junio de 2020 fue aprobado el Documento CONPES 3993 “Concepto favorable al patrimonio autónomo Fondo DIAN para Colombia para la contratación de operaciones de crédito con la Banca Multilateral (…) y declaración de importancia estratégica que la Nación proyecta realizar al Programa de Apoyo a la Modernización de la DIAN”. Dicho CONPES señala que en términos de modernización tecnológica, la DIAN ha adelantado esfuerzos para poner al día los sistemas de información y servicios digitales ante los cambios normativos; sin embargo, en los últimos 15 años no se ha realizado una renovación de sus soluciones frente a posibilidades que brindan actualmente las tecnologías digitales, además cuenta con deficiencias relacionadas con gobierno de datos, seguridad de la información, escalabilidad de las soluciones tecnológicas, baja adopción de tecnologías emergentes y estandarización de componentes tecnológicos, lo cual dificulta el desarrollo y despliegue de nuevas funcionalidades, incrementa costos por pagos de soportes a CONSULTORES exclusivos de tecnología, limita el escalamiento tanto vertical como horizontal, e incrementa los problemas de disponibilidad en el servicio.

El 24 de diciembre de 2020, el Fondo DIAN para Colombia y el Banco Interamericano de

Desarrollo (BID), suscribieron el Contrato de Préstamo BID 5148/OC-CO, con el objeto de contribuir a la financiación y ejecución de la primera operación de un programa multifase de Apoyo a la Modernización de la DIAN cuyo objetivo general es mejorar la eficacia y eficiencia de la gestión tributaria, aduanera y cambiaria de la DIAN y cuyos objetivos específicos se han orientado a:

1. Mejorar el modelo de gobernanza institucional para el fortalecimiento de la planificación estratégica y la estructura institucional y la actualización del modelo de gestión de talento humano.
2. Optimizar procesos de gestión tributaria, aduanera y cambiaria para el aumento de su eficiencia en términos de mayor recaudo y mejor gestión de riesgo.
3. Mejorar la eficiencia de la gestión tecnológica, los datos y la seguridad de la información para optimizar la toma de decisiones y proteger la información.

Para alcanzar los objetivos indicados, el Programa comprende tres componentes:

1. Organización Institucional y Recursos Humanos (RR.HH.).
2. Control y cumplimiento tributario, aduanero y cambiario.
3. Plataforma Tecnológica (PT), datos y seguridad de la información.

De acuerdo con lo anterior, y con el propósito de mejorar la experiencia de los usuarios, lograr una mayor digitalización de los servicios y adicionalmente facilitar el intercambio de información con diferentes actores, se hace necesario diseñar e implementar los siguientes componentes transversales:

- Plataforma Digital de Integración de Servicios, es un grupo de componentes transversales que permiten lograr una mayor digitalización de los servicios, mejorar la experiencia de los usuarios y facilitar el intercambio de información con los diferentes actores.
- Aplicaciones para la Gestión Corporativa, consiste en una plataforma tecnológica de procesos e información diseñada para facilitar y controlar de manera eficiente tres (3) procesos: i) gestión del talento humano; ii) gestión de asuntos disciplinarios; iii) gestión de logística e inventarios.
- Aplicaciones para la Gestión Tributaria, es una plataforma tecnológica de procesos e

información diseñada por la DIAN para facilitar y controlar de manera eficiente los procesos tributarios de recaudación de impuestos y derechos, control cambiario y fiscalización.

- Aplicaciones para la Gestión Aduanera, es una plataforma tecnológica de procesos e información diseñada por la DIAN en el que se pretende reflejar la visión de un ecosistema eficiente, en el que la DIAN sea el habilitador de condiciones propicias para robustecer la actividad económica, articulando los esfuerzos de los actores del comercio exterior en Colombia.
- Repositorio único de datos (Data-R), que permitirá contar con una sola fuente de datos e información que facilite la gestión y el aprovechamiento de estos en los distintos sistemas transaccionales, así como en los procesos analíticos.
- Seguridad, establecerá un marco conceptual y normativo de seguridad de la información que incluye: (I) preparación de diagnóstico de la situación actual, diseño de la situación futura y período de transición, y propuesta de un nuevo marco consistente con el PETI; (II) desarrollo de los manuales de política de seguridad; (III) implantación del marco incluyendo campañas de concientización; y (IV) difusión de los instrumentos de seguridad de la información y ciberseguridad.
- Multinube híbrida, servicio de nube híbrida (pública y privada basada en contenedores) para toda la Información Pública Reservada la plataforma de aplicaciones y servicios institucionales y para el Data-R, incluyendo almacenamiento, comunicación, seguridad, procesamiento de las aplicaciones, licencias de software, actualizaciones y soporte. Es importante mencionar que dentro del ecosistema de la DIAN se encuentran aplicativos, componentes de software, servicios, integraciones de la DIAN, desarrollados a la medida, otros de tipo COTS, SaaS, PaaS y open source desplegados en diferentes infraestructuras como OnPremises, nube pública (Azure o AWS) o nubes públicas de terceros y sirve a más de veinte millones (20.000.000) de usuarios tanto internos como externos que pueden tener acceso a estos componentes. Por lo anterior, la DIAN requiere una Solución de Identidades centralizada.

El presente documento se centra en la adquisición del diagnóstico, análisis, diseño, aprovisionamiento de tecnologías en alta disponibilidad, implementación, operación y mejora continua del Centro Operaciones de Seguridad (SOC) para la infraestructura on premises y nube en operación normal y en contingencia (DRP).

3. GENERALIDADES DEL SOC

3.1 Alcance

La DIAN requiere disponer de un Centro de Operaciones en Seguridad SOC (Security Operations Center) que permita realizar el monitoreo 7x24x365, gestión de eventos e incidentes de seguridad de acuerdo con el MSPI de MINTIC, cacería de amenazas, inteligencia de amenazas, automatización de servicios, para el ecosistema tecnológico (propio y de terceros) de la DIAN que soporta los procesos, basado en herramientas tecnológicas (hardware y software) y técnicas de ciber inteligencia.

Se deberá realizar el diagnostico, análisis, diseño, aprovisionamiento de tecnologías en alta disponibilidad, implementación, operación y mejora continua del Centro Operaciones de Seguridad (SOC) para la infraestructura on premises en operación normal, infraestructura en contingencia (DRP), e infraestructura en las nubes con que cuente la DIAN, resultado del programa “Apoyo a la Modernización de la DIAN”. En las fases de diseño, implementación y operación, deberá incluir las herramientas requeridas para cumplir con las necesidades de operación, aprovisionando lo necesario y contando con la asesoría de personal especializado en la materia.

3.2 Modelo General del SOC

Gráfico 1 Modelo de operación - SOC fuente OSI.

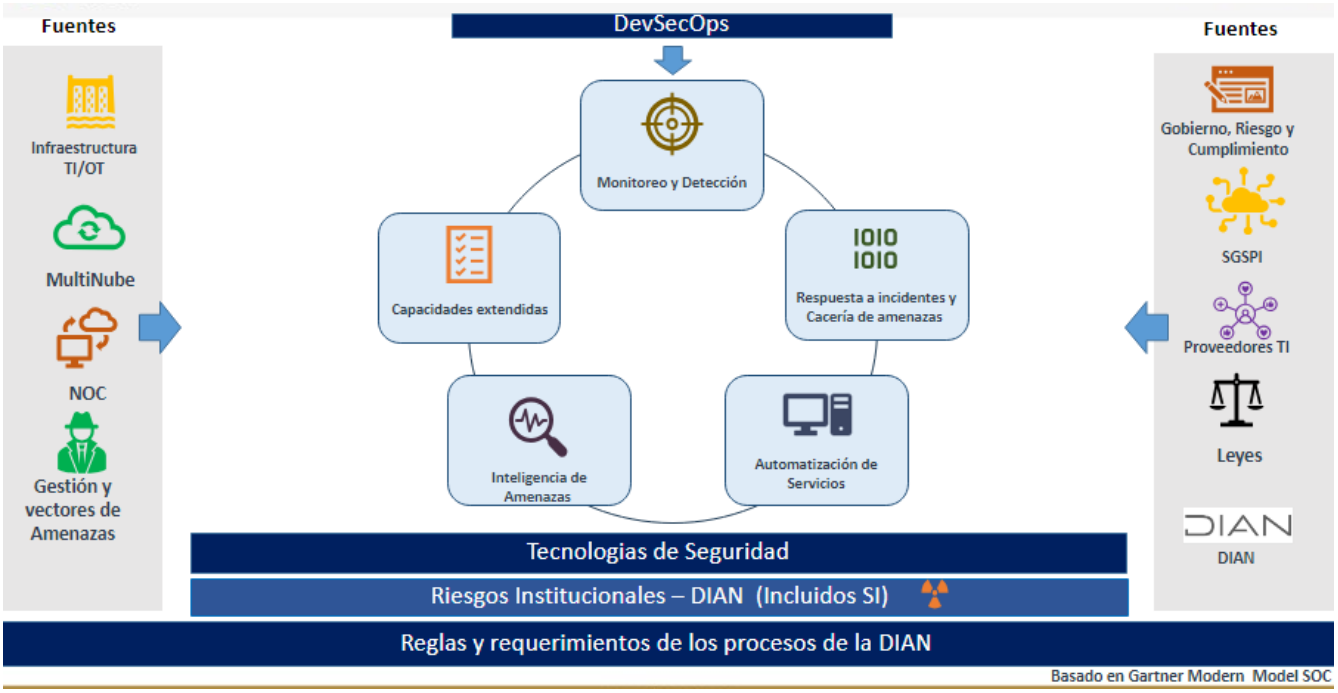
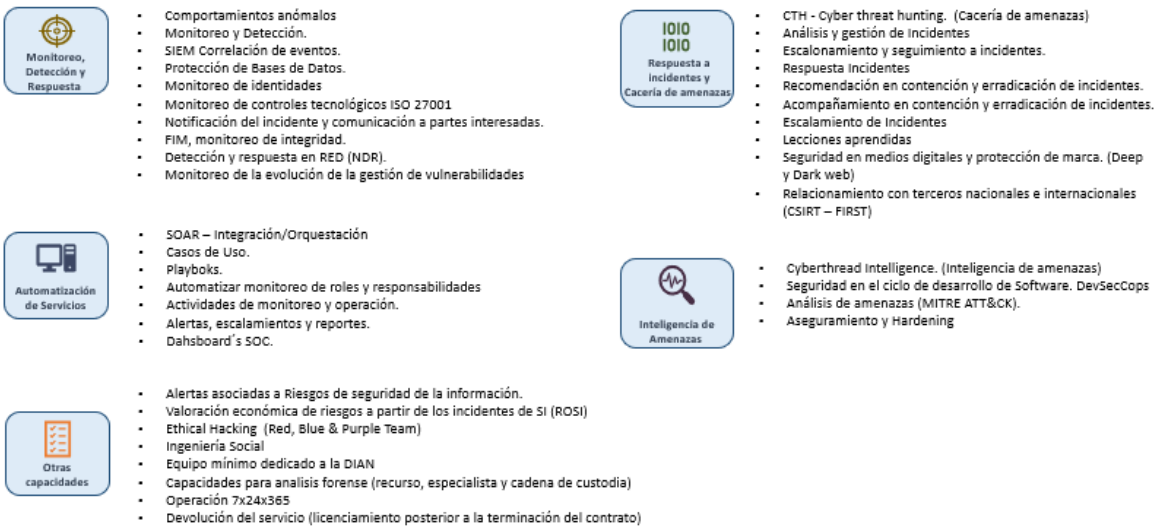


Gráfico 2 Modelo de operación - SOC fuente OSI.



3.3 Condiciones generales

El SOC debe incluir:

a. SIEM - Correlacionador de Eventos (Ver características en el Ítem 2).
b. SOAR - Orquestación, automatización y respuesta de seguridad) (Ver características en el Ítem 3).
c. Herramienta de protección de bases de datos (Ver características en el ítem 4).
d. Monitoreo a la Gestión de Vulnerabilidades (Ver características en el ítem 5).
e. Caza de amenazas (Ver características en el ítem 6).
f. NDR (Network Detection and Response) - Detección y respuesta en red e Inteligencia de amenazas (Ver características en el ítem 7).
g. Solución de análisis de código estático y dinámico para aplicaciones (Ver características en el ítem 8).
h. Protección de marca (Ver características en el ítem 9).
i. Ethical hacking (Ver características en el ítem 10).
j. Implementación de toda la plataforma y los dispositivos adquiridos (Ver características en el ítem 11).
k. Servicios de Monitoreo (Ver características en el ítem 12).
l. Garantía y Soporte técnico de tres (3) años (Ver características en el Ítem 13).
m. Capacitación (Ver características en el Ítem 14).
n. Transferencia de Conocimiento + lecciones aprendidas (Ver características en el Ítem 15).
o. Documentación (Ver características en el Ítem 16).
p. Equipo Mínimo de Trabajo (Ver características en el Ítem 17).
q. Certificaciones (Ver características en el Ítem 18).
r. Gestión de Incidentes (Ver características en el Ítem 19).
s. Devolución del servicio (Ver características en el Ítem 20).

El detalle de los servicios mencionados previamente se encuentra el en **Anexo 1. Anexo Técnico SOC.** Anexo Técnico Proyecto SOC DIAN 24 de Abril de 2024.xlsx

1. 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).
2. El CONSULTOR dispondrá para la prestación del SOC, el equipo humano, capacidades

técnicas y físicas, herramientas, metodologías y estructuras organizativas necesarias.

3. El CONSULTOR deberá manejar la gestión del contrato bajo una metodología de Gestión de Proyectos reconocida y con personal certificado en gestión de proyectos.
4. El CONSULTOR deberá generar planes de choque por fase. El(los) plan(es) de Choque deberá(n) contemplar las acciones, herramientas y recursos adicionales (humanos y técnicos) requeridas para poner al día el plan o el cronograma respectivo; en caso de aplicar, esta situación no generará sobrecostos al proyecto.
5. Todos los entregables que el CONSULTOR genere durante la prestación del servicio serán propiedad de la DIAN.
6. El CONSULTOR deberá aplicar y mantener protocolos de seguridad para preservar la confidencialidad, integridad, privacidad y disponibilidad de la información entregada y recibida por la DIAN.
7. El CONSULTOR deberá cumplir con la legislación vigente y las medidas de seguridad que permitan mantener la confidencialidad, secreto e integridad de los datos de carácter personal, privados, semiprivados o sensibles a los que tenga acceso.
8. El CONSULTOR deberá firmar los compromisos de confidencialidad requeridos por la DIAN, además asegurar los compromisos de confidencialidad con sus colaboradores participantes en el proyecto. La DIAN se reserva el derecho de solicitarlos.
9. El CONSULTOR deberá tener en cuenta para el desarrollo de los productos finales, la documentación normativa existente y futura, tales como; el Manual de Políticas y Lineamientos de Seguridad y Privacidad de la Información, Manual de protección de datos personales y demás normativa interna definida en la DIAN.
10. El CONSULTOR podrá realizar los trabajos de manera física (si requiere acceso a las instalaciones de la DIAN para realizar tareas específicas).
11. El CONSULTOR contará con sus instalaciones para la ubicación del personal que realice las tareas del SOC.
12. El CONSULTOR deberá generar al inicio del proyecto, actualizar (mínimo 2 veces al año) y suministrar una matriz de riesgos del proyecto asociados a situaciones que puedan afectar el cumplimiento de este.
13. El CONSULTOR deberá contar con las metodologías, procedimientos y demás herramientas de gestión propias (Project, Visio, herramientas de ofimática, entre otras) asociadas al proyecto para planificar, desarrollar, implementar y controlar las actividades necesarias para cumplir con los requisitos definidos por el presente documento y deberán ser presentadas a la OSI para su aprobación.

14. El CONSULTOR deberá elaborar y entregar una(s) metodología(s), herramienta(s) y métrica(s) que permita medir el servicio del SOC - MSSP.
15. El CONSULTOR deberá realizar la carga de todas las evidencias digitales generadas durante la ejecución del contrato, en el repositorio oficial de la Oficina de Seguridad de la Información (ruta que será suministrada oportunamente).
16. 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.
17. El CONSULTOR se responsabilizará durante la vigencia del contrato de la correcta gestión, operación, mantenimiento y actualización de los servicios requeridos, así como de la infraestructura, soluciones y herramientas que el diseño proponga para la prestación de estos.
18. 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.
19. Para la atención de los servicios, El CONSULTOR deberá trabajar en conjunto con el personal de la Dirección de Gestión de Innovación y Tecnología (DGIT) o quien haga sus veces.
20. El CONSULTOR deberá diseñar, implementar, medir y realizar acciones de mejora en la gestión del cambio de los temas asociados a las labores desarrolladas por el SOC, para lo que deberá generar un cronograma asociado a estos temas y contar con el equipo requerido.
21. El CONSULTOR deberá contar con un equipo mínimo de trabajo exclusivo asignado al SOC de acuerdo a lo requerido en el anexo técnico, este equipo se encargará de la gerencia, operación y relacionamiento entre el SOC y la DIAN; el CONSULTOR deberá organizarlo como esta consignado en el anexo técnico y deberá describir su conformación indicando como mínimo el rol, sus responsabilidades y tiempo asignado; esta estructura y modelo de operación deberá ser presentada a la DIAN para su aprobación y deberá mantenerse durante toda la ejecución del proyecto.

4. SOLICITUD DE INFORMACIÓN (RFI)

Por favor responda las siguientes preguntas.

4.1. Información del interesado

4.1.1. Nombre (razón social)_____

4.1.2. Identificación tributaria _____

4.1.3. Dirección/ciudad/país _____

4.1.4. ¿Ha implementado anteriormente la solución ofrecida? (Sí / No) _____

4.1.5. ¿Tiene oficinas o representación en Colombia? (Sí / No) ___

4.1.6. Información de la persona de contacto

- Nombre: _____
- Cargo: _____
- Teléfono: _____
- e-mail: _____

4.1.7. Describa las experiencias de implementación y operación de SOC ofrecida en el siguiente cuadro:

No.	Inicio (mes/año)	Fin (mes/año)	País/Estado	Descripción del proyecto	# de activos de información gestionados	% participación	Valor en USD	Adquisición de herramientas (SI/NO)	Servicios de Implementación SOC(SI/NO)	Servicios Operación SOC (SI/NO)

4.2. Información del SOC.

4.2.1. Ubicación Física
4.2.2. Que servicios o capacidades presta.
4.2.3. Disponibilidad de los servicios.
4.2.4. Distribución geográfica para la operación.
4.2.5. Cuántos sitios y dónde se encuentran ubicados.
4.2.6. Cuenta con contingencia o respaldo.
4.2.7. Cuenta con grupos de escalamiento a niveles de especialización y bases de conocimiento con las nuevas tendencias tecnológicas.
4.2.8. Estándares y Certificaciones: Indique los estándares que cumple y certificaciones con las que cuenta.
4.2.9. Describa de manera general como es su modelo operación SOC.
4.2.10. Indique sus herramientas tecnológicas para el SOC.

4.3. Información metodológica

4.3.1. Describa la metodología usada para diagnóstico, análisis, diseño, aprovisionamiento de tecnologías en alta disponibilidad, implementación, operación y mejora continua que ha llevado a cabo para este tipo de proyectos SOC.
4.3.2. ¿Ofrece un plan de capacitaciones y una estrategia de transferencia y gestión del conocimiento de un SOC para equipos internos de la DIAN y/o otro proveedor? Indique cuál es el modelo que utiliza y el alcance de esta.
4.3.3. Describa la estrategia de gestión del cambio a utilizar en la implementación y operación SOC.
4.3.4. Basado en su experiencia previa, ¿cuál es el cronograma típico y mapa de ruta de implementación de la solución (fases, hitos, duración) para un proyecto SOC de esta magnitud? (adjuntar un cronograma típico).
4.3.5. Maneja alguna metodología o procedimiento para llevar a cabo el análisis del ROSI?. (Return of Security Investment). ¿Cual?
4.3.6. ¿La solución o servicio proporciona un dashboard que muestre información o datos a nivel del ROSI en la entidad donde se ha implementado el SOC?
4.3.7. Tiene alguna herramienta o presta algún servicio que permita conocer el retorno sobre la inversión en seguridad de la información (ROSI).

4.3.8. Describa como dimensiona o tarifica la prestación de este servicio o como cuantifica el licenciamiento en caso de que sea una herramienta (ROSI).

4.3.9. Describa detalladamente las características técnicas especificas del servicio o la herramienta (software – hardware) que presta, así como consideraciones técnicas y de servicio para implementación, garantía y soporte técnico (ROSI).

4.3.10. Aparte del ROSI, el servicio o herramienta prestada permite conocer otra información relevante para la seguridad de la información de una Entidad como la DIAN (ROSI).

4.3.11. ¿Qué servicios vienen implícitos al contratar la implementación de este tipo de soluciones?

4.3.12. ¿Qué obligaciones deben cumplir ustedes como contratistas cuando prestan un servicio o entregan una herramienta para conocer el retorno sobre la inversión en seguridad de la información (ROSI)?

4.3.13. ¿Si dentro de las modalidades ofrecidas se encuentra licenciamiento de una herramienta en específico, este puede ser entregado a perpetuidad (ROSI)?

4.4. Modelo Costos

Indicar en el “Anexo 2. PropuestaValoresEconómicosSOC”, PropuestaValoresEconomicaSOC.xlsx los valores que permitan a la entidad tener un estimado del proyecto y el estimado del valor base para poder dimensionar la sostenibilidad.

4.5. Continuidad del servicio SOC.

Indique cuál va a ser la forma de pasar el servicio SOC a la entidad o a un nuevo proveedor del servicio, siempre pensando en la continuidad de la operación SOC y mitigando el riesgo de quedar desprotegidos en la transición de un contrato a otro.

5. ANEXOS

- ANEXO 1. Anexo Técnico Proyecto SOC DIAN 24 de Abril de 2024.xlsx
- ANEXO 2. PropuestaValoresEconomicaSOC.xlsx