Presidencia	**ESTUDIOS PREVIOS SELECCIÓN ABREVIADA POR SUBASTA INVERSA**

1. DESCRIPCIÓN Y JUSTIFICACIÓN DE LA NECESIDAD:

El Departamento Administrativo de la Presidencia de la República, de naturaleza especial, tiene por objeto asistir al Presidente de la República en su calidad de Jefe de Estado, Jefe de Gobierno y Suprema Autoridad Administrativa en el ejercicio de sus atribuciones constitucionales y legales, prestando, entre otras funciones, el apoyo logístico y administrativo que se demande para el ejercicio de las facultades y funciones presidenciales.

Son funciones generales del Departamento Administrativo de la Presidencia, según el artículo 4 del Decreto 2647 de 2022, entre otras, las señaladas en los numerales, *"(…) 1. Asistir al Presidente de la República, en su condición de Jefe del Estado, en su labor de coordinación de los diferentes órganos del Estado para que se colaboren armónicamente en la realización de sus objetivos. 2. Organizar, dirigir, coordinar y realizar las actividades necesarias que demande el Presidente de la República, para el ejercicio de las facultades constitucionales que le corresponde ejercer, en relación con los órganos del Estado que integran las ramas del poder público y los demás órganos estatales, autónomos e independientes. (…) 4. Organizar, asistir y coordinar las actividades necesarias que demande el Presidente de la República, para el ejercicio de las facultades constitucionales que le corresponde ejercer como Jefe del Estado y suprema autoridad administrativa. (…) 12. Prestar el apoyo logístico y administrativo que demande el ejercicio de las facultades y funciones presidenciales. (…)"*

Dentro de las funciones de la Oficina de Tecnologías y Sistemas de Información establecidas en el artículo 36 del Decreto 2647 de 2022, se encuentran, entre otras, las siguientes: *"(…) 1. Impartir los lineamientos en materia tecnológica para definir políticas, estrategias y prácticas que soporten la gestión del Sector. (…) 4. Aplicar los lineamientos y procesos de arquitectura tecnológica del Departamento Administrativo de la Presidencia de la República en materia de software, hardware, redes y telecomunicaciones, acorde con los parámetros gubernamentales para su adquisición, operación, soporte especializado y mantenimiento. 5. Asesorar al Departamento en la definición de los estándares de datos de los sistemas de información y de seguridad informática. (…) 12. Prestar el soporte técnico básico o de primer nivel a los usuarios internos del Departamento garantizando el adecuado funcionamiento de la infraestructura tecnológica base. (…)".*

La Oficina de Tecnologías y Sistemas de Información, tiene establecida la estrategia de *"Fortalecer los mecanismos que garantizan el correcto funcionamiento de las TIC con los cuales se soportan los procesos de la Entidad y se mantiene el Sistema de Gestión de Seguridad de la Información",* en razón de la cual se celebró el Contrato de Consultoría No. BID062-2022 con la firma MANAGEMENT AND QUALITY S.A.S., con el objeto de: *"Identificar la situación actual y formular el proceso de modernización Tecnológica para la Casa de Nariño de la Presidencia de la República, durante el periodo de Gobierno 2022-2026, así como establecer las acciones requeridas que permitan una Presidencia con altos estándares tecnológicos en el marco del Programa de Fortalecimiento de las Capacidades de Gestión Estratégica del Sector Público financiado con el préstamo BID 4848/OC-CO",* con plazo de ejecución hasta el 12 de mayo de 2023.

El alcance de la consultoría fue formular e implementar el mapa de ruta de transformación digital de la Presidencia de la República, durante el periodo de Gobierno 2022-2026, con el fin de alcanzar una Presidencia con altos estándares tecnológicos que impacte en la cercanía con las personas. Lo anterior, para establecer el proceso de transformación digital para la Presidencia de la República que permite fortalecer las capacidades de gestión y análisis de información para la toma de decisiones de manera informada y con tecnología de punta, reduciendo de esta forma la obsolescencia tecnológica y dando cumplimiento a las prioridades presidenciales.

En el marco del diagnóstico que arrojo la ejecución del contrato de consultaría No BID062-2022 con la firma MANAGEMENT AND QUALITY S.A.S, se identificó la necesidad de adquirir una herramienta de seguridad, orquestación, automatización y respuesta (SOAR) que permitan estandarizar las actividades de respuesta a incidentes de la Entidad, lo anterior, como un proceso de modernización y mejora tecnológica , a efectos de aumentar la eficiencia, la productividad y la compatibilidad, incluyendo actualización de hardware, software procesos, procedimientos y nuevas tecnologías.

Esta iniciativa busca adquirir y configurar una herramienta de seguridad, orquestación, automatización y respuesta (SOAR) que permitan estandarizar las actividades de respuesta a incidentes de la Entidad, agilizando su operación de manera correcta.

Actualmente, la Entidad está en proceso de madurar la postura de seguridad del DAPRE por lo cual se requiere de una herramienta que les ayude a automatizar la respuesta a incidentes de seguridad con el fin de evitar posibles ataques y/o minimizar el impacto ante la materialización de un posible riesgo de ciberseguridad.

Lo anterior, es indispensable por cuanto al adquirir y configurar una herramienta con estas características se da una solución auto-contenida e instalada en la Infraestructura del DAPRE, que permite integrarse con otras herramientas y soluciones mediante diferentes medios como los son: API, Correo electrónico, Syslog, etc, así como la posibilidad de tener un amplio conjunto de integraciones con otros sistemas ya desarrolladas (Fuentes de Threat Intelligence, MISP, etc) y librería de integraciones y automatizaciones con el equipamiento y/o software de los fabricantes más conocidos de la industria, entre otros.

La modernización tecnológica en este punto es fundamenta y esencial en el mundo actual en constante evolución y cambio, las organizaciones que no se adaptan y actualizan sus tecnologías, se arriesgan a quedar rezagadas en términos de competitividad y eficiencia.

En el informe y productos entregados en marco del contrato No. BID062-2022 suscrito con la firma MANAGEMENT AND QUALITY S.A.S se destacaron algunos aspectos importantes para la modernización tecnológica, en los que encontramos los siguientes:

1. Mayor eficiencia: La tecnología moderna permite realizar tareas más rápido y con mayor precisión, lo que lleva a mayor productividad y eficiencia.

2. Mejoras en la en la calidad: La tecnología adecuada permite realizar inspecciones más precisas de los productos y servicios, lo que conduce a mayor calidad y a la satisfacción del cliente.
3. Seguridad mejorada: La tecnología moderna ayuda a proteger la información crítica de las organizaciones y a prevenir el acceso no autorizado.
4. Reducción de costos: La modernización tecnológica reduce los costos, al contribuir en la automatización de procesos, reduciendo los tiempos de ejecución de tareas y mejorando la eficiencia general.

En conclusión, la modernización tecnológica puede ayudar a la Entidad a ser más eficaz y moderna, lo que se traduce en beneficios para los funcionarios, ciudadanos, terceros y en general para todos los actores que interactúan con la entidad.

Teniendo en cuenta el "Análisis del componente de seguridad" adelantado en ejecución del contrato de consultoría No. BID062-2022, en el cual se relaciona posibles servicios y herramientas de modernización con el objetivo de salvaguardar los componentes tecnológicos y velar por la integridad, disponibilidad y confidencialidad de la Entidad, se estableció la necesidad de adquirir y configurar una herramienta de seguridad, orquestación, automatización y respuesta (SOAR) que permitan estandarizar actividades de respuesta, coordinar herramientas de seguridad, automatizar tareas repetitivas y optimizar los flujos de trabajo de respuesta a incidentes y amenazas a incidentes de la Entidad, complementando los controles de seguridad que exige la norma ISO 27001:2002 para obtener su certificación, lo anterior, en virtud del análisis que arrojo la ejecución del contrato de interventoría mencionado, así como, las mesas técnicas de seguridad realizadas en la entidad.

Adicional a ello, esta herramienta aumenta la capacidad de respuesta ante ataques informáticos detectados en la plataforma tecnológica institucional, teniendo en cuenta las funcionalidades de automatización, agilizando tiempo que requiere restringir el análisis de todos los eventos de seguridad que producen las diferentes plataformas de seguridad que tiene la Entidad.

Acorde a lo anterior, el Departamento Administrativo de la Presidencia de la República – DAPRE requiere contratar un conjunto de herramientas de organización, automatización y respuesta a incidentes de seguridad (SOAR), garantizando su licenciamiento, soporte técnico, implementación, configuración y mantenimiento, en la infraestructura tecnológica del Departamento Administrativo de la Presidencia de la República, de conformidad con las especificaciones técnicas establecidas por la Entidad

Como conclusión la herramienta de SOAR busca agilizar de manera correcta la automatización de las tareas básicas de respuesta a incidentes, haciendo que sus analistas sean más eficientes y efectivos.

Puede indicarse que está contratación de la Entidad se encuentra contenida en el Plan Anual de Contratación, y que ya se cuenta con el CDP correspondiente para adelantar este proceso de contratación.

2. OBJETO A CONTRATAR:

Adquirir un conjunto de herramientas de organización, automatización y respuesta a incidentes de seguridad (SOAR), garantizando su licenciamiento, soporte técnico, implementación, configuración y mantenimiento, en la infraestructura tecnológica del departamento administrativo de la presidencia de la república.

3. FICHA TÉCNICA Y ESPECIFICACIONES TÉCNICAS

1. REQUERIMIENTOS GENERALES
Se requiere una solución SOAR para los siguientes casos de uso como mínimo: • Case Management • Phishing • Access Investigation • Malware
Debe ser una solución auto-contenida, instalada on-premise, la cual deberá integrarse con otras herramientas y soluciones mediante diferentes medios como son: API, Correo electrónico, Syslog
Debe contar con un amplio conjunto de integraciones con otros sistemas ya desarrolladas mínimo (Fuentes de Threat Intelligence, MISP).
Debe contar con una librería de integraciones y automatizaciones con el equipamiento y/o software de los fabricantes más conocidos de la industria.
La solución debe soportar investigaciones interactivas que permitan la colaboración, la revisión histórica y la documentación en tiempo real de todas las acciones.
La solución debe soportar flujos de trabajo y secuencias de comandos modulares
2. REQUERIMEINTO DE LA SOLUCIÓN
La herramienta de SOAR debe tener la flexibilidad suficiente para también orquestar y automatizar casos o requerimientos que se salgan de la ciberseguridad, y que agreguen valor a la operación de la organización
Debe ser una solución auto-contenida, con contenido instalado en la Infraestructura de DAPRE, la cual deberá integrarse con otras herramientas y soluciones mediante diferentes medios como mínimo: API, Correo electrónico, Syslog
Deberá ejecutar flujos de trabajo de forma programática o cuando se tengan nuevos indicadores reportados por las fuentes o feeds de threat intel

La solución de SOAR debe contar con una herramienta tipo marketplace/ecosystem con la cual se entreguen nuevos contenidos de forma periódica y frecuente.
Deberáer disponible un playbook debugger con el cual se puedan ejecutar los flujos de trabajo en modo de prueba antes que sean pasados a producción.
Contar con cifrado de las comunicaciones. Todas las comunicaciones entre los módulos de la solución son cifrados, inclusive si se utiliza estructuras de multitenant las comunicaciones entre el tenant principal y los subtenant son cifradas
Deberá crear nuevas integraciones y automatización desarrollando en Python, JavaScript y Powershell
Se deben entregar dashboards y reportes por defecto con la plataforma, además debe ser posible generar nuevos de forma intuitiva y sencilla
Deberá programar la generación y envió de reportes de forma automática
Deberá ejecutar los playbooks de forma programática, y/o cuando se reciban nuevos indicadores de compromiso de los feeds de threat intel
Deberá tener una pieza de Threat Intel Managment, en donde se tenga un feed nativo con la plataforma, y la posibilidad de integrar nuevos feeds de theat intel, pagos o abiertos
Deberá tener la posibilidad de alojar unos servicios de EDLs, con el cual se pueda compartir información de Threat Intel
Deberá contar con una interfaz gráfica para la creación de nuevos flujos de trabajo o playbooks, utilizando un método drag and drop.
Deberá con una herramienta tipo Playbook debugger, con la cual se puedan probar los nuevos flujos de trabajo desarrollados antes de ser pasados a producción
Tener un Playground en donde ejecutar comandos y/o playbooks sin afectar los casos, tickets, investigaciones o incidentes existentes.
Contar con una pieza de colaboración en tiempo real, en donde se pueda interactuar con otros analistas de la plataforma, además de poder ejecutar comandos y automatizaciones en tiempo real y bajo demanda, además de auto documentar todas las acciones tomadas ya sea de forma manual o automática en pro de responder al incidente
Deberá contar con automatizaciones que ayuden con la detección de incidentes similares, y las administraciones de lo encontrado
La herramienta debe contar con la posibilidad de cubrir por lo menos todas las tareas de nivel 1, la verificación de falsos positivos y duplicidades.
La solución de SOAR debe tener una pieza de administración de casos con la cual se puedan incluir nuevos casos, investigaciones, requerimientos, tickets e incidentes de forma automática mediante las integraciones, además de poder crear nuevos casos de forma manual, para que sean vinculados a un playbook y así su respuesta se realice de forma automática
Se debe poder crear nuevos tipos de incidentes y de indicadores, siendo estos objetos en la plataforma. Con lo cual personalizar y adaptar la orquestación y automatización a las necesidades de la organización.
Deberá generar Threat Intel Reports basados en los layouts que existen por defecto, además de poder crear nuevos layouts personalizados.

Poder crear y utilizar listas como parte de las automatizaciones o playbooks. Estas listas deben soportar Text, HTML, JSON, CSS y Marckdown.
Se debe tener el control granular sobre las integraciones, para limitar acceso a ciertas automatizaciones y comandos, dependiendo del Rol del analista.
La solución de SOAR debe contar con sub componentes que hagan las veces de Proxy para herramientas de terceros que se quieran hacer parte de la automatización y orquestación y no sean alcanzadas directamente por el servicio de SOAR.
Deberá crear nuevos scripts de automatización desde ceros, o basándose en los ya existentes. Se deben poder crear nuevos scripts en Python, JavaScript y Powershell
La solución debe permitir como mínimo la conexión de 5 usuarios concurrentes
La solución debe admitir integraciones bidireccionales y/o integradas, a través de API, capacidades push/pull, scripts o programación.
3. NECESIDADES PARA ANALISTAS
Automatización de procedimientos de respuesta a incidentes de forma parcial o total, pudiendo tomar acciones locales o en sistemas remotos.
Contar con herramientas de diseño de procedimientos de respuesta de forma gráfica y simple, disponibilidad todas las opciones por medio de ayudas contextuales.
Contar con una biblioteca de procedimientos de respuesta genéricos precargados y customizables.
Categorización de severidad de incidentes automatizada en base a información contextual.
Enriquecimiento del incidente agregando datos de diferentes fuentes, tanto propias (del mismo sistema) como de terceros.
Condicionar el acceso a la información contenida en los incidentes dependiendo del rol del usuario. Teniendo en cuenta que el propietario del incidente puede cambiar y por lo que el rol puede cambiar, el sistema deberá adaptar la información disponible para el nuevo propietario del incidente.
Disponibilidad de una interfaz que permita trabajar sobre los incidentes de forma colaborativa.
Relacionar incidentes en base a características similares.
Buscador de incidentes en base a cualquier característica de estos.
Mapeo de incidentes con diferentes frameworks (ejemplo: Mitre Attack).
Guiar al analista en la toma de decisiones, siguientes pasos y seguimiento de los procedimientos después de categorizar el incidente.
NECESIDADES DE GESTIÓN
Contar con Dashboards personalizables de acuerdo con el rol del usuario.
Contar con capacidad de reportería que permita realizar reportes automáticos y/o programados sobre cualquier conjunto de indicadores.
Definición de métricas en base a los datos disponibles en los incidentes.
Contar con la posibilidad de medir la eficiencia en la respuesta a incidentes, midiendo el tiempo que transcurre entre un conjunto de acciones dadas, tanto sean manuales como automáticas.
Gestión de pasaje de turno entre analistas.
Integración con otros sistemas de tickets o de gestión de incidentes (ejemplo: Service Desk, entre otros).
Generación de indicadores de compromiso en base a los incidentes generados en el sistema.

El sistema deberá ser capaz de ser operado a través de la interfaz web, CLI y API.
El sistema deberá ser capaz de agregar información a los incidentes mediante correo electrónico.
El sistema deberá tener la capacidad de depurar, exportar e importar los incidentes del sistema en base a un criterio dado, manteniendo opcionalmente los indicadores de compromiso asociados a este.
El sistema debe tener una interfaz de usuario (UI) intuitiva y fácil de usar.
Generar como mínimo los siguientes reportes mensuales: • Disponibilidad de los componentes monitoreados. • Eventos de seguridad que incluyan clasificación, estado, recomendaciones y acciones ejecutadas • Cantidad de incidencias remitidas, que incluyan estado actual y fechas estimadas de cierre Informe de análisis de riesgos y amenazas emergentes (tendencias, nuevos ataques, técnicas, entre otros).
La solución debe tener capacidades de generación de informes/inteligencia empresarial con la capacidad de utilizar informes basados en plantillas y crear informes personalizables.
4. NECESIDADES DE AUTOMATIZACIÓN
Generar incidentes en base a reglas de automatización del sistema.
Aplicar operaciones en dispositivos de terceros de forma manual o automática. Ejemplo: Aplicar una regla de bloqueo en un Firewall de un fabricante dado.
Contar con capacidad de desarrollo para integración con herramientas y soluciones de terceros.
Modificar incidentes en base a reglas de automatización.
El sistema debe servir como una gestión integral de eventos/incidentes/casos, automatización de respuesta a incidentes, plataforma de investigación, automatización de manual de estrategias y repositorio único de pruebas.
5. AUTOMATIZACIÓN
La herramienta de SOAR debe automatizar las tareas básicas de respuesta a incidentes, haciendo que sus analistas sean más eficientes y efectivos.
La plataforma debe soportar investigaciones interactivas que permitan colaboración, revisión histórica y ejecución en tiempo real y documentación de todas las acciones.
Para cualquier acción de seguridad, debe ofrecer flexibilidad para automatizar manualmente ejecutar en tiempo real según los requisitos del caso de uso.
La automatización se debe lograr utilizando flujos de trabajo modulares y scripts.
Las tareas automatizadas se deben visualizar en flujos de trabajo basados en interfaz gráfica y ser impulsadas por scripts de automatización en el backend.
Cualquier script puede ser adjunta una tarea automatizada dentro de flujos o playbooks visuales.
Los flujos de trabajo que la plataforma de SOAR utiliza para automatizar y ejecutar acciones deben ser compatible al menos con Python y JavaScript, debe tener la capacidad de exportar paquetes de Python a Dockers para que librerías de Python existentes puedan ser reutilizadas.
La solución debe incluir nuevas integraciones de productos y automatizaciones automáticas comparte de actualizaciones de contenido.
6. INTEGRACIONES

Herramientas SIEMs: Debe tener integraciones bidireccionales con APIs de SIEM terceros, la herramienta debe recolectar incidentes desde los SIEM, buscar alertas del SIEM durante una investigación y actualizar el SIEM de ser necesario. Debe integrarse con al menos 30 soluciones de SIEM o analítica de logs, entre ellos ArcSight, RSA Netwitness, IBM Qradar, Securonix, Exabeam, LogRythm, Splunk, JASK, ELK, McAfee ESM y AlienVault
Endpoint Security: Debe integrarse con soluciones de punto final, incluidas Forcepoint Symantec, Trend, FireEye, Crowdstrike, Cylance, Sentinel One, Cisco AMP, CybeReason y muchos más. Debe utilizar los APIs de las soluciones para hacer consultas en los productos, desencadenar nuevos incidentes, y activar acciones como parte de las acciones de respuesta (como por ejemplo aislar al punto final o matar procesos).
Seguridad de red: Debe integrarse con productos de seguridad de Red a través de API bidireccionales para realizar acciones de prevención tales como agregar reglas y desplegar IOCs. Los productos compatibles deben incluir marcas líderes del mercado como, Check Point, Forcepoint, Cisco, Palo Alto Networks, Fortinet y otros. Debe ofrecer la capacidad de agregar más productos de ser necesario.
Directorio Activo: Debe proveer todas las acciones permitidas por Directorio Activo vía API. Debe incluir consultar información acerca de usuarios, maquinas, contraseñas que expiran, control de afiliaciones a grupos, etc. Debe integrarse con servidores de email, permitiendo leer los buzones de correo entrante como enviar correos, actualizar usuarios, pedir aprobaciones, ejecutara tareas basadas en respuestas a correos, etc.
Threat Intelligence: Debe contar con más de 40 integraciones para enriquecimiento de datos e Inteligencia de amenazas, incluidas todas las principales plataformas de inteligencia de amenazas, incluidos AlienVault, AWS Sagemaker, Anomali, Cisco Umbrella, Palo Alto Networks Autofocus
Análisis de malware dinámico: Debe integrarse con productos relacionados con análisis de malware. Debe incluir Lastline, MISP, CrowdStrike, Trellix, Falcon Sandbox, Palo Alto Networks WildFire.
Análisis de Vulnerabilidades: Debe ser compatible con soluciones de assesment de vulnerabilidades como Nessus, Rapid7 y Qualys para proveer enriquecimiento de la información y para disparar acciones de parchado de vulnerabilidades. Debe incluir integraciones con herramientas de monitoreo de nube, como GuardDuty, AWS Security Hub, servicios de compliance como Palo Alto Networks Prisma, servicios de TI (S3, EC2), loggign (CloudTrail, CloudWatch) y otros.
La solución debe ser lo suficientemente flexible para permitir que las operaciones de seguridad creen fácilmente integraciones bidireccionales con productos de seguridad que no son compatibles de forma predeterminada
7. INDICADORES DE COMPROMISO
La Plataforma debe poder admitir formatos de código abierto estándar como OpenIOC, Yara, STIX 1.0, STIX 1.2, STIX 2.0, XML, CSV, JSON
La Plataforma debe tener la capacidad de mapear datos de origen al modelo interno de datos TIP y clasificar los datos con una combinación de valores de hash, incluidos MD5, SHA1, SHA256 y SHA512
La plataforma debe poder mapear los IOC que ingiere al TTP, y puede mapear el TTP a grupos APT para reducir a cero los grupos APT dirigidos a su organización.

La plataforma debe facilitar la atribución de amenazas con nombre: mapeo de TTP a actores de amenazas, grupos, y el marco de Mitre Att&ck
La plataforma debe poder admitir indicadores personalizados como IBAN, tarjetas de crédito, números de teléfonos celulares y números de identificación
La plataforma deberá recopilar indicadores de compromiso de muchas fuentes diferentes y deducir, según el valor de cada indicador, manteniendo el contexto de cada fuente.
Debe permitir al analista buscar indicadores en función de campos como etiquetas, estado o tipo de indicador para llevar a cabo acciones determinada o la plataforma debe automatizar la consolidación de la normalización tanto desde herramientas internas como externas para responder a los ataques en tiempo real
La plataforma debe realizar la des duplicación automática de indicadores
La plataforma debe admitir la inclusión de indicadores internos como IP y URL en la lista blanca, para garantizar que no sean marcados como maliciosos
8. FLUJOS O PLAYBOOK DE AUTOMATIZACIÓN
La herramienta debe contar con un mínimo de 100 casos de usos y playbooks de respuesta a incidentes
Los playbooks deben ser de código abierto y están alojados en GitHub o un repositorio público.
Debera permitir crear playbooks copiando flujos existentes, debe poseer una interface sencilla de utilizar que permita realizar drag-and-drop de acciones u otros flujos/playbooks
Debera permitir embeber un playbook dentro de otro, de forma de que este sea reutilizado continuamente
Un playbook puede contener acciones totalmente automatizadas o tareas manuales, tareas de collection de datos o tareas condicionadas
Los playbooks pueden ser ejecutadas automáticamente al crear un incidente y asociando al playbook correspondiente
Los playbooks deben poder ser ejecutados como tareas y también ejecutados en tiempo real
La ejecución de los playbooks y la actividad relacionada por el analista debe ser automáticamente documentada para cada incidente de seguridad
La herramienta debe de tener la capacidad de ejecutar flujos/playbooks en modo debug, de tal forma que permita observar la ejecución paso a paso del mismo y resolver cualquier inconveniente de ser necesario
Las acciones de los playbooks deben ser totalmente personalizables por el usuario y deben poder utilizarse para adherirse a cualquier requisito de proceso organizacional o industrial.
Deberá poseer la capacidad de asignar a cualquiera de los usuarios disponibles en el sistema basado en las capacidades RBAC.
La herramienta debe tener un API capaz de ejecutar las mismas funciones que la interfaz gráfica
9. GESTIÓN DE INCIDENTE
La herramienta debe soportar la asignación de tickets a usuarios o equipos de trabajo a través de roles de capacidad. Los incidentes pueden ser asignados a un equipo a través de un rol de grupo.
La herramienta debe estandarizar o escalar la administración de SLAs
Deberá manejar campos obligatorios a ser llenados antes de cerrar un incidente de seguridad

Deberá enviar notificaciones mediante herramientas de integración de mensajes tales como Okta, Slack y correos sobre cambios en incidentes changes, alertas sla, etc.
La notificación debe poder enviarse como parte de los pasos del playbook. O la herramienta debe poder enviar recordatorios para las tareas mientras se crea el playbook. Debe poder fijar SLA y usuario mientras se crea el playbook o Los incidentes pueden ser generados usando fetch trigger en cualquiera de los productos integrados o usando un modelo de push mediante Rest API, adicionalmente también pueden ser creados manualmente.
Deberá ofrecer una visión optimizada de cómo se relacionan los ataques en el tiempo, personalizar esa visión para adecuarse a su línea de trabajo, y codificar sus perspectivas para abordar de una mejor manera incidentes similares en el futuro.
Deberá poseer la capacidad de asignar tags o características personalizables a los incidentes, estas características deberán poder utilizarse para distintos usos, entre ellos medir KPIs, medir estadísticas, ejecutar atomizaciones basadas en ellas, etc.
La solución debe permitir la delegación de tareas a otro usuario y asignar SLAs
10.DOCUMENTACIÓN
La herramienta debe incluir una instancia donde usuarios puedan ver evidencia y documentación de incidentes anteriores, la herramienta debe agregar información de investigaciones pasadas
Deberá incluir un ambiente de Real-Time collaboration donde los incidentes se auto-documenten, ofreciendo una vista detallada de registros basada en una línea de tiempo con cada actividad realizada durante la investigación de un incidente
La herramienta debe detectar alertas redundantes y agregar incidentes duplicados en uno solo, desplegando los datos de la agregación realizada
Como parte de un incidente, la herramienta debe documentar cualquier cambio, los analistas parte del incidente, tareas terminadas, comandos de interacción, evidencia, chats, notas y tareas de playblooks
Los usuarios pueden marcar resultados de comandos o notas como evidencia, o automatizar la recolección de evidencia dentro de un playbook.
Toda la información recolectada debe ser inmutable y no debe ser modificada, la documentación debe ser exportable para producir un documento de cadena de custodia
Los analistas deben poder ver todos los indicadores de compromiso y el detalle alrededor de ellos deben poder asociados a las distintas fases del ataque o kill chain
Los analistas deben ser capaces de utilizar campos customizados para por ejemplo atribuir indicadores a campañas de ataque
Entregar la documentación de la implementación de la solución indicando la cantidad total de dispositivos, la cantidad total de subredes y el ancho de banda de los medios procesados.
Entregar el reporte de dispositivos tipo TOP, donde se indiquen condiciones de alta prioridad afectadas o vulneradas
11.MACHING LEARNING
La solución debe incluir aprendizaje dinámico de los IOCs e incidentes que se investigan y ayudar a los analistas a identificar incidentes que pueden estar relacionados
La solución debe ser capaz de sugerir próximos pasos de acuerdo con el aprendizaje de máquina realizado durante investigaciones previas.

Debe ser capaz de aprender qué analistas son contactados usualmente por tipo de incidente y puede sugerir a los nuevos analistas a quien ellos pueden querer contactar para recibir ayuda.
La solución debe tener integración con varias herramientas de enriquecimiento como Whois, VirusTotal, DomainTools y MISP. Debe tener una integración completa de la plataforma de inteligencia de amenazas lista para usar
12.SEGURIDAD DE LA APLICACIÓN
La solución debe admitir autenticación LDAP o cuentas de usuarios locales.
La solución debe admitir un conjunto de permisos de usuario granular y grupos de AD, o definiciones de roles personalizadas. El control de acceso granular debe admitirse para ejecutar comandos de integración para herramientas de seguridad de terceros.
13.ASPECTOS GENERALES
La solución propuesta deberá ser implementada in-situ (on premises en el DataCenter de EL CLIENTE), donde la empresa proveedora se encargue de suministrar la instalación e implementación del producto ofrecido; así como la documentación y entrenamiento necesario para los siguientes perfiles: administradores, usuarios avanzados y analistas, contemplando todos los requerimientos y licenciamiento de la solución.
En el caso de que la solución requiera el uso de servicios externos, se deberá especificar qué información se requiere transferir.
Se busca que el proveedor contemple y especifique todos los requerimientos técnicos necesarios para el funcionamiento óptimo de la solución (sistema operativo, base de datos, licencias, hardware/máquinas virtuales, networking). Así como la posibilidad de una instalación en alta disponibilidad y describir las capacidades de escalamiento de la solución.
La solución debe poder ser instalada en alta disponibilidad en cada uno de sus componentes sin la necesidad de que se requieran de licenciamientos externos de balanceadores y de replicación de datos.
La solución en su arquitectura debe ser implementada en alta disponibilidad en cada data center sin que incurra en problemas de latencia y licenciamiento.
Se deberá especificar el esfuerzo en cantidad de horas tanto del proveedor como de los técnicos de EL CLIENTE para la implementación y puesta en funcionamiento de la solución parametrizada, lista para utilizar.
Se deberá incluir dos niveles de capacitación, uno para la administración y gestión de la solución y otro para los analistas. El equipo de EL CLIENTE deberá ser capaz de formar a terceros en el uso de esta, en caso de ser necesario. Los cursos y todos los materiales utilizados deberán estar disponibles para ser utilizados en cualquier momento por EL CLIENTE durante la duración de la licencia de la solución.
Se deberá especificar cuáles son los diferentes esquemas de soporte y mantenimiento que puede utilizar la solución, de qué forma se accede al mismo y si es requerida alguna suscripción recurrente para la utilización de misma.
El CONTRATISTA deberá incluir servicio de implementación y soporte 7x24 por 3 años

El CONTRATISTATA deberá garantizar un banco de 70 horas x año para para cubrir desarrollo de nuevos conectores, nuevas implementaciones, afinamientos y asesoría
TIEMPOS DE RESPUESTA DE SOPORTE Y GARANTÍA
En caso de que un fallo supere 48 horas, el contratista debe proveer de manera temporal los componentes necesarios para que la solución continúe su operación.
Se debe prestar el servicio de soporte con las siguientes características: • Tiempo de Respuesta a Solicitudes**:** Se debe dar atención a las solicitudes en las ciudades donde están instaladas las herramientas de máximo cuatro (4) horas, de manera presencial o remota. • Tiempo Máximo de Diagnóstico: Se debe dar diagnóstico a las solicitudes efectuadas en un tiempo no mayor a ocho (8) horas. • Tiempo Máximo de Solución: Se debe establecer un plan de solución al supervisor del contrato y establecer un tiempo de solución no mayor a cuarenta y ocho (48) horas, en caso de requerirse mayor tiempo, deberá ser documentado y justificado ante el supervisor del contrato. Para la ejecución de la solución deberá cumplir con los procedimientos establecidos por la Entidad.
REQUERIMIENTOS DE MANTENIMIENTO
Se debe realizar mínimo dos (2) mantenimientos anuales preventivos de la plataforma (Hardware y software) durante la garantía, que deberá garantizarse por tres (3) anos. Los mantenimientos correctivos se realizarán cuando se presenten incidentes de funcionamiento de la plataforma de la Entidad tales como: Fallas técnicas, daños, degradaciones de desempeño o mal funcionamiento de las herramientas.
El contratista o fabricantes deberán realizar la actualización de versiones de software y firmware disponibles para las versiones inicialmente instaladas y el acompañamiento en la estabilización de la solución, para lo cual deberá presentar un plan de actualización a realizar en una ventana de mantenimiento a convenir con el supervisor del contrato.
En el mantenimiento, el contratista debe verificar el correcto funcionamiento de la plataforma (Hardware y software) de la Entidad, y si es el caso deberá planear, programar y realizar los ajustes en la configuración de estas herramientas, con el fin de mantener un correcto funcionamiento de acuerdo con las recomendaciones y buenas prácticas establecidas por el fabricante.
En el mantenimiento, el contratista debe revisar el consumo de recursos sobre la plataforma (Hardware y software) de la Entidad.
En el mantenimiento, el contratista debe revisar los agentes instalados que permiten la recolección de la información desde las herramientas.
En el mantenimiento, el contratista debe verificar el funcionamiento del registro de los LOGS, generación de alarmas de la plataforma (Hardware y software) de la Entidad.
Después de cada visita de mantenimiento, el contratista debe entregar un informe donde se describan cada una de las actividades realizadas
En el mantenimiento, el contratista debe generar recomendaciones orientadas a optimizar el funcionamiento de la plataforma (Hardware y software) de la Entidad.
ANS

El contratista deberá cumplir con las siguientes características del servicio y acuerdos de nivel de servicio ANS para LA ENTIDAD:

- Disponer de un buzón para reportar casos de soporte a través de correo electrónico.
- Disponer de una herramienta de tickets o ITSM que permita realizar el seguimiento de los casos y el cumplimiento de los ANS. Este servicio deberá ser atendido mínimo por un especialista (con personal calificado y certificado por el fabricante).
- El contratista o fabricante deberá realizar el registro de los casos de soporte y realizar el seguimiento de los casos abiertos o escalados
- Deberá cumplir con unos tiempos de atención estimados como:

Nivel escalamiento Caso Urgente		
Niveles de Escalamientos y Tiempos Nivel de Escalamiento	**Notificación**	**Escalamiento**
Ingeniero Nivel 1	15 minutos	30 minutos
Ingeniero Senior Nivel 2	30 minutos	30 minutos

Nivel escalamiento Caso Medio		
Niveles de Escalamientos y Tiempos Caso Medio	**Notificación**	**Escalamiento**
Ingeniero Nivel 1	15 minutos	40 minutos
Ingeniero Senior Nivel 2	40 minutos	80 minutos

Nivel escalamiento Caso Bajo		
Niveles de Escalamientos y Tiempos Caso Bajo	**Notificación**	**Escalamiento**
Ingeniero Nivel 1	15 minutos	60 minutos
Ingeniero Senior Nivel 2	45 minutos	120 minutos

Niveles de servicio que debe cumplir el fabricante y tiempo de reacción:

TIEMPO DE RESPUESTA INICIAL	
Soporte Online **Soporte telefónico**	7x24x365
Severidad 1- Critica El producto está caído, lo que afecta críticamente la producción del ambiente de la Entidad. Aún no hay ninguna solución disponible.	Menor o igual a 1 hora
Severidad 2- Alta El producto está deteriorado. Entorno de producción de la Entidad este arriba, pero impactado. Aún no hay solución disponible.	Menor o igual a 2 horas
Severidad 3- Media Una función del producto ha fallado, la producción del ambiente de la Entidad no se ha afectado. El soporte es consciente del problema. Y hay una solución disponible.	Menor o igual a 4 horas
Severidad 4- Baja Problema no crítico. No afecta el ambiente de producción de la Entidad. Característica, información, documentación, procedimientos y solicitudes de mejora para la Entidad.	Menor o igual a 8 horas

EL CONTRATISTA, deberá atender las solicitudes de mantenimiento en los tiempos de respuesta establecidos en los ANS, so pena de ser aplicadas las sanciones establecidas en las normas que rigen la materia, en caso de no cumplimiento de los parámetros de servicios ofrecidos y determinados en los Acuerdo de Nivel de Servicios (ANS).

IMPLEMENTACIÓN
EL CONTRATISTA deberá incluir la siguiente información: Deberá tener un cronograma aproximado de implementación con tareas generales y la duración de estas para que la entidad tenga este conocimiento. Deberá adjuntar la matriz de riesgo asociada al proyecto. Deberá adjuntar un cuadro con los documentos entregables de la implementación, incluyendo: una descripción breve de cada uno, que criterio se usará para su aceptación, el procedimiento de aceptación y el responsable

4. OBLIGACIONES DE LAS PARTES

4.1. OBLIGACIONES GENERALES DEL CONTRATISTA

1. Cumplir con sus obligaciones frente al Sistema de Seguridad Social Integral, Parafiscales (Cajas de Compensación Familiar, Sena e ICBF), y demás obligaciones a que haya lugar, de acuerdo con la normatividad vigente al respecto. El incumplimiento de esta obligación será causal para que **LA ENTIDAD** inicie el procedimiento sancionatorio a que haya lugar.

2. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones que puedan presentarse y en general se obliga a cumplir con lo establecido en las Leyes 80 de 1993, 1150 de 2007 y sus decretos reglamentarios.

3. No acceder a peticiones o amenazas de quienes actúen por fuera de la ley, con el fin de obligarlo a hacer u omitir algún acto o hecho, informando inmediatamente al Departamento Administrativo de la Presidencia de la República, y demás autoridades competentes cuando se presenten tales peticiones o amenazas**.**

4. Mantener y garantizar la debida confidencialidad respecto de la información y documentación que llegare a conocer, tener acceso o bajo su control durante la vigencia del contrato.

5. Responder por sus actuaciones y omisiones derivadas de la celebración del contrato, y de la ejecución del mismo, de conformidad con lo establecido en la Leyes 80 de 1993, 1150 de 2007 y sus decretos reglamentarios.

6. Mantener actualizado su domicilio durante la vigencia del contrato y seis (6) meses más.

7. Satisfacer las demás obligaciones a su cargo que se deriven de la naturaleza del contrato y aquellas otras que el funcionario designado por **LA ENTIDAD** para ejercer el control de ejecución del contrato, pueda determinar en cumplimiento del objeto contractual. **PARÁGRAFO: EL CONTRATISTA** declara y garantiza que la responsabilidad contractual ante **LA ENTIDAD** por el cumplimiento de las obligaciones establecidas, recae exclusivamente en su cabeza; razón por la cual el comportamiento de sus subcontratistas no lo excusará del cumplimiento de las obligaciones y la asunción de los riesgos que este contrato le asigna.

4.2. OBLIGACIONES ESPECIFICAS DEL CONTRATISTA

1. Cumplir a cabalidad con las especificaciones y condiciones técnicas requeridas para el cumplimiento del objeto contractual, así como disponer lo necesario para que el objeto del contrato se cumpla a cabalidad, conforme las especificaciones técnicas exigidas por **LA ENTIDAD** y la propuesta presentada por **EL CONTRATISTA**

2. Adelantar las actividades del contrato, empleando el personal idóneo que se requiera para el desarrollo del objeto contractual.
3. Tener en cuenta las instrucciones de orden técnico y operativo que para el desarrollo del objeto del contrato disponga LA ENTIDAD.
4. Responder por la calidad del objeto contratado, de acuerdo con las previsiones de las normas vigentes aplicables a esta materia.
5. Responder por todas aquellas obligaciones de la naturaleza del contrato que, pese a no estar escritas se consideren obligaciones a su cargo o estén contempladas en las reglamentaciones expedidas por el Gobierno Nacional.
6. Rendir los informes de gestión de manera oportuna que le sean requeridos por el supervisor del contrato.
7. Las demás actividades necesarias para dar cumplimiento a los aspectos relacionados con el contrato.

4.3. OBLIGACIONES DE ORDEN AMBIENTAL Y DE SEGURIDAD Y SALUD EN EL TRABAJO.

a) De orden ambiental:

El contratista, sin perjuicio de la obligación de cumplir con las disposiciones legales asociadas con la gestión ambiental, debe acatar las disposiciones de tipo ambiental que le fije el **DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA – DAPRE**, en especial las siguientes:

i. Dar estricto cumplimiento a los lineamientos, normas, reglamentos, estándares, orientaciones, políticas, y leyes ambientales aplicables para la ejecución de las actividades que contratadas por esta entidad.
ii. Procurar el cuidado de la casa común, y los recursos naturales.
iii. Cumplir, sin excepción, la legislación ambiental vigente, sin necesidad de requerimiento previo o expreso; y obtener mantener vigentes las licencias o permisos de autoridades ambientales que de conformidad con la normatividad vigente sean necesarias para cumplir sus obligaciones contractuales y/o post-contractuales, si a ello hubiere lugar.

PARÁGRAFO PRIMERO: Igualmente **EL CONTRATISTA** debe prever los costos en los que deben incurrir para el cumplimiento de las normas ambientales, antes, durante y después de la ejecución del contrato.

PARÁGRAFO SEGUNDO: Las obligaciones ambientales que se consignan dentro del contrato se harán extensivas y serán de obligatorio cumplimiento por parte de

los subcontratistas que hagan parte de la actividad que **EL CONTRATISTA** contractualmente desarrolla, si a ello hubiere lugar.

b) <u>De Seguridad y Salud en el Trabajo:</u>

El contratista, sin perjuicio de la obligación de cumplir con las disposiciones legales asociadas con la gestión de seguridad y salud en el trabajo, debe acatar las disposiciones de tipo ambiental que le fije el **DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA – DAPRE**, en especial las siguientes:

i. Suministrar al personal que se encuentre a su cargo y que dispondrá para la ejecución del contrato, todos los elementos de protección personal necesarios para desarrollar la actividad contratada, para lo cual asumirá su costo, si a ello hubiere lugar.
ii. El personal de **EL CONTRATISTA** que se encuentre a su cargo y que dispondrá para la ejecución del contrato, deberá contar con todos los permisos y certificaciones necesarias para el desarrollo de la actividad o actividades requeridas, si a ello hubiere lugar.
iii. Cumplir con las normas, reglamentos e instrucciones del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST.
iv. Cuando a ello hubiere lugar, dar cumplimiento a los protocolos de bioseguridad requeridos para la actividad a realizar.

4.4. <u>OBLIGACIONES DEL DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA – DAPRE.</u>

1. Pagar el valor estipulado del contrato, en las condiciones establecidas en la forma de pago.
2. Exigir al contratista la ejecución idónea y oportuna del objeto contractual.
3. Aprobar los mecanismos de cobertura del riesgo.
4. Designar el supervisor del contrato
5. Las demás que se deriven de la naturaleza del contrato que sean indispensable para cumplir su objeto.

5. CÓDIGO DEL CLASIFICADOR DE BIENES Y SERVICIOS DE LAS NACIONES UNIDAS - UNSPSC.

De acuerdo con la codificación de Bienes y Servicios del Código Estándar de Productos y Servicios de Naciones Unidas, el bien, obra o servicio se encuentra codificado de la siguiente manera:

SEGMENTO	FAMILIA	CLASE	PRODUCTO
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	43220000 Equipos o plataformas y accesorios de redes multimedia o de voz y datos	43222500 Equipo de Seguridad de red	43222500 Equipo de Seguridad de red
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	43220000 Equipos o plataformas y accesorios de redes multimedia o de voz y datos	43222600 Equipo de Servicio de Red	43222600 Equipo de Servicio de Red
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	43230000 Software	43231500 Software funcional especifico de la empresa	43231500 Software funcional especifico de la empresa
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	43230000 Software	43232400 Programas de Desarrollo	43232400 Programas de Desarrollo
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	43230000 Software	43233200 Software de seguridad y protección	43233200 Software de seguridad y protección
81000000 Servicios Basados en Ingeniería, Investigación y Tecnología	81110000 Servicios Informáticos	81111800 Servicios de sistemas y administración de componentes de sistemas	81111819 Servicios de garantía de calidad
81000000 Servicios Basados en Ingeniería, Investigación y Tecnología	81110000 Servicios Informáticos	81112200 Mantenimiento y soporte de software	81112200 Mantenimiento y soporte de software
81000000 Servicios Basados en Ingeniería, Investigación y Tecnología	81110000 Servicios Informáticos	81112200 Mantenimiento y soporte de software	81112204 Mantenimiento de software de sistemas operativos

6. IDENTIFICACIÓN DEL CONTRATO A CELEBRAR:

El **DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA – DAPRE** como resultado de la presente selección, celebrará un contrato de compraventa, para atender las necesidades que se enuncian en la descripción y justificación de la necesidad y del objeto del presente proceso.

7. MODALIDAD DE SELECCIÓN Y SU JUSTIFICACIÓN:

Dada la naturaleza del objeto a contratar y teniendo en cuenta que los bienes y servicios que se necesitan adquirir son de características técnicas uniformes y de común utilización, la modalidad de selección del presente proceso será la de Selección Abreviada por Subasta Inversa prevista en el literal a), numeral 2 del artículo 2º de la Ley 1150 de 2007.

El contrato resultante del proceso de Selección Abreviada por Subasta Inversa, se regirá por lo prescrito en las Leyes 80 de 1993 y 1150 de 2007 y su Decreto Reglamentario 1082 de 2015 y demás normas que adicionen, modifiquen o reglamenten la materia

8. VALOR ESTIMADO DEL PRESUPUESTO OFICIAL Y JUSTIFICACIÓN DEL MISMO:

De acuerdo con la información contenida en el Análisis del Sector y Estudio del Mercado, adjunto al presente documento, el valor del presupuesto oficial estimado para adelantar el presente proceso de selección es hasta por la suma de **MIL NOVECIENTOS VEINTICUATRO MILLONES CUATROCIENTOS VEINTIOCHO MIL NOVECIENTOS NOVENTA Y NUEVE PESOS M/CTE. ($1.924.428.999)**, incluido IVA y demás impuestos, tasas, contribuciones, costos directos e indirectos que conlleven la celebración y ejecución del contrato.

De acuerdo con la información contenida en el Análisis del Sector y Estudio del Mercado, adjunto al presente documento.

De conformidad con las cotizaciones allegadas se realizó el análisis económico y se determinaron los precios referencia de la siguiente manera:

	SUSCRIPCION HERRAMIENTA SOAR POR 3 AÑOS*		
	VALOR	**IVA**	**VALOR TOTAL**
COTIZANTE 1	$ 1.959.983.738	N/A*	$ 1.959.983.738
COTIZANTE 2	$ 1.866.018.706	N/A*	$ 1.866.018.706
COTIZANTE 3	$ 1.752.997.030	N/A*	$ 1.752.997.030
COTIZANTE 4	$ 2.118.716.522	N/A*	$ 2.118.716.522
	PROMEDIO		**$ 1.924.428.999**
	DESVIACION		$ 154.717.445
	% DESVIACION		8%
	*Solución excluida de IVA según Art. 476 del Estatuto Tributario – Modificado L. 2010/2019, Art. 11 Núm. 21		

Conforme lo anterior, el valor del presupuesto oficial estimado para adelantar el presente proceso de selección es hasta por la suma de **MIL NOVECIENTOS VEINTICUATRO MILLONES CUATROCIENTOS VEINTIOCHO MIL NOVECIENTOS NOVENTA Y NUEVE PESOS M/CTE. ($1.924.428.999)**, incluido todos los impuestos, tasas, contribuciones, costos directos e indirectos que conlleven la celebración y ejecución del contrato.

- Rubro presupuestal: _C_0299_1000_6_53105b
- Fortalecimiento de la plataforma de TIC del Departamento Administrativo de la Presidencia de la Republica en las sedes de Bogotá, Cartagena y Sopó.

- Funcionamiento: ___ o Inversión: _X_

9. INDICACIÓN DE REQUISITOS HABILITANTES:

9.1. REQUISITOS HABILITANTES TÉCNICOS

9.1.1. EXPERIENCIA GENERAL:

Se tendrá como experiencia general mínima habilitante del proponente la acreditación de contratos suscritos y ejecutados por el proponente, que sumados tengan la siguiente equivalencia expresada en Salarios Mínimos Legales Mensuales Vigentes:

SMLMV	**1.480,33**

La experiencia general se acreditará y verificará directamente con el Registro Único de Proponentes (RUP).

Se verificará por parte de la Entidad que el o los contrato(s) ejecutado(s) se encuentra(n) identificado(s) *en los siguientes códigos del Clasificador de Bienes y Servicios*, a nivel de clase, así:

SEGMENTO	FAMILIA	CLASE
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	43220000 Equipos o plataformas y accesorios de redes multimedia o de voz y datos	43222500 Equipo de Seguridad de red
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	43220000 Equipos o plataformas y accesorios de redes multimedia o de voz y datos	43222600 Equipo de Servicio de Red
43000000	43230000 Software	43231500

Difusión de Tecnologías de Información y Telecomunicaciones		Software funcional especifico de la empresa
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	43230000 Software	43232400 Programas de Desarrollo
43000000 Difusión de Tecnologías de Información y Telecomunicaciones	43230000 Software	43233200 Software de seguridad y protección
81000000 Servicios Basados en Ingeniería, Investigación y Tecnología	81110000 Servicios Informáticos	81111800 Servicios de sistemas y administración de componentes de sistemas
81000000 Servicios Basados en Ingeniería, Investigación y Tecnología	81110000 Servicios Informáticos	81112200 Mantenimiento y soporte de software
81000000 Servicios Basados en Ingeniería, Investigación y Tecnología	81110000 Servicios Informáticos	81112200 Mantenimiento y soporte de software

NOTA: En caso que los contratos que acreditan la experiencia tengan algún tipo de multa o sanción, no serán tenidos en cuenta por parte de **LA ENTIDAD**.

9.1.2. CERTIFICADO DE DISTRIBUIDOR AUTORIZADO

El oferente deberá certificar y demostrar que es distribuidor autorizado del fabricante, así:

Para demostrar el cumplimiento de esta obligación, el oferente deberá anexar certificación vigente con fecha no mayor a 30 días a partir de la fecha de cierre del proceso de selección, expedida por el fabricante y deberá indicar que el oferente es su distribuidor autorizado, indicando la fecha a partir de la cual es su distribuidor autorizado, indicando la fecha a partir de la cual es su distribuidor autorizado.

Si la misma se encuentra en un idioma diferente al español, deberá anexarse la traducción correspondiente.

En caso de Unión Temporal o Consorcio, al menos uno de los integrantes deberá acreditar la presente certificación.

9.1.3. CERTIFICADO DE CENTRO DE SOPORTE Y MANTENIMIENTO AUTORIZADO

El oferente deberá certificar y demostrar que cuenta con certificación vigente no mayor a 30 dias anteriores a la fecha de cierre del proceso de selección, expedida por el fabricante, en la que se acredite que es centro de soporte y mantenimiento autorizado, sin intermediarios.

Si la misma se encuentra en un idioma diferente al español, debe anexarse la traducción correspondiente.

En caso de Unión Temporal o Consorcio, uno de los integrantes deberá acreditar la presente certificación.

9.2. INDICADORES FINANCIEROS:

De acuerdo con lo establecido en el artículo 2.2.1.1.1.6.2 del Decreto 1082 de 2015, la Entidad verificará la totalidad de los siguientes indicadores financieros registrados en el RUP para el año 2023.

NOTA 1: Los proponentes que terminan su año contable en una fecha distinta al 31 de diciembre, deben actualizar la información financiera en el RUP en las fechas correspondientes a sus cierres contables, esta situación debe ser certificada por el representante legal, contador y revisor fiscal.

NOTA 2: Cuando el proponente cuente con menos de un año de constituido, **LA ENTIDAD** tendrá en cuenta la información registrada en el Registro Único de Proponentes – RUP del Balance de Apertura.

NOTA 3: OFERENTES EXTRANJEROS: Las empresas extranjeras interesadas en participar en el presente proceso deben enviar los Estados Financieros del año 2023, de conformidad con la legislación propia del país de origen, avalados con la firma de quien se encuentre en obligación de hacerlo de acuerdo con la normativa vigente del país de origen, en idioma español y debidamente apostillados, (respecto de la apostilla aplica el numeral 2.1.3.2. de este documento), adicionalmente deben especificar la moneda en la cual están presentados; con la anterior información **LA ENTIDAD** procederá a establecer el valor en pesos de acuerdo con la tasa de cambio establecida por el Banco de la República a diciembre 31 de dicho año fiscal, con el fin de calcular los índices financieros requeridos por **LA ENTIDAD**. De igual manera deberán diligenciar el **Anexo 8** del pliego de condiciones.

9.2.1. CAPACIDAD FINANCIERA:

De acuerdo con lo establecido en el artículo 2.2.1.1.1.6.2 del Decreto 1082 de 2015, la Entidad verificará **la totalidad** de los siguientes indicadores financieros registrados en el RUP, la cual deberá estar actualizada y en firme con corte a diciembre 31 de 2023.

INDICADOR	INDICE REQUERIDO
Liquidez	Igual o superior a **1.4**
Endeudamiento	Menor o igual a **70 %**
Razón de Cobertura de Intereses	Mayor o igual **0** o Indeterminada
Capital de Trabajo	Mayor o igual a 25 % de la sumatoria del presupuesto oficial

Adicionalmente y de conformidad con las características del objeto a contratar y la naturaleza del presente proceso de selección, la Entidad verificará el **Tamaño Patrimonial** en la información financiera registrada en el RUP, es decir el valor registrado en el patrimonio a diciembre 31 de 2023, así:

Las MIPYMES, deben contar con el siguiente Tamaño Patrimonial:

INDICADOR	VALOR REQUERIDO
Tamaño Patrimonial	Mayor o igual a $1.924 Millones

Los oferentes deben cumplir con los cuatro índices requeridos por la Entidad para determinar la capacidad financiera.

Los oferentes cuyos gastos de intereses sean cero (0), no podrán calcular el indicador de razón de cobertura de intereses. En este caso el oferente cumple el indicador, salvo que la utilidad operacional sea negativa, caso en el cual NO cumple con el indicador de cobertura de intereses.

NOTA: En caso de presentarse la propuesta a través de **consorcio o unión temporal** se tomarán las cifras registradas en el RUP, de la información financiera por cada uno de los integrantes del consorcio o la unión temporal en su propuesta y se sumarán las cifras, con el fin de calcular los

índices específicos de este documento para la asociación. Aplica de igual manera para la capacidad organizacional.

Cuando, como resultado de éste cálculo se generen cifras con decimales, **LA ENTIDAD** procederá a efectuar la aproximación de éstos así: si el resultado obtenido es inferior o igual a 50 decimales se baja a la unidad anterior y si por el contrario el resultado obtenido es superior o igual a 51 decimales se sube a la unidad siguiente, ejemplo: en una operación que genere un valor de 20.50 el valor registrado será 20 y para un resultado de 20.51 el valor final será de 21.

- **Para el caso de consorcios o uniones temporales, la liquidez se determina así**

IL= AC1+AC2+AC3+ …

PC1+PC2+PC3+ …

IL: Índice de Liquidez

AC : Activo Corriente de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

PC: Pasivo Corriente de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

Una vez aplicada la fórmula anterior, la cifra resultante deberá ser mayor o igual a **1.4**

- **Para el caso de consorcios o uniones temporales, el endeudamiento se determina así:**

IE= PT1+PT2+PT3 ...

AT1+AT2+AT3...

IE: Índice Endeudamiento

PT: Pasivo Total de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

AT: Activo Total de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

Una vez aplicada la fórmula anterior el porcentaje resultante deberá ser menor o igual al **70 %.**

- **Para el caso de consorcios o uniones temporales, la razón de cobertura de intereses se determina así:**

RCI = (UO1+UO2+UO3….)

(GI1+GI2+GI3…)

RCI: Razón de Cobertura de Intereses

UO: Utilidad Operacional de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

GI: Gastos de Intereses de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

Una vez aplicada la fórmula anterior, la Razón de Cobertura deberá ser mayor o igual a **0 veces** o **Indeterminada**.

Para el caso de consorcios o uniones temporales, cuando la suma de los gastos de intereses sean cero (0), no podrán calcularse el indicador de razón de cobertura de intereses. En este caso el oferente cumple el indicador, salvo que el total de la utilidad operacional de los integrantes de la unión temporal o consorcio sea negativo, caso en el cual NO cumple con el indicador de cobertura de intereses.

- **Para el caso de consorcios o uniones temporales, el Tamaño del Patrimonio se determina así:**

TP = TP1+TP2+TP3….

TP = Sumatoria del Tamaño Patrimonial de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

Una vez aplicada la fórmula anterior, el proponente deberá contar con el siguiente tamaño patrimonial, así:

Las MIPYMES, deben contar con el siguiente Tamaño Patrimonial:

INDICADOR	VALOR REQUERIDO
Tamaño Patrimonial	Mayor o igual a $1.924 Millones

Los oferentes que <u>NO estén clasificadas como MIPYMES</u>, deben contar con el siguiente Tamaño Patrimonial:

INDICADOR	VALOR REQUERIDO
Tamaño Patrimonial	Mayor o igual a $2.866 Millones

9.2.2. CAPACIDAD ORGANIZACIONAL

Para medir la Capacidad Organizacional, los oferentes deben acreditar los siguientes indicadores, a diciembre 31 de diciembre del 2023:

INDICADOR	INDICE REQUERIDO
Rentabilidad del patrimonio	Mayor o igual a **0 %**
Rentabilidad del activo	Mayor o igual a **0 %**

Los oferentes deben cumplir con los dos índices establecidos por la Entidad para verificar la capacidad organizacional.

- **En caso de consorcio o unión temporal, el DAPRE calculará el indicador de <u>Rentabilidad del Patrimonio</u>, así**:

$$RP = \frac{(UO1+UO2+UO3\ldots.)}{(P1+PT2+PT3\ldots)}$$

RP = Rentabilidad del Patrimonio

UO = Utilidad Operacional de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

P = Patrimonio de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

Una vez aplicada la fórmula anterior, la rentabilidad del patrimonio requerida deberá ser mayor o igual a **0 %.**

- **En caso de consorcio o unión temporal, el DAPRE calculará el indicador de Rentabilidad del Activo, así:**

$$RA = \frac{(UO1+UO2+UO3\ldots.)}{(AT1+AT2+AT3\ldots)}$$

RA = Rentabilidad del Activo

UO = Utilidad Operacional de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

AT = Activo Total de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

Una vez aplicada la fórmula anterior, la rentabilidad del activo requerida deberá ser mayor o igual a **0 %.**

9.3. DOCUMENTOS HABILITANTES JURÍDICOS

Los interesados podrán participar como proponentes bajo alguna de las siguientes modalidades:

A. Individualmente como: a) personas naturales nacionales o extranjeras, b) personas jurídicas nacionales o extranjeras.
B. Conjuntamente, como proponentes plurales en cualquiera de las formas de asociación previstas en el artículo 7 de la Ley 80 de 1993.

Los proponentes deben:

A. Tener capacidad jurídica para la presentación de la oferta.
B. Tener capacidad jurídica para la celebración y ejecución del contrato.
C. No estar incursos en ninguna de las circunstancias de inhabilidad, incompatibilidad, conflicto de interés o prohibición para contratar previstas en la Constitución y en la Ley.
D. No estar reportados en el último Boletín de Responsables Fiscales vigente publicado por la Contraloría General de la República. Esta disposición aplica para el proponente e integrantes de un proponente plural con domicilio en Colombia. Tratándose de proponentes extranjeros sin domicilio o sin sucursal en Colombia, deben declarar que no son responsables fiscales por actividades ejercidas en Colombia en el pasado y que no tienen sanciones vigentes en Colombia que impliquen inhabilidad para contratar con el Estado.

La entidad consultará los antecedentes judiciales en línea en los registros de las bases de datos, al igual que el certificado de antecedentes disciplinarios conforme el artículo 1 de la Ley 1238 de 2008 y el Registro Nacional de Medidas Correctivas del Ministerio de Defensa Nacional – Policía Nacional, de acuerdo con lo dispuesto en el artículo 184 de la Ley 1801 de 2016 – Código Nacional de Seguridad y Convivencia Ciudadana.

Los documentos para verificar la capacidad jurídica de los oferentes, serán los establecidos en el documento de términos y condiciones adicionales.

10.CRITERIOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE:

Para la escogencia del ofrecimiento más favorable, el Departamento Administrativo de la Presidencia de la República tendrá como único criterio de selección **el menor precio**.

11.FORMA DE PAGO DEL CONTRATO:

El valor del contrato se pagará a través de la pagaduría de LA ENTIDAD contra facturación presentada por parte de EL CONTRATISTA, con base en el recibo a satisfacción del conjunto de herramientas de

organización, automatización y respuesta a incidentes de seguridad (SOAR), incluida su instalación, configuración y puesta en funcionamiento, previo cumplimiento de los siguientes requisitos:

a) Aprobación por parte de la Entidad de la Garantía Única.
b) Certificación expedida por el Contratista o su Revisor Fiscal, cuando corresponda, donde se acredite estar a Paz y Salvo por conceptos de pago de sus obligaciones a los sistemas de salud, riesgos laborales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, de todo el personal a su cargo que así lo requiera.
c) Ingreso a la bodega virtual de software.
d) Certificación emitida por parte del supervisor del contrato, en la cual se acredite la entrega y recibo a satisfacción del conjunto de herramientas.
e) Tramite de la respectiva cuenta por parte de la Entidad.

NOTA 1: No obstante, la forma de pago prevista, ésta queda sujeta a la situación de los recursos por parte del Ministerio de Hacienda y Crédito Público, una vez se encuentre aprobado el **PAC** (Programa Anual Mensualizado de Caja)
NOTA 2: La Entidad pagará al **CONTRATISTA,** dentro de los diez (10) días hábiles siguientes a la radicación de los documentos por parte del Supervisor del contrato en el Área Financiera de la Entidad
NOTA 3. Si la factura no ha sido correctamente elaborada o no se acompañan los documentos requeridos para el pago y/o se presentan de manera incorrecta, el término para éste sólo empezará a contarse desde la fecha en que se aporte el último de los documentos y/o se presenten en debida forma. Las demoras que se presenten por estos conceptos serán responsabilidad del contratista y no tendrán por ello derecho al pago de intereses o compensación de ninguna naturaleza
NOTA 4. En caso de que aplique tratándose del pago con factura electrónica, el proponente deberá dar cumplimiento a lo establecido en la circular publicada en la página WEB de la Entidad

12.PLAZO DE EJECUCIÓN DEL CONTRATO A CELEBRAR:

El plazo para la entrega del conjunto de herramientas de organización, automatización y respuesta a incidentes de seguridad (SOAR), incluida su instalación, configuración y puesta en funcionamiento hasta el 31 de diciembre del 2024, contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato.

No obstante lo anterior, el Contratista deberá mantener el licenciamiento, la garantía, el soporte técnico y mantenimiento por tres (3) años.

13.LUGAR DE ENTREGA DE LOS BIENES O DE PRESTACIÓN DEL SERVICIO:

El lugar de entrega será en la Ciudad de Bogotá D.C. en la Calle 7 # 6-54, Departamento Administrativo de la Presidencia de la República.

14.ANÁLISIS DEL RIESGO Y LA FORMA DE MITIGARLO:

Conforme lo establecido en el artículo 4 de la Ley 1150 de 2007 y en el numeral 6° del artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015, debe existir un soporte que permita la tipificación, estimación y asignación de los riesgos previsibles.

Se entienden como riesgos involucrados en la contratación cualquier evento que puede generar efectos adversos y de distinta magnitud en el logro de los objetivos del Proceso de Contratación o en la ejecución de un contrato (artículo 2.2.1.1.1.3.1. del Decreto 1082 de 2015), así como todas aquellas circunstancias que, de presentarse durante el desarrollo y ejecución del contrato, tienen la potencialidad de alterar el equilibrio económico del contrato, pero que dada su previsibilidad se regulan en el marco de las condiciones inicialmente pactadas en los contratos y se excluyen así del concepto de imprevisibilidad de que trata el artículo 27 de la Ley 80 de 1993. La Entidad realizó el ejercicio de previsibilidad ordenado por las normas ya mencionadas el cual tuvo en consideración adicionalmente lo dispuesto en Documento CONPES sobre Riesgo Previsible en el Marco de la Política de Contratación Pública expedido por el Consejo Nacional de Política Económica y Social del Departamento Nacional de Planeación.

En el ejercicio de previsibilidad se analizaron aspectos tales como la naturaleza del contrato, el plazo de ejecución, las obligaciones a cargo del contratista, el tipo de bienes o servicios a contratar, así como los demás aspectos enunciados en el estudio del sector, entre otros, así:

N	Clase	Fuente	Etapa	Tipo	Descripción	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración	Categoría	¿A quién se le asigna?	Tratamiento/Control a ser implementado	Impacto después del tratamiento				¿Afecta la ejecución del	Responsable por	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración	Categoría					¿Cómo se realiza el monitoreo?	Periodicidad

1	Específico	Externo	Planeación	Financiero	Variación de la TRM cuando sea un producto importado	Desequilibrio económico del contrato	3	3	6	Alto	Contratista y entidad	Aceptar el Riesgo. No puede ser evitado ni ser transferido o el costo de evitarlo o transferirlo es muy alto. En este caso se recomienda al contratista tomar medidas para reducir el Riesgo o mitigar su impacto, como son: la adquisición de suficientes existencias para la atención del Contrato, planeación acorde con las necesidades de la Entidad	3	2	5	Alto	Sí	Contratista	Etapa de ejecución si ocurre la situación	Pago	Cumplimiento de las cláusulas económicas y plan financiero	Revisión periódica o por facturación
2	General	externa	ejecución	regulatorio	Modificaciones del régimen tributario que implique afectación a la ejecución del contrato y la prestación del servicio	Desequilibrio de la ecuación contractual	3	2.	5	Medio	Contratista y entidad	Reducir las consecuencias a través de planes de contingencia	3	2	4	Medio	Sí	Contratista	Etapa de ejecución si ocurre la situación	Pago	Cumplimiento de las cláusulas económicas y plan financiero	Revisión periódica o por facturación
3	General	externa	ejecución	regulatorio	Modificaciones del marco legal que implique afectación a la ejecución del contrato y la prestación del servicio	Desequilibrio de la ecuación contractual	3	2	5	Medio	Contratista y entidad	Reducir las consecuencias a través de planes de contingencia	3	2	4	Medio	Sí	Contratista	Etapa de ejecución si ocurre la situación	Pago	Cumplimiento de las cláusulas económicas y plan financiero	Revisión periódica o por facturación

14.1. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:

Los riesgos de seguridad y privacidad de la información que se pueden presentar durante el desarrollo del contrato, son perdida de confidencialidad, integridad, disponibilidad y privacidad de los datos, los cuales podrían ocasionar que se interrumpa la prestación de los servicios.

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles

1	Posibilidad de afectación reputacional, por la pérdida de disponibilidad de los servicios TICs, debido a la falta de seguimiento y monitoreo de las herramientas TICS-SGSI	Corresponde a los servicios que hacen parte de la Oficina de Tecnologías y Sistemas de Información, que puedan estar no disponibles.	SGSI	Mala identificación de los requisitos técnicos y funcionales	Indisponibilidad de los servicios de TICs	Alta	Mayor	Aplicar el procedimiento de control de cambios
				Errores humanos	Violación a las políticas de seguridad			Implementar actualizaciones de las diferentes aplicaciones utilizadas en la Entidad
				No cumplimiento del procedimiento establecido	Pérdida de imagen			Monitorear los servicios tecnológicos
				Error en la manipulación de la Plataforma Tecnológica	Quejas, reclamos frente a la prestación de servicios			Realizar la entrega de Rol con las respectivas actividades
				Dualidad de tareas en los funcionarios				Ejecutar pruebas de los servicios tecnológicos replicados en el centro alterno
				No activación de registros de logs				
				Error en las configuraciones de los controles				
2	Posibilidad de afectación reputacional, por la pérdida de la documentación pública reservada y publica clasificada, o identificable de carácter personal (datos personales) que se encuentra en la Plataforma de TI o repositorios físicos, debido a accesos no autorizados - SGSI	En caso de que se presente perdida de información pública reservada o pública clasificada, o de carácter privado (información identificable como personal - datos personales) puede ocasionar afectación en la imagen de la Entidad.	Tecnología	Deficiencias en cultura de la seguridad de la información e Informática	Retrasos en los procesos de los funcionarios y contratistas	Media	Mayor	Utilizar la herramienta de prevención de perdida de información (DLP)
				Fallas Técnicas de Hardware	Problemas de Seguridad Nacional (perdida de Información reservada)			Emplear la Autenticación de dos factores
				Conflicto Armado	Afectación derechos a titulares de datos personales			Aplicar Cifrado de Información pública clasificada y pública reservada
				Vandalismo Informático	Sanciones legales y disciplinarias			Realizar la verificación de vulnerabilidades de la plataforma TICs
				Desconocimiento del manual de políticas de seguridad.	Afectación de la imagen de la Entidad			Mantener operativas las herramientas tecnológicas
				Usuarios inconformes que puedan atentar contra la seguridad de la información				Realizar la entrega de Rol con las respectivas actividades
				Falta de conocimiento técnico en el personal que administra la plataforma informática o la información.				Ejecutar los procedimientos de backup, configuración de SAN
				Gestión de vulnerabilidades de la plataforma				Monitorear las herramientas de seguridad de la información
				Errores Humanos				Aplicar Políticas de Seguridad de la información
				Ataques cibernéticos y delitos informáticos				Utilizar contraseñas seguras.
				Obsolescencia de la plataforma				
				Deficiencias en definición, aplicación o seguimiento de las políticas de seguridad				
				Dualidad de tareas en los funcionarios				
				Deficiencias en el procedimiento de Borrado Seguro				
				Pérdida de equipos tecnológicos con información contenida				
3	Posibilidad de afectación reputacional, por pérdida de la gestión de la continuidad del negocio en activos de información, debido a situaciones adversas - SGSI	La Entidad puede ser afectada por no disponer de una gestión de la continuidad del negocio al no tener la prestación de sus servicios, por situaciones adversas.	SGSI	Fallas en los equipos tecnológicos	Afectación de la Imagen de la Entidad	baja	Mayor	Realizar pruebas de disponibilidad y continuidad para los servicios que proporciona la Entidad.
				Falta de Mantenimientos preventivos	Retrasos en los procesos de los funcionarios			Aplicar los cambios a los sistemas mediante el uso de procedimientos formales de control de cambios.

				Desconocimiento del manual de políticas de seguridad	Retrasos en los procesos de los contratistas			Actualizar la documentación para la continuidad de la seguridad de la información.
				Equipos desactualizados	Problemas de Seguridad Nacional (pérdida de Información reservada)			
					Pérdida de credibilidad de las herramientas informáticas			
					Sanciones legales y disciplinarias			
					Retrasos en los procesos de los funcionarios			
4	Posibilidad de afectación reputacional, por el uso indebido de la información pública clasificada y/o pública reservada de la Entidad, así como de aquella identificable de carácter personal (datos personales), debido a la falta de controles para la protección de la información -SGSI	La información activa o cuando ha dejado de utilizarse debe gestionarse de una forma segura, porque la información clasificada o reservada, así como aquella identificable de carácter personal (datos personales) contenida en medios digitales o físicos (hojas de papel, carpetas, folletos, dispositivos de almacenamiento - memoria USB, disco duro -, medios magnéticos y ópticos) puede ser manipulada o utilizada por delincuentes para aprovechar su contenido con fines distintos a la finalidad de dicha información (sea organizacional o personal) y afectar la imagen de la Entidad.	SGSI	Deficiencias en el procedimiento de Borrado Seguro	Retrasos en los procesos de los funcionarios y contratistas	media	catastrófico	Aplicar el procedimiento de borrado seguro para equipos.
				Pérdida de equipos tecnológicos con información contenida.	Problemas de Seguridad Nacional (perdida de Información reservada)			Realizar la eliminación de documentos de archivo de acuerdo al procedimiento establecido por la Entidad.
				Desconocimiento de Baja de Bienes	Afectación derechos a titulares de datos personales			Utilizar la criptografía para mantener protegida información
				Desconocimiento del manual de políticas de seguridad	Sanciones legales y disciplinarias			Proteger la información mediante políticas y procedimientos de la Seguridad de la Información
				Deficiencias en cultura de la seguridad de la información e Informática	Afectación de la imagen de la Entidad			
				Desconocimiento procedimiento de eliminación de Documentos				
5	Posibilidad de afectación reputacional, por hurto, perdida o fuga de información, debido a ataques cibernéticos - SGSI	Los ataques cibernéticos se pueden presentar en la Entidad ocasionados por personas malintencionadas (ciberatacantes), afectando sistemas de información, aplicativos informáticos, páginas Web, equipos de cómputo, servidores que contienen y procesan información, comprometiendo la Confidencialidad, Integridad y Disponibilidad de la información.	SGSI	Ataques cibernéticos y delitos informáticos	Afectación de la Imagen de la Entidad	Muy Alta	Catastrófico	Gestionar las vulnerabilidades técnicas
				Falta de conocimiento técnico en el personal que administra la plataforma informática	Retrasos en los procesos de los funcionarios			Aplicar la seguridad de servicios de las aplicaciones en redes públicas.
				Falta de Verificación de vulnerabilidades de la plataforma TIC	Retrasos en los procesos de los contratistas			Proteger los activos de información contra los códigos maliciosos
				Obsolescencia de la plataforma	Problemas de Seguridad Nacional (pérdida de Información reservada)			Realizar la separación de redes
				Desconocimiento Manual de políticas de Seguridad de la Información	Pérdida de credibilidad de las herramientas informáticas			Utilizar Perímetros de Seguridad Física
					Sanciones legales y disciplinarias			Restringir el acceso a código fuente de Programas evitar cambios involuntarios.
								Utilizar contraseñas seguras
								Revisar la configuración y afinamiento de las herramientas de seguridad informática.
								Contener el Ataque Cibernético

15. PROYECTOS DE INVERSIÓN:

La presente contratación hace parte de un proyecto de Inversión: SI _**X**__ NO___

- **Nombre del Proyecto**: FORTALECIMIENTO DE LA PLATAFORMA DE TIC DEL DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA EN LAS SEDES DE BOGOTÁ, CARTAGENA, SOPÓ
- **Código BPIN**: 2018011000642
- **Objetivo específico del proyecto:** Fortalecer la Plataforma de TIC del Departamento Administrativo de la Presidencia de la República.
- **Actividad e Indicador al cual se encuentra relacionada la contratación:** Implementar Herramientas que brinden Seguridad y Protección a la información, **indicador:** Sistemas de Información Actualizados.

Conforme lo anterior, se certifica que el presente proceso de selección se encuentra alineado con el proyecto de inversión respectivo.

16. GARANTÍAS

16.1. GARANTÍA DE SERIEDAD DE LA OFERTA

El proponente acompañará con su propuesta una garantía de seriedad, mediante cualquiera de los mecanismos vigentes previstos en el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015.

La garantía será expedida y cumplirá los requisitos establecidos para cada instrumento en el Decreto 1082 de 2015:

BENEFICIARIO: La Nación y/o Departamento Administrativo de la Presidencia de la República. (NIT. 899999083-0)

AFIANZADO: El Oferente

VIGENCIA: Tres (03) meses, contados a partir de la presentación de la propuesta. En todo caso, su vigencia deberá extenderse hasta la aprobación de la garantía que ampara los riesgos propios de la etapa contractual

CUANTÍA: Diez por ciento (10%) del valor del presupuesto oficial. En caso de que el proceso se divida por grupos o lotes el valor del amparo corresponderá al valor del presupuesto oficial por grupo o lote ofertado.

16.2. OTRAS GARANTÍAS

16.2.1 GARANTÍA ÚNICA DE CUMPLIMIENTO:

De conformidad con lo establecido en los artículos 2.2.1.2.3.1.1. y siguientes del Decreto 1082 de 2015, el Departamento Administrativo de la Presidencia de la República, en razón al objeto, la naturaleza y las características del contrato a ejecutar, considera como mecanismo de cobertura del riesgo la constitución de una garantía a favor de entidades estatales que garantice de cumplimiento de sus obligaciones y que cubra los perjuicios derivados del incumplimiento de las obligaciones legales o contractuales del contratista cuyo monto, vigencia y amparos, cumplan con lo siguiente:

El contratista con el fin de dar cobertura a los riesgos que se puedan presentar durante la vigencia del contrato deberá constituir una garantía única para avalar el cumplimiento de las obligaciones surgidas del contrato, con los siguientes amparos:

AMPARO	VIGENCIA	MONTO ASEGURADO
Cumplimiento del contrato	La vigencia será igual al plazo del mismo y seis (6) meses más contados a partir de la fecha de expedición de la garantía	Veinte 20% del valor del contrato
Pago de salarios, prestaciones sociales legales e	La vigencia será igual al plazo del mismo y tres (3) años más.	Cinco por ciento (5%) del valor total del contrato

AMPARO	VIGENCIA	MONTO ASEGURADO
indemnizaciones laborales		
Calidad del servicio	La vigencia será igual al plazo del mismo y tres (3) años más después de la entrega e instalación de la herramienta.	Veinte 20% del valor del contrato
Calidad y correcto funcionamiento de los bienes	La vigencia será igual al plazo del mismo y un (1) año más después de la entrega e instalación de la herramienta.	Veinte 20% del valor del contrato

17. INDICACIÓN DE SI EL PROCESO DE CONTRATACIÓN ESTÁ COBIJADO POR UN ACUERDO COMERCIAL.

En cumplimiento de lo dispuesto en el numeral 10 del artículo 2.2.1.1.2.1.3 del Decreto 1082 de 2015 y en atención al Manual para el manejo de los Acuerdos Comerciales en Procesos de Contratación expedido por Colombia Compra Eficiente, para la presente contratación aplican los siguientes tratados de Libre Comercio:

Acuerdo Comercial		Vigente	Entidad Estatal incluida	Valor del Proceso de Contratación superior al umbral del Acuerdo Comercial	Excepción Aplicable al Proceso de Contratación	Proceso de Contratación cubierto por el Acuerdo Comercial
Alianza Pacífico	Chile	SI	SI	SI	NO	SI
	México	SI	SI	SI	NO	SI
	Perú	SI	SI	SI	NO	SI
Canadá		SI	SI	SI	NO	SI
Chile		SI	SI	SI	NO	SI
Corea		SI	SI	SI	NO	SI
Costa Rica		SI	SI	SI	NO	SI
Estados Unidos		SI	SI	SI	NO	SI
Estados AELC		SI	SI	SI	NO	SI
México		SI	SI	SI	NO	SI
	El Salvador	SI	SI	SI	NO	SI

Acuerdo Comercial		Vigente	Entidad Estatal incluida	Valor del Proceso de Contratación superior al umbral del Acuerdo Comercial	Excepción Aplicable al Proceso de Contratación	Proceso de Contratación cubierto por el Acuerdo Comercial
Triángulo Norte	Guatemala	SI	SI	SI	NO	SI
	Honduras	SI	NO	NO	NO	NO
Unión Europea		SI	SI	SI	NO	SI
Israel		SI	SI	SI	NO	SI
Reino Unido e Irlanda del Norte		SI	SI	SI	NO	SI
Comunidad Andina de Naciones		SI	SI	SI	NO	SI

18. SUPERVISIÓN

Se solicita designar como supervisor al Coordinador(a) del Grupo de Redes, de la Oficina de Tecnologías y Sistemas de Información.

19. **NECESIDAD DE CONTAR CON INTERVENTORÍA:**

La presente contratación SI ____ NO_X_ requiere de interventoría.

20.OTRAS OBSERVACIONES: Ninguna

René Guarín Cortés

Firmado digitalmente por René Guarín Cortés
Fecha: 2024.09.10 09:04:49 -05'00'

RENÉ GUARÍN CORTÉS
JEFE, OFICINA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN