ESTUDIOS PREVIOS
CONTRATACIÓN DIRECTA[1]

1.- NECESIDAD Y CONVENIENCIA

El Decreto 1258 del 17 de junio de 2013 señala que la Unidad de Planeación Minero Energética -UPME es una unidad administrativa especial de carácter técnico, adscrita al Ministerio de Minas y Energía, con personería jurídica, patrimonio propio y régimen especial en materia de contratación.

De conformidad con lo definido en el artículo 10 del Decreto 1258 de 2013, es responsabilidad de la Oficina de Gestión de Información de la Unidad de Planeación Minero Energética – UPME "*Velar por el adecuado y óptimo funcionamiento de la plataforma tecnológica de la Unidad, garantizando los sistemas de seguridad y gestión de la información*", por lo cual, desde la OGI se definen e implementan diferentes mecanismos que permitan garantizar la seguridad de la información.

De acuerdo con los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión- MIPG, dentro de la dimensión de Gestión de Valores para Resultados, las entidades deben adoptar la política de Seguridad Digital, a través de la cual se pretende "*fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país*".

Es así como la UPME, formuló los siguientes planes:

1. Plan de Seguridad y Privacidad de la Información, el cual se plantea como objetivos: "*Establecer actividades, responsables y tiempo de ejecución para la mejora, implementación y monitoreo del Sistema de Gestión de Seguridad de la información de la UPME; Cumplir la normatividad vigente en relación con la Seguridad y Privacidad de la Información en el marco de los procedimientos, políticas y la normatividad interna, contribuyendo a fortalecer la confianza del ciudadano en el uso de servicios digitales de la entidad; Apoyar el proceso de capacitación y/o socialización relacionada con la seguridad y privacidad de la información, generando campañas de comunicación y sensibilización para la divulgación al interior de la UPME; y Mantener un enfoque actualizado de los aspectos de seguridad y privacidad de la información en la UPME.*"

2. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información, el cual pretende: *"Establecer las acciones para gestionar de manera integral los riesgos de seguridad y privacidad de la información, a partir de la metodología de análisis de riesgo (identificación, análisis, valoración, manejo y monitoreo)"*

Con el fin de dar cumplimiento a los objetivos de la OGI y los Planes formulados, alineados al MIPG, se formuló el proyecto de inversión: "Fortalecimiento de los servicios digitales aumentando la capacidad para la transformación digital e interacción con el ciudadano", el cual define como una de las estrategias a desarrollar adelantar proyectos enmarcados en la definición, implementación y sostenimiento del sistema de gestión de seguridad de la información, de acuerdo con el MSPI

[1] Excepto la causal de contratación directa **46.6. Contratos de prestación de servicios profesionales o de apoyo a la gestión**, los cuales tienen su respectivo formato de estudios previos.

(modelo de seguridad y privacidad de la información), así como el uso de la infraestructura tecnológica para el procesamiento y almacenamiento de la información institucional, lo anterior, considerando que la información es el activo más importante de la entidad.

Para desplegar la estrategia anteriormente mencionada, el proyecto se plantea como uno de sus objetivos específicos *aumentar la capacidad institucional a nivel de arquitectura tecnológica y de sistemas de información* y la actividad *de administrar de manera eficiente el Software a nivel Institucional, de cara a la mejora de los productos y servicios prestados a la ciudadanía*, dentro de la cual se efectúa la planeación, programación, asignación de recursos, ejecución, seguimiento y entrega de proyectos de software, el cual contempla la implementación de un servicio de administración de la información.

Así mismo, el proyecto anteriormente mencionado se plantea como uno de sus objetivos específicos "Incrementar el desarrollo de los habilitadores transversales de la política de gobierno digital" y la actividad "Mantener y fortalecer el modelo Operativo de TI", se pretende incrementar la efectividad en la prestación de servicios de TI, se requiere fortalecer el modelo operativo de TI y la prestación de servicios integrales de tecnología.

Es así como se plantea la adquisición de un centro de operaciones de seguridad (SOC), el cual es fundamental para fortalecer nuestra capacidad de respuesta y proteger los activos de la organización. Este centro nos permitirá monitorear en tiempo real todas las operaciones, identificar amenazas y vulnerabilidades de manera proactiva, y coordinar de manera eficiente las acciones necesarias para mitigar cualquier riesgo.

Con la adquisición del SOC la UPME contará con los siguientes beneficios:

- Detección Temprana de Amenazas: La implementación de herramientas avanzadas de análisis de logs, correlación de eventos y detección de anomalías nos permitirá identificar posibles intrusiones y actividades maliciosas en las primeras etapas, minimizando el impacto de posibles ataques.

- Respuesta Rápida: Contar con un equipo dedicado de analistas de seguridad o servidor trabajando las 24/7 que garantizará una respuesta rápida y coordinada ante incidentes de seguridad. Podremos llevar a cabo investigaciones exhaustivas, aislar sistemas comprometidos y aplicar contramedidas de manera inmediata.

- Inteligencia de Amenazas: El SOC nos proporcionará acceso a bases de datos de inteligencia de amenazas actualizadas, lo que permitirá una mejor comprensión de las tácticas, técnicas y procedimientos utilizados por actores maliciosos, ayudando así a afinar nuestras estrategias de defensa.

- Monitorización Integral: A través de la implementación de sistemas de monitorización en tiempo real, seremos capaces de supervisar nuestra infraestructura de TI, proporcionando una visión holística de nuestra postura de seguridad.

- Colaboración Efectiva: El SOC actuará como un punto centralizado para la colaboración entre equipos de seguridad, TI y otros departamentos relevantes. Esto facilitará la

comunicación y la toma de decisiones informadas en tiempo real, mejorando la coordinación entre diferentes áreas.

La inversión en este centro de operaciones de seguridad se traducirá en una mejora significativa de nuestra postura de seguridad, garantizando la continuidad del negocio y la confidencialidad de la información sensible en un entorno cada vez más desafiante en términos de ciberamenazas y riesgos.

2.- OBJETO

Contratar los servicios de un Centro de Operaciones de Seguridad SOC para realizar la gestión y el monitoreo de la infraestructura tecnológica y la gestión de eventos e incidentes de seguridad.

3. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

1. Garantizar que la solución se integra y puede interoperar con los diferentes assets de la entidad
2. Realizar la instalación, implementación y puesta en marcha de los componentes requeridos para la prestación de los servicios de SOC.
3. Brindar la operación las 24 horas del día, los 7 días de la semana, para garantizar un monitoreo constante de la infraestructura y los sistemas de la entidad. Esto implica la supervisión en tiempo real de registros de eventos, alertas de seguridad y otras fuentes de datos relevantes.
4. En caso de que se confirme una amenaza o incidente de seguridad, el SOC debe tomar medidas inmediatas para mitigar el impacto. Esto podría incluir el aislamiento de sistemas comprometidos, la eliminación de malware y la implementación de medidas de seguridad adicionales.
5. Integrarse y alimentarse con diferentes Framework (MITRE ATT&CK), con el fin de contar con una clasificación de los eventos, las técnicas y tácticas utilizadas por los atacantes a nivel mundial.
6. Garantizar las interfaces para la integración con las plataformas assets de la entidad.
7. Suministrar el personal idóneo para realizar la implementación, afinamiento y mantenimiento del servicio de SOC.
8. Garantizar que la plataforma, cuenta con reportes predefinidos y personalizados que permitan visualizar los eventos de forma eficiente y tomar decisiones en torno a estos.
9. Realizar la gestión, monitoreo, correlación de eventos y resolución de eventos e incidentes de seguridad, sobre la infraestructura tecnológica de la UPME, objeto del contrato.
10. Realizar transferencia de conocimientos sobre la herramienta o solución a los profesionales designados, con el fin de que estén en la capacidad de realizar modificaciones en caso de requerirse
11. Contar con la capacidad de identificar y analizar amenazas cibernéticas, como intrusiones, malware, intentos de acceso no autorizado y otras actividades anómalas.
12. Generar informes detallados sobre actividades de seguridad, alertas, incidentes y acciones tomadas.
13. Ayudar a la UPME, en el proceso de revisión y/o actualización de políticas y procedimientos de seguridad informática, en función de las amenazas encontradas y las mejores prácticas de la industria.
14. Cumplir con las regulaciones y estándares de seguridad aplicables a la industria y a la ubicación geográfica donde la UPME desarrolla las actividades
15. Establecer una comunicación efectiva con la UPME y otras partes interesadas. Esto implica la colaboración en la planificación de estrategias de seguridad, la coordinación de actividades de respuesta a incidentes y la transmisión de información relevante.
16. Monitorear los siguientes dispositivos:

Dispositivo	Sistema Operativo	Cantidad	Ubicación
Servidor Página Web	Windows server 2016	1	Bogotá
ORFEO	Linux	1	Bogotá
LDAP	Windows server 2016	1	Bogotá
Virtualizacion	Vmware	1	Bogotá
Srvarchivos01	Windows server 2016	1	Bogotá
Sophos Endpoint-Servers	Sophos	1	Bogotá
Firewall Palo Alto	Linux	1	Bogotá
WAF (Fortiweb)	Linux	1	Bogotá
Flujos	Windows server 2016	1	Bogotá
Correo	Gmail	1	Cloud
Switch core	Linux	1	Bogotá

17. Permitir crear una línea base de comportamientos asociados a los dispositivos, usuarios y demás fuentes de información que hagan parte de la correlación, de tal manera que se pueda determinar cambios de comportamiento de los diferentes eventos de seguridad y alertar dichos eventos.
18. Configurar en las soluciones que apoyan la prestación del servicio de SOC; a través de reglas, alertas y notificaciones preconfiguradas y parametrizables aplicables a los activos monitoreados. Las alertas mínimas para monitorear son:
    a) Actividades asociadas a la administración de cuentas de usuario final
    b) Actividades asociadas a cuentas de altos privilegios, automáticas de procesos o asignadas a usuarios administradores
    c) Ejecución de comandos especiales sobre sistemas operativos.
    d) Cambios en archivos de configuración. (host, .ini).
    e) Cambios de parámetros técnicos, de configuración o de seguridad.
    f) Cambios de configuración horaria.
    g) Cambios no autorizados en recursos tecnológicos críticos como Firewall, WAF, plataforma EDR.
    h) Actividades de conexión con cuentas de usuario final o administradores.
    i) Actividades asociadas a manipulación de bitácoras técnicas (log) o interrupciones en el envío de los logs a la plataforma de correlación.
    j) Actividades asociadas a conexión de acceso remoto (RDP).

k) Monitoreo y cambios de los registros DNS internos del servidor de la entidad.
l) Ataques de fuerza bruta.
m) Actividades sospechosas de login por sistemas Web.
n) Múltiples login fallidos desde una misma estación de trabajo.
o) Intentos fallidos de login de forma persistente.
p) Cuentas de Windows creadas y eliminadas
q) Malware o programas potencialmente no deseados detectados.
r) Ataques DoS (Denial of Services attack) y DDoS (Distributed Denial of Services Attack).
s) También las sugeridas por las buenas prácticas de monitoreo de infraestructuras tecnológicas

4.- PRODUCTOS A ENTREGAR

Entrega de bienes

- Centro de Operaciones de Seguridad (SOC) en funcionamiento
- Entregar la documentación requerida para la gestión del Centro de Operaciones de Seguridad (SOC).
- Brindar soporte técnico para la implementación, administración, mantenimiento del Centro de Operaciones de Seguridad (SOC) vía telefónica y por correo electrónico al contacto técnico de la Unidad, durante el plazo de ejecución del contrato.
- Informe Mensual de Operación del Servicio
- Informe Mensual técnico Vulnerabilidades
- Licencias que evidencien la vigencia del SOC

5. OBLIGACIONES GENERALES DE LAS PARTES

Del Contratista:

- Cumplir el objeto del contrato/orden.
- Cumplir con las condiciones y lineamientos ofertados en la propuesta.
- Ejecutar el contrato/orden dentro del plazo establecido, y bajo las condiciones técnicas y financieras definidas en el presente proceso.
- Presentar cuenta de cobro o facturación electrónica, si por ley está obligado a ello, dentro de los plazos definidos en el contrato/orden.
- Mantener vigente y al día durante la ejecución del contrato la afiliación y aportes al sistema Integral de Seguridad Social Integral, Parafiscales y Sistema General de Riesgos Laborales. Está obligación no será exigible si el contratista o proveedor es una persona jurídica o natural extranjera.
- Constituir y modificar la garantía única de cumplimiento, si hay lugar.
- Las demás que le sean asignadas por el supervisor del contrato, en el marco del contrato/orden.

De la Upme:

- Designar el supervisor del contrato.
- Efectuar un seguimiento efectivo al cumplimiento de las obligaciones del contratista/proveedor a través del supervisor del contrato.
- Autorizar el pago del valor del contrato de acuerdo con la forma establecida.
- Verificar el cumplimiento de las obligaciones del contratista frente al sistema General de Seguridad Social. Está obligación no será exigible si el contratista o proveedor es una persona jurídica o natural extranjera.
- Proporcionar toda la información que el contratista/proveedor requiera para el cumplimiento de sus actividades contractuales.

- Velar por el cumplimiento de las obligaciones del contrato.

6.- VERIFICACIÓN DE LA INCLUSIÓN DE LA PRESENTE CONTRATACIÓN EN LOS ACUERDOS MARCO DE PRECIOS

El objeto de la presente contratación no está en los Acuerdos Marco de Precios.

7. ANALISIS DE APLICACIÓN DE TRATADOS INTERNACIONALES DE LIBRE COMERCIO

De conformidad con la Guía para las Entidades Estatales con régimen especial de contratación, literal D, la Unidad de Planeación Minero Energética – UPME debe verificar los acuerdos comerciales internacionales.

No obstante, teniendo en cuenta que el proceso de selección de la presente contratación es directa, no procede la verificación de aplicación de dichos acuerdos comerciales internacionales.

8.- VERIFICACIÓN DE LA INCLUSIÓN DE LA PRESENTE CONTRATACIÓN EN EL PLAN ANUAL DE ADQUISICIONES

Los bienes y/o servicios a adquirir con la presente contratación se encuentran contemplados en el Plan Anual de Adquisiciones de la presente vigencia fiscal.

9.- IDENTIFICACIÓN DEL OBJETO EN EL CLASIFICADOR DE BIENES Y SERVICIOS

Se consultó el link **http://www.colombiacompra.gov.co/clasificador-de-bienes-y-servicios**, encontrando que el objeto de la presente contratación se encuentra clasificado así:

43233200 - Software de seguridad y protección
81111800 - Servicios de sistemas y administración de componentes de sistemas
81111801- Seguridad de los computadores, redes o internet
81112208 - Mantenimiento de software de protección y seguridad

10.- MODALIDAD DE SELECCIÓN DEL CONTRATISTA

De conformidad con lo establecido en el artículo 46 de la Resolución UPME No. 513 del 12 de julio de 2023 la modalidad de selección es DIRECTA, bajo la causal 46.4 *"Contratos cuya cuantía sea* igual *o inferior a 150 SMMLV"*

11.- NATURALEZA JURÍDICA DEL CONTRATO

La naturaleza jurídica del contrato a suscribir es de: prestación de servicios.

12.- ANÁLISIS QUE SOPORTA EL VALOR ESTIMADO

Para determinar el valor estimado del contrato, la Unidad realizó el siguiente estudio del sector:

12.1.- Análisis de contrataciones similares en entidades Públicas

La Unidad de Planeación Minero Energética – UPME consultó el link de Colombia Compra con el fin de identificar los valores de los contratos de los bienes o servicios similares al de la presente contratación, encontrando lo siguiente:

Entidad	Colombia Compra Eficiente

Contrato	CCE-274-2023
Objeto	Prestar el Servicio de Centro de Operaciones de Seguridad para la ADRES
Costo	262.253.705
Duración	7 meses

Entidad	SECRETARÍA DISTRITAL DE MOVILIDAD
Contrato	CONTRATO No. 2023-2705
Objeto	REALIZAR LA GESTIÓN Y MONITOREO DE LA SEGURIDAD INFORMÁTICA SOBRE LA PLATAFORMA TECNOLÓGICA DE LA SECRETARÍA DISTRITAL DE MOVILIDAD A TRAVÉS DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC)
Costo	621.082.296
Duración	6 meses

Entidad	FINANCIERA DE DESARROLLO TERRITORIAL S.A
Contrato	CON-0048-2021
Objeto	PRESTACIÓN DEL SERVICIO DE SEGURIDAD GESTIONADA SOPORTADO EN UN SOC (CENTRO DE OPERACIÓN DE SEGURIDAD) QUE INCLUYA LA RECOLECCIÓN, MONITOREO, ANÁLISIS, CORRELACIÓN Y GESTIÓN DE ALARMAS, EVENTOS E INCIDENTES.
Costo	1.378.400.930
Duración	36 (Meses)

12.2.- Análisis de histórico de contrataciones de la entidad.

La Unidad de Planeación Minero-Energética – UPME consultó el histórico de contratación de la Entidad con el fin de identificar los valores de los contratos de los bienes o servicios similares al de la presente contratación, sin embargo, revisando los procesos de contratación de la UPME no se encuentra un proceso de contratación similar, por lo cual se genera una base de referencia soportado en el ítem 12.1.- Análisis de contrataciones similares en entidades públicas.

12.3.- Sondeo de Mercado

De conformidad con la causal de contratación directa, se realizó el siguiente sondeo de mercado, se solicitó cotización a cuatro empresas y se recibieron 3 cotizaciones, así:

Empresa	**Servicio a un año**	**Valor del Servicio IVA incluido**
FORTINET	Servicios de un Centro de Operaciones de Seguridad SOC para realizar la gestión y el monitoreo de la infraestructura tecnológica y la gestión de eventos e incidentes de seguridad + SIEM VIRTUALIZADO PERPETUO PARA 1500 EPS	$638.978.505,64
NEOSECURE	Servicios de un Centro de Operaciones de Seguridad SOC para realizar la gestión y el monitoreo de la infraestructura tecnológica y la gestión de eventos e incidentes de seguridad.	$196.922.871,00

RTM	Servicios de un Centro de Operaciones de Seguridad SOC para realizar la gestión y el monitoreo de la infraestructura tecnológica y la gestión de eventos e incidentes de seguridad + NDR Network Detection and Response	$147.740.900,00

Conclusión

De lo anterior se concluye que el valor para la presente contratación se encuentra ajustado al Mercado y, es coherente con lo que la Entidad y/u otras, ha pagado por servicios o bienes similares en años anteriores, con los correspondientes incrementos de ley.

13.- JUSTIFICACIÓN DE LOS FACTORES TÉCNICOS DE SELECCIÓN QUE PERMITEN IDENTIFICAR LA OFERTA MÁS FAVORABLE

El factor de selección que permitió identificar que la oferta presentada por la empresa Redes Tercer Milenio SAS es la más favorable radica en que adicional a ser la de menor costo y ofrecer los servicios de SOC requeridos en la presente solicitud, la empresa también nos ofrece el servicio de monitoreo de red, lo que permite ampliar el rango de gestión, seguimiento, seguridad y operación de la UPME.

Por otra parte la Entidad actualmente cuenta con el servicio de EDR Endpoint Detection and Response (EDR) que es un enfoque integrado en capas para la protección de endpoints que combina el monitoreo constante en tiempo real y el análisis de datos de endpoints con una respuesta automatizada basada en reglas, esta solución se complementa con el servicio de centro de operaciones de seguridad (SOC) requerido en el presente proceso de contratación, dado que desde la actual consola podemos realizar el monitoreo continuo de la plataforma tecnológica de la UPME detectando y respondiendo a posibles amenazas y/o incidentes de seguridad con la integración del firewall palo alto, la protección de correo, y la inclusión de la solución de NDR (Network Detection and Response) que es el valor agregado que nos brindan a través de la suite de herramienta de SOPHOS, brindándonos un servicio SOC 24/7 sobre la infraestructura de la UPME (endpoints, servidores, dispositivos de red y correo), servicio totalmente gestionado prestado por expertos que detectan y responden a ciberataques dirigidos contra sus ordenadores, servidores, redes, cargas de trabajo en la nube, cuentas de correo electrónico y más.

14.- PRESUPUESTO ASIGNADO Y VALOR MÁXIMO DEL CONTRATO:

De conformidad con lo precedido, el presupuesto asignado para esta contratación es de $147.740.900 que se pagará con cargo al:

Rubro: C-2199-1900-5-0-2199067-02
Recurso: 20 Ingresos Corrientes.
Del presupuesto de. Inversión

Rubro: C-2199-1900-5-0-2199066-02
Recurso: 20 Ingresos Corrientes.
Del presupuesto de. Inversión

Este valor incluye todos los costos asociados, directos e indirectos, IVA sí hay lugar, retención en la fuente y cualquier otro costo o impuesto en que incurra el contratista para la ejecución de la presente orden o contrato.

INFORMACIÓN SOBRE EL PROYECTO DE INVERSIÓN

Sección: Plan Anual de Adquisiciones - PAA	
¿Está incluido en el PAA?	Ítem 130-30 y 130-59

Sección: Información Proyecto de Inversión: Ítem 130-30	
(1) Proyecto de Inversión	C-2199-1900-5 Fortalecimiento de los Servicios Digitales Aumentando la Capacidad para la Transformación Digital e Interacción con el Ciudadano Nacional.
(2) Objetivo Específico Proyecto de Inversión:	2 - Aumentar la capacidad institucional a nivel de arquitectura tecnológica y de sistemas de información
(3) Producto de Inversión.	C-2199-1900-5-0-2199067-02 1 - SERVICIOS TECNOLÓGICOS
(4) Actividad Proyecto de Inversión:	Administrar de manera eficiente el Software a nivel Institucional, de cara a la mejora de los productos y servicios prestados a la ciudadanía.
(5) Recursos	20 Ingresos Corrientes
Valor	$88.228.499

Sección: Información Proyecto de Inversión : Ítem 130-59	
(1) Proyecto de Inversión	C-2199-1900-5 Fortalecimiento de los Servicios Digitales Aumentando la Capacidad para la Transformación Digital e Interacción con el Ciudadano Nacional.
(2) Objetivo Específico Proyecto de Inversión:	1 - Incrementar el desarrollo de los habilitadores transversales de la política de gobierno digital
(3) Producto de Inversión.	1 - DOCUMENTO PARA LA PLANEACIÓN ESTRATÉGICA EN TI C-2199-1900-5-0-2199066-02
(4) Actividad Proyecto de Inversión:	Mantener y fortalecer el modelo Operativo de TI
(5) Recursos	20 Ingresos Corrientes
Valor	$74.941.884

15.- FORMA DE PAGO

El valor del contrato/orden se pagará en un único pago contra las licencias que certifiquen la activación del SOC y documento de compromisos de realizar actividades de monitoreo, durante el tiempo de vigencia de la licencia (12 meses), previa radicación de la cuenta de cobro o factura electrónica correspondiente, si hay

lugar, acompañada del certificado del pago de los aportes a la Seguridad Social Integral y Parafiscales, expedida por el Representante Legal o el Revisor Fiscal (cuando aplique).

16.- PLAZO ESTIMADO DE LA EJECUCION DEL CONTRATO

El plazo de ejecución será de 3 meses, contados a partir del día hábil siguiente a la expedición del registro presupuestal o aprobación de garantía, si hay lugar a solicitarla, o hasta el 31 de diciembre de 2023, los que primero ocurra; sin embargo las licencias tendrán una vigencia de 12 meses a partir de la activación y el soporte estará activo durante este periodo.

17. ESTIMACIÓN, TIPIFICACIÓN Y ASIGNACIÓN DE RIESGOS PREVISIBLES INVOLUCRADOS EN LA PRESENTE CONTRATACIÓN Y DESARROLLO DEL PROCESO

Los riesgos que puedan afectar el equilibrio económico del contrato a celebrar, se estiman, tipifican y asignan de acuerdo con el Formato de tipificación, estimación y asignación de riesgos, de conformidad con la siguiente tabla:

Tabla Estimación, tipificación y asignación riesgos

No.	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 contrato?	Responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se completa el tratamiento	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración	Categoría					¿Cómo se realiza el monitoreo?	Periodicidad
1	General	Interno	Pre-Contratación	Operacional	**Retraso en la consecución de documentos o en la firma del contrato**	**Retraso en la ejecución del contrato**	2	3	5	Medio	Contratista	Requerimientos y ajuste del cronograma de ejecución	1	2	3	Bajo	Si	Grupo de contratación	**Desde la adjudicación o selección**	**Mediante requerimientos, correos electrónicos**	Inmediatamente	Diaria
2	General	Interno	Pre-Contratación	Operacional	**Retraso en la presentación de las garantías**	**Retraso en la ejecución del contrato**	2	3	5	Medio	Contratista	Requerimientos y ajuste del cronograma de ejecución	1	2	3	Bajo	Si	Grupo de contratación	**Desde la adjudicación o selección**	**Mediante requerimientos, correos electrónicos**	Inmediatamente	Diaria
3	Específico	Externo	Ejecución	Operacional	**Demora en la prestación del servicio**	**Retraso en la ejecución del contrato**	3	3	6	Alto	Contratista	Efectuar seguimiento permanente por parte del supervisor del contrato para que se un adecuado cumplimiento al objeto del contrato	2	3	5	Medio	Si	Contratista Entidad	**Desde el inicio del contrato**	**Mediante informes.**	Cuando ocurra.	Diario

Tabla Estimación, tipificación y asignación riesgos

No.	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 contrato?	Responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se completa el tratamiento	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración	Categoría					¿Cómo se realiza el monitoreo?	Periodicidad
4	Especifico	Externo	Ejecución	Operacional	**No contar con el personal certificado y calificado para la prestación del servicio**	**Poner en riesgo a la entidad debido a que no se cuente con el personal calificado para el desarrollo del contrato.**	3	2	5	Medio	Contratista	Efectuar seguimiento permanente por parte del supervisor del contrato Demostrar la idoneidad de la persona Garantías	2	2	4	Bajo	Si	Contratista	Desde la firma del acta de inicio	Mediante informes y certificado de cumplimiento a satisfacción	Cuando ocurra.	Cuando ocurra
5	Especifico	Externo	Ejecución	Operacional	**Cambio de profesionales del Grupo de Trabajo**	**Cambio del profesional, previa verificación de cumplimiento de requisitos de los TdR.**	3	3	6	Alto	Contratista	Efectuar seguimiento permanente por parte del supervisor del contrato – Realizar requerimientos de cumplimiento	2	3	5	Medio	Si	Contratista y Entidad	Desde el inicio de ejecución	Mediante informes.	Cuando ocurra.	Cuando ocurra
6	Especifico	Externo	Ejecución	Operacional	**No pago de las obligaciones a proveedores, salarios y seguridad social del personal a cargo**	**Demora en las labores diarias y misionales de la entidad y por consecuencia a él o los usuarios finales.** **Incumplimiento contractual**	2	2	4	Bajo	Contratista	Garantías No efectuar el pago hasta que no cumpla con los requisitos exigidos por la normatividad.	2	1	3	Bajo	Si	Supervisor del contrato	Desde el comienzo de la ejecución del contrato	Mediante informes y certificado de cumplimiento a satisfacción	Cuando ocurra.	Cuando ocurra

18. GARANTÍAS.

El contratista deberá constituir una garantía que cubra los siguientes riesgos:

Clase de Riesgos	%	Sobre el valor	Vigencia
Cumplimiento del contrato	20	Del contrato	La del contrato y seis (6) meses más.
Calidad del servicio	20	Del contrato	La del contrato y un (1) año más.
Responsabilidad Civil Extracontractual	200 SMMLV	---	Desde la firma del contrato, hasta el término del contrato.

19. LUGAR DE EJECUCIÓN

El desarrollo del contrato/orden será en la(s) ciudad(es) de Bogotá.

20. SUPERVISIÓN

La supervisión del contrato/orden será ejercida por: Claudia Marcela Beltrán Bermúdez Profesional Especializado Grado 15.

21. RELACIÓN ESPECÍFICA DEL OBJETO Y/U OBLIGACIONES CON EL PROYECTO DE INVERSIÓN QUE LO FINANCIA

ÍTEM PAA: 130-30 y 130-59

El proyecto de inversión: "Fortalecimiento de los servicios digitales aumentando la capacidad para la transformación digital e interacción con el ciudadano", el cual define como una de las estrategias a desarrollar adelantar proyectos enmarcados en la definición, implementación y sostenimiento del sistema de gestión de seguridad de la información, de acuerdo con el MSPI (modelo de seguridad y privacidad de la información), así como el uso de la infraestructura tecnológica para el procesamiento y almacenamiento de la información institucional, lo anterior, considerando que la información es el activo más importante de la entidad.

Para desplegar la estrategia anteriormente mencionada, el proyecto se plantea como uno de sus objetivos específicos *aumentar la capacidad institucional a nivel de arquitectura tecnológica y de sistemas de información* y la actividad *de administrar de manera eficiente el Software a nivel Institucional, de cara a la mejora de los productos y servicios prestados a la ciudadanía*, dentro de la cual se efectúa la planeación, programación, asignación de recursos, ejecución, seguimiento y entrega de proyectos de software, el cual contempla la implementación de un servicio de administración de la información.

Así mismo, el proyecto anteriormente mencionado se plantea como uno de sus objetivos específicos "Incrementar el desarrollo de los habilitadores transversales de la política de gobierno digital" y la actividad "Mantener y fortalecer el modelo Operativo de TI", se pretende incrementar la efectividad en la prestación de servicios de TI, se requiere fortalecer el modelo operativo de TI y la prestación de servicios integrales de tecnología.

22. VALIDACIÓN DEL GIT DE PLANEACIÓN. Este numeral lo diligencia el GIT Planeación.

Concepto de Planeación para inversión	
Capacidad de respuesta	¿Cuenta con la capacidad operativa para la recepción y supervisión de los productos derivados? Si x No
Coherencia con el PEI	Objetivo Estratégico: El Plan Estratégico Institucional estuvo vigente hasta el año 2022, en la actualidad se encuentra en proceso de planeación para su construcción.
	Estrategia: El Plan Estratégico Institucional estuvo vigente hasta el año 2022, en la actualidad se encuentra en proceso de planeación para su construcción.

	Alineación del objetivo estratégico con la estrategia El Plan Estratégico Institucional estuvo vigente hasta el año 2022, en la actualidad se encuentra en proceso de planeación para su construcción
Coherencia con el proyecto de inversión	* El objeto contractual guarda coherencia con el proyecto de inversión y sus actividades. Si x No * Los productos a recibir guardan coherencia con los estipulados en el proyecto de inversión. Si x No
Viabilidad presupuestal	El proyecto de inversión cuenta con disponibilidad presupuestal Si x No
Observaciones	

Vo.Bo. Planeación: 28/09/2023 - Oliver Quintero Perdomo – Coordinador (E) del GIT de Planeación

23. DOCUMENTOS ANEXOS

- Radicado Memo Solicitud de CDP y CDP.
- Cotizaciones del estudio de mercado.

Cordialmente,

Elaboró	Claudia Marcela Beltrán Bermúdez- Profesional Especializado Grado 15. Oficina de Gestión de la Información
Revisó	María Alejandra Núñez Briñez- Contratista Oficina de Gestión de la Información
Aprobó	John Alejandro Barrios Ávila- Jefe (E) Oficina de Gestión de la Información

24.- CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Fecha	**Versión**	**Descripción de los cambios**
18/09/2023	01	Se crea el formato conforme la plantilla.