ANALISIS DEL SECTOR

1. **OBJETO:** CONSULTORÍA PARA ACTUALIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI, Y LA REALIZACIÓN DEL ANÁLISIS DE VULNERABILIDADES Y HACKING ÉTICO PARA LOS ACTIVOS DE INFORMACIÓN.

2. **JUSTIFICACIÓN DE LA NECESIDAD:** La Personería de Bogotá D.C., en virtud de sus atribuciones establecidas en el Decreto Ley 1421 de 1993 y el Acuerdo Distrital 034 de 1993, desarrolla funciones como Agente del Ministerio Publico, Veedor Ciudadano y Defensor de los Derechos Humanos; es un Organismo de Control que hace presencia en la Capital a través de sus funcionarios en cada una de sus sedes y puntos de atención, con la finalidad de atender en forma oportuna y eficiente a la inmensa población que acude a la entidad para solicitar la protección de sus derechos, lo cual hace que se gestione gran cantidad de datos y de información frente a los requerimientos y peticiones de la comunidad, haciendo que para el correcto funcionamiento de la entidad se requiera resguardar la información de manera eficiente y efectiva.

   En este sentido, y en el marco estratégico, lineamientos y ejes de acción de LA PERSONERIA DE BOGOTA, D.C. prioriza el impulso en el uso y apropiación de las tecnologías de información y las comunicaciones, a través de la consolidación de un ecosistema de aplicaciones y servicios que soporten los procesos, y que se conviertan en fuente única de datos útiles para apoyar o argumentar las decisiones institucionales. De esta manera, se hace de vital importancia el preservar la confidencialidad, integridad y disponibilidad de los datos tratados.

   Por lo tanto, se plantea la necesidad de fortalecer el ámbito de la seguridad y privacidad de la información de la entidad, en base a normas técnicas como la ISO27001, el Modelo de Seguridad y Privacidad de la Información (MSPI), y este a su vez el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y la Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas; este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital, que busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, tramites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información.



De la misma manera, a través de la Resolución 406 de 2020, mediante la cual se adopta el Modelo Integrado de Planeación y Gestión MIPG, estableciendo en su artículo 22, que el Director de Tecnologías de la Información y las Comunicaciones es la responsable de liderar la ejecución del Sistema de Gestión de Seguridad de la Información – SGSI, el cual se define como el "Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Por tal razón, y en ejercicio de la mejora continua y el fortalecimiento de la seguridad de la información a través del avance en la implementación del Sistema de Gestión de Seguridad de la Información SGSI, la entidad requiere realizar una CONSULTORÍA PARA ACTUALIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI, Y LA REALIZACIÓN DEL ANÁLISIS DE VULNERABILIDADES Y HACKING ÉTICO PARA LOS ACTIVOS DE INFORMACIÓN.

3. ESPECIFICACIONES TÉCNICAS

3.1. GLOSARIO DE TÉRMINOS

Teniendo en cuenta las características técnicas específicas del proyecto a contratar, se determina construir un glosario de términos que facilite la comprensión de la necesidad y el objeto del presente proceso de contratación.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Ethical Hacking: Técnicas informáticas aprobadas y controladas por la Entidad, para identificar, y en algunos casos explotar vulnerabilidades en un sistema informático.

OSSTMM: Open Source Security Testing Methodology Manual (por sus siglas en inglés), corresponde a la Metodología de Pruebas de Seguridad de Código Abierto.

OWASP: Open Web Application Security Project (por sus siglas en inglés), corresponde a la metodología abierta de seguridad de aplicaciones web.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Declaración de aplicabilidad (SOA): Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Análisis de brecha – GAP: en el contexto del proceso contractual, corresponde a la evaluación del estado actual y el estado objetivo del SGSI, que incluya el análisis de necesidades, determinando la distancia existente y los recursos necesarios para alcanzar los objetivos.

Criticidad: Corresponde al nivel de sensibilidad del activo en términos de confidencialidad, integridad y disponibilidad. Es decir, que tan crítico es que se divulgue, modifique o elimine.

Informática forense: Aplicación de la ciencia para la identificación, recolección, examen y análisis de los datos, preservando correctamente su integridad, llevando a cabo a su vez una estricta cadena de custodia de la información.

Cadena De Custodia: Su objetivo principal es demostrar 3 aspectos: El primero, que la información o evidencia está intacta al momento de presentarse, segundo, que la hora y fecha en la que se hace entrega al proveedor o las autoridades sea

exacta y tercero, que no fue manipulada o alterada mientras se encontraba en custodia del proveedor.

3.2. ESPECIFICACIONES Y CONDICIONES TÉCNICAS

La presente contratación estará enmarcada en dos (2) aspectos:

- Definición de las fases
- Equipo de Trabajo Mínimo Requerido

3.2.1. Definición de las fases:

A continuación de describe cada una de las fases propuestas para el desarrollo del objeto del contrato, con los productos a entregar y el contenido de cada producto.

FASE I: DIAGNOSTICO		
OBJETIVO	**ACTIVIDADES**	**PRODUCTOS**
Elaborar la actualización del análisis GAP (análisis de brecha) frente a la norma ISO 27001 y el Modelo de seguridad y privacidad de la información MSPI, que permita determinar el estado actual de la Gestión de Seguridad y Privacidad de la Información en la PERSONERIA DE BOGOTA, referente a los procesos misionales de la entidad.	Identificar y entender el contexto interno y externo de LA PERONERIA, partes interesadas y factores críticos de éxito. A través de entrevistas y recopilación de documentación con las personas responsables de liderar la operación de cada uno de los procesos, se pretende: - Actualizar la operación de la entidad con relación al flujo de información y los activos que la soportan, en los procesos misionales e identificar los responsables del SGSI, las tecnologías utilizadas y terceras partes involucradas. - Actualizar el contexto de los procesos misionales, de la entidad teniendo en cuenta los factores internos y externos que puedan afectar la información en términos de disponibilidad, integridad y confidencialidad.	- Documento con la actualización del diagnóstico de la situación actual e Identificación de brechas ISO/IEC 27001:2013 y MSPI (Modelo de seguridad y Privacidad de la Información del MINTIC). - Documento de recomendaciones sobre las brechas identificadas con el instrumento de evaluación y nivel de madurez en línea base de seguridad MSPI (Modelo de seguridad y Privacidad de la Información del MINTIC). - Documento con el análisis del contexto de la entidad que determine los elementos externos e internos que son relevantes con las actividades que realiza la Entidad en el desarrollo de su misión y que podrían influir en las capacidades para lograr los objetivos del modelo, alineado con los objetivos estratégicos de la Entidad.

FASE II: PLANIFICACIÓN		
OBJETIVO	**ACTIVIDADES**	**PRODUCTOS**
Actualizar políticas y procedimientos de seguridad conforme a la estructura propuesta por la norma ISO 27001 de 2013 y alineados al Modelo Integrado de Planeación y Gestión MIPG y los requisitos establecidos en la guía para la elaboración de documentos controlados de la Entidad.	- Actualizar la Política y los Procedimientos de Seguridad de la Información. - Actualizar los roles y responsabilidades de Seguridad y Privacidad de la Información - Actualizar el Plan Estratégico de Seguridad de la Información de forma general.	- Documentos con la actualización y/o construcción de políticas, procedimientos, guías, plantillas, formatos e Instructivos de Seguridad de la Información, en cumplimiento con los requisitos y respetando la estructura propuesta por la norma ISO 27001 de 2013 y acorde con los requisitos establecidos en la guía para la elaboración de documentos controlados del Modelo Integrado de Planeación y Gestión MIPG de la Personería de Bogotá, D.C. - Actualización de los resultados del análisis GAP (análisis de brecha). - Actualización de las normativas que deba satisfacer la PERSONERIA DE BOGOTA. - Propuesta de acto administrativo (Resolución, circular, decreto, entre otros), indicando los roles y sus responsabilidades frente a la seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) y la creación del Comité de Seguridad de la información y el rol de Oficial de Seguridad de la Información con sus correspondientes funciones.

FASE III: ACTUALIZACION Y ANÁLISIS DE RIESGOS		
A. Identificación de activos de información		
OBJETIVO	**ACTIVIDADES**	**PRODUCTOS**
- Validar y actualizar los activos de información de los procesos	- Validar y actualizar los activos de información, según la norma ISO 27005 y la guía	- Documento con la actualización del Inventario de activos de

misionales de LA PERSONERIA DE BOGOTA, D.C. - Actualizar la matriz de clasificación de los activos de información de acuerdo con los requerimientos de confidencialidad definidos y establecer los requerimientos exigidos por la norma ISO 27001:2013 y normas relacionadas ISO 27002 e ISO 27005 así como la guía para la gestión y clasificación de activos de información de MINTIC	para la gestión y clasificación de activos de información de MINTIC. Estos se clasifican en dos tipos: Primarios y de apoyo: **Primarios:** • Información (Datos e Información Impresa). • Procesos y actividades de la operación **Apoyo:** • Hardware (Equipos informáticos) • Software (Aplicaciones) • Redes de comunicaciones • Personal • Medios de Almacenamiento • Servicios de Terceros - Actualizar los posibles impactos de seguridad que afectarían a la PERSONERIA DE BOGOTA o a los objetivos de la operación que se deriven directamente de la divulgación de información sensible. - Actualizar las reglas para medir los niveles de confidencialidad de los activos de información identificados en los procesos misionales de la entidad.	información de los procesos misionales la entidad. - Documento con el Inventario de bases de datos personales.

FASE III: ACTUALIZACION Y ANÁLISIS DE RIESGOS		
B. Análisis de riesgos de seguridad de la información		
OBJETIVO	**ACTIVIDADES**	**PRODUCTOS**
Actualizar el mapa de riesgos de seguridad de la información de los procesos misionales de la entidad, con base en los lineamientos establecidos en la norma ISO 31000, ISO 27005:2008 y Guía de Administración del Riesgo del Departamento Administrativo de la función pública y acorde con la guía para la administración del riesgo de la Personería de Bogotá, D.C.	Con base en el levantamiento de los activos de información se deberá proceder a actualizar el análisis de riesgos, en base a las actividades de: - Identificación del Nivel de riesgo Aceptable. - Revisión del plan de tratamiento de Riesgos. - Determinar la declaración de aplicabilidad, en concordancia con la cláusula 6.1.3 de ISO 27001 versión 2013.	- Documento con la actualización del Plan de tratamiento de riesgos de seguridad de la información. - Documento con la actualización del Informe de Análisis de riesgos para los procesos definidos en el alcance. - Documento de actualización de la declaración de aplicabilidad (SOA)

FASE III: ACTUALIZACION Y ANÁLISIS DE RIESGOS		
C. Actualización del modelo de medición del SGSI		
OBJETIVO	**ACTIVIDADES**	**PRODUCTOS**
Actualizar los indicadores (métricas) adecuados para medir la madurez, eficiencia, eficacia, implantación o impacto de controles de seguridad de la información. Se deberá tener como referencia la norma ISO 27004:2016	Actualizar las métricas e indicadores adecuados que resulten útiles para el seguimiento de los resultados. Una vez aprobado por la Entidad las métricas e indicadores, se deberá ejecutar procedimiento de medición abarcando los indicadores actualizados.	- Actualización del (de los) documento(s) de indicadores de gestión de acuerdo con las dimensiones del modelo de seguridad y privacidad de la información de MINTIC. - Actualización del documento que contenga el modelo de medición del SGSI (Sistema de Gestión de Seguridad de Información) y MSPI (Modelo de Seguridad y privacidad de la Información del MINTIC).

FASE III: ACTUALIZACION Y ANÁLISIS DE RIESGOS		
D. Auditoria de seguimiento ISO 27001		
OBJETIVO	**ACTIVIDADES**	**PRODUCTOS**
Evaluación técnica y de gestión de la conformidad bajo los lineamentos de la norma ISO-27001	Realizar las acciones de auditoria parte interna y gestionar la realización de la auditoria de tercera parte para la gestión y control de los riesgos de la seguridad de la información en entidad para el proceso de direccionamiento TIC.	- Documento con el informe de resultados de auditoría y recomendaciones sobre los hallazgos y/o acciones de mejora que se deben realizar.

FASE IV: IMPLEMENTACIÓN Y ANÁLISIS DE RIESGOS		
E. HACKING ÉTICO Y ANÁLISIS DE VULNERABILIDADES		
OBJETIVO	**ACTIVIDADES**	**PRODUCTOS**
Mediante estas pruebas se busca evidenciar las vulnerabilidades que existen dentro de la configuración física y lógica de los sistemas informáticos de la entidad.	Realizar un ejercicio de Ethical Hacking y el análisis de vulnerabilidades, sobre los diferentes elementos tecnológicos de la entidad tanto a nivel externo como interno. El ejercicio de Ethical Hacking, deberá contener: • Recolección de información. • Identificación de sistemas y servicios. • Identificación y verificación de vulnerabilidades. • Presentación informe de resultados. El ejercicio de Ethical Hacking deberá realizarse con las siguientes metodologías: **a)** Realizar pruebas de Hacking Ético con el uso de la metodología OSSTMM v3. **b)** Realizar pruebas sobre aplicaciones Web con el uso de la metodología OWASP, como mínimo se deberán	Informe final de Hacking Ético y las recomendaciones que se dan a conocer a la PERSONERIA DE BOGOTA sobre las pruebas de hacking ético definidas, con el siguiente alcance mínimo: • 20 servidores • 15 aplicaciones misionales • 5 aplicaciones administrativas • Hasta 5 dispositivos de seguridad perimetral con IP pública configurada. • 5 dispositivos de red y/o comunicaciones. • 5 equipos de cómputo cliente usuario. Documento en idioma español que incluya como mínimo: • Descripción de las pruebas • Listado de vulnerabilidades encontradas • Descripción de las vulnerabilidades y nivel de la criticidad. • Acciones de mitigación de las vulnerabilidades detectadas • Recomendaciones con el paso a paso para remediar cada vulnerabilidad.

FASE IV: IMPLEMENTACIÓN Y ANÁLISIS DE RIESGOS		
E. HACKING ÉTICO Y ANÁLISIS DE VULNERABILIDADES		
OBJETIVO	**ACTIVIDADES**	**PRODUCTOS**
	realizar las siguientes pruebas: • Ataque de inyección de código malicioso (XSS) • Autenticación y Gestión de Sesiones • Referencias inseguras a objetos directos • Configuración errónea de Seguridad • Redirecciones y reenvíos no validados El análisis de vulnerabilidades deberá contener como mínimo: • Pruebas de patchlevel, de sistemas operativos y aplicaciones • Pruebas de registro de Windows • Pruebas de IDS-IPS (Intrusion Detection System-Intrusion Prevention System), Routers, Switches • Pruebas de Hosts y redes VPN • Escaneo de host virtuales • Análisis externo e interno	• Plan de acción para reducir las brechas encontradas Documento en idioma español y formato Excel con la relación de vulnerabilidades identificadas para cada uno de los activos analizados, por niveles de criticidad y con las acciones y recomendaciones para la remediación de cada una de ellas. Informe Ejecutivo: • Descripción de las tareas llevadas a cabo para cada una de las actividades • Información recopilada en el proceso • Conclusiones del estudio • Recomendaciones asociadas.

FASE V: CIERRE		
OBJETIVO	**ACTIVIDADES**	**PRODUCTOS**
Verificar la entrega de los productos requeridos por la Entidad en el marco de la ejecución contractual.	Revisar y verificar todos los productos correspondientes a cada una de las fases.	Todos los productos deben ser entregados en su última versión, y se verifican con la relación de productos definidos en cada fase. • Repositorio Final. • Documentación final con todos los productos en su última versión.

3.2.2. Equipo de Trabajo Mínimo Requerido

Integrante	Formación y Certificaciones	Experiencia
Gerente de Proyecto	Título profesional en Ingeniería de Sistemas, Telemática, Electrónica o Administración de Sistemas de Información. Título de posgrado en la modalidad de especialización o maestría en Gestión de Proyectos de TI, Gerencia de Proyectos de Sistemas de información, Gerencia de Proyectos, Gerencia de Proyectos de sistemas, Gestión de proyectos, dirección de proyectos. Con certificación Gerente líder de proyectos ISO 21500:2021 o Certificación PMP (Project Management Professional)	Mínimo ocho (8) años de experiencia profesional certificada, contada a partir de la fecha de expedición de la matrícula profesional. Experiencia específica en el rol de gerente o director, o coordinador de proyectos, de mínimo tres (3) proyectos diferentes y terminados, relacionados con Seguridad de la información o Seguridad informática o ciberseguridad.
Consultor Senior de Seguridad	Título profesional en Ingeniería de Sistemas, Telemática, Electrónica o Administración de Sistemas de Información. Título de posgrado en la modalidad de especialización o maestría en seguridad de la información, seguridad Informática, seguridad de las tecnologías de la información y las comunicaciones, seguridad informática y de las comunicaciones, en seguridad de la información e informática. Con certificaciones: Auditor Líder ISO/IEC 27001:2013 Auditor Líder ISO/IEC 27032:2012	Mínimo ocho (8) años de experiencia profesional certificada, contada a partir de la fecha de expedición de la matrícula profesional. Experiencia específica en el rol de consultor o líder de seguridad de mínimo tres (3) proyectos diferentes y terminados, relacionados con Seguridad de la información o Seguridad informática o ciberseguridad.
Consultor Junior de Seguridad	Título profesional en Ingeniería de Sistemas, Telemática,	

	Electrónica o Administración de Sistemas de Información. Título de posgrado en la modalidad de especialización o maestría en seguridad de la información, seguridad Informática, seguridad de las tecnologías de la información y las comunicaciones, seguridad informática y de las comunicaciones, en seguridad de la información e informática. Con certificaciones: Implementador Líder ISO/IEC 27003:2017 Auditor técnico seguridad de información ISO/IEC 27007:2020 – ISO/IEC 27008:2019	Mínimo tres (6) años de experiencia profesional certificada, contada a partir de la fecha de expedición de la matrícula profesional. Experiencia específica en el rol de experto o analista o ingeniero de riesgos de seguridad de información o aplicaciones, de mínimo tres (3) proyectos diferentes y terminados, relacionados con Seguridad de la información o Seguridad informática o ciberseguridad.
Analista de Seguridad de la Información	Título profesional en Ingeniería de Sistemas, Telemática, Electrónica o Administración de Sistemas de Información. Título de posgrado en la modalidad de especialización o maestría en seguridad de la información, seguridad Informática, seguridad de las tecnologías de la información y las comunicaciones, seguridad informática y de las comunicaciones, en seguridad de la información e informática. Con certificación CISM (Certified Information SecurityManager).	Mínimo cinco (5) años de experiencia profesional certificada, contada a partir de la fecha de expedición de la matrícula profesional. Experiencia específica en el rol de analista, consultor o líder de seguridad de mínimo tres (3) proyectos diferentes y terminados, relacionados con Seguridad de la información o Seguridad informática o ciberseguridad.
Analista Pruebas ETH y vulnerabilidades	Título profesional en Ingeniería de Sistemas, Telemática, Electrónica o Administración de Sistemas de Información.	Mínimo cinco (5) años de experiencia profesional certificada, contada a partir de la fecha de expedición de la matrícula profesional.

	Con certificación CEH (Certified Ethical Hacker - EC-Council)	Experiencia específica en el rol de analista, consultor o líder de pruebas de Ethical Hacking o pruebas de vulnerabilidades de mínimo tres (3) proyectos diferentes y terminados, relacionados con Seguridad de la información o Seguridad informática o ciberseguridad.

4. OBLIGACIONES DEL CONTRATISTA:

a) Específicas

En el desarrollo del objeto contractual, EL CONTRATISTA se compromete a cumplir las siguientes obligaciones específicas:

1. Elaborar el análisis de brecha (GAP) frente a la norma ISO 27001:2013 y el Modelo de Seguridad y Privacidad de la Información del MINTIC.
2. Diseñar y/o actualizar políticas y procedimientos de seguridad conforme a la Norma ISO 27001:2013, teniendo en cuenta los lineamientos definidos en el Modelo Integrado de Planeación y Gestión MIPG de la Personería.
3. Construir el documento manual de políticas y procedimientos de seguridad de la información, con base en la Norma ISO 27001:2013, teniendo en cuenta los lineamientos definidos en el Modelo Integrado de Planeación y Gestión MIPG de la Personería.
4. Actualizar y/o construir la matriz de activos para los procesos misionales de la entidad, teniendo en cuenta la clasificación y criticidad con base en la Norma ISO 27001:2013 y la Guía para la gestión y clasificación de activos de información de MINTIC.
5. Identificar y describir los posibles impactos de seguridad que afectarían a la PERSONERIA DE BOGOTÁ, D.C. y/o a los objetivos de operación y que se deriven directamente de la divulgación de la información.
6. Elaborar y/o actualizar el mapa de riesgos de seguridad de la información de los procesos contemplados en el alcance, con base en los lineamientos establecidos en la norma ISO 31000, ISO 27005:2008, la Guía de Administración del Riesgo del Departamento Administrativo de la función pública DAFP y acorde con la guía para la administración del riesgo de la Personería de Bogotá, D.C.
7. Documentar el plan de tratamiento de riesgos de seguridad de la información para los procesos contemplados en el alcance.
8. Actualizar y/o construir la declaración de aplicabilidad SOA para la entidad.

9. Ajustar, crear, definir e implementar los indicadores (métricas) adecuados para medir la madurez, eficiencia, eficacia, implantación o impacto de controles de seguridad de la información.
10. Realizar actividades de análisis de vulnerabilidades y pruebas de Hacking ético, a los sistemas de información de la entidad de acuerdo con lo establecido en el anexo técnico.
11. Construir y presentar los informes (técnico y ejecutivo) de las pruebas del análisis de vulnerabilidades y Hacking ético.
12. Documentar las recomendaciones sobre aspectos a mejorar a nivel de cultura de seguridad.
13. Planificar, ejecutar documentar las auditorías realizadas a lo largo de la ejecución del contrato, que contenga los riesgos detectados y se propongan acciones preventivas y/o correctivas y/o reparación de defectos.
14. Realizar la auditoria parte interna y gestionar la realización de la auditoria de tercera parte para el proceso de direccionamiento TIC.
15. Proporcionar garantía y acompañamiento durante los 2 meses posteriores al término de ejecución del contrato, para verificar y acompañar el cierre de las brechas encontradas.

b) Generales

1. Dar cumplimiento a lo dispuesto en el artículo 50 de la Ley 789 de 2002 y Ley 828 de 2003, relacionadas con el Control a la evasión de los recursos parafiscales y demás concordantes vigentes o las que la reemplacen al momento de dar cumplimiento a la obligación, para el efecto debe acreditar para cada pago, que se encuentra al día en el pago de aportes parafiscales relativos al Sistema de Seguridad Social Integral, así como los propios del SENA, ICBF, y Cajas de Compensación Familiar cuando corresponda.

2. Suscribir la correspondiente acta de inicio en el momento que determine la Personería de Bogotá D. C.

3. Cumplir con los gastos e impuestos que se requieren para la suscripción, perfeccionamiento, legalización y ejecución del contrato.

4. Discriminar el IVA en caso de pertenecer al régimen común o esté obligado declararlo.

5. Garantizar en desarrollo del objeto contractual el cumplimiento de los programas y disposiciones del Sistema de Gestión Ambiental de la entidad, las disposiciones de la normatividad ambiental vigente y la adopción de conductas ambientales responsables.

6. Cumplir a cabalidad con las responsabilidades establecidas en el Decreto 1072 de 2015 para los efectos del Sistema de Gestión de la Seguridad y Salud en el

Trabajo SG-SST, y poner dicho plan de Seguridad y Salud en el Trabajo a disposición de la entidad cuando el supervisor del contrato lo requiera.

7. Cumplir, en el marco del desarrollo de las obligaciones contractuales con las medidas de bioseguridad que sean necesarias para mitigar cualquier factor de riesgo que pueda conllevar transmisión de la enfermedad por COVID-19.

8. Garantizar en el desarrollo del objeto contractual el cumplimiento de las disposiciones del Sistema de Gestión de Seguridad de la Información de la entidad, así como las disposiciones de la normatividad ambiental vigente.

9. Garantizar en desarrollo del objeto contractual el cumplimiento de las disposiciones del Sistema de Gestión de la Calidad de la entidad.

10. Contar con el personal idóneo que se requiera para atender y dar solución a las solicitudes realizadas por la Personería de Bogotá, D.C. en relación con el alcance y el objeto del contrato.

11. Guardar la debida reserva y confidencialidad sobre la información y el contenido de los documentos que deba conocer con ocasión de las actividades realizadas durante la ejecución del contrato, y firmar un acuerdo de confidencialidad con el fin de garantizar el cumplimiento de esta obligación.

12. Las demás que correspondan de acuerdo con la naturaleza del contrato.

5. NORMAS DE CONTRATACIÓN PÚBLICA

Estatuto General de Contratación - Ley 80 de 1993
Ley 1150 de 2007
Decreto Ley 019 de 2012
Ley 1474 de 2011
Ley 1712 de 2014
Decreto 1082 de 2015
Ley 57 de 1887 (Código Civil Colombiano)
Decreto 410 de 1971 (Código de Comercio Colombiano)

6. CLASIFICACIONES UNSPSC.

La clasificación UNSPSC es un sistema estándar de codificación adoptado por el Estado, diseñado para fines comerciales de compras y adquisiciones, el cual provee un esquema de directrices y parámetros que agrupa y desagrupa productos similares. Proporciona una manera fácil para las entidades compradoras de identificar necesidades de productos y servicios y oportunidades de negocio a futuros proveedores.

De acuerdo con el clasificador de bienes y servicios, la clasificación de los servicios que se pretenden contratar entidad es la siguiente:

NIVELES	NÚMERO	DESCRIPCIÓN
Segmento	80000000	Servicios de gestión, Servicios profesionales de empresa y Servicios administrativos
Familia	80100000	Servicios de Asesoría de Gestión
Clase	80101500	Servicios de consultoría de negocios y administración corporativa
Segmento	80000000	Servicios de gestión, Servicios profesionales de empresa y Servicios administrativos
Familia	80100000	Servicios de Asesoría de Gestión
Clase	80101600	Gerencia de Proyectos
Segmento	81000000	Servicios basados en ingeniería, investigación y tecnología
Familia	81110000	Servicios Informáticos
Clase	81111800	Servicios de sistemas y administración de componentes de sistemas

Fuente: Colombia Compra Eficiente – SECOP

7. ANÁLISIS DEL SECTOR:

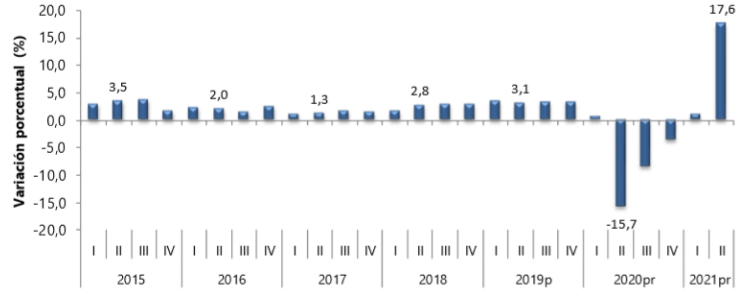
7.1. Análisis económico

7.1.1. Comportamientos Producto Interno Bruto (PIB) II trimestre de 2021

Para la economía colombiana el PIB ha crecido un 17.6% en su serie original respecto de mismo periodo del año 2020, según el Boletín Técnico del DANE del 17 de agosto de 2021.[1]

Producto Interno Bruto (PIB)
II trimestre 2021 preliminar

Gráfico 1. Producto Interno Bruto (PIB)
Tasas de crecimiento en volumen[1]
2015-I / 2021ᵖʳ-II



Las actividades económicas que más contribuyen a la dinámica del valor agregado son:

[1] https://www.dane.gov.co/index.php/estadisticas-por-tema/cuentas-nacionales/cuentas-nacionales-trimestrales/pib-informacion-tecnica

- Comercio al por mayor y al por menor; reparación de vehículos automotores y motocicletas; Transporte y almacenamiento; Alojamiento y servicios de comida crece 40,3% (contribuye 6,1 puntos porcentuales a la variación anual).

- Industrias manufactureras crece 32,5% (contribuye 3,5 puntos porcentuales a la variación anual).

- Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios; Actividades de los hogares individuales en calidad de empleadores; actividades no diferenciadas de los hogares individuales como productores de bienes y servicios para uso propio crece 83,8% (contribuye 1,9 puntos porcentuales a la variación anual).

Durante el primer semestre de 2021, respecto al mismo periodo del año anterior, el Producto Interno Bruto presenta un crecimiento 8,8%. Esta variación se explica principalmente por:

- Comercio al por mayor y al por menor; reparación de vehículos automotores y motocicletas; Transporte y almacenamiento; Alojamiento y servicios de comida crece 15,7% (contribuye 2,8 puntos porcentuales a la variación anual).

- Industrias manufactureras crece 18,2% (contribuye 2,1 puntos porcentuales a la variación anual).

- Administración pública y defensa; planes de seguridad social de afiliación obligatoria; Educación; Actividades de atención de la salud humana y de servicios sociales crece 6,4% (contribuye 1,1 puntos porcentuales a la variación anual)

Respecto al trimestre inmediatamente anterior, el Producto Interno Bruto en su serie corregida de efecto estacional y calendario decrece 2,4%. Esta variación se explica principalmente por la siguiente dinámica:

- Comercio al por mayor y al por menor; reparación de vehículos automotores y motocicletas; Transporte y almacenamiento; Alojamiento y servicios de comida decrece 6,7%.

- Industrias manufactureras decrece 5,3%.

- Construcción decrece 3,1%

DANE
INFORMACIÓN PARA TODOS

17 de agosto de 2021

Boletín Técnico
Producto Interno Bruto (PIB)
II trimestre 2021pr

1.1PIB desde el enfoque de la producción

Tabla 1. Valor agregado por actividad económica
Tasas de crecimiento en volumen[1]
2021pr– Segundo trimestre

Actividad económica	Tasas de crecimiento		
	Serie original		Serie corregida de efecto estacional y calendario
	Anual	Año corrido	Trimestral
	2021pr- II / 2020pr-II	2021pr / 2020pr	2021pr - II / 2021pr - I
Agricultura, ganadería, caza, silvicultura y pesca	3,8	3,8	0,0
Explotación de minas y canteras	7,1	-5,1	0,2
Industrias manufactureras	32,5	18,2	-5,3
Suministro de electricidad, gas, vapor y aire acondicionado[2]	9,1	3,7	-0,6
Construcción	17,3	3,6	-3,1
Comercio al por mayor y al por menor[3]	40,3	15,7	-6,7
Información y comunicaciones	10,0	6,3	2,6
Actividades financieras y de seguros	3,3	4,1	-0,3
Actividades inmobiliarias	2,1	1,9	0,2
Actividades profesionales, científicas y técnicas[4]	14,4	7,8	0,5
Administración pública, defensa, educación y salud[5]	9,0	6,4	2,4
Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios[6]	83,8	38,5	12,6
Valor agregado bruto	**17,1**	**8,6**	**-2,9**
Total impuestos menos subvenciones sobre los productos	22,1	11,2	1,6
Producto Interno Bruto	**17,6**	**8,8**	**-2,4**

7.1.2. Actividades de Información y Comunicaciones

En el segundo trimestre de 2021, el valor agregado de información y comunicaciones crece 10,0% en su serie original, respecto al mismo periodo de 2020. Para la serie corregida de efecto estacional y calendario, el valor agregado crece en 2,6%, respecto al trimestre inmediatamente anterior.

Tabla 8. Información y comunicaciones
Tasas de crecimiento en volumen[1]
2021pr– Segundo trimestre

Actividad económica	Tasas de crecimiento		
	Serie original		Serie corregida de efecto estacional y calendario
	Anual	Año corrido	Trimestral
	2021pr- II / 2020pr-II	2021pr / 2020pr	2021pr - II / 2021pr - I
Información y comunicaciones	**10,0**	**6,3**	**2,6**

Fuente: DANE, Cuentas nacionales

7.1.3. Actividades Profesionales, Científicas y Técnicas

En el segundo trimestre de 2021, el valor agregado de las actividades profesionales, científicas y técnicas; y actividades de servicios administrativos y de apoyo crece 14,4% en su serie original, respecto al mismo periodo de 2020. Esta dinámica se explica por los siguientes comportamientos:

- Actividades profesionales, científicas y técnicas crece 11,4%.
- Actividades de servicios administrativos y de apoyo crece 17,1%.

Respecto al trimestre inmediatamente anterior en su serie corregida de efecto estacional y calendario, el valor agregado de las actividades profesionales, científicas y técnicas; y actividades de servicios administrativos y de apoyo crece en 0,5%, explicado por:

- Actividades profesionales, científicas y técnicas crece 0,5%.
- Actividades de servicios administrativos y de apoyo decrece 1,1%.

Tabla 11. Actividades profesionales, cientificas y tecnicas[1]
Tasas de crecimiento en volumen[2]
2021[pr]– Segundo trimestre

Actividad económica	Tasas de crecimiento		
	Serie original		Serie corregida de efecto estacional y calendario
	Anual	Año corrido	Trimestral
	2021[pr]- II / 2020[pr]-II	2021[pr] / 2020[pr]	2021[pr] - II / 2021[pr] - I
Actividades profesionales, científicas y técnicas	11,4	6,6	0,5
Actividades de servicios administrativos y de apoyo	17,1	8,8	-1,1
Actividades profesionales, científicas y técnicas[1]	**14,4**	**7,8**	**0,5**

Fuente: DANE, Cuentas nacionales

7.1.4. Perspectiva Comercial

Las actividades económicas están divididas en sectores económicos de los cuales cada uno de ellos conserva características comunes, guardan una unidad y se diferencian de otras agrupaciones. Su división se realiza de acuerdo con los procesos de producción que ocurre al interior de cada uno de ellos.

La economía clásica establece que son tres los grandes sectores de la economía:

- Sector primario o sector agropecuario
- Sector secundario o sector industrial
- Sector terciario o sector de servicios

El sector analizado en el presente estudio se ubica dentro del sector terciario o de servicios, el cual relaciona las actividades relacionadas con los servicios no productores o transformadores de bienes materiales. Generan servicios que se

ofrecen para satisfacer las necesidades de cualquier población en el mundo. Entre los subsectores encontramos los siguientes: comercio, comunicación, tecnología, turismo, administración pública, finanzas, consultorio e interventoría, entre otros más.

De acuerdo con el objeto y las condiciones del presente proceso se determina que el sector económico a estudiar corresponde al Sector de comunicaciones o mejor conocido como Sector de tecnologías de la Información y las Comunicaciones, en el cual se incluyen servicios de consultoría y de análisis de sistemas informáticos. El sector de las tecnologías de la información y las comunicaciones se compone de diferentes actividades tanto industriales como de servicios y comerciales, a través de la fabricación, comercialización, distribución, instalación y soporte de hardware y software.

La industria de las tecnologías de la información y las comunicaciones demanda un alto nivel de investigación, avance tecnológico, nuevos desarrollos y capacitación de personas que sean capaces de satisfacer las necesidades resultantes de la expansión y crecimiento acelerado del sector de las tecnologías y las comunicaciones, así como los requerimientos de seguridad para proteger la información como uno de los activos más importantes para cualquier organización.

Las tecnologías de la información y las comunicaciones (TIC) se constituyen en un sector económico que al estar constituido por la creación, proceso, comunicación y transmisión de todo tipo de información (textual, imagen y sonido), tiene mucha incidencia en los procesos mentales que surgen durante la adquisición de conocimientos. Es un sector que, al estar entramado a las actividades humanas, requiere de innovación y de permanentes cambios, que lo hacen amigable a nuevos entornos y a las nuevas formas de producción de conocimientos.

La rápida evolución y adopción de las tecnologías de la información y las comunicaciones a nivel mundial y el creciente uso de herramientas informáticas para el desarrollo de las operaciones normales de los negocios y las funciones de las entidades públicas, han hecho que gobierno nacional implemente políticas públicas y estrategias con el fin de contrarrestar los riesgos, amenazas, vulnerabilidades e incidentes a los que se ven expuestas mediante el fortalecimiento de las capacidades de las entidades del estado para afrontar la amenazas que atentan contra la ciberseguridad nacional y la información institucional.

En el marco de estas políticas públicas como la “Política de Ciberseguridad y Ciberdefensa, y la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, la entidades estatales han implementado estrategias para su cumplimiento como son el fortalecimiento de su infraestructura tecnológica, y la implementación de buenas prácticas de TI, mediante las cuales se ha ido avanzando en el cumplimiento de los objetivos propuestos en materia de ciberseguridad y ciberdefensa.

Sumado a esto, tenemos la contingencia actual de salud pública ocasionada por el coronavirus COVID-19, la cual incrementó el teletrabajo y el trabajo en casa, y que, según los expertos, "*señalan que esta tendencia llegó para quedarse, por lo que los líderes deberían centrar su atención en seis áreas, entre las que se encuentra ciberseguridad y seguridad de datos internos. "Esta necesidad crecerá a medida que más empleados trabajen en un entorno híbrido, los entornos impredecibles aumentan el riesgo de ataques de seguridad. Solo 30% de la ciberseguridad es tecnología, el otro 70% depende de la cultura, el comportamiento y la conciencia de los trabajadores".*[2]

Lo anterior se traduce en un incremento significativo en la demanda en los servicios de ciberseguridad y seguridad de la información que ofrecen soluciones para hacerle frente a los retos que implica la definición de estrategias para dar cumplimiento a los mandatos establecidos mediante políticas públicas, estrategias de gobierno y normatividad vigente, y el incremento en el uso de las tecnologías de la información y las comunicaciones que soportarán la operación de las organizaciones.

Las firmas expertas en consultorías y prestación de servicios relacionados con ciberseguridad y seguridad de la información centran su portafolio de servicios en la identificación, evaluación y tratamiento de riesgos y la implementación de controles y procedimientos que contribuyan a salvaguardar la información institucional, bajo el cumplimiento de requisitos normativos y estándares como la norma ISO 27001 de 2013 e ITIL.

Para el desarrollo de sus actividades, estas firmas cuentan con personal especializado y con experiencia en la implementación de sistemas de gestión de seguridad, análisis de riesgos, gestión de incidentes y ejecución de análisis de sistemas de información y pruebas de Ethical Hacking, el cual debe cumplir con requisitos de estudio y capacitaciones en diferentes campos de estudio, así como certificaciones en estándares internacionales, que garanticen su idoneidad para el desarrollo de las actividades con la calidad exigida por el mercado.

Las siguientes son algunas de las empresas dedicadas a la prestación de servicios relacionados con seguridad informática y/o seguridad de la información, con capacidad para proveer los servicios requeridos en el presente proceso:

Nombre Empresa	Sitio Web
Adalid Corp S.A.S	https://www.adalid.com/
Trust and legal	https://trustandlegal.com/

[2] https://www.larepublica.co/internet-economy/la-demanda-de-los-servicios-de-ciberseguridad-se-incremento-40-a-nivel-nacional-3039341

Delta IT solutions	http://www.deltaits.com/
Cloud Seguro	https://www.cloudseguro.co/
DATASECURE S.A.S	https://www.datasecure.com.co/
BDO Colombia	https://www.bdo.com.co
Lavenir	https://www.lavenir.com.co
RENATA Colombia	https://www.renata.edu.co/
2Secure Services	https://2secure.co
Five Strategy	http://www.fivestrategy.com/
Globaltek Security	https://www.globalteksecurity.com/

7.2. Análisis técnico

Los requerimientos técnicos y tecnológicos que abarcan el objeto del presente proceso incluyen aspectos fundamentales que garanticen el cumplimiento de los requisitos exigidos por la entidad para dar solución a la necesidad planteada:

- **Características de los productos:** Los servicios requeridos en el proceso son ofrecidos por diversas firmas de consultoría en el país, lo que garantiza la participación y pluralidad de oferentes.

- **Capacidad técnica:** Los requisitos técnicos del proceso corresponden a requerimientos ajustados a normas y estándares internacionales, que son incluidos en el portafolio de servicios de las diferentes firmas consultoras que encontramos en el mercado colombiano.

- **Requerimientos de calidad:** Los requisitos de calidad se definen claramente en el anexo técnico del presente proceso, y para su cumplimiento se han definido unos requisitos de estudio y experiencia de personal que garanticen la idoneidad del equipo de trabajo de los oferentes, así como los requisitos de experiencia específica de las firmas oferentes en ejecución de contratos relacionados con el objeto del proceso.

- **Tiempos de entrega de productos**: Se especifican en el anexo técnico del presente proceso.

7.3. Estudio de precios en el mercado

Teniendo en cuenta que para la contratación solicitada la Dirección de Tecnologías de la Información y las Comunicaciones DTIC debe ajustarse a la disponibilidad presupuestal vigente, se adelantó estudio de mercado con el fin de establecer el valor de los servicios requeridos para satisfacer la necesidad planteada, para lo cual se envió solicitud de cotización mediante correo electrónico a diferentes proveedores de los servicios requeridos en el proceso con los siguientes resultados:

Invitación a cotizar - ACTUALIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI, Y LA REALIZACIÓN DEL ANÁLISIS DE VULNERABILIDADES Y HACKING ÉTICO PARA LOS ACTIVOS DE INFORMACIÓN

Darley Ocampo García <docampo@personeriabogota.gov.co>
Lun 4/10/2021 9:54 AM
Para: juan.alarcon@alsun.com.co <juan.alarcon@alsun.com.co>

2 archivos adjuntos (404 KB)
Anexo_tecnico_Consultoria_SGSI_FINAL-2.pdf; OFERTA_ECONOMICA_SGSI-2.xlsx;

Cordial saludo,

La Personería de Bogotá, D.C. requiere adelantar el proceso de contratación de la referencia; por lo cual se invita de manera atenta a presentar cotización hasta el martes **5 octubre de 2021**, antes de las 5 p.m., con el fin de realizar el estudio de mercado del mencionado proceso.

Se adjunta el anexo técnico, donde se indica, el objeto, alcance, entregables, obligaciones entre otros aspectos y el formato de cotización sobre el cual deben realizar dicha cotización.

Agradeciendo su interés y participación.

Cordialmente,

ACTUALIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI, Y LA REALIZACIÓN DEL ANÁLISIS DE VULNERABILIDADES Y HACKING ÉTICO PARA LOS ACTIVOS DE INFORMACIÓN				
FECHA:	5/10/21			
		ALSUN	Q-TECH	OLIMPIA
ITEM	FASE/ENTREGABLE	VALOR PRESUPUESTO INCLUIDO IVA	VALOR PRESUPUESTO INCLUIDO IVA	VALOR PRESUPUESTO INCLUIDO IVA
1	FASE I: DIAGNOSTICO	$ 35.000.000	$ 59.100.000	$ 65.500.000
2	FASE II: PLANIFICACIÓN	$ 80.000.000	$ 62.700.000	$ 62.300.000
3	FASE III: ACTUALIZACION Y ANÁLISIS DE RIESGOS			
	A.Identificación de activos de información	$ 50.000.000	$ 56.012.000	$ 49.200.000
	B.Análisis de riesgos de seguridad de la información	$ 80.000.000	$ 62.324.000	$ 66.010.000
	C. Actualización del modelo de medición del SGSI	$ 120.000.000	$ 57.123.098	$ 63.040.000
	D. Auditoria de seguimiento ISO 27001	$ 8.000.000	$ 68.500.000	$ 51.700.000
4	FASE IV: IMPLEMENTACIÓN Y ANÁLISIS DE RIESGOS			
	E.Hacking ético y analisis de vulnerabilidades	$ 110.000.000	$ 130.098.345	$ 125.900.000
5	FASE IV: CIERRE PROYECTO	$ 0	$ 0	$ 0
	VALOR TOTAL INCLUIDO IVA	$ 483.000.000	$ 495.857.443	$ 483.650.000
	VALOR PROMEDIO	$ 487.502.481		

De igual manera, se solicitaron cotizaciones mediante publicación en la plataforma SECOP II con proceso No. PB-SIP-002-2021 recibiendo ofertas de las firmas 2Secure y BPM Global Soluciones, con los siguientes resultados:

Cotización presentada por 2Secure:

A	B	C
ITEM	FASE/ENTREGABLE	VALOR PRESUPUESTO INCLUIDO IVA
1	FASE I: DIAGNOSTICO	89.250.000
2	FASE II: PLANIFICACIÓN	89.250.000
3	FASE III: ACTUALIZACION Y ANÁLISIS DE RIESGOS	71.350.000
	A.Identificación de activos de información	71.350.000
	B.Análisis de riesgos de seguridad de la información	71.350.000
	C. Actualización del modelo de medición del SGSI	71.350.000
	D. Auditoria de seguimiento ISO 27001	71.350.000
4	FASE IV: IMPLEMENTACIÓN Y ANÁLISIS DE RIESGOS	15.000.000
5	E.Hacking ético y analisis de vulnerabilidades	15.000.000
6	FASE IV: CIERRE PROYECTO	29.750.000
	VALOR TOTAL INCLUIDO IVA	595.000.000

Cotización presentada por BPM Global Soluciones:

A	B	C
ITEM	FASE/ENTREGABLE	VALOR PRESUPUESTO INCLUIDO IVA
1	FASE I: DIAGNOSTICO	20.000.000
2	FASE II: PLANIFICACIÓN	28.000.000
3	FASE III: ACTUALIZACION Y ANÁLISIS DE RIESGOS	
	A.Identificación de activos de información	15.000.000
	B.Análisis de riesgos de seguridad de la información	15.000.000
	C. Actualización del modelo de medición del SGSI	15.000.000
	D. Auditoria de seguimiento ISO 27001	20.000.000
4	FASE IV: IMPLEMENTACIÓN Y ANÁLISIS DE RIESGOS	30.000.000
5	E.Hacking ético y analisis de vulnerabilidades	30.000.000
6	FASE IV: CIERRE PROYECTO	15.000.000
	VALOR TOTAL INCLUIDO IVA	188.000.000

Una vez analizadas los valores cotizados encontramos lo siguiente:

Para la cotización presentada por 2Secure encontramos que en los ítems No. 3 y 4 se cotizan valores que no deberían ser incluidos de acuerdo con lo solicitado en el formato de cotización y que generan diferencia frente a las demás cotizaciones recibidas y diligenciadas correctamente.

Para la cotización presentada por BPM Global Soluciones, encontramos que en el ítem No. 4 se cotizan valores que no deberían ser incluidos de acuerdo con lo solicitado en el formato de cotización y que generan diferencia frente a las demás cotizaciones recibidas y diligenciadas correctamente, y adicionalmente los valores cotizados son atípicos siendo significativamente inferiores al promedio cotizado.

Por lo anterior, las cotizaciones recibidas mediante el proceso No. PB-SIP-002-2021 publicado en SECOP II, no serán tenidas en cuenta para el estudio de mercado objeto del presente proceso.

De acuerdo a lo anterior, según el estudio de mercado realizado y dada su viabilidad técnica y presupuestal, se determina que la opción para solucionar la necesidad planteada es contratar una CONSULTORÍA PARA ACTUALIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI, Y LA REALIZACIÓN DEL ANÁLISIS DE VULNERABILIDADES Y HACKING ÉTICO PARA LOS ACTIVOS DE INFORMACIÓN.

7.4. Estudio de la demanda

Los procesos de contratación de consultorías para implementación, mantenimiento y actualización de Sistemas de Gestión de Seguridad de la Información SGSI, son frecuentes en varias entidades estatales que invierten parte de su presupuesto en búsqueda de cumplir con los requisitos y mandatos establecidos mediante políticas públicas, estrategias de gobierno y la normatividad legal vigente, a través de la implementación de sistemas de información, fortalecimiento de la infraestructura tecnológica y adopción de estándares y buenas prácticas de TI, que coadyuven a la protección de los datos y la información institucional como uno de los activos más importantes para la normal operación y cumplimiento de las funciones de las entidades estado.

7.4.1. Contrataciones previas de la Personería de Bogotá D.C.:

Entidad contratante	**PERSONERÍA DE BOGOTÁ, D.C.**
Número de proceso	PB-PCM 002-2019
Número de contrato	719-2019
Contratista	FIVE STRATEGYT CONSULTING GROUP SAS
Plazo de ejecución	seis (06) meses
Objeto del contrato	CONTRATAR UNA CONSULTORÍA PARA IMPLEMENTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA PERSONERÍA DE BOGOTÁ, D.C.
Valor del contrato	$98.000.000.oo incluido IVA.

7.4.2. Contrataciones de otras entidades estatales:

Entidad contratante	**AGENCIA NACIONAL DE HIDROCARBUROS**
Número de proceso	ANH-02-CM-2019
Número de contrato	634-2019
Contratista	UTANH-2019
Plazo de ejecución	CINCO (5) MESES
Objeto del contrato	CONTRATAR LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI, LA ADQUISICIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA ADMINISTRACIÓN, EVALUACIÓN, GESTIÓN DE RIESGOS Y LAS ETAPAS DEL CICLO DE VIDA DEL SGSI Y EL APOYO ESPECIALIZADO EN SEGURIDAD INFORMÁTICA Y FORENSE, ALINEADA A LA ESTRATEGIA DE GOBIERNO DIGITAL, CONFORME A LAS NECESIDADES DE LA ANH Y A LAS BUENAS PRÁCTICAS VIGENTES.
Valor del contrato	$1.624.149.547.oo incluido IVA

Entidad contratante	**El MINISTERIO DE DEFENSA NACIONAL- EJÉRCITO NACIONAL- CENAC IMI**
Número de proceso	173-CENACINTELIGENCIA-2020
Número de contrato	169-2020
Contratista	PASSWORD CONSULTING SERVICES S.A.S
Plazo de ejecución	Hasta el 30 de noviembre de 2020
Objeto del contrato	ADQUIRIR EL SERVICIO DE IMPLEMENTAR Y DIAGNOSTICAR EL SGSI HASTA NIVEL BRIGADAS DE INTELIGENCIA, BASADO EN LA NORMA TÉCNICA ISO/27001 (O SU VERSION ACTUAL), PARA EL SUBSISTEMA DE CONTRAINTELIGENCIA
Valor del contrato	$ 220.000.000.50 incluido IVA

Entidad contratante	**UNIDAD NACIONAL PARA LA GESTIÓN DEL RIESGO DE DESASTRES**
Número de proceso	FNGRD/UNGRD-CMA-001-2021
Número de contrato	9677-PPAL001-1171-2021
Contratista	PASSWORD CONSULTING SERVICES S.A.S
Plazo de ejecución	Seis (06) meses
Objeto del contrato	REALIZAR EL DIAGNÓSTICO, ACTUALIZACIÓN E IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), BAJO LOS REQUISITOS DE LA NORMA ISO 27001:2013 Y LOS

	LINEAMIENTOS DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y LAS POLÍTICAS DE GOBIERNO DIGITAL Y SEGURIDAD DIGITAL; CON EL FIN DE GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA NACIONAL DE GESTIÓN DEL RIESGO DE DESASTRES SNGRD
Valor del contrato	$270.000.000.oo incluido IVA

8. ANÁLISIS FINANCIERO Y ORGANIZACIONAL

En el desarrollo del presente estudio y la construcción de los subsiguientes ratios financieros se generó una muestra significativa (Anexo – Ejercicio Indicadores) que permite visualizar las características del sector, para la cual se toman los datos correspondientes a la situación financiera empresarial dentro del macro sector "Información y Comunicaciones", el siguiente sector económico: "Desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas), consultoría informática y actividades relacionadas". Basados en la "Clasificación Industrial Internacional Uniforme Versión 4 A.C". Se toman las siguientes actividades de comercio CIIU:

- J6201 - Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas)
- J6202 - Actividades de consultoría informática y actividades de administración de instalaciones informáticas
- J6209 - Otras actividades de tecnologías de información y actividades de servicios informáticos

El total de la muestra es de 260 empresas; 52 correspondientes a la información de los estados financieros de plenas y 208 correspondientes a la información de estados financieros de pymes. Dicha muestra fue obtenida de la referencia de información oficial para el análisis de cada sector económico, consulta realizada en el aplicativo: "Sistema Integrado de Información Societaria" (SIIS) de la Superintendencia de Sociedades.

REQUISITOS CAPACIDAD FINANCIERA

Los participantes del presente proceso deberán cumplir los siguientes indicadores financieros:

INDICADOR	INDICE REQUERIDO
Índice de Liquidez	Mayor o igual a 1.0
Índice de Endeudamiento	Menor o igual al 86.0%
Cobertura de intereses	Mayor o igual a 0.4

Capital de trabajo	Mayor o igual al valor del presupuesto oficial destinado para este proceso

Verificación de Capacidad Financiera

La verificación financiera de las propuestas se efectúa con el propósito de medir la solvencia económica, patrimonial y la fortaleza financiera del proponente como requisito habilitante dentro del proceso en mención.

Los indicadores de capacidad financiera buscan establecer unas mínimas condiciones que reflejan la salud financiera de los proponentes a través de su liquidez y endeudamiento. Estas condiciones muestran la aptitud del proponente para cumplir oportuna y cabalmente el objeto del contrato.

De conformidad con lo establecido en el Decreto 1082 de 2015 y el manual para determinar y verificar los requisitos habilitantes en los procesos de contratación expedido por Colombia Compra Eficiente, se ha establecido como requisito habilitante, los siguientes indicadores de capacidad financiera y organizacional los cuales se analizarán de acuerdo con la información financiera reflejada en el Certificado de Registro Único de Proponentes –RUP– con corte a 31 de diciembre de los años 2018 – 2019 y 2020. (de acuerdo con el decreto 579 de 31 de mayo de 2021).

a. **Índice de Liquidez:** se establece con el fin de verificar la disponibilidad de recursos de la empresa a corto plazo para afrontar sus compromisos, representando las veces que el activo corriente puede cubrir el pasivo corriente.
El Índice de Liquidez del proponente se determina dividiendo el Activo Corriente por el Pasivo Corriente.

b. **Índice de endeudamiento:** Permite establecer el grado de apalancamiento utilizado por la empresa e indica la participación de los acreedores sobre los activos de la misma.
Este porcentaje se obtiene de dividir el Pasivo Total por el Activo Total y el resultado se multiplicará por 100.

c. **Razón de cobertura de intereses:** Permite medir el grado hasta el cual las utilidades de la empresa pueden disminuir sin transformarse en pérdidas al cubrir los costos de intereses. Es la relación de los gastos financieros de una empresa frente a su capacidad para brindar servicios.
Se determina dividiendo la utilidad operacional por los gastos de los intereses.

d. **Capital de Trabajo:** Permite medir la capacidad del proponente para el desarrollo normal de las actividades operativas, superando cualquier obstáculo o situación que afecte financieramente a la empresa, en otros términos, son los

recursos básicos que se necesitan para poder operar en un ambiente sano.
Se determina restando del activo corriente el pasivo corriente. Este indicador debe ser mayor o igual al valor del presupuesto oficial destinado para este proceso.

Para los indicadores de Liquidez y Razón de Cobertura de intereses, cuando al aplicar la fórmula y su denominador sea cero (0), su resultado sería indeterminado, porque el proponente no registra pasivo corriente o gastos por intereses; por consiguiente, el indicador se calificará como CUMPLE.

REQUISITOS DE CAPACIDAD ORGANIZACIONAL

Los participantes del presente proceso deberán cumplir los siguientes indicadores organizacionales:

INDICADOR	INDICE REQUERIDO
Rentabilidad del patrimonio	Mayor o igual al 4.0%
Rentabilidad del activo	Mayor o igual al 1.0%

La capacidad organizacional es la aptitud de un proponente para cumplir a cabalidad el objeto del contrato en función de su organización interna. Los siguientes indicadores miden el rendimiento de las inversiones y la eficiencia de la administración del proponente en el uso de sus activos; para su cálculo se toma la información contenida en el Certificado de Registro Único de Proponentes o la certificación de indicadores financieros, con corte a 31 de diciembre de los años 2018 – 2019 y 2020. (de acuerdo con el decreto 579 de 31 de mayo de 2021).

a. **Rentabilidad del patrimonio**: Permite medir el rendimiento del patrimonio de los inversionistas de la empresa con base en la actividad operacional, sin tener en cuenta los impuestos o gastos financieros.
La Rentabilidad del Patrimonio se determina dividiendo la utilidad operacional por el patrimonio, multiplicado por 100.

b. **Rentabilidad del activo**: Se establece con el fin de verificar la eficiencia administrativa de los activos de la empresa, en términos de rentabilidad recibida mediante la ejecución de la actividad operacional.
La Rentabilidad del Activo del proponente se determina dividiendo utilidad operacional por el activo total, multiplicada por 100.

PROPONENTES PLURALES

Procedimiento para calcular los indicadores de los oferentes plurales:
Para el caso de los Consorcios o Uniones Temporales la verificación financiera se realizará mediante el Certificado de Registro Único de Proponentes de cada uno de los miembros, con corte a 31 de diciembre de los años 2018 – 2019 y 2020. (de acuerdo con el decreto 579 de 31 de mayo de 2021), y estos se calcularán de

acuerdo con la fórmula de suma de los componentes de los indicadores, establecida en el Manual de Colombia Compra Eficiente, de la siguiente forma:

$$\text{(iii) Indicador} = \frac{\sum n \text{ Componente 1 del Indicador}}{\sum n \text{ Componente 2 del Indicador}}$$

Se toma el componente de cada indicador de cada uno de los integrantes que componen la propuesta y se suman, los resultados de la sumatoria, se lleva a la respectiva fórmula de cada uno de los indicadores solicitados, para determinar si cumple.
Esta fórmula se aplicará para todos y cada uno de los indicadores cuando exista número plural de oferentes en la propuesta.

NOTA: De acuerdo con el decreto 579 de 31 de mayo de 2021

Artículo 2. Sustitución del parágrafo transitorio 1 del artículo 2.2.1.1.1.5.6. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional.

"PARÁGRAFO TRANSITORIO 1: *De conformidad con los parágrafos transitorios del artículo 2.2.1.1.1.5.2. del presente Decreto, los requisitos e indicadores de la capacidad financiera y organizacional de que trata el literal (b) del artículo 2.2.1.1.1.5.6. del Decreto número 1082 de 2015 corresponderán a los últimos tres (3) años fiscales anteriores a la inscripción o renovación, dependiendo de la antigüedad del proponente. En armonía con lo anterior, a partir del 1 de julio de 2021, las cámaras de comercio certificarán la información de que tratan los parágrafos transitorios 1 y 2 del artículo 2.2.1.1.1.5.2. de este Decreto".*

Artículo 3. Sustitución del parágrafo transitorio del artículo 2.2.1.1.1.6.2. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional.

"PARÁGRAFO TRANSITORIO: *De conformidad con los parágrafos transitorios de los artículos 2.2.1.1.1.5.2. y 2.2.1.1.1.5.6., y en desarrollo del deber de análisis de las Entidades Estatales, de que trata el artículo 2.2.1.1.1.6.1. de este Decreto, a partir del 1 de julio de 2021 las Entidades Estatales establecerán y evaluarán los requisitos habilitantes de capacidad financiera y organizacional teniendo en cuenta la información que conste en el Registro Único de Proponentes. En todo caso, se establecerán indicadores proporcionales al procedimiento de contratación.*

Para ello, atendiendo a las condiciones aludidas, en relación con los indicadores de la capacidad financiera y organizacional, de los procesos de selección cuyo acto administrativo de apertura o invitación se publique a partir del 1 de julio de 2021, se tendrá en cuenta la información vigente y en firme en el RUP, por lo que las

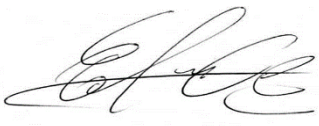
Entidades Estatales evaluarán estos ***indicadores, teniendo en cuenta el mejor año fiscal que se refleje en el registro de cada proponente".***

9. CONCLUSIÓN

Conforme a la necesidad de fortalecer el ámbito de la seguridad y privacidad de la información de la entidad, en base a normas técnicas como la ISO 27001 de 2013 y el Modelo de Seguridad y Privacidad de la Información (MSPI) de la política de gobierno digital de MINTIC, que permita a la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, garantizar el cumplimiento de las políticas de gobierno y legislación vigente en materia de ciberseguridad y seguridad de la información, así como contribuir al cumplimiento de su obligación de *"Desarrollar estrategias de gestión de información para garantizar la calidad, oportunidad, seguridad e intercambio para el uso en la gestión y la toma de decisiones en la Entidad"*, establecidos en el acuerdo 755 de 2019, mitigando así los riesgos ante las constantes amenazas de malware y ataques cibernéticos que puedan afectar los datos, las comunicaciones y transacciones de los aplicativos misionales y de apoyo de la entidad, y con ello, la seguridad de la información institucional y la normal operación de la Personería de Bogotá, D.C., y en atención a lo anteriormente expuesto en el análisis del sector, se concluye que la solución es contratar una CONSULTORÍA PARA ACTUALIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI, Y LA REALIZACIÓN DEL ANÁLISIS DE VULNERABILIDADES Y HACKING ÉTICO PARA LOS ACTIVOS DE INFORMACIÓN.

Plazo: El plazo del contrato es hasta el treinta y uno (31) de diciembre de 2021, contados a partir de la suscripción del acta de inicio, previa legalización y cumplimiento de los requisitos de ejecución del contrato.

Cordialmente,



EDGAR MARTÍN CUBIDES ROJAS
Director de Tecnologías de la Información y las Comunicaciones

Elaboró: Darley Ocampo García, Profesional Dirección DTIC 

Henry A. Villate S, Profesional universitario 219-01 (E) – Subdirección de Gestión Financiera

Aprobó Análisis Financiero: José Hugo Torres Hernández, Subdirector de Gestión Financiera