ANEXO 1
ANALISIS DEL SECTOR
AUDITORÍA DE SEGUIMIENTO AL SGSI

Justificación de las Necesidad:

La Personería de Bogotá D.C., es una entidad de derecho público perteneciente a los órganos de control y vigilancia del estado, que según lo consagrado en los Art. 117 y 118 de la Constitución Política, tiene a su cargo la guarda y promoción de los derechos humanos, la protección del interés público y la vigilancia de la conducta oficial de quienes desempeñan funciones públicas. Para el cabal cumplimiento de sus obligaciones constitucionales y legales, el Acuerdo 034 de 1993 y el Art. 104 del Decreto Ley 1421 de 1993, confirieron a la Personería de Bogotá, D.C., autonomía administrativa, facultad que le permite ejecutar su presupuesto, es decir, dictar los actos y celebrar los contratos necesarios para el desarrollo normal de sus funciones.

Con la expedición del acuerdo No.755 de 2019, artículo 23, numerales 6, 7 y 8, determina, entre otros, que la Dirección de Tecnologías de la Información y las Comunicaciones es la encargada de: i) 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; ii) Propender y facilitar el uso y apropiación de las tecnologías, los sistemas de información y los servicios digitales por parte de los (as) servidores(as), las personas y los grupos de interés a quienes están dirigidos; y iii) Establecer lineamientos tecnológicos para cumplir los estándares de integridad, disponibilidad y confidencialidad de la información. Adicionalmente, la Resolución No. 406 de 2020, artículo 22. “Responsables de los sistemas de gestión”, designa al Director(a) de Tecnologías de la Información y las comunicaciones, como responsable del Sistema de Gestión de Seguridad de la Información - SGSI, el cual se encuentra implementado en la entidad teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información MSPI que se basa en la norma técnica NTC-ISO-IEC 27001: 2013

El CONPES 3995 de 2020, Política Nacional de Confianza y Seguridad Digital, explica como la “creciente participación de ciudadanos en el entorno digital, la alta dependencia” – de todo tipo de organizaciones – “de la infraestructura digital y el aumento en el uso y adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC), traen consigo una serie de riesgos e incertidumbres relacionados con la seguridad digital, lo cual exige contar con suficientes y adecuadas capacidades para su gestión. Las amenazas, los ataques e incidentes de seguridad digital cada día son más sofisticados y complejos e implican graves consecuencias de tipo económico o social” lo cual soporta la necesidad de mantener actualizado el Sistema de Gestión de seguridad de la información, la ciberseguridad, y la privacidad en la entidad, determinando cambios en el contexto y los riesgos para asegurar su idoneidad y eficacia.

De igual manera, conforme a los criterios generales para los organismos de certificación de sistemas de gestión establecidos tanto a nivel internacional como en Colombia por el Organismo Nacional de Acreditación de Colombia (ONAC), se tiene como vigencia del ciclo de certificación un término de tres (3) años y la norma ISO 17021, ”por medio de la cual se

rigen los organismos de certificación", establece en los numerales 9.3.2.1 que "Las auditorías de seguimiento son auditorías in situ, que no son necesariamente auditorías de todo el sistema, y serán programadas junto con las otras actividades de vigilancia a fin de que el organismo de certificación pueda mantener la confianza que el sistema de gestión certificado cumple los requisitos y 9.3.2.2 las visitas de seguimiento a las organizaciones deben realizarse de forma anual para poder mantener el respectivo certificado.

Todo lo anterior soporta el esfuerzo que viene realizando el proceso Direccionamiento TIC de la Personería de Bogotá en establecer, operar, y mejorar de manera continua el Sistema de Gestión de Seguridad de la Información - SGSI, que debe mantenerse vigente, actualizado e idóneo, para ofrecer respuestas eficaces a los crecientes retos a nivel local y global.

En este sentido, la entidad y en particular el proceso de direccionamiento TIC, en el año 2021 realiza la gestión de acreditación mediante la ejecución de la auditoria de tercera parte efectuada por el organismo europeo "LL-C CERTIFICATION", a través de su operador técnico-comercial IMS Global autorizado en el país, el cual encontró conforme el sistema, y por ende procedió a emitir el respectivo certificado de cumplimiento de auditoría el día 2 de febrero de 2022 con # 572328.

Por lo anterior, se hace obligatorio para mantener la certificación, realizar auditorías de seguimiento anualmente por los siguientes dos años después de certificarse, y de una auditoría externa de recertificación, igual que la primera, después de tres años. En resumen, el ciclo de certificación de ISO 27001 es así:

- Año 1: Auditoría de Certificación.
- Año 2: Auditoría de Seguimiento.
- Año 3: Auditoría de Seguimiento.
- Año 4: Auditoría de Recertificación.

En consecuencia, es necesario realizar la primera auditoría de seguimiento de tercera parte o auditoría externa para verificar y asegurar la conformidad con los requisitos y la misma evolución del sistema.

De la misma manera, es importante mencionar que la norma ISO 27001:2013 con la que fue certificada la entidad, se actualizó recientemente a la norma ISO 27001:2022, lo cual obliga a las organizaciones que quieren mantener la certificación en realizar la transición a la revisión de 2022 de la norma dentro del periodo de transición establecido como máximo.

En general, se hace necesario realizar las autorías de seguimiento y dado que el proveedor IMS Global es el único operador técnico-comercial autorizado en Colombia por el ente certificador "LL-C CERTIFICATION" para promover en su nombre servicios de auditoría de tercera parte, así como realizar el respectivo proceso de evaluación de seguimiento con su propio equipo evaluador es necesario que se contrate las respectivas auditorías de seguimiento de forma tal que se pueda determinar el nivel de conformidad frente a la norma

ISO/IEC 27001:2013, y se mantenga la recomendación de mantener el respectivo certificado.

En virtud de lo expuesto anteriormente, la Personería de Bogotá, requiere suscribir un contrato en la modalidad de contratación directa con la firma IMS Global de conformidad con el literal g, numeral del artículo de la Ley 1150 de 2007, concordante con el artículo 2.2.1.2.1.4.8 del Decreto 1082 de 2015, teniendo en cuenta que fue esta firma quien otorgó la certificación, para que realice la primera auditoria de seguimiento el Sistema de Gestión de Seguridad de la Información - SGSI de forma tal que la Personería de Bogotá pueda mantener la certificación recibida al Sistema de Gestión de Seguridad de la Información de la Entidad, la cual está supeditada a evidenciar la mejora continua y la conformidad respecto a los requisitos de las normas, para lo cual la firma IMS Global, deberá monitorear dicha conformidad a través de auditorías de seguimiento anuales.

Al respecto, el artículo 2.2.1.2.1.4.8. del Decreto 1082 de 2015 establece que se contratará directamente cuando no exista pluralidad de oferentes en los siguientes términos: “Se considera que no existe pluralidad de oferentes cuando existe solamente una persona que puede proveer el bien o el servicio por ser titular de los derechos de propiedad industrial o de los derechos de autor, o por ser proveedor exclusivo en el territorio nacional. Estas circunstancias deben constar en el estudio previo que soporta la contratación”.

Especificaciones y condiciones técnicas

Fase: Auditoría seguimiento (de tercera parte)		
Objetivo	**Actividades mínimas**	**Entregable**
Evaluar el grado de conformidad del actual Sistema de Gestión de Seguridad de la Información de la organización frente a la norma ISO/IEC 27001:2013 en la cual la entidad está certificada con el OEC LL-C.	Las actividades previstas, tomando como criterio de auditoría a ISO/IEC 27001:2013, son: - Elaboración plan de auditoría (según ISO 19011:2018 e ISO/IEC 27006) - Revisión documental - Revisión técnica y entrevista - Preparación de informe	• Plan de auditoría (el cual debe observar los elementos descritos en ISO 19011:2018) • Informe de auditoría (el cual debe observar los elementos descritos en ISO 19011:2018). Este informe debe incluir una sección específica de potenciales no conformidades (así como de observaciones, oportunidades de mejora, y fortalezas) que incluya requisito, desviación o incumplimiento, y evidencia.

Fase: Pre-Auditoría (Diagnóstico transición de la norma a su nueva versión ISO/IEC 27001:2022)

Objetivo	Actividades mínimas	Entregables
Evaluar el grado de conformidad del Sistema de Gestión de Seguridad de la Información de la organización frente a la norma ISO/IEC 27001:2022.	Las actividades previstas, tomando como criterio de auditoría a ISO/IEC 27001:2013, son: - Elaboración plan de auditoría - Revisión documental y técnica (Análisis de brechas de seguridad de ISO/IEC 27001:2022, declaración de aplicabilidad (SOA), plan de tratamiento de riesgos, nuevos controles) - Preparación de informe .	• Plan de auditoría (el cual debe observar los elementos descritos en ISO 19011:2018) • Informe diagnóstico transición de la norma a su nueva versión ISO/IEC 27001:2022

Actividades mínimas en desarrollo del objeto contractual:

1. La contratista una vez suscrita el acta de inicio, establecerá un cronograma de ejecución de la auditoría de seguimiento a realizar, durante el desarrollo del contrato, en el cual se indiquen las actividades a desarrollar, el tiempo establecido para cada una y los nombres de los profesionales responsables de su ejecución.

2. El contratista deberá elaborar el Plan de Auditoría basado en la documentación proporcionada por la Personería de Bogotá D.C.

3. El contratista deberá programar la reunión de apertura de la auditoría de seguimiento al SGSI con los responsables del proceso a auditar. En esta reunión se deben acordar y confirmar el plan de auditoría y presentar al equipo que desarrollará la auditoría. La evidencia de la ejecución del entregable es el acta de la reunión de apertura, con el desarrollo de las misma y la lista de asistentes.

4. El contratista deberá presentar el reporte de hallazgos de la auditoría de seguimiento al SGSI. Los hallazgos pueden indicar conformidad, no conformidad y oportunidades de mejora.

5. El contratista deberá presentar el diagnóstico de transición de la norma a ISO/IEC 27001:2013 a la norma a ISO/IEC 27001:2022, indicando los cambios en aspectos como evaluación de riesgos, plan de tratamiento de riesgos, declaración de aplicabilidad, controles y

6. El contratista deberá preparar los documentos de trabajo requeridos para el desarrollo de las auditoria de seguimiento al SGSI como son listas de chequeo, entrevistas, y/o registros de reuniones.

Aviso de privacidad: Sus datos personales serán tratados conforme a la Política de Tratamiento de Datos Personales, que podrá ser consultada en www.personeriabogota.gov.co.

7. El contratista realizará la reunión de cierre de la auditoría de seguimientos al SGSI, presentando a los responsables del Sistemas de Gestión de Seguridad de la Información los hallazgos, oportunidades de mejora y las conclusiones de la auditoría. La evidencia de la ejecución de este entregables es el acta de reunión de cierre, describiendo los detalles de la reunión junto al listado de asistentes.

8. El contratista deberá elaborar y entregar el informe final de auditoría de seguimiento al SGSI, el cual debe describir los siguientes aspectos:

    a. Objetivos de la auditoría de seguimiento al SGSI
    b. Alcance de la auditoría de seguimiento al SGSI.
    c. Identificación del equipo auditor y de los auditados del SGSI
    d. Fechas en las que se realizaron las actividades de auditoría.
    e. Criterios de la auditoría de seguimiento al SGSI.
    f. Hallazgos de la auditoría de seguimiento al SGSI.
    g. Oportunidades de mejora.
    h. Conclusiones de la auditoría.

9. Posterior a la presentación de los hallazgos derivados de la auditoría de seguimiento al SGSI y que el líder del sistema formule el plan de mejoramiento, el contratista realizará la revisión de este plan y de los análisis de causa raíz con los cuales se planea subsanar las No Conformidades encontradas en la auditoría de seguimiento al SGSI, generar las recomendaciones que serán presentadas y aprobadas por la oficina de control interno de las Personería de Bogotá.

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)

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:

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

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 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 el 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, el continuo incrementó del teletrabajo y el trabajo en casa, que, según los expertos, “*llegó para quedarse, por lo que los líderes deberían centrar su atención en seis áreas, entre las que se encuentra ciberseguridad y seguridad de*

Aviso de privacidad: Sus datos personales serán tratados conforme a la Política de Tratamiento de Datos Personales, que podrá ser consultada en www.personeriabogota.gov.co.

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 las actividades, la firma IMS GLOBAL es el único operador técnico-comercial autorizado por *LL-C Certification* para promover en su nombre auditorias de tercera parte y seguimiento, presentar las respectivas ofertas, así como realizar el respectivo proceso de evaluación con su propio equipo evaluador.

Cabe mencionar que el organismo de certificación *LL-C Certification* está obligado a realizar auditorías de vigilancia todos los años en el lugar de las actividades de la entidad certificada, a menos que un requisito normativo o legal establezca excepcionalmente lo contrario. La primera auditoría de seguimiento después de la certificación inicial se iniciará a los 12 meses a partir de la fecha de finalización de la auditoría de certificación; la segunda auditoría de seguimiento debe iniciarse en el período anual desde la fecha de finalización de la primera auditoría de seguimiento con una tolerancia máxima de 45 días calendario.

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:** Las características de los servicios requeridos se definen claramente en el anexo técnico del presente proceso

- **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 firma consultora (única autorizada por la entidad certificadora) que encontramos en el mercado colombiano.

- **Requerimientos de calidad:** Los requisitos de calidad se definen claramente en el anexo técnico del presente proceso.

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

Estudio de la oferta: En el mercado nacional se encuentran varios proveedores de los servicios requeridos por la Entidad en desarrollo del objeto contractual, y todos ellos usan como política de calidad interna que las auditorias de seguimiento a cada comprador certificado por uno d ellos entes certificadores, debe ser realizada por el proveedor que ejecutó el contrato primigenio de certificación, ello hace que se conviertan en proveedores exclusivos de los servicios de recertificación, auditorias de seguimiento y demás servicios que se requieran para mantener e implementar cada una de las faces exigidas por el órgano que otorga la certificación primigenia.

Estudio de precio 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 a la firma IMS GLOBAL como único operador técnico-comercial autorizado por *LL-C Certification,* (entidad certificadora), para promover en su nombre auditorias de tercera parte y seguimiento de acuerdo a los servicios requeridos en el proceso con el siguiente resultado:

Aviso de privacidad: Sus datos personales serán tratados conforme a la Política de Tratamiento de Datos Personales, que podrá ser consultada en www.personeriabogota.gov.co.

SERVICIO	**Auditoría de tercera parte del sistema de gestión**		
ALCANCE	A ser confirmado en auditoría		
SITIOS	Una sede principal		
SECTOR	Gobierno		
PERSONAL	A ser confirmado en auditoría		
METODOLOGÍA	Observación, entrevista a personal, examen de documentos; modalidad 100% virtual o híbrida		
	Pre-Auditoría (Incluye diagnóstico transición de la norma a su nueva versión ISO/IEC 27001:2022)	▪ Elaboración (off-site) plan de auditoría ▪ Fase I: Revisión documental (offline) ▪ Fase II: Revisión técnica y entrevista (virtual) ▪ Preparación de informe (off-site)	0.50 días 5.00 días 1.00 días 0.50 días
		TIEMPO TOTAL DE AUDITORÍA	7.00 días
		TIEMPO AUDITORÍA EN SITIO (UN AUDITOR)	1.00 días
	Auditoría seguimiento (de tercera parte)	▪ Elaboración (off-site) plan de auditoría ▪ Fase I: Revisión documental (offline) ▪ Fase II: Revisión técnica y entrevista (virtual) ▪ Preparación de informe (off-site)	0.50 días 3.00 días 2.00 días 0.50 días
		TIEMPO TOTAL DE AUDITORÍA	6.00 días
		TIEMPO AUDITORÍA EN SITIO (UN AUDITOR)	2.00 días

Inversión (IVA incluido):

SERVICIO	Subtotal
SERVICIO DE PRE-AUDITORÍA Y DE TERCERA PARTE (SEGUIMIENTO)	$ 76,160,000

Fuente: cotización enviada por IMS Global a Personería de Bogotá por concepto de SERVICIO DE PRE-AUDITORÍA Y DE TERCERA PARTE (SEGUIMIENTO)

Así las cosas, el costo estimado de la contratación será de setenta y seis mil ciento sesenta pesos Mcte. ($ 76.160.000), incluidos los impuestos y retenciones aplicables según cotización del proveedor exclusivo del servicio.

Decantado lo anterior, también se consultó la herramienta de abastecimiento estratégico de Colombia Compra Eficiente donde se verificó que por ejemplo el Distrito Capital en lo corrido de la vigencia ha realizado contrataciones con diferentes oferentes del mercado por el orden de 959 mil millones de pesos. (ver anexo análisis de la oferta.)

Estudio de la demanda

Los procesos de contratación para implementación, mantenimiento y actualización de Sistemas de Gestión de Seguridad de la Información SGSI, son frecuentes en las entidades estatales que invierten parte de su presupuesto para cumplir con los requisitos y mandatos establecidos mediante políticas públicas, estrategias de gobierno y la normatividad legal vigente aplicable, 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.

Aviso de privacidad: Sus datos personales serán tratados conforme a la Política de Tratamiento de Datos Personales, que podrá ser consultada en www.personeriabogota.gov.co.

En ese sentido se verificó la herramienta de abastecimiento estratégico donde se logra evidenciar que para lo corrido de esta vigencia entidades distritales han demandado este tipo de servicios en diferentes contratos que ascienden al orden de los diecinueve mil millones de pesos. (ver anexo Análisis de la demanda).

Conclusión

Conforme a la necesidad de asegurar el cumplimiento de la norma técnica ISO 27001 de 2013 que es la base del Sistema de Gestión de Seguridad de la Información de la entidad 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, y en atención a lo anteriormente expuesto en el análisis del sector, se concluye que la solución es contratar la PRESTACIÓN DE SERVICIOS PARA LA AUDITORIA DE SEGUIMIENTO DEL NIVEL DE CONFORMIDAD FRENTE A LA NORMA ISO 27001.

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

Anexos: CDP y documentación contratación

Elaboró: Michael Parra - DTIC

Revisó: Flor E. Hortua M. - DTIC

Aprobó: Edgar Martin Cubides R. - DTIC

Aviso de privacidad: Sus datos personales serán tratados conforme a la Política de Tratamiento de Datos Personales, que podrá ser consultada en www.personeriabogota.gov.co.