

CONDICIONES DE CONTRATACIÓN - AUDITORÍA DE SEGUIMIENTO AL SGSI 202398

Justificación:

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. 250 del 29 de junio de 2023, 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”.

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 y amenazas a nivel local y global.

En este sentido, la entidad y en particular el proceso de Direccionamiento TI en el año 2022 realizó la gestión de certificación de la auditoría y seguimiento mediante la ejecución de las auditorías obligatorias logrando resultados satisfactorios de la 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 número de identificación 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 27001:2013 se encuentra así:

- Año 1: Auditoría de certificación. Realizada en febrero de 2022
- Año 2: Auditoría de seguimiento. Realizada en diciembre 2022
- Año 3: Auditoría de seguimiento. A realizarse en enero - febrero de 2024
- Año 4: Auditoría de recertificación. A realizarse en febrero de 2025

En consecuencia, es necesario realizar la segunda auditoría de seguimiento (Año 3) 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 este sentido, se hace necesario realizar la auditoría 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 la respectiva auditoría de seguimiento de forma tal que se pueda determinar el nivel de conformidad frente a la norma ISO/IEC 27001:2013 para 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 segunda 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”.

Término de ejecución: El plazo de ejecución del contrato será de hasta de treinta (30) días calendario, contados a partir de la fecha del oficio de inicio.

Lugar de Ejecución: Sede principal de las Personería de Bogotá D.C.

Objeto del contrato: Prestación de servicios para la auditoria de seguimiento del nivel de conformidad frente a la norma ISO 27001:2013.

Alcance del objeto

Evaluar el grado de conformidad del actual Sistema de Gestión de Seguridad de la Información de la Personería de Bogotá D.C. frente a la norma ISO/IEC 27001:2013

Obligaciones del contratista

Específicas:

1. Realizar la auditoría de seguimiento al Sistema de Gestión de Seguridad de la Información - SGSI de la Personería de Bogotá, D.C con el fin de verificar la conformidad y eficacia del Sistema conforme a los criterios de la Norma Técnica NTC-ISO/IEC 27001:2013.
2. Proyectar y entregar el plan de auditoria al director de Tecnologías de las Información y las Comunicaciones, como líder del SGSI, dentro de los dos (2) días hábiles siguientes al perfeccionamiento del contrato.
3. Entregar el informe de auditoría, a más tardar dentro de los dos (2) días hábiles siguientes de finalizada la auditoría de seguimiento, previa revisión del Director de Tecnologías.
4. Entregar el informe de diagnóstico de transición de la norma a ISO/IEC 27001:2013 a la norma a ISO/IEC 27001:2022

5. Verificar la pertinencia de las acciones correctivas y planes de mejora propuestos por la Personería de Bogotá D.C., si se presentan hallazgos de no conformidad.
6. EL contratista se compromete a realizar las reuniones de apertura y cierre de auditoría de seguimiento, dejando evidencia audiovisual de dichas reuniones.
7. Revisar y aprobar el plan de mejora para subsanar las no conformidades si llegaran a presentarse.
8. Garantizar que las auditoria de seguimiento sea desarrollada por personal calificado y competente para el cumplimiento del objeto contractual.
9. Mantener absoluta reserva y confidencialidad, no dar a conocer información o documentos suministrados por la Personería de Bogotá D.C., durante y después de la ejecución del proceso de auditoría de seguimiento.
10. Cumplir con las actividades establecidas como mínimas dentro de las especificaciones técnicas.

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, que certifica con el OEC LL-C.	<p>Las actividades previstas, tomando como criterio de auditoría a ISO/IEC 27001:2013, son:</p> <ul style="list-style-type: none"> - Elaboración plan de auditoría (según ISO 19011:2018 e ISO/IEC 27006) - Revisión documental - Revisión técnica y entrevista - Preparación de informe 	<ul style="list-style-type: none"> • 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 como mínimo 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.	<p>Las actividades previstas, tomando como criterio de auditoría a ISO/IEC 27001:2013, son:</p> <ul style="list-style-type: none"> - 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 	<ul style="list-style-type: none"> • 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 iniciada la ejecución, 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.
6. El contratista deberá preparar los documentos de trabajo requeridos para el desarrollo de las auditoría de seguimiento al SGSI como son listas de chequeo, entrevistas, y/o registros de reuniones.

7. El contratista realizará la reunión de cierre de la auditoría de seguimientos al SGSI, presentando a los responsables del Sistema 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 entregable 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 la Personería de Bogotá.

Valor del proceso contractual:

Para todos los efectos legales y fiscales, el valor total del presente proceso de contratación será de **OCHENTA Y DOS MILLONES QUINIENTOS MIL PESOS M/CTE. (\$82.500.000)**, incluido IVA y demás impuestos, tasas, estampillas, contribuciones, costos directos e indirectos asociados a que hubiera lugar, el presente proceso se encuentra respaldado según certificado de disponibilidad presupuestal **No. 62 del (03) tres de enero de 2024, rubro presupuestal 021202020090191116**, Servicios de los órganos de control y otras instituciones.

Forma de pago: El 100% del valor del contrato será pagado al contratista en un único pago, el cual se efectuará mediante consignación a la cuenta que el contratista acredite como propia a través de la certificación bancaria aportada, adjuntando los siguientes documentos:

- a. Factura.
- b. Informe de ejecución final del contrato.
- c. Recibo de pago por concepto de aportes al sistema de seguridad social en salud, pensión, riesgos laborales y aportes parafiscales (si a ello hubiere lugar).
- d. Certificación de pago emitida por el supervisor donde conste el recibo del servicio a entera satisfacción.

La forma de pago estipulada está sujeta a la programación de los recursos del Programa Anual de Caja-PAC y a los recursos disponibles de la Tesorería Distrital. Los recursos que

no puedan girarse en esta vigencia se constituirán como rezago presupuestal compuesto por las reservas presupuestales y las cuentas por pagar.

Parágrafo: En caso de estar obligado a facturar, el contratista *"En atención al artículo 20 de la Resolución No. 42 del 05 de mayo de 2020 expedida por la DIAN, deberá expedir su factura, como Factura electrónica, para lo cual tendrá que realizar la Actualización del RUT y Resolución de facturación incluyendo la responsabilidad como facturador electrónico."*

GARANTÍA EXIGIBLE:

EL CONTRATISTA de acuerdo con lo establecido en el artículo 7 de la ley 1150 de 2007 y el Decreto 1082 de 2015, se compromete a otorgar como mecanismo de cobertura del riesgo, a favor de la PERSONERIA DE BOGOTA D.C. cualquiera de las siguientes garantías: 1. Contrato de seguro contenido en una póliza, 2. Patrimonio autónomo, 3. Garantía Bancaria, dentro de los dos (02) días hábiles siguientes a la firma del contrato.

La garantía deberá amparar los perjuicios que se derivan del incumplimiento del contrato que se señalan a continuación:

- Cumplimiento, equivalente al veinte por ciento (20%) del valor del contrato para garantizar el cumplimiento de sus obligaciones y cuya vigencia será igual al plazo de ejecución del contrato y veinticuatro (24) meses más.
- Calidad del servicio, equivalente al veinte por ciento (20%) del valor del contrato para garantizar la calidad del servicio prestado y cuya vigencia será igual al plazo de ejecución del contrato y cuatro (4) meses más.
- Pago de salarios, prestaciones sociales e indemnizaciones, equivalente al cinco por ciento (5%) del valor total del contrato y cuya vigencia será igual al plazo de ejecución del contrato y tres (3) años más.

PARÁGRAFO PRIMERO: Las garantías no podrán ser canceladas sin la autorización escrita de LA PERSONERÍA

Supervisor del contrato:



EDGAR MARTIN CUBIDES ROJAS

Director de Tecnologías de la Información y las Comunicaciones

Carrera 7a No. 21 - 24 Bogotá - Colombia ♦ Conmutador (601) 382 0450/80 ♦ Código Postal 111321

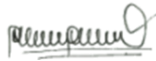
 **PersoneriaDeBogota** ♦  **@personeriadebogota** ♦  **@personeriabta** ♦  **PERSONERIADEBOGOTA**

www.personeriabogota.gov.co ♦ Línea 143

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.

Anexos: CDP y documentación contratación

Elaboró: Luz Mery Caviedes Ramirez- DTIC



Revisó: Michael Parra - DTIC 

Aprobó: Edgar Martin Cubides R. - DTIC