

CONTRALORÍA GENERAL DE LA REPÚBLICA

PROYECTO MEJORAMIENTO DE LOS SERVICIOS DE CONTROL GUBERNAMENTAL PARA UN CONTROL EFECTIVO, PREVENTIVO Y FACILITADOR DE LA GESTIÓN PÚBLICA

		Código
NOMBRE COMPONENTE	ADECUADO ACCESO A TIC EN LOS PROCESOS DE CONTROL GUBERNAMENTAL	3
PRODUCTO	IMPLEMENTACIÓN DEL NUEVO MODELO DE GESTIÓN DE TI INCLUYENDO UN MODELO DE ARQUITECTURA TI	3.1
PROYECTO	DISEÑO E IMPLEMENTACIÓN DEL NUEVO MODELO DE GOBIERNO Y GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	3.1.1



TÉRMINOS DE REFERENCIA

CONTRATACIÓN DEL SERVICIO DE UN CONSULTOR LÍDER DE SUPERVISIÓN SGSI PARA QUE BRINDE SOPORTE AL PRODUCTO 3.1 NUEVO MODELO DE GESTIÓN DE TI INCLUYENDO ARQUITECTURA DE TI DISEÑADO E IMPLEMENTADO

1. Introducción
2. Antecedentes
3. Objetivo
4. Alcance del trabajo
5. Metodología de trabajo
6. Actividades o tareas a realizar
7. Productos e informes a entregar
8. Plazo
9. Perfil
10. Monto
11. Forma y condiciones de pago
12. Coordinación, supervisión y conformidad
13. Derechos de propiedad y confidencialidad de la información
14. Anexo

ENERO 2024

TÉRMINOS DE REFERENCIA
CONTRATACIÓN DEL SERVICIO DE UN CONSULTOR LÍDER DE SUPERVISIÓN SGSI
PARA QUE BRINDE SOPORTE AL PRODUCTO 3.1 NUEVO MODELO DE GESTIÓN DE TI
INCLUYENDO ARQUITECTURA DE TI DISEÑADO E IMPLEMENTADO

1. INTRODUCCIÓN

La Contraloría General de la República (CGR) es el órgano superior del Sistema Nacional de Control que cautela el uso eficiente, eficaz y económico de los recursos del Estado, la correcta gestión de la deuda pública, así como la legalidad de la ejecución del presupuesto del sector público y de los actos de las instituciones sujetas a control; coadyuvando al logro de los objetivos del Estado en el desarrollo nacional y bienestar de la sociedad peruana.

En el marco del Proyecto de Inversión Pública “Mejoramiento de los Servicios de Control Gubernamental para un Control Efectivo, Preventivo y Facilitador de la Gestión Pública”, se han elaborado los términos de referencia para la contratación de un Líder de Supervisión SGSI.

2. ANTECEDENTES

El Proyecto de Inversión (CUI) N°2412703 “Mejoramiento de los Servicios de Control Gubernamental para un control Efectivo, Preventivo y Facilitador de la Gestión Pública-BID3” fue declarado viable por la Unidad Formuladora de la Contraloría General de la República (Gerencia Técnico Normativo) ahora Subgerencia de Formulación de Proyectos con fecha 28 de agosto de 2018 e inscrito en el Banco de Inversiones del MEF; el referido proyecto tiene como objetivo central brindar adecuados servicios de control gubernamental en el Estado”.

El plazo de ejecución del Proyecto es de 5 años, del 2019 al 2023 con financiamiento de 50% con recursos de endeudamiento con el Banco Interamericano de Desarrollo (BID) y 50% con recursos ordinarios, como contrapartida nacional de acuerdo al Contrato de Préstamo” (N° 4724/OC-PE). El Proyecto contempla la ejecución de los siguientes componentes:

- Componente 1. Adecuados procesos para un control efectivo y eficiente.
- Componente 2. Adecuadas capacidades de los RRHH en temas de control gubernamental.
- Componente 3. Adecuado acceso a TIC en los procesos de control gubernamental.
- Componente 4. Adecuada capacidad operativa para la prestación de servicios de control desconcentrados.

En el marco del componente 3, se prevé implementar un modelo de gestión de las tecnologías de la información y comunicaciones (TIC) que permita la adopción de las mejoras prácticas para la mejora de la gestión de TI basada en procesos, así como establecer un adecuado gobierno y arquitectura de datos conjugados con el establecimiento de políticas de Seguridad de Información que normen futuros desarrollos de sistemas de información y coadyuven a proporcionar un enfoque holístico para administrar, mejorar y aprovechar la información de forma que pueda ayudarnos a ganar percepción y generar confianza en decisiones y operaciones institucionales.

A la fecha, se viene realizando el proceso de licitación de un (1) servicio que forma parte del Producto 3.1 “Implementación de un nuevo modelo de Gestión de TI incluyendo un modelo de Arquitectura TI”, bajo el método de Selección Basada en la Calidad y el Costo (SBCC), de conformidad con el numeral 2.6 de las Políticas para la Selección y Contratación de Consultores financiados por el Banco Interamericano de Desarrollo, edición actual (GN-2350-15), según el siguiente detalle:

- a) Contratación de una firma consultora para que diseñe, desarrolle e implemente el Sistema de Gestión de Seguridad de la Información (SGSI) para la CGR, desarrollar una auditoría externa de tercera parte al SGSI para obtener la certificación ISO 27001, así como entregar e implementar una herramienta para la gestión del SGSI.

Al respecto, considerando la importancia de las actividades de supervisión que se requerirán durante la ejecución contractual del servicio, se hace necesario e imprescindible la contratación de un consultor líder en supervisión SGSI, para que preste su servicio durante la etapa de ejecución, así como en la validación de entregables que presente el contratista seleccionado. Asimismo, brindar seguimiento al proyecto durante la etapa post implementación.

3. **OBJETIVO**

Objetivo general

Brindar soporte especializado de supervisión durante la etapa de ejecución contractual, así como en la validación de entregables correspondientes al Sistema de Gestión de Seguridad de la Información (SGSI) en el Producto: 3.1 *Nuevo Modelo de Gestión de TI incluyendo Arquitectura de TI*.

Objetivos específicos

- Validación del cumplimiento técnico de los entregables, coordinación, supervisión, seguimiento y control a la implementación de la Consultoría ***“Diseño, desarrollo e implementación del Sistema de Gestión de Seguridad de la Información (SGSI) para la CGR, desarrollar una auditoría externa de tercera parte al SGSI para obtener la certificación ISO 27001, así como entregar e implementar una herramienta para la gestión del SGSI”***.
- Realizar la gestión y administración de las actividades desarrolladas por el contratista, bajo la normativa vigente y mejores prácticas en cumplimiento con el contrato y especificaciones técnicas.

4. **ALCANCE DEL TRABAJO**

El consultor realizará la coordinación, supervisión técnica, seguimiento y control relacionada a la ejecución del servicio ***“Diseño, desarrollo e implementación del Sistema de Gestión de Seguridad de la Información (SGSI) para la CGR, desarrollar una auditoría externa de tercera parte al SGSI para obtener la certificación ISO 27001, así como entregar e implementar una herramienta para la gestión del SGSI”***; revisará y validará los informes técnicos correspondientes a la verificación de los entregables e informes presentados por el contratista. Asimismo, seguimiento y control a la etapa de operatividad, asegurando el cumplimiento de las condiciones técnicas contempladas en los términos de referencia.

Los trabajos se realizarán de manera presencial y remota (mixto), según lo indicado por la Subgerencia de Gobierno Digital, quien proporcionará los ambientes necesarios para la labor presencial, en las instalaciones de la Contraloría General de la República ubicada en la ciudad de Lima.

5. **METODOLOGÍA DE TRABAJO**

La metodología de trabajo será establecida por la Subgerencia de Gobierno Digital, en concordancia con las metodologías de gestión de proyectos establecidas por la Gerencia de Tecnologías de la Información o la que haga sus veces en la CGR, según corresponda.

6. **ACTIVIDADES O TAREAS A REALIZAR**

El presente servicio requiere la ejecución de las siguientes actividades relacionadas con la supervisión del Servicio ***“Diseño, desarrollo e implementación del Sistema de Gestión de Seguridad de la Información, para la CGR, desarrollar una auditoría externa de tercera parte al SGSI para obtener la certificación ISO 27001, así como entregar e implementar una herramienta para la gestión del SGSI”***:

- i. Elaborar informes técnicos de supervisión de las actividades realizadas en materia de Seguridad de la Información que formen parte del Producto: 3.1 Implementación del Nuevo Modelo de Gestión de TI, incluyendo un modelo de Arquitectura de TI.

- ii. Revisar, validar y supervisar la actualización de la documentación técnica relacionada al Producto: 3.1 Implementación de un nuevo modelo de Gestión de TI, incluyendo un modelo de Arquitectura TI en materia de Seguridad de la Información
- iii. Integrar equipos de trabajo entre otros relacionados al Producto 3.1. requeridos por la Subgerencia de Gobierno Digital, en materia seguridad de la información.
- iv. Elaborar informes de seguimiento y monitoreo del desarrollo de la ejecución contractual del servicio indicando el porcentaje de avance, riesgos identificados y estrategias de mitigación durante la ejecución contractual del proyecto del Producto 3.1 en materia seguridad de la información.
- v. Revisar y validar los informes correspondientes a la verificación de los entregables previstos en los términos de referencia del producto 3.1, en materia de Seguridad de la Información.
- vi. Integrar comités de evaluación de ser necesario por la Subgerencia de Gobierno Digital.
- vii. Revisión de las respuestas a las observaciones absueltas respecto a los entregables e informes presentados por los contratistas de los proyectos del Producto 3.1 en materia de Seguridad de la Información.
- viii. Velar por el cumplimiento del cronograma de los servicios a contratarse del producto 3.1 Implementación del Nuevo Modelo de Gestión de TI, incluyendo un modelo de Arquitectura de TI, en materia de Seguridad de la Información.
- ix. Participar en las reuniones de trabajo con los contratistas y áreas usuarias en la etapa de ejecución contractual del Producto 3.1, en materia de Seguridad de la Información.
- x. Velar por el cumplimiento del Plan de Tratamiento de Riesgos de Seguridad de la Información.
- xi. Revisar los informes técnicos elaborados por los especialistas de la Subgerencia de Gobierno Digital relacionados al Producto 3.1, en materia de Seguridad de la Información.
- xii. Participar en las reuniones de trabajo que requiera la Subgerencia de Gobierno Digital, relacionados al Producto 3.1, en materia de Seguridad de la Información.
- xiii. Desarrollar las acciones que la Subgerencia de Gobierno Digital estime pertinentes para el cumplimiento de los objetivos del proyecto.
- xiv. Realizar seguimiento en la etapa de operatividad, soporte y mantenimiento del Producto 3.1, en materia de Seguridad de la Información.
- xv. Elaborar informes correspondientes a la etapa de operatividad, soporte y mantenimiento del Producto 3.1, en materia de Seguridad de la Información.
- xvi. Otras actividades relacionadas al objeto del servicio.

7. PRODUCTOS E INFORMES A ENTREGAR

El consultor realizara la supervisión de la siguiente firma consultora:

- SBCC N° 005-2023, Contratación de una firma consultora para que diseñe, desarrolle e implemente el Sistema de Gestión de Seguridad de la Información (SGSI) para la CGR, desarrollar una auditoría externa de tercera parte al SGSI para obtener la certificación ISO 27001, así como entregar e implementar una herramienta para la gestión del SGSI (Detalle Anexo B)

El consultor elaborará informes por la ejecución del servicio, los cuales deberán ser presentados por cada producto a través de la Mesa de Partes de la Contraloría General de la República, con atención a la Subgerencia de Gobierno Digital con copia a la Subgerencia de Gestión de Inversiones

Producto	Entregable	Contenido (*)	Plazo desde el día siguiente de la suscripción del contrato hasta
Producto 1	Entregable 1	Documento técnico de análisis y revisión del entregable presentado por la firma consultora encargada de la Implementación SBCC N° 005-2023. <ul style="list-style-type: none"> • Entregable 1, plan de gestión del proyecto • Entregable 2, plan de gestión del cambio organizacional 	30 días calendario

Producto 2	Entregable 2	<p>Documento técnico de análisis y revisión del entregable presentado por la firma consultora encargada de la Implementación SBCC N° 005-2023.</p> <ul style="list-style-type: none"> Entregable 3, documento de Diagnóstico de Seguridad Entregable 4, documento de establecimiento del SGSI Entregable 5, documento de la Declaración de Aplicabilidad (SoA) Entregable 6, documento de Normograma de Seguridad 	60 días calendario
Producto 3	Entregable 3	<p>Documento técnico de análisis y revisión del entregable presentado por la firma consultora encargada de la Implementación SBCC N° 005-2023.</p> <ul style="list-style-type: none"> Entregable 7, documento de la organización de seguridad 	90 días calendario
Producto 4	Entregable 4	<p>Documento técnico de análisis y revisión del entregable presentado por la firma consultora encargada de la Implementación SBCC N° 005-2023.</p> <ul style="list-style-type: none"> Entregable 8, política general del SGSI de la CGR y políticas específicas de seguridad 	120 días calendario
Producto 5	Entregable 5	<p>a) Documento técnico de análisis y revisión del entregables presentados por la firma consultora encargada de la Implementación SBCC N° 005-2023.</p> <ul style="list-style-type: none"> Entregable 9, procedimientos de Seguridad Entregable 10, documento con la definición de la Gestión de Activos Entregable 11, documentos acordados para la Gestión de los Riesgos de Seguridad Entregable 12, indicadores del SGSI Entregable 15, documento con las recomendaciones generales y específicas de la revisión de la Arquitectura de Seguridad Entregable 16, informe con las recomendaciones para mejorar la gestión del cierre de las vulnerabilidades Entregable 17, informe con los resultados de las pruebas de ingeniería social 	150 días calendario
Producto 6	Entregable 6	<p>Documento técnico de análisis y revisión del entregables presentados por la firma consultora encargada de la Implementación SBCC N° 005-2023.</p> <ul style="list-style-type: none"> Entregable 18, informe Revisión de configuración de componentes de seguridad Entregable 19, documento de instalación de la herramienta del SGSI Entregable 20, documento de la Auditoría Interna del SGSI 	180 días calendario
Producto 7	Entregable 7	<p>Documento técnico de análisis y revisión del entregable presentado por la firma consultora encargada de la Implementación SBCC N° 005-2023.</p> <ul style="list-style-type: none"> Entregable 21, documento de la Auditoría Externa del SGSI 	210 días calendario
Producto 8	Entregable 8	Documento Técnico respecto a la operatividad del primer mes de la Implementación, problemas presentados y soluciones implementadas o propuestas (de existir)	240 días calendario
Producto 9	Entregable 9	Documento Técnico respecto a la operatividad del segundo mes de la Implementación, problemas presentados y soluciones implementadas o propuestas (de existir)	270 días calendario
Producto 10	Entregable 10	Documento Técnico respecto a la operatividad del tercer mes de la Implementación, problemas presentados y soluciones implementadas o propuestas (de existir)	300 días calendario
Producto 11	Entregable 11	Documento Técnico respecto a la operatividad del cuarto mes de la Implementación, problemas presentados y soluciones implementadas o propuestas (de existir)	330 días calendario
Producto 12	Entregable 12	Informe final de la consultoría, que incluya hallazgos, lecciones aprendidas y recomendaciones para optimizar las implementaciones en el futuro en la CGR.	360 días calendario

(*) En caso no se puedan culminar las actividades o revisión del mes, estas serán cubiertas en el siguiente mes o posteriormente, siempre y cuando haya sido por una demora de las Firma consultora contratada a supervisar.

En caso de existir observaciones a los productos, la Contraloría General de la República notificará al Consultor dentro de un plazo máximo de tres (3) días hábiles posteriores a la recepción del producto. Para lo cual, el Consultor tendrá un plazo máximo de tres (3) días hábiles para levantar estas observaciones, cuyo plazo comenzará a partir del día siguiente de notificada la comunicación.

Los requerimientos de revisión a las observaciones realizadas al producto podrán ser solicitados hasta en dos (2) oportunidades.

De caer el día de entrega del producto un día no laborable, el Consultor presentará el producto al día siguiente hábil.

8. PLAZO

El plazo para la ejecución del servicio será de trecientos sesenta (360) días calendario, contados a partir del día siguiente de suscrito el contrato.

No se incluye en el plazo el tiempo que demore la revisión y aprobación de los productos.

9. PERFIL

El consultor que se encargará de realizar el servicio deberá cumplir con los siguientes requisitos:

A. Formación Académica

Ingeniero (a) en la carrera universitaria en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería de Sistemas y/o Cómputo o Ingeniería Electrónica o Ingeniería de Telecomunicaciones o Ingeniería Industrial o afines.

B. Capacitación

- Curso o certificación en ISO 27001 o Seguridad de la Información o Gobierno Electrónico o Gobierno Digital o Gestión de TI.
- Curso o certificación en Gestión de Proyectos o Scrum.
- Deseable curso o certificación ITIL
- Deseable curso o certificación como Auditor líder ISO 27001.

C. Experiencia General

Experiencia mínima de siete (7) años laborando como jefe, analista, especialista, o coordinador en los departamentos de sistemas o informática o TI

D. Experiencia Específica

- Experiencia mínima de tres (3) años en actividades relacionada a TI o Seguridad de la Información
- Deseable Experiencia mínima de un (01) año en proyectos con financiamiento externo.

E. Características Personales y Profesionales

- Capacidad de trabajo en equipo y bajo presión.
- Compromiso y responsabilidad en el cumplimiento de metas y objetivos.
- Habilidad de trabajo con grupos interdisciplinarios de profesionales.
- Comportamiento ético.
- Vocación de servicio.
- Reserva y confidencialidad de la información.

La experiencia se contabilizará a partir de la condición de egresado.

La formación académica y la capacitación se acreditará mediante copia simple del diploma o constancias o certificados o cualquier otra documentación que de manera fehaciente demuestre la formación académica requerida.

La experiencia general y específica se acreditará mediante copia simple de contratos y su respectiva conformidad o constancias o certificados o cualquier otra documentación que de manera fehaciente demuestre la experiencia requerida.

10. **MONTO**

La retribución económica máxima que se pagará por concepto de honorarios profesionales por los servicios contratados, asciende a la suma de ciento cuarenta y cuatro mil 00/100 soles (S/ 144,000.00), incluyendo los impuestos de Ley o retención que recaiga en el servicio. No se procederá con pagos a cuenta por servicios no efectuados, ni adelanto alguno.

No incluye los costos por concepto de pasajes y viáticos que resulten necesarios para el desarrollo de la consultoría.

11. **FORMA Y CONDICIONES DE PAGO**

El pago se efectuará contra la presentación de los productos señalados en los presentes términos de referencia, al cual se deberá adjuntar el respectivo recibo de honorarios profesionales.

El pago se realizará en armadas iguales de acuerdo al siguiente detalle:

N° de pago	N° de Producto	Plazo	Retribución producto (*) S/
1er Pago	1°	A ser presentado hasta los treinta (30) días calendario, contados a partir del día siguiente hábil del perfeccionamiento del contrato o de la recepción de la orden de servicio.	12,000.00
2do Pago	2°	A ser presentado hasta los sesenta (60) días calendario, contados a partir del día siguiente hábil del perfeccionamiento del contrato o de la recepción de la orden de servicio.	12,000.00
3er Pago	3°	A ser presentado hasta los noventa (90) días calendario, contados a partir del día siguiente hábil del perfeccionamiento del contrato o de la recepción de la orden de servicio.	12,000.00
4to Pago	4°	A ser presentado hasta los ciento veinte (120) días calendario, contados a partir del día siguiente hábil del perfeccionamiento del contrato o de la recepción de la orden de servicio.	12,000.00
5to Pago	5°	A ser presentado hasta los ciento cincuenta (150) días calendario, contados a partir del día siguiente hábil del perfeccionamiento del contrato o de la recepción de la orden de servicio.	12,000.00
6to Pago	6°	A ser presentado hasta los ciento ochenta (180) días calendario, contados a partir del día siguiente hábil del perfeccionamiento del contrato o de la recepción de la orden de servicio.	12,000.00
7mo Pago	7°	A ser presentado hasta los doscientos diez (210) días calendario, contados a partir del día siguiente hábil del perfeccionamiento del contrato o de la recepción de la orden de servicio.	12,000.00
8vo Pago	8°	A ser presentado hasta los doscientos cuarenta (240) días calendario, contados a partir del día siguiente hábil del perfeccionamiento del contrato o de la recepción de la orden de servicio.	12,000.00
9no Pago	9°	A ser presentado hasta los doscientos setenta (270) días calendario, contados a partir del día siguiente hábil del perfeccionamiento del contrato o de la recepción de la orden de servicio.	12,000.00
10mo Pago	10°	A ser presentado hasta los trescientos (300) días calendario, contados a partir del día siguiente hábil del perfeccionamiento del contrato o de la recepción de la orden de servicio.	12,000.00
11vo Pago	11°	A ser presentado hasta los trescientos treinta (330) días calendario, contados a partir del día siguiente hábil del perfeccionamiento del contrato o de la recepción de la orden de servicio.	12,000.00
12vo Pago	12°	A ser presentado hasta los trescientos sesenta (360) días calendario, contados a partir del día siguiente hábil del perfeccionamiento del contrato o de la recepción de la orden de servicio.	12,000.00

(*) Luego de la presentación y aprobación del producto respectivo, conforme a lo señalado en el Numeral 12 "Coordinación, Supervisión y Conformidad" del presente documento.

12. COORDINACIÓN, SUPERVISIÓN Y CONFORMIDAD

El consultor deberá reportar y coordinar sus actividades con la Subgerencia de Gobierno Digital, responsable técnico y área usuaria, quienes serán los encargados de brindar la conformidad a los productos e informes.

La conformidad del servicio será emitida por la Subgerencia de Gobierno Digital.

13. DERECHOS DE PROPIEDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

El consultor deberá declarar que en la medida de que el servicio prestado es por encargo, y el costo de su ejecución es asumida por la CGR; todo producto o materiales (impresos, estudios, informes, gráficos, programas, software de computación u otros), que se genere por el servicio, es de propiedad de la CGR, no constituyéndose títulos de propiedad, derechos de autor y otro tipo de derechos para el consultor; el mismo que a mérito de los presente TDR, cede en forma exclusiva y gratuita, sin generar retribución adicional a lo estipulado en el presente documento.

Asimismo, durante la vigencia del servicio y dentro de los dos (2) años siguientes a su término, el consultor no podrá revelar ninguna información confidencial o de propiedad de la CGR relacionada con los servicios, con el contrato que se genere o las actividades u operaciones de la CGR. Toda la información a la que el consultor tuviere acceso, durante o después de la ejecución del servicio, tendrán carácter confidencial, quedando expresamente prohibido su divulgación a terceros (excepto al BID) por parte del consultor, a menos que la CGR otorgue mediante pronunciamiento escrito la autorización correspondiente.

14. ANEXO

- En el anexo A se establecen las especificaciones y estructura de los documentos a ser presentados por tipo de producto.
- En el anexo B se detallan los entregables de la SBCC N° 005-2023, Contratación de una firma consultora para que diseñe, desarrolle e implemente el Sistema de Gestión de Seguridad de la Información (SGSI) para la CGR, desarrollar una auditoría externa de tercera parte al SGSI para obtener la certificación ISO 27001, así como entregar e implementar una herramienta para la gestión del SGSI

ANEXO A – ESPECIFICACIONES DE LOS ENTREGABLES

I. ESPECIFICACIONES GENERALES

Los informes deben redactarse teniendo en cuenta las siguientes especificaciones:

1. Letra arial 11.
2. Espacio simple.
3. Carátula indicando entre otros, nombre de consultoría, nombre del consultor y número de entregable.
4. Impresión a doble cara.
5. Páginas numeradas en la parte inferior derecha.
6. Índice numerado de páginas.

II. ESPECIFICACIONES PARA LOS ENTREGABLES

Tendrá la siguiente estructura:

1. Carátula
2. Índice
3. Introducción
4. Objetivo de consultoría
5. Productos a alcanzar
6. Actividades a cumplir por cada producto
7. Cronograma
8. Anexo(s)

III. CONSIDERACIONES GENERALES DEL PRODUCTO, A SER TENIDAS EN CUENTA:

- Tapa del documento en el que se precisa el nombre de la consultoría, nombre del producto, el nombre del autor, la fecha de presentación y el nombre y logo de la CGR.
- Incluir índice de capítulos, así como de tablas o cuadros y de gráficos cuando corresponda.
- Incluir una lista de abreviaturas o acrónimos, en caso que se usen siglas en el documento.
- Incluir un glosario de términos que requieran de explicación inicial para facilitar la lectura del documento.
- El resumen ejecutivo dará cuenta de los aspectos más relevantes del trabajo encargado.
- De acuerdo con la naturaleza y características del producto a entregar, el documento se dividirá en capítulos, los que estarán debidamente numerados.
- Las páginas del documento estarán debidamente numeradas.
- Las referencias bibliográficas deberán incluirse al final del documento.
- El consultor presentará sus entregables en la Unidad Orgánica supervisora.
- A cada producto corresponde un pago y, en consecuencia, una fecha improrrogable de entrega.
- El consultor se compromete a ceder los derechos patrimoniales de autor de los productos y documentos elaborados.
- El consultor se compromete a guardar reserva de toda aquella información interna a la que tenga acceso para la ejecución de esta consultoría, cualquier uso de esta información, deberá ser autorizada previamente por la CGR.
- Todos los productos deberán de ser entregados y sustentados en la forma y plazos que se indican en estos términos de referencia.
- A la entrega del último producto, se adjuntarán las bases de datos, códigos de programación u otros materiales utilizados por el consultor o que le hayan sido entregados a este por la CGR durante el proceso de ejecución de la consultoría.

ANEXO B – PRODUCTOS A PRESENTAR POR LA FIRMA CONSULTORA SBCC N° 005-2023¹

PRODUCTO	DESCRIPCIÓN
Producto 1 (Gestión del proyecto de SGSI)	<ul style="list-style-type: none"> • Ent01: Plan de gestión del proyecto que incluya: <ul style="list-style-type: none"> ○ Cronograma detallado. ○ Plan de Gestión. ○ Plan de Calidad del Proyecto. ○ Plan de Gestión y Respuesta a Riesgos. ○ Plan de Comunicaciones. ○ Plan de Gestión de Cambios. ○ Plan de Recursos del proyecto. ○ Presentación de Kick-Off.
	<ul style="list-style-type: none"> • Ent02: Plan de gestión del cambio organizacional para el proyecto, que incluya: <ul style="list-style-type: none"> ○ Estrategia de gestión del cambio organizacional. ○ Plan de comunicaciones a los impactados por el proyecto. ○ Plan de capacitaciones.
Producto 2 (Diseño e implementación del SGSI)	<ul style="list-style-type: none"> • Ent03: Documento de Diagnostico de Seguridad respecto a la ISO 27001, que incluya: <ul style="list-style-type: none"> ○ Definición de niveles y criterios de madurez en seguridad. ○ Valoración de las cláusulas de la ISO 27001 ○ Valoración de los controles de la ISO 27001 ○ Informe de evaluación de madurez de la seguridad en la CGR. ○ Recomendaciones generales y específicas ○ Conclusiones del Diagnóstico.
	<ul style="list-style-type: none"> • Ent04: Documento de establecimiento del SGSI, que incluya: <ul style="list-style-type: none"> ○ Contexto. ○ Partes interesadas. ○ Requisitos de partes interesadas. ○ Principios de seguridad ○ Alcance del SGSI ○ Objetivos del SGSI ○ Relación de todos los documentos necesarios para el SGSI
	<ul style="list-style-type: none"> • Ent05: Documento de la Declaración de Aplicabilidad (SoA) para el SGSI de la CGR.
	<ul style="list-style-type: none"> • Ent06: Documento de Normograma de Seguridad
	<ul style="list-style-type: none"> • Ent07: Documento de la organización de seguridad que incluya: <ul style="list-style-type: none"> ○ Diseño y desarrollo de la Matriz RACI del SGSI. ○ Matriz RACI (Responsable, Aprobador, Consultado e Informado) del SGSI.
	<ul style="list-style-type: none"> • Ent08: Política General del SGSI de la CGR, y Políticas Específicas de Seguridad de la Información, Ciberseguridad y Seguridad Digital, del SGSI de la CGR.
	<ul style="list-style-type: none"> • Ent09: Procedimientos de Seguridad necesarios para el establecimiento y mejora continua del SGSI, acordados en el diseño del SGSI, debidamente aprobados por la CGR y formalizados, que además incluya: <ul style="list-style-type: none"> ○ Evidencias de la divulgación de cada uno de los procedimientos a los diferentes interesados. ○ Evidencias a través de actas del acompañamiento en la implementación de cada uno de los procedimientos.
	<ul style="list-style-type: none"> • Ent10: Documento con la definición de la Gestión de Activos de Seguridad, que incluya: <ul style="list-style-type: none"> ○ La manera en cómo se deben identificar, clasificar y valorar los activos de seguridad de la información, ○ Como se deben mantener actualizados ○ Responsabilidades en cuanto a la gestión de los activos de seguridad. ○ Matriz de Activos de seguridad del proceso de Gestión de Tecnologías de la Información y Comunicaciones (Gerencia de TI y sus tres subgerencias). ○ Evidencias de la ejecución de los Talleres para socializar la manera en cómo se deben gestionar los activos de seguridad de la información.
	<ul style="list-style-type: none"> • Ent11: Documentos acordados para la Gestión de los Riesgos de Seguridad, que incluya: <ul style="list-style-type: none"> ○ La manera en cómo se deben identificar, caracterizar, valorar, definir planes de tratamiento y responsables de los activos de seguridad de la información. ○ Como se debe realizar el debido seguimiento y control. ○ Responsabilidades en cuanto a la gestión de los riesgos de seguridad. ○ Matriz de Riesgos de Seguridad de la Información, de la Gerencia de Tecnologías de la Información (GTI y sus tres subgerencias) llenadas y aprobadas.

¹ Contratación de una firma consultora para que diseñe, desarrolle e implemente el Sistema de Gestión de Seguridad de la Información (SGSI) para la CGR, desarrollar una auditoría externa de tercera parte al SGSI para obtener la certificación ISO 27001, así como entregar e implementar una herramienta para la gestión del SGSI

PRODUCTO	DESCRIPCIÓN
	<ul style="list-style-type: none"> o Actas resultantes de la gestión de riesgos que incluya la lista de los participantes. o Evidencias de la ejecución de los Talleres para socializar la manera en cómo se deben gestionar los riesgos de seguridad de la información. <ul style="list-style-type: none"> • Ent12: Indicadores del SGSI, debidamente aprobados por la CGR, formalizados y divulgados. • Ent13: Documento con las evidencias de la ejecución del Plan de cambio organizacional. • Ent14: Documento con las evidencias de la ejecución de los cursos como se solicitaron.
Producto 3 (Revisión del SGSI)	<ul style="list-style-type: none"> • Ent15: Documento con las recomendaciones generales y específicas de la revisión de la Arquitectura de Seguridad. • Ent16: Informe con las recomendaciones para mejorar la gestión del cierre de las vulnerabilidades. • Ent17: Informe con los resultados de las pruebas de ingeniería social, que incluya: <ul style="list-style-type: none"> o Evidencia de cada una de las pruebas de ingeniería social. o Recomendaciones generales y específicas como resultado de las pruebas, definiendo planes de tratamiento para el cierre de las brechas identificadas. • Ent18: Informe Revisión de configuración de componentes de seguridad, que incluya: <ul style="list-style-type: none"> o Proceso de revisión realizado por cada uno de los componentes de seguridad. o Recomendaciones por cada uno de los componentes de seguridad. o Actas con el reporte de las horas de asesoría y acompañamiento para la implementación de las recomendaciones. • Ent19: Documento de instalación de la herramienta del SGSI, que incluya: <ul style="list-style-type: none"> o Evidencia de la configuración de la herramienta del SGSI. o Entrega de licenciamiento de la herramienta del SGSI a nombre de la CGR (modalidad SaaS). o Evidencias de la configuración de cada uno de los módulos de la herramienta con todas las funciones y actividades del SGSI y el cargue de todos los entregables del proyecto. o Documentación relacionada con soporte y asistencia técnica directamente con el fabricante y proveedor de la herramienta del SGSI.
Producto 4 (Evaluación del SGSI)	<ul style="list-style-type: none"> • Ent20: Documento de la Auditoría Interna del SGSI, que incluya como mínimo, lo siguiente, más la información que tenga establecida la CGR para el desarrollo de Auditorías Internas de los sistemas de gestión: <ul style="list-style-type: none"> o Plan de Auditoría o Presentación de Inicio de la Auditoría o Informe de la Auditoría con las No Conformidades, observaciones y recomendaciones que se consideren. o Matriz de Riesgos identificados en la auditoría, en el formato establecido por la CGR. o Presentación ejecutiva con los resultados de la auditoría. o Acta de reunión de presentación de resultados de la Auditoría. o Actas de sesiones de acompañamiento y asesoría en el cierre de No Conformidades y oportunidades de mejora identificadas en la Auditoría Interna. • Ent21: Documento de la Auditoría Externa del SGSI, que incluya como mínimo, lo siguiente: <ul style="list-style-type: none"> o Contrato de la Auditoría Externa entre la firma de certificación de tercera parte y la firma consultora. o Acuerdo de Confidencialidad firmado entre la CGR y la firma de Certificación de tercera parte. o Plan de Auditoría Externa o Presentación de Inicio de la Auditoría Externa. o Informe de la Auditoría Externa con las No Conformidades, observaciones y recomendaciones que se consideren. o Entrega de la Matriz de Riesgos identificados en la auditoría externa, en el formato establecido por la CGR. o Presentación ejecutiva con los resultados de la auditoría externa. o Acta de reunión de presentación de resultados de la Auditoría externa. o Actas de sesiones de acompañamiento y asesoría por parte de la firma consultora en el cierre de No Conformidades y oportunidades de mejora identificadas en la Auditoría Externa, dentro de los plazos definidos por la firma de certificación de tercera parte para la obtención de la certificación de la ISO 27001 para el SGSI con alcance al proceso o procesos seleccionados en coordinación con la Gerencia de TI y sus tres subgerencias. o Una vez que el resultado de la auditoría de certificación sea favorable con respecto al cumplimiento de la ISO 27001 del SGSI de la CGR, se debe generar y entregar a la CGR el certificado para el SGSI con alcance al proceso o procesos definidos en coordinación con la Gerencia de TI y sus tres subgerencias.