CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ

PROYECTO:

"MEJORAMIENTO DE LOS SERVICIOS DE CONTROL GUBERNAMENTAL PARA UN CONTROL EFECTIVO, PREVENTIVO Y FACILITADOR DE LA GESTIÓN DE PÚBLICA" – BID3

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

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

LA CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

TÉRMINOS DE REFERENCIA

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

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

MAYO 2023

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

1. INTRODUCCIÓN

La Contraloría General de la República (CGR) es el órgano superior del Sistema Nacional de Control (SNC) 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.

Así mismo, es el ente rector del SNC, dotado de autonomía administrativa, funcional, económica y financiera, que tiene por misión dirigir y supervisar con eficiencia y eficacia el control gubernamental orientando su accionar al fortalecimiento y transparencia de la gestión de las entidades, la promoción de valores y la responsabilidad de los funcionarios y servidores públicos, así como contribuir con los Poderes del Estado en la toma de decisiones y con la ciudadanía para su adecuada participación en el control social.

La actual gestión de la CGR tiene como uno de sus objetivos principales modernizar y mejorar el SNC a fin de asegurar su eficacia y eficiencia en el control contra la corrupción y la inconducta funcional para así crear valor público. El Sistema de Gestión de Seguridad de la Información (SGSI), diseñado e implementado conforme a las necesidades de la Entidad, se enmarca en la normativa del Estado Peruano, y en estándares internacionales de buenas prácticas como ISO 27001, aplicado al entorno y lineamientos de las estrategias institucionales como el Plan Estratégico Institucional (PEI), el Plan de Gobierno Digital 2021-2024, la cadena de valor institucional y las políticas de Transformación Digital del Gobierno Peruano.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Con la implementación del Sistema de Gestión de Seguridad de la Información en la CGR se busca:

- Definir y establecer los lineamientos en seguridad de la información y seguridad digital, que permitan garantizar la confidencialidad, integridad y disponibilidad de la información, conservando, salvaguardando y protegiendo la información producida y recibida en los procesos de la CGR.
- Servir de apoyo a la CGR frente al cumplimiento de su visión y misión.
- Documentar los lineamientos que permitan dar una directriz sobre los controles de seguridad a implementar en la CGR con el fin de proteger los activos de información.
- Fortalecer la cultura en seguridad de la información, por parte de los trabajadores, contratistas y terceros que tengan acceso o hagan uso de la información de la CGR.
- Generar las políticas, lineamientos, procedimientos, guías y en general toda la documentación necesaria para el establecimiento del Sistema de Gestión de Seguridad de la Información.

2. ANTECEDENTES

Actualmente, la CGR está en la etapa de planeación de una serie de proyectos enmarcado en el Contrato Préstamo Nº 4724/OC-PE entre la República del Perú y el Banco Interamericano de Desarrollo (BID) para financiar el Proyecto “Mejoramiento de los servicios de control gubernamental para un control efectivo, preventivo y facilitador de la gestión pública”, el mismo que está diseñado para contribuir a la mejora de los servicios de control gubernamental, con el fin de mejorar la eficiencia y efectividad en el uso de los recursos del Estado.

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

El Proyecto mencionado comprende 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.

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

El “Componente 3. Adecuado acceso a TIC en los procesos de control gubernamental” está conformado por varias acciones asociadas a proyectos de Gobierno y Gestión de TI, Arquitectura Empresarial, Seguridad de la información, y proyectos para el fortalecimiento de los sistemas de información y de la infraestructura tecnológica de la CGR, particularmente, este proyecto de Seguridad de la Información se enmarca en el Proyecto Interno 3.1.1 “Diseño e Implementación del Nuevo Modelo de Gobierno y Gestión de Tecnologías de la Información y Comunicaciones”.

Los Objetivos Estratégicos Institucionales (OEI) que orientan las acciones y funciones de la CGR, y asocian proyectos e iniciativas internas que propenden por la mejora de los servicios de la CGR. A continuación, se listan los Objetivos Estratégicos Institucionales que deben ser considerados dentro de la ejecución del proyecto del Sistema de Gestión de Seguridad de la Información:

Código del Objetivo Estratégico	**Objetivo Estratégico Institucional (OEI)**	**Descripción OEI**
OEI.01	Contribuir a la reducción de la inconducta funcional y la corrupción en las entidades públicas	Orientado a que La Contraloría pueda accionar e implementar medidas de prevención, detección, investigación, resarcimiento y sanción que permitan una mayor eficiencia y eficacia en los servicios de control; así como asegurar el oportuno deslinde de responsabilidades de orden administrativo funcional, civil y penal, contribuyendo a la reducción de la inconducta funcional y actos de corrupción en las entidades públicas.
OEI.02	Contribuir a la gestión eficiente y eficaz de los recursos públicos en beneficio de la población	Orientado a que La Contraloría, mediante el ejercicio del control previo y simultáneo, contribuya a mejorar la toma de decisiones y el cumplimiento de metas y resultados de las entidades públicas, promoviendo mejoras en la gestión pública, la prestación de servicios públicos de calidad y la implementación del control interno; así como la realización de controles concurrentes efectivos que alerten oportunamente sobre los riesgos de las operaciones de la entidad o situaciones adversas, contribuyendo a través de la mitigación de riesgos a la reducción de la inconducta funcional y la corrupción. Así como la ampliación de la cobertura del control a través del desarrollo del control itinerante en entidades descentralizadas bajo un enfoque que oriente la administración de sus recursos.
OEI.03	Promover la participación ciudadana a través del control social y la formación en valores de integridad	De carácter preventivo orientado a promover la formación de valores de integridad en el sector público y la participación efectiva de la ciudadanía y sus organizaciones representativas en el control social, sobre la base de los mecanismos de transparencia, rendición de cuentas y acceso a la información establecidos para mejorar la relación Estado - sociedad; asimismo, fomentará el derecho ciudadano a denunciar las inconductas funcionales y el uso indebido de recursos públicos por los/las funcionarios/as del Estado, y su atención oportuna por parte del Sistema Nacional de Control. Involucra, además, la formación en valores de integridad entre quienes desempeñan función pública, y otros estamentos clave de la sociedad.
OEI.04	Fortalecer la gestión institucional del Sistema Nacional de Control	Orientado a mejorar los recursos, procesos y capacidades institucionales para dar soporte a las operaciones misionales y administrativas, incidiendo en el cumplimiento de los otros objetivos estratégicos. Involucra el desarrollo normativo para los servicios de control, la mejora de los procesos internos estratégicos, misionales y administrativos; el desarrollo de competencias en el capital humano, la modernización tecnológica y el desarrollo de sistemas de información y comunicación; así mismo, en el campo organizacional, persigue mejoras en el modelo de gestión del SNC y el fortalecimiento de la articulación interinstitucional con las entidades públicas conformantes de la cadena de valor del control.
OEI.05	Implementar la gestión de riesgos de desastres	Orientado a institucionalizar la gestión de riesgos de desastres en la Contraloría, priorizando los planes, programas y acciones de prevención y reducción de los riesgos operacionales; así como la sensibilización y preparación del personal en la sede central y

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

Código del Objetivo Estratégico	Objetivo Estratégico Institucional (OEI)	Descripción OEI
		gerencias regionales para prever y enfrentar los daños físicos o materiales de origen natural o inducidos que origine la ocurrencia del desastre, evitando las pérdidas de bienes, documentos e información que garanticen la sostenibilidad y continuidad de las labores de control y administrativas en el logro de los Objetivos Estratégicos Institucionales.

En las siguientes secciones se describe el objetivo y alcance del proyecto del Sistema de Gestión de Seguridad de la Información que debe ser ejecutado para la CGR.

3. OBJETIVO

Objetivo general

Diseñar, desarrollar e implementar el Sistema de Gestión de Seguridad de la Información (SGSI) para la CGR, definir el alcance de la auditoría para la certificación en coordinación con la Gerencia de TI y 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, y apalancar el cumplimiento de los objetivos estratégicos de la Entidad, contribuyendo a proteger la información y los diferentes servicios que se brindan[1]

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Objetivos específicos:

La CGR persigue los siguientes objetivos específicos para la seguridad de la información institucional:

- Elaborar y/o actualizar desarrollar toda la documentación requerida y necesaria para establecer el Sistema de Gestión de Seguridad de la Información.
- Implementar el Sistema de Gestión de Seguridad de la Información.
- Realizar una Auditoría Interna al Sistema de Gestión de Seguridad de la Información con el fin de identificar oportunidades de mejora en el Sistema de Gestión de Seguridad de la Información.
- Entregar e implementar una herramienta que permita gestionar de manera completa y oportuna el Sistema de Gestión de Seguridad de la Información.
- Realizar una Auditoría Externa del SGSI con alcance al proceso de Gestión de Tecnologías de la Información y Comunicaciones, con el fin de aplicar a la certificación ISO 27001 vigente.
- Como parte del servicio, la firma consultora debe garantizar la certificación del SGSI de la CGR ante el ente certificador[2].

4. ALCANCE DE LA CONSULTORÍA: ACTIVIDADES Y ENFOQUE

1.

Para la ejecución de este proyecto se debe hacer uso de buenas prácticas en seguridad de la información como normas técnicas de la familia ISO 27000, ISO 22301 Continuidad del Negocio, ISO 27032 Ciberseguridad, entre otras, y la normatividad, definiciones y lineamientos del Gobierno Peruano referentes al Sistema Nacional de Transformación Digital, la Ley de Gobierno Digital y a los planteamientos del Plan de Gobierno Digital de la CGR.

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Acompañado de la estrategia institucional, su organización de procesos, durante la ejecución del proyecto, la firma consultora debe entender y analizar, entre otros, la siguiente información:

[1] El objetivo tiene como alcance la generación de la documentación requerida para implementar y certificar el SGSI bajo la norma ISO 27001 en su versión vigente.

2 Se refiere a la entidad que realiza la auditoría externa, Esta entidad es la que se contrata para tal labor.

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

- Estructura organizacional y de roles de TI y de la CGR de la sede central y de las sedes regionales (ROF_Integrado actual de la CGR).
- Plan de Gobierno Digital 2021-2024 (RC_292-2021 CG Plan de Gobierno Digital), que contiene información sobre la integración de la CGR con el portal GOB.PE, servicios de interoperabilidad, y lineamientos que deben ser integrados como parte de las definiciones de la Seguridad de la Información institucional.
- Comité de Gobierno y Transformación Digital (RC_382-2019-CG Mod Comité Gobierno Digital), que estructura iniciativas relacionadas con la transformación digital de la CGR para considerar el uso de nuevas tecnologías que apoyen la implementación del Gobierno Digital, la definición de estándares y buenas prácticas en gestión y gobierno de tecnologías digitales, interoperabilidad, seguridad digital, e identidad digital en la CGR.
- Plan Estratégico Institucional – PEI – (RC_124-2022-CG PEI 2022 – 2024) que define los objetivos estratégicos institucionales, y su alineación con la política institucional, la misión y valores institucionales.
- Cadena de Valor de la CGR (RC_124-2022-CG PEI 2022 – 2024), que vincula la calidad de los productos y servicios de control y expresa los beneficios que reportan a las partes interesadas, y su articulación con la ciudadanía, con las entidades públicas sujetas de control, con las Procuradurías, el Ministerio Público y Poder Judicial.
- Trámites y servicios de la CGR que se encuentran publicados en el portal web institucional, y que ofrecen cerca de 34 trámites que los ciudadanos pueden utilizar en su interacción con la CGR (https://www.gob.pe/institucion/contraloria/tramites-y-servicios).
- GU-MODER-01 Guía Gestión del Riesgo en la Contraloría General de la República.
- Resolución Nº 382-2020-CG. "Gestión del Riesgo en la Contraloría General de la República".
- Resolución N°382-2019-CG. Estructura de Puestos Clasificados y el cuadro de Puestos de la CGR.
- Propuesta de Política de Seguridad de la Información.
- Propuesta de Indicadores del Sistema de Gestión de Seguridad de la Información.
- Ley de Protección de Datos Personales N°29733
- Reglamento de la Ley N°29733 Decreto Supremo N°003-2013-JUS
- PR-TI-02 Atención de Requerimientos de Accesos Informáticos
- PR-TI-03 Análisis, Diseño y Desarrollo de Sistemas
- PR-TI-04 Pruebas de Control de Calidad del Software
- PR-TI-05 Puesta a Producción del Software
- PR-TI-06 Respaldo y Restauración de Información
- PR-GSEG-02 Procedimiento Evaluación a las Medidas de Seguridad Implementadas para la Protección de Datos Personales
- PR-GSEG-03 Procedimiento Gestión del Ejercicio de los Derechos del Titular de Datos Personales
- PR-GSEG-04 Gestión de Riesgos en Seguridad de la Información.
- PR-GSEG-05 Procedimiento de Gestión de Incidentes de seguridad de la información.
- PR-GSEG-08 Procedimiento Inspecciones de Seguridad
- PR-GSEG-09 Procedimiento Recepción de Ciudadanos y Atención de Visitas en las Instalaciones de la Contraloría General de la República
- PR-GSEG-10 Procedimiento Gestión de Requerimientos de Áreas restringidas

De forma paralela a la ejecución del proyecto de Seguridad de la Información, la CGR tiene planeada la ejecución de otros proyectos liderados por la Gerencia de Tecnologías de la Información, por lo que el consultor debe trabajar en pro de sincronizar los diseños realizados desde la seguridad de la información con los siguientes proyectos, esto implica mantener reuniones con el equipo de supervisión de la CGR para lograr una cohesión entre los proyectos:

- Proyecto para el diseño e implementación del Modelo de Gobierno y Gestión de TI: de este proyecto se deben contemplar las definiciones y responsabilidades que se hagan para los comités de “Gobierno y Transformación Digital" y el "Comité Estratégico de TI", que deben ser

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

integradas con el modelo de gobierno de la seguridad de la información de la CGR, de tal manera que el Gobierno y Gestión de TI se encuentre sincronizado con el modelo de gobierno de la seguridad de la información institucional.

Para la estructuración de estos términos de referencia, se realizó un diagnóstico de seguridad teniendo en cuenta la norma NTP-ISO-IEC 27001 versión 2014, desde el punto de vista de los controles implementados y de su documentación exigida a nivel de seguridad de la información, el cual se puede ver en el documento "DIAGNÓSTICO SITUACIONAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI"[3], y en el que se puede ver el detalle de las actividades realizadas, los criterios de evaluación y los resultados obtenidos, los cuales se pueden tomar como información base que debe ser contrastada y actualizada según el alcance del proyecto propuesto. Dicho diagnóstico será entregado a la firma consultora adjudicada, al inicio de la ejecución del proyecto.

El proyecto debe iniciar con una definición del contexto de la CGR, identificando las partes interesadas internas y externas, los requisitos de seguridad de estas partes interesadas, la definición del alcance y de los objetivos del Sistema de Gestión de Seguridad de la Información, así como la identificación de todos los documentos necesarios para el establecimiento y mejora continua del SGSI de la CGR. (por ejemplo: políticas, procesos, procedimientos, guías, lineamientos, estándares, etc.). El Sistema de Gestión de Seguridad de la Información debe ser integrado al Sistema Integrado de Gestión de la CGR.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Luego se debe verificar y asegurar la elaboración y/o actualización de todos los documentos acordados en la Fase de "Definición y diseño del SGSI", necesarios para establecer el SGSI de la CGR, siguiendo los lineamientos estructurales para la elaboración de cada uno de ellos.

Se debe realizar la identificación y caracterización de los activos de seguridad de la información para el proceso de Gestión de Tecnologías de la Información y Comunicaciones (Gerencia de TI y sus tres subgerencias), y así mismo, la identificación, valoración, planes de tratamiento y responsables de los riesgos de seguridad de la información para el proceso de Gestión de Tecnologías de la Información y Comunicaciones (Gerencia de TI y sus tres subgerencias).

Revisión de la Arquitectura de Seguridad de los diferentes componentes de seguridad onpremise y cloud, se debe revisar como mínimo aspectos de alta disponibilidad, únicos puntos de fallo, riesgos, capacidad, licenciamiento, componentes de seguridad necesarios y con los cuales la CGR no cuenta y su correspondiente justificación, etc.

Realizar el análisis del aseguramiento y configuración de los componentes o dispositivos de seguridad con que cuenta la CGR, emitiendo las recomendaciones del caso, y acompañando a los administradores por parte de la CGR en el cierre de las brechas identificadas.

Analizar la gestión en el cierre de brechas de seguridad de las pruebas de vulnerabilidades de la plataforma tecnológica, emitiendo las recomendaciones del caso, para lo cual, en el inicio de la ejecución del proyecto, la CGR le entregará a la firma consultora los informes de vulnerabilidades que se hayan ejecutado en los dos últimos años.

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Realizar pruebas de Ingeniería Social (Phishing, Suplantación de Identidad, Recorridos internos para identificar falencias y riesgos, y 2 más, propuestas por la Consultoría para revisar y acordar en conjunto con la CGR).

Realizar la adquisición y parametrización de una Herramienta para la Gestión del SGSI (documentación del SGSI, Activos, Riesgos, Continuidad del Negocio, etc.), sobre la cual se debe

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

[3] Parte del servicio de la consultoría realizada según contrato 038-2022-CG-UE002-BID.

realizar toda la parametrización del SGSI de la CGR y realizar todo el cargue de la información correspondiente.

Se debe realizar una transferencia de conocimiento y capacitación del personal de la CGR, las cuales deben incluir talleres, retroalimentación y evaluación final.

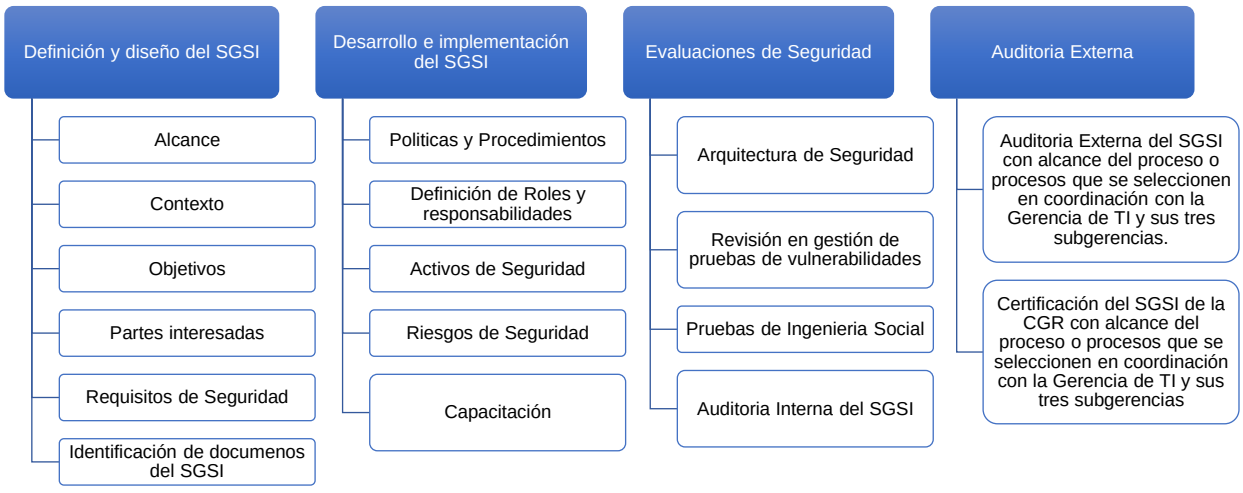
Se debe elaborar e implementar un plan de auditoría interna al Sistema de Gestión de Seguridad de la Información, con el fin de verificar si el sistema es conforme con los requisitos de la norma ISO 27001 vigente y publicada por la ISO al momento de iniciar la ejecución del proyecto, y los que la Entidad defina se deban tener implementados, y con el fin de contar con la evidencia de los registros de las evaluaciones realizadas al Sistema de Gestión, la auditoría interna tendrá como alcance el proceso de Gestión de Tecnologías de la Información y Comunicaciones (Gerencia de TI y sus tres subgerencias).

Realizar una Auditoría Externa del SGSI teniendo como alcance el o los procesos definidos en coordinación con la Gerencia de Ti y sus subgerencias (Preparación, desarrollo de la auditoria por ente de certificación autorizado para validar y certificar el SGSI, acompañamiento de auditoría por parte de la consultora, acompañamiento cierre NO Conformidades y Oportunidades de mejora por parte de la consultora), para lo cual se deben considerar entes de certificación establecidos en Perú, y aplicar para obtener la Certificación ISO 27001 para el alcance que haya sido definido.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Y durante todo el desarrollo del proyecto, realizar el acompañamiento para la resolución de dudas o consultas y desarrollo de actividades que le competan a la firma consultora y que requiera la CGR para la implementación de los diferentes documentos (políticas, procedimientos, guías, matrices, formatos, etc.) y controles de seguridad (técnicos, administrativos y físicos) definidos durante el diseño y desarrollo del SGSI.

Como parte del presente servicio de seguridad de la información, se incluyen los siguientes componentes:



Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Ilustración 1 – Componentes en alcance del proyecto

Como se puede observar, se tienen cuatro (4) componentes en el alcance del proyecto. El primero está enmarcado en la definición y diseño del SGSI, el segundo en el desarrollo e implementación del SGSI, el tercero en la evaluación de la madurez de aspectos documentales y técnicos de seguridad y la preparación para que en el cuarto componente se realice la auditoría externa de tercera parte a través de una firma de certificación para el SGSI de la CGR, y se obtenga la certificación ISO 27001 para el SGSI de la CGR.

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

a) Estructura de trabajo

Para la ejecución del proyecto se presenta la estructura de desglose de trabajo, que está asociado a las fases en las que se sugiere sea estructurada la ejecución del proyecto.

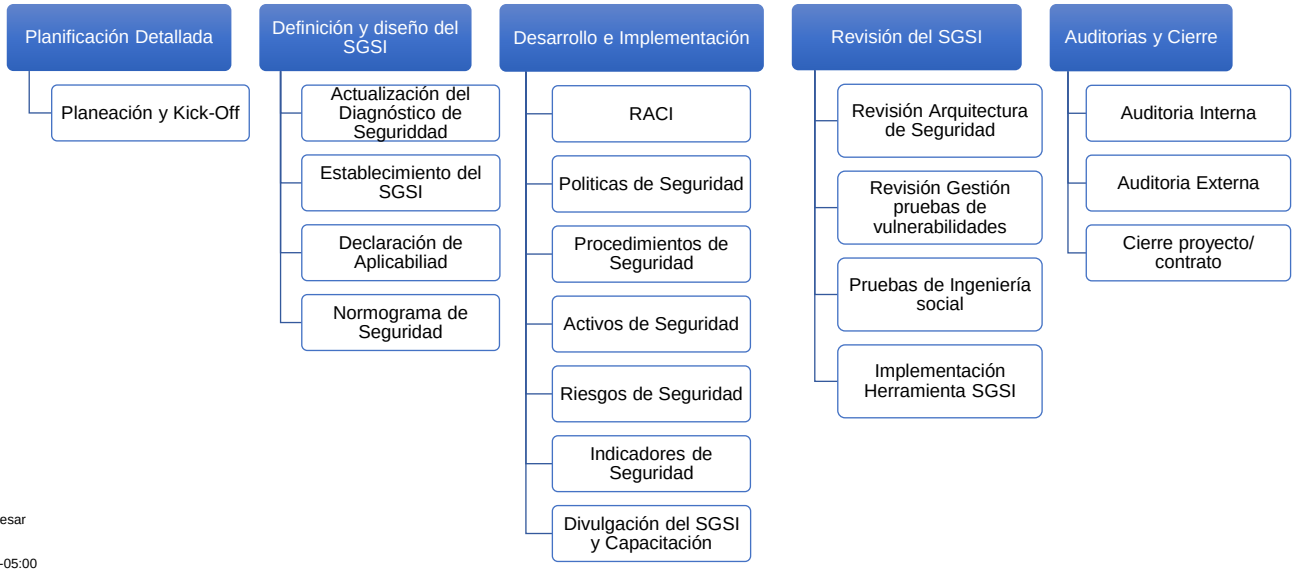


Ilustración 2 – Organización del proyecto

La anterior ilustración esquematiza la estructura de descomposición de trabajo para el presente proyecto, donde cada uno de los paquetes de trabajo contiene actividades y entregables que se deben generar durante la ejecución del proyecto para cada uno de los componentes en alcance.

El proyecto debe diseñarse, desarrollarse e implementarse teniendo en cuenta la última versión de la norma ISO 27001 publicada oficialmente por la ISO en el momento de iniciar la ejecución del proyecto.

La siguiente tabla describe en detalle actividades que debe realizar la firma consultora, y los entregables que se deben producir para dar cubrimiento al alcance del proyecto. La tabla se encuentra organizada en fases y etapas que organizan las actividades a realizar, y finalmente los entregables a elaborar:

Fase	Etapa	Actividades	Entregable
Planificación	Estructura de Gobierno	• Identificar los actores clave tanto a nivel funcional como técnico. • Identificar Interlocutores y Stakeholders. • Estructurar el modelo de gobierno del Proyecto. • Definir los roles y funciones de cada actor • Hacer la estimación de la dedicación. • Hacer la revisión, ajustes y conseguir la aprobación de la estructura de gobierno del proyecto.	• Ent01: Plan de gestión del proyecto que incluya: o Cronograma detallado. o Plan de Gestión. o Plan de Calidad del Proyecto. o Plan de Gestión y Respuesta a Riesgos. o Plan de Comunicaciones. o Plan de Gestión de Cambios. o Plan de Recursos del proyecto. o Presentación de Kick-Off. - Ent02: Plan de gestión del cambio organizacional para el proyecto, que incluya:
	Planeación	• Elaborar el Plan de gestión del proyecto y cronograma de actividades, que contenga el detalle de las actividades a desarrollar, tiempo estimado de duración, fecha de inicio, fecha fin, recurso o responsable de la	

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

Fase	Etapa	Actividades	Entregable
ón Detallada		actividad, actividad o producto entregado y el listado de hitos. • Elaborar el Plan de Calidad del Proyecto, que contenga el equipo de trabajo por parte de la firma consultora, los criterios de calidad y aceptación de productos/entregables, el proceso de gestión del proyecto. • Elaborar el Plan de Gestión y Respuesta a Riesgos. • Elaborar el Plan de Comunicaciones de la gestión del proyecto, que contenga la definición de las entidades, actores o interesados en el proyecto y sus necesidades de comunicación, los formatos y medios de comunicación o divulgación, organización del equipo de trabajo y el proceso de comunicación. • Elaborar el Plan de Gestión de Cambios del proyecto. Este debe incluir la descripción del proceso de Gestión de cambios, el formato de solicitudes de cambio, registro de controles de cambio y la definición de las instancias de decisión. • Elaborar el Plan de Recursos del proyecto, que contenga el listado de colaboradores y sus perfiles, la descripción de las responsabilidades al interior del proyecto, estimación de tiempo y dedicación de los colaboradores. • Desarrollar el plan de gestión del cambio organizacional del proyecto que cubra los componentes de Diseño, Desarrollo e Implementación del SGSI, las evaluaciones al mismo y la Auditoría Externa de certificación en ISO 27001, acompañado de una estrategia de gestión del cambio organizacional, un plan de comunicaciones y un plan de capacitaciones, de transferencia de conocimiento y divulgación del SGSI a todos los interesados internos y externos.	○ Estrategia de gestión del cambio organizacional. ○ Plan de comunicaciones a los impactados por el proyecto. ○ Plan de capacitaciones y de transferencia de conocimiento y divulgación del SGSI a todos los interesados internos y externos.
	Kick-Off	• Hacer el lanzamiento del proyecto al interior de la CGR.	
Definición y diseño del SGSI	Actualización Diagnóstico de Seguridad	• Revisar el Diagnóstico de Seguridad realizado en junio de 2022. • Solicitar a la CGR toda la información que exista relacionada con seguridad. • Analizar la información que exista relacionada con seguridad. • Identificar las áreas y responsable de los temas para evaluar el nivel de desarrollo, implementación y madurez de las cláusulas y controles de la ISO 27001. • Planear las sesiones con las áreas y responsables requeridos para la actualización del Diagnóstico de Seguridad. • Realizar las sesiones de trabajo para la actualización del Diagnóstico de Seguridad. • Documentar y calificar el estado de las cláusulas y controles de la ISO 27001.	• Ent03: Documento de Diagnostico de Seguridad respecto a la ISO 27001, que incluya: ○ 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 especificas ○ Conclusiones del Diagnóstico.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

Fase	Etapa	Actividades	Entregable
		• Comparar el estado actual de seguridad contra el evidenciado en junio de 2022 • Generar los entregables del Diagnóstico de Seguridad • Realizar la socialización de los resultados con los diferentes interesados de la CGR • Elaboración de documentos normativos del proceso de GTI y sus subprocesos	
	Establecimiento del SGSI	• Revisar y documentar el contexto interno y externo de la CGR • Identificar las partes internas y externas interesadas en el SGSI • Identificar y documentar los requisitos de seguridad de las partes interesadas • Establecer los principios del SGSI • Definir el alcance del SGSI del proceso de gestión de TIC. • Definir los objetivos generales y específicos del SGSI. • Definir cuáles son los documentos necesarios para el establecimiento y mejora continua del SGSI de la CGR. (por ejemplo, políticas, procesos, procedimientos, guías, lineamientos, estándares, etc.) • Formalizar el Sistema de Gestión de Seguridad de la Información de acuerdo con los procedimientos establecidos en la CGR.	• Ent04: Documento de establecimiento del SGSI, que incluya: ○ 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
	Declaración de Aplicabilidad	• Identificar cuales controles del Anexo A de la ISO 27001 aplican para el SGSI de la CGR • Documentar las inclusiones y exclusiones de los controles del Anexo A de la ISO 27001 • Valorar el nivel de madurez de cada uno de los controles que aplican para el SGSI	• Ent05: Documento de la Declaración de Aplicabilidad (SoA) para el SGSI de la CGR.
	Normograma de Seguridad (Matriz con la relación de toda la normatividad interna y externa aplicable al SGSI de la CGR)	• Identificar y documentar las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a seguridad de la información. • Para cada una de las anteriores se debe indicar como mínimo: tipo, nombre, quien la expide, fecha de expedición, fecha de entrada para cumplimiento, URL de ubicación, estado actual de aplicación en la CGR	• Ent06: Documento de Normograma de Seguridad
Desarrollo e implementación	RACI	• Identificar todos los roles y responsabilidades relacionados con el SGSI • Definir todas las actividades del SGSI y relacionarlas con los diferentes roles definidos, indicando su relación RACI	• Ent07: Documento de la organización de seguridad que incluya: ○ Diseño y desarrollo de la Matriz RACI del SGSI. ○ Matriz RACI (Responsable, Aprobador, Consultado e Informado) del SGSI.
	Políticas de Seguridad	• Documentar todas las políticas de seguridad definidas en la etapa del Establecimiento del SGSI	• Ent08: Política General del SGSI de la CGR, conforme a los procedimientos establecidos, debidamente aprobada por la CGR, publicada y divulgada a todos los interesados. • Políticas Específicas de Seguridad de la Información, y Seguridad Digital, del SGSI de la CGR, conforme a los procedimientos establecidos, debidamente aprobada por la CGR, publicada y divulgada a todos los interesados.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

Fase	Etapa	Actividades	Entregable
	Procedimientos de Seguridad	• Documentar todos los procedimientos de seguridad definidas en la etapa del Establecimiento del SGSI • Para los procedimientos con los que cuente la CGR, el proveedor revisará e identificar oportunidades de mejora y ajustar. • Para los procedimientos que no estén definidos en la CGR, el proveedor elaborará la documentación teniendo en cuenta los recursos y procesos de la CGR. • Divulgación de cada uno de los procedimientos a los diferentes interesados, los cuales se deben identificar durante el desarrollo de cada uno de los procedimientos del SGSI. • Actas del acompañamiento en la implementación de cada uno de los procedimientos.	• 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: o Evidencias de la divulgación de cada uno de los procedimientos a los diferentes interesados. o Evidencias a través de actas del acompañamiento en la implementación de cada uno de los procedimientos.
	Activos de Seguridad	• Definir, establecer y documentar los lineamientos y la manera en cómo se gestionarán los Activos de Seguridad, definiendo la forma de identificar, clasificar y valorar los activos de seguridad de la información, (por ejemplo, Información, Roles, Hardware, Software, Servicios, Instalaciones, etc.). • Identificar los activos de seguridad del proceso de Gestión de Tecnologías de la Información y Comunicaciones (Gerencia de TI y sus tres subgerencias), con sus propietarios, su clasificación y valoración para identificar su criticidad. • Talleres a los diferentes interesados de la CGR, para socializar la manera en cómo se deben gestionar los activos de seguridad de la información.	• Ent10: Documento con la definición de la Gestión de Activos de Seguridad, que incluya: o La manera en cómo se deben identificar, clasificar y valorar los activos de seguridad de la información, o Como se deben mantener actualizados o Responsabilidades en cuanto a la gestión de los activos de seguridad. o Matriz de Activos de seguridad del proceso de Gestión de Tecnologías de la Información y Comunicaciones (Gerencia de TI y sus tres subgerencias). o Evidencias de la ejecución de los Talleres para socializar la manera en cómo se deben gestionar los activos de seguridad de la información.
	Riesgos de Seguridad	• Revisar la manera en cómo se gestionan los riesgos en la CGR, para lo cual se debe tener presente: El procedimiento “PR-GSEG-04 Gestión de Riesgos en Seguridad de la Información", la Directiva de Riesgos, el procedimiento de riesgos (PR-MODER-04) y los formatos de identificación, análisis y tratamiento de riesgos y demás documentos relacionados que tiene actualmente la CGR, los cuales se deben actualizar, formalizar y ser aprobados por la CGR. • En caso de ser necesario, se deben generar otros documentos que permitan mejorar la gestión del riesgo, los cuales se deben formalizar y aprobar por parte de la CGR. • Identificar los riesgos de seguridad del proceso de Gestión de Tecnologías de la Información y Comunicaciones (Gerencia de TI y sus tres subgerencias), caracterizados, valorados, con planes de tratamiento,	• Ent11: Documentos acordados para la Gestión de los Riesgos de Seguridad, que incluya: o La manera en cómo se deben identificar, caracterizar, valorar, definir planes de tratamiento y responsables de los activos de seguridad de la información. o Como se debe realizar el debido seguimiento y control. o Responsabilidades en cuanto a la gestión de los riesgos de seguridad. o Matriz de Riesgos de Seguridad de la Información de la Gerencia de Tecnologías de la Información (Gerencia de TI y sus tres subgerencias) llenadas y aprobadas. o Actas resultantes de la gestión de riesgos que incluya la lista de los participantes.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

Fase	Etapa	Actividades	Entregable
		responsables y fechas, debidamente formalizados y aprobados. • Talleres a todos los procesos de la CGR, para socializar la manera en cómo se deben gestionar los riesgos de seguridad de la información.	○ Evidencias de la ejecución de los Talleres para socializar la manera en cómo se deben gestionar los riesgos de seguridad de la información.
	Indicadores de Seguridad	• De acuerdo con cómo lo establezca la CGR se deben definir y documentar todos los indicadores del SGSI de la CGR, que permitan evaluar diferentes aspectos y controles de seguridad, estos se deben revisar en conjunto con la CGR para determinar cuáles se deben empezar a medir, y en la medida que este proceso de medición vaya madurando, se deben ir incorporando en la medición otros nuevos indicadores que deje definidos la firma consultora.	• Ent12: Indicadores del SGSI, debidamente aprobados por la CGR, formalizados y divulgados.
	Capacitación	• Ejecutar el Plan de cambio organizacional, que incluye el plan de capacitación, de transferencia de conocimiento y divulgación del SGSI a todos los interesados internos y externos. • Realizar los cursos como se establecen en el "Anexo 1. Cursos relacionados con el SGSI de la CGR". • Los cursos deben incluir talleres, retroalimentación y evaluación final	• 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.
Revisión del SGSI	Revisión Arquitectura de Seguridad	• Revisión de la Arquitectura de Seguridad de los diferentes componentes de seguridad onpremise y cloud, se debe revisar como mínimo aspectos de alta disponibilidad, únicos puntos de fallo, riesgos, capacidad, licenciamiento, componentes de seguridad necesarios y con los cuales la CGR no cuenta y su correspondiente justificación, etc. • Generar las recomendaciones a partir del análisis realizado.	• Ent15: Documento con las recomendaciones generales y específicas de la revisión de la Arquitectura de Seguridad.
	Revisión Gestión pruebas de vulnerabilidades	• Revisar los informes de las dos últimas pruebas de vulnerabilidades y de ethical hacking realizadas a la CGR, y analizar la gestión en el cierre de las brechas de seguridad. • Generar las recomendaciones para mejorar la gestión del cierre de las vulnerabilidades identificadas	• Ent16: Informe con las recomendaciones para mejorar la gestión del cierre de las vulnerabilidades.
	Pruebas de Ingeniería Social	• Planear y ejecutar las pruebas de ingeniería social, correspondiente a: ○ Phishing, la cual se debe enviar como mínimo a todos los usuarios que cuenten con email de la CGR. ○ Suplantación de Identidad, la cual se debe realizar a través de llamadas telefónicas al menos a 100 usuarios[4]. ○ Se debe realizar recorridos dentro de las oficinas de la Sede Central de la CGR, con el fin de identificar riesgos, tomando	• Ent17: Informe con los resultados de las pruebas de ingeniería social, que incluya: ○ Evidencia de cada una de las pruebas de ingeniería social. ○ Recomendaciones generales y específicas como resultado de las pruebas, definiendo planes de tratamiento para el cierre de las brechas identificadas.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

[4] Se consideran 100 usuarios una muestra suficiente para identificar oportunidades de mejora a juicio de experto. El aumento de esta cantidad establecida no debe afectar los costos en la propuesta del proveedor.

Fase	Etapa	Actividades	Entregable
		registro fotográfico de los mismos, evaluando la totalidad de las áreas y evidenciando los riesgos que afecten la seguridad física de las instalaciones, las oficinas y la información física y digital que se encuentra en cada una de ellas[5]. • Se deben proponer otras 4 opciones de pruebas de ingeniería social, diferentes a las anteriores, y en conjunto con la CGR se escogerán 2 ejecutar. • Planear y ejecutar las 2 pruebas de ingeniería social escogidas.	
	Revisión de configuración de componentes de seguridad	• La firma consultora revisará la configuración y parametrización de los componentes de seguridad de la CGR. • Asignar un usuario de lectura por cada componente a revisar (FIREWALL, WAF, SANDBOX, TREND MICRO y otros, de existir) para que la firma consultora ingrese a revisar el aseguramiento (hardening) y configuración de cada uno de los componentes de seguridad. • Revisión del aseguramiento (hardening) y configuración de cada uno de los componentes de seguridad. • Generar las recomendaciones como resultado de la revisión realizada, que permita mejorar los niveles de seguridad y de disponibilidad de los componentes de seguridad. • Brindar asesoría y acompañamiento para resolver todas las dudas que tenga la CGR en la implementación de las recomendaciones, a través de una bolsa de 20 horas[6], las cuales se deben usar antes de iniciar la auditoría externa del SGSI.	• Ent18: Informe Revisión de configuración de componentes de seguridad, que incluya: ○ Proceso de revisión realizado por cada uno de los componentes de seguridad. ○ Recomendaciones por cada uno de los componentes de seguridad. ○ Actas con el reporte de las horas de asesoría y acompañamiento para la implementación de las recomendaciones.
	Implementación Herramienta SGSI	• Trabajar con el equipo de operaciones de la CGR para preparar la conectividad requerida para el uso de la herramienta del SGSI que entregará la firma consultora. • Hacer la configuración de la herramienta del SGSI en la plataforma de la firma consultora (modalidad SaaS). • Configurar los roles y accesos en la herramienta para la construcción y gobierno de todas las funciones y entregables del SGSI. • Configurar en cada uno de los módulos de la herramienta todas las funciones y actividades del SGSI y el cargue de todos los entregables del proyecto. • Establecer las acciones y procedimientos para poner en funcionamiento la herramienta del SGSI. • Hacer entrega de las licencias de la herramienta del SGSI a nombre de la CGR.	• Ent19: Documento de instalación y configuración de la herramienta del SGSI, que incluya: ○ Evidencia de la configuración de la herramienta del SGSI. ○ Entrega de licenciamiento de la herramienta del SGSI a nombre de la CGR (modalidad SaaS). ○ 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. ○ Documentación relacionada con soporte y asistencia técnica directamente con el fabricante y proveedor de la herramienta del SGSI.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

[5] Se propone que el recorrido debe realizarse entre un 80% a un 100% del total de las oficinas de la sede central de la CGR.
[6] Se considera que 20 horas es un tiempo suficiente de acuerdo con el juicio del experto, para resolver las dudas que surjan para implementar las recomendaciones realizadas a la CGR, después de haber revisado la configuración de los componentes de seguridad.

Fase	Etapa	Actividades	Entregable
		• Hacer entrega de toda la información relacionada con el soporte y asistencia técnica con el fabricante y proveedor de la herramienta, donde se indiquen los mecanismos, tiempos atención, y canales de comunicación (modelo SaaS).	
Auditorias y Cierre	Auditoría Interna	• La firma consultora debe realizar una Auditoría Interna al SGSI de la CGR • Revisar y seguir los formatos establecidos por la CGR para documentar las auditorías internas de los sistemas de gestión. • Elaborar un plan de auditoría interna al Sistema de Gestión de Seguridad de la Información, con el fin de verificar si el sistema es conforme con los requisitos de la norma ISO 27001 vigente y publicada por la ISO al momento de iniciar la ejecución del proyecto, y los que la Entidad defina que se deban tener implementados, y con el fin de contar con la evidencia de los registros de las evaluaciones realizadas al Sistema de Gestión, cuando éste sea implementado, la auditoría interna tendrá como alcance el SGSI y el proceso de Gestión de Tecnologías de la Información y Comunicaciones (Gerencia de TI y sus tres subgerencias). • Ejecutar el plan de la auditoría interna • Acompañamiento y apoyo por parte de la firma consultora en el cierre de No Conformidades y oportunidades de mejora identificadas en la Auditoria Interna., resolviendo las dudas que pueda tener la CGR para el cierre de estas, además, la firma consultora deberá ajustar o desarrollar todos los documentos del SGSI que hayan sido comentados u observados como parte de la Auditora Interna, así como los documentos internos que requieran ser actualizados o elaborados.	• 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: ○ Plan de Auditoria ○ Presentación de Inicio de la Auditoria ○ Informe de la Auditoria con las No Conformidades, observaciones y recomendaciones que se consideren. ○ Matriz de Riesgos identificados en la auditoria, en el formato establecido por la CGR. ○ Presentación ejecutiva con los resultados de la auditoria. ○ Acta de reunión de presentación de resultados de la Auditoria. ○ Actas de sesiones de acompañamiento y asesoría en el cierre de No Conformidades y oportunidades de mejora identificadas en la Auditoria Interna.
	Auditoría Externa[7]	• Contratar una firma de certificación de tercera parte para realizar una Auditoría Externa del SGSI teniendo como alcance el proceso de Gestión de Tecnologías de la Información y Comunicaciones (Gerencia de TI y sus tres subgerencias), esta firma de certificación debe estar autorizada para validar y certificar el SGSI de acuerdo con la ISO 27001 de acuerdo a la última versión publicada por la ISO al momento de iniciar la ejecución del proyecto, para lo cual se deben considerar firmas de certificación establecidas en Perú, y aplicar para obtener la Certificación ISO 27001 para el o los procesos definidos en coordinación con la Gerencia de TI y sus tres subgerencias.	• Ent21: Documento de la Auditoría Externa del SGSI, que incluya como mínimo, lo siguiente: ○ Contrato de la Auditoría Externa entre la firma de certificación de tercera parte y la firma consultora. ○ Acuerdo de Confidencialidad firmado entre la CGR y la firma de Certificación de tercera parte. ○ Plan de Auditoría Externa ○ Presentación de Inicio de la Auditoría Externa ○ Informe de la Auditoría Externa con las No Conformidades, observaciones y recomendaciones que se consideren.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

[7] La auditoría externa debe ser ejecutada por una entidad competente e independiente a la firma consultora. Es una auditoria de tercera parte que debe ser ejecutada por la entidad correspondiente, la cual esté catalogada como ente certificador, de acuerdo con lo indicado a la ISO 19011 – Guía de Auditoria de sistemas de Gestión.

Fase	Etapa	Actividades	Entregable
		• Firmar Acuerdo de Confidencialidad entre la CGR y la firma de Certificación de tercera parte. • La firma de certificación de tercera parte debe elaborar un plan de auditoría externa al Sistema de Gestión de Seguridad de la Información, con el fin de verificar si el sistema es conforme con los requisitos de la norma ISO 27001, y los que la CGR haya definido para el SGSI de la Entidad. • Revisar y acordar el plan de auditoría externa del SGSI de la CGR. • Ejecutar el plan de la auditoría externa. • Desarrollar y entregar los documentos acordados como resultado de la auditoría externa. • Realizar la reunión del cierre de la Auditoría Externa al SGSI de la CGR. • En caso de que aplique, la firma consultora deberá acompañar y apoyar a la CGR en el cierre de No Conformidades y oportunidades de mejora identificadas en la Auditoría Externa, dentro del plazo definido por la firma de certificación de tercera parte para la obtención de la certificación de la ISO 27001 para el SGSI con alcance del procesos o procesos seleccionados en coordinación con la Gerencia de TI y sus tres subgerencias.. • Una vez que el resultado de la auditoría de certificación sea favorable respecto al cumplimiento de la ISO 27001 del SGSI de la CGR, se debe generar el certificado para el SGSI con alcance del proceso o procesos seleccionados en coordinación con la Gerencia de TI y sus tres subgerencias. • Como parte del servicio, la firma consultora debe garantizar la certificación del SGSI de la CGR ante el ente certificador. En consecuencia deberá trabajar en coordinación con la CGR en la subsanación de posibles no conformidades u observaciones y en caso corresponda, preparar el plan de acción, hacer el seguimiento de este, hasta el logro de la certificación del SGSI de la CGR ante el ente certificador. Asimismo, deberá asumir los gastos necesarios en caso se requiera contratar una nueva auditoría de tercera parte.	○ Matriz de Riesgos identificados en la auditoría externa, en el formato establecido por la CGR. ○ Presentación ejecutiva con los resultados de la auditoría externa. ○ Acta de reunión de presentación de resultados de la Auditoría externa. ○ 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 GTI y sus tres subgerencias.. ○ 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 GTI y sus tres subgerencias.
	Cierre proyecto / contrato	• Elaboración de acta de cierre • Cierre del proyecto y del contrato	• Acta de cierre del proyecto y del contrato.

Tabla 1 – Fases, Etapas, Actividades y Entregables del Proyecto
Fuente de Elaboración Propia

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

b) Herramienta para el Sistema de Gestión de Seguridad de la Información (SGSI)

La CGR requiere de una herramienta que soporte el Sistema de Gestión de Seguridad de la Información y permita gestionar de manera oportuna y completa administrar el SGSI de la CGR, logrando procesos ágiles, sencillos y automatizados. La cual debe cumplir de manera efectiva con la normativa vigente publicada por la ISO al momento de iniciar la ejecución del contrato en materia

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

de ISO 27001, ISO 27005, ISO 31000, ISO 22301, ISO 27032, la normatividad de protección de datos personales del Perú, como mínimo.

La herramienta de seguridad de la información debe permitir documentar y visualizar toda la información del Sistema de Gestión de Seguridad de la Información de forma centralizada, que se convierta en la única fuente de la verdad del estado actual de la seguridad, lo que habilitará a la CGR para la toma de decisiones más rápida y de forma precisa con la automatización de la seguridad de la información institucional.

Esta herramienta tecnológica debe soportar la práctica de Seguridad de la Información, lo cual involucra custodiar, actualizar y hacer oficiales los diferentes artefactos generados en el proyecto.

Para dar cumplimiento a los requerimientos de la herramienta de Seguridad de la Información, la firma consultora debe incluir dentro de su oferta los costos para la entrega de las licencias solicitadas por la CGR, la instalación y configuración de la herramienta para la CGR.

A continuación, se listan los requerimientos mínimos que debe cumplir la herramienta del Sistema de Gestión de Seguridad de la Información:

- **<u>Requerimientos de Herramienta de SGSI</u>:**

La herramienta debe cumplir con los siguientes requerimientos:

- Debe ser una solución modular que permita gestionar como mínimo todos los aspectos del SGSI en temas de seguridad de la información, seguridad digital, análisis de brechas, ciberseguridad, protección de datos personales, continuidad del negocio, auditorias, gestión de incidentes de seguridad y gestión de activos y de riesgos, como se defina en el diseño, desarrollo e implementación del SGSI, así mismo, contar como mínimo con módulos de gestión de roles y perfiles, gestión documental del SGSI y seguimiento y control.
- Debe permitir realizar comparaciones de mediciones actuales con mediciones anteriores.
- Debe permitir integración con diferentes tipos de bases de datos.
- Debe permitir la integración con el Directorio Activo de la CGR.
- Debe permitir su visualización y gestión desde cualquier dispositivo con acceso a la red/internet usando un navegador.
- Debe permitir generar reportes de tipo radar, barra, pie, circulares y lineales.
- Centralizar en un único repositorio toda la información de la seguridad de la información.
- Permitir trabajo colaborativo entre diferentes roles de la CGR.
- Contar con una interfaz web intuitiva y de fácil manejo para el usuario.
- Tener un sistema de acceso multiusuario.
- Capacidad para poder importar y exportar en diferentes formatos.
- Monitoreo y control, permitiendo generar reportes de trazabilidad.
- Diversos formatos de imágenes para guardar diagramas o esquemas.
- Generar documentación y reportes con base en los artefactos construidos en la herramienta.
- Debe permitir generar tableros de control (*dashboard*) con base en la documentación de la seguridad de la información.
- La herramienta debe funcionar en modalidad SaaS (Software as a Services).

- **<u>Licenciamiento</u>:**

Al inicio del proyecto, la firma consultora debe implementar a nombre de la CGR las licencias y entregar toda la información y documentación del fabricante de la herramienta y del proveedor del servicio SaaS. El licenciamiento solicitado es el siguiente:

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

- Modalidad de licenciamiento: Suscripción en servicio SaaS (*Software as a Service*)
- Número de licencias: 50[8]
- Tiempo de licenciamiento: cinco (5) años[9].
- Mantenimiento y soporte por el tiempo de licenciamiento.
- Horas de capacitación: 20 horas de capacitación sobre las funcionalidades de la herramienta, para trabajadores de la CGR. Ver Anexo A de este documento.
- Configuración de la herramienta para uso de la CGR.

5. METODOLOGÍA DE TRABAJO

El consultor deberá revisar, en primer lugar, toda la documentación relativa al Contrato y cualquier otra documentación que sea necesaria para el desarrollo de las actividades a su cargo, a fin de que guarden coherencia y consistencia con los objetivos de la consultoría. La Gerencia de Tecnologías de Información (GTI), pondrá a disposición del consultor toda la documentación antes mencionada.

El consultor deberá tomar en cuenta las características del producto y las disposiciones específicas correspondientes establecidas en el presente documento en la sección de Antecedentes. El consultor podrá hacer presentaciones (en Power Point o Prezi) sobre los avances en la ejecución de la consultoría, a pedido de la Gerencia de Tecnologías de Información (GTI), como Propietaria del Proyecto Interno, o la Dirección Estratégica de Gestión de Proyectos (DEGP).

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Para la ejecución del proyecto la firma consultora debe aplicar las mejores prácticas y metodologías como la del PMI (*Project Management Institute*) para la gestión del proyecto, el marco de ISO 27000 para la estructuración de la seguridad de la información, metodologías de gestión del cambio organizacional para la planeación y ejecución de las actividades de gestión del cambio organizacional del proyecto, y otras metodologías que sean propias de la Entidad, y que serán proporcionadas por la Contraloría General de la República de Perú al inicio del proyecto, de ser aplicable.

6. PRODUCTOS E INFORMES PARA ENTREGAR

-

Los informes de los respectivos Entregables deberán presentarse a la Entidad en formato físico o en formato digital, según se acuerde al inicio del proyecto, en mesa de pares virtual de la Contraloría General de la República, dirigido a la Subgerencia de Gobierno Digital.

PRODUCTO	DESCRIPCIÓN
Producto 1 (Gestión del proyecto de SGSI)	• **Ent01: Plan de gestión del proyecto que incluya:** ○ 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.

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

[8] La licencia va dirigida a usuarios que deban mantener los activos seguridad de la información, los riesgos de seguridad de la información, los planes de trabajo resultados de auditorías internas y/o externas, además, para el responsable del SGSI, por lo que se consideraron en promedio 3 usuarios por proceso.

[9] El periodo contratado se contabiliza a partir del día siguiente a la instalación y configuración de la herramienta. El pago total por el periodo contratado se realizará de manera anticipada, según se especifica en la sección 7, PLAZO DEL SERVICIO.

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

PRODUCTO	DESCRIPCIÓN
	○ Presentación de Kick-Off.
	• **Ent02: Plan de gestión del cambio organizacional para el proyecto, que incluya:** ○ Estrategia de gestión del cambio organizacional. ○ Plan de comunicaciones a los impactados por el proyecto. ○ Plan de capacitaciones. Ver Anexo A.
Producto 2 (Diseño e implementación del SGSI)	• **Ent03: Documento de Diagnostico de Seguridad respecto a la ISO 27001, que incluya:** ○ 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 especificas ○ Conclusiones del Diagnóstico.
	• **Ent04: Documento de establecimiento del SGSI, que incluya:** ○ 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
	• **Ent05: Documento de la Declaración de Aplicabilidad (SoA) para el SGSI de la CGR.**
	• **Ent06: Documento de Normograma de Seguridad**
	• **Ent07: Documento de la organización de seguridad que incluya:** ○ Diseño y desarrollo de la Matriz RACI del SGSI. ○ Matriz RACI (Responsable, Aprobador, Consultado e Informado) del SGSI.
	• **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.**
	• **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:** ○ 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.
	• **Ent10: Documento con la definición de la Gestión de Activos de Seguridad, que incluya:** ○ 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.

V°B°

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

V°B°

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

V°B°

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

PRODUCTO	DESCRIPCIÓN
	○ 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.
	• **Ent11: Documentos acordados para la Gestión de los Riesgos de Seguridad, que incluya:** ○ 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. ○ Actas resultantes de la gestión de riegos que incluya la lista de los participantes. ○ Evidencias de la ejecución de los Talleres para socializar la manera en cómo se deben gestionar los riesgos de seguridad de la información.
	• **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)	• **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:** ○ Evidencia de cada una de las pruebas de ingeniería social. ○ 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:** ○ Proceso de revisión realizado por cada uno de los componentes de seguridad. ○ Recomendaciones por cada uno de los componentes de seguridad. ○ 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[10]:** ○ Evidencia de la configuración de la herramienta del SGSI.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

[10] Se aclara que el pago total anticipado de la herramienta realizado por la CGR incluye: Evidencia de la configuración de la herramienta de SGSI: Entrega de licenciamiento de la herramienta del SGSI a nombre de la CGR (modalidad SaaS), 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, Diseño y documentación correspondiente, Documentación relacionada con la asistencia del fabricante y proveedor de la herramienta, para el periodo contratado.

PRODUCTO	DESCRIPCIÓN
	○ Entrega de licenciamiento de la herramienta del SGSI a nombre de la CGR (modalidad SaaS). ○ 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. ○ Documentación relacionada con soporte y asistencia técnica directamente con el fabricante y proveedor de la herramienta del SGSI.
Producto 4 (Evaluación del SGSI)	• **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:** ○ Plan de Auditoria ○ Presentación de Inicio de la Auditoria ○ Informe de la Auditoria con las No Conformidades, observaciones y recomendaciones que se consideren. ○ Matriz de Riesgos identificados en la auditoria, en el formato establecido por la CGR. ○ Presentación ejecutiva con los resultados de la auditoria. ○ Acta de reunión de presentación de resultados de la Auditoria. ○ Actas de sesiones de acompañamiento y asesoría en el cierre de No Conformidades y oportunidades de mejora identificadas en la Auditoria Interna.
	• **Ent21: Documento de la Auditoría Externa[11] del SGSI, que incluya como mínimo, lo siguiente:** ○ Contrato de la Auditoría Externa entre la firma de certificación de tercera parte y la firma consultora. ○ Acuerdo de Confidencialidad firmado entre la CGR y la firma de Certificación de tercera parte. ○ Plan de Auditoría Externa ○ Presentación de Inicio de la Auditoría Externa. ○ Informe de la Auditoría Externa con las No Conformidades, observaciones y recomendaciones que se consideren. ○ Entrega de la Matriz de Riesgos identificados en la auditoría externa, en el formato establecido por la CGR. ○ Presentación ejecutiva con los resultados de la auditoría externa. ○ Acta de reunión de presentación de resultados de la Auditoría externa. ○ 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. ○ 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.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

[11] La auditoría externa debe ser ejecutada por una entidad competente e independiente a la firma consultora. Es una auditoria de tercera parte que debe ser ejecutada por la entidad correspondiente, la cual esté catalogada como ente certificador.

7. PLAZO DEL SERVICIO

El plazo para la ejecución de la consultoría será de doscientos diez (210) días calendario, computados desde el día siguiente de la firma del contrato.

El plazo de servicio de los entregables en la siguiente tabla se cuenta desde la firma del contrato:

Producto	Entregable	Contenido	Plazo del Servicio
Producto 1 (Gestión del proyecto de SGSI)	Ent01	Plan de gestión del proyecto	A los 14 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent02	Plan de gestión del cambio organizacional para el proyecto	A los 14 días calendario contados desde el día siguiente de la suscripción del contrato
Producto 2 (Diseño e implementación del SGSI)	Ent03	Documento de Diagnóstico de Seguridad	A los 28 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent04	Documento de establecimiento del SGSI	A los 28 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent05	Documento de la Declaración de Aplicabilidad (SoA)	A los 28 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent06	Documento de Normograma de Seguridad	A los 28 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent07	Documento de la organización de seguridad	A los 84 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent08	Política General del SGSI de la CGR, y Políticas Específicas de Seguridad	A los 84 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent09	Procedimientos de Seguridad	A los 140 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent10	Documento con la definición de la Gestión de Activos	A los 140 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent11	Documentos acordados para la Gestión de los Riesgos de Seguridad	A los 140 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent12	Indicadores del SGSI	A los 140 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent13	Documento con las evidencias de la ejecución del Plan de cambio organizacional.	A los 161 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent14	Documento con las evidencias de la ejecución de los cursos como se solicitaron	A los 161 días calendario contados desde el día siguiente de la suscripción del contrato
Producto 3	Ent15	Documento con las recomendaciones generales y	A los 126 días calendario contados desde el día siguiente de la suscripción del contrato

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

Producto	Entregable	Contenido	Plazo del Servicio
(Revisión del SGSI)		específicas de la revisión de la Arquitectura de Seguridad.	
	Ent16	Informe con las recomendaciones para mejorar la gestión del cierre de las vulnerabilidades	A los 126 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent17	Informe con los resultados de las pruebas de ingeniería social	A los 126 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent18	Informe Revisión de configuración de componentes de seguridad	A los 161 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent19	Documento de instalación de la herramienta del SGSI[12]	A los 161 días calendario contados desde el día siguiente de la suscripción del contrato
Producto 4 (Evaluación del SGSI)	Ent20	Documento de la Auditoría Interna del SGSI	A los 161 días calendario contados desde el día siguiente de la suscripción del contrato
	Ent21	Documento de la Auditoría Externa del SGSI	A los 210 días calendario contados desde el día siguiente de la suscripción del contrato

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

En caso de existir observaciones a los productos la CGR notificará a la firma consultora dentro de un plazo máximo de tres (03) días hábiles posteriores a la recepción de cada producto, para lo cual la firma consultora tendrá un plazo máximo de tres (03) días hábiles para levantar estas observaciones; dicho plazo comenzará a partir del primer día siguiente de notificada la comunicación.

Los plazos de revisión no son contabilizados dentro del plazo efectivo del servicio.

Los requerimientos de revisión a las observaciones realizadas a los productos podrán ser solicitados hasta en dos (02) oportunidades por cada producto.

El siguiente diagrama de Gantt presenta la línea estimada de ejecución del proyecto, donde se pueden ver las fases y etapas en las cuales se ha estructurado la ejecución del proyecto:

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

[12] Se aclara que el pago total anticipado de la herramienta realizado por la CGR incluye: Evidencia de la configuración de la herramienta de SGSI: Entrega de licenciamiento de la herramienta del SGSI a nombre de la CGR (modalidad SaaS), 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, Diseño y documentación correspondiente, Documentación relacionada con la asistencia del fabricante y proveedor de la herramienta, para el periodo contratado.

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

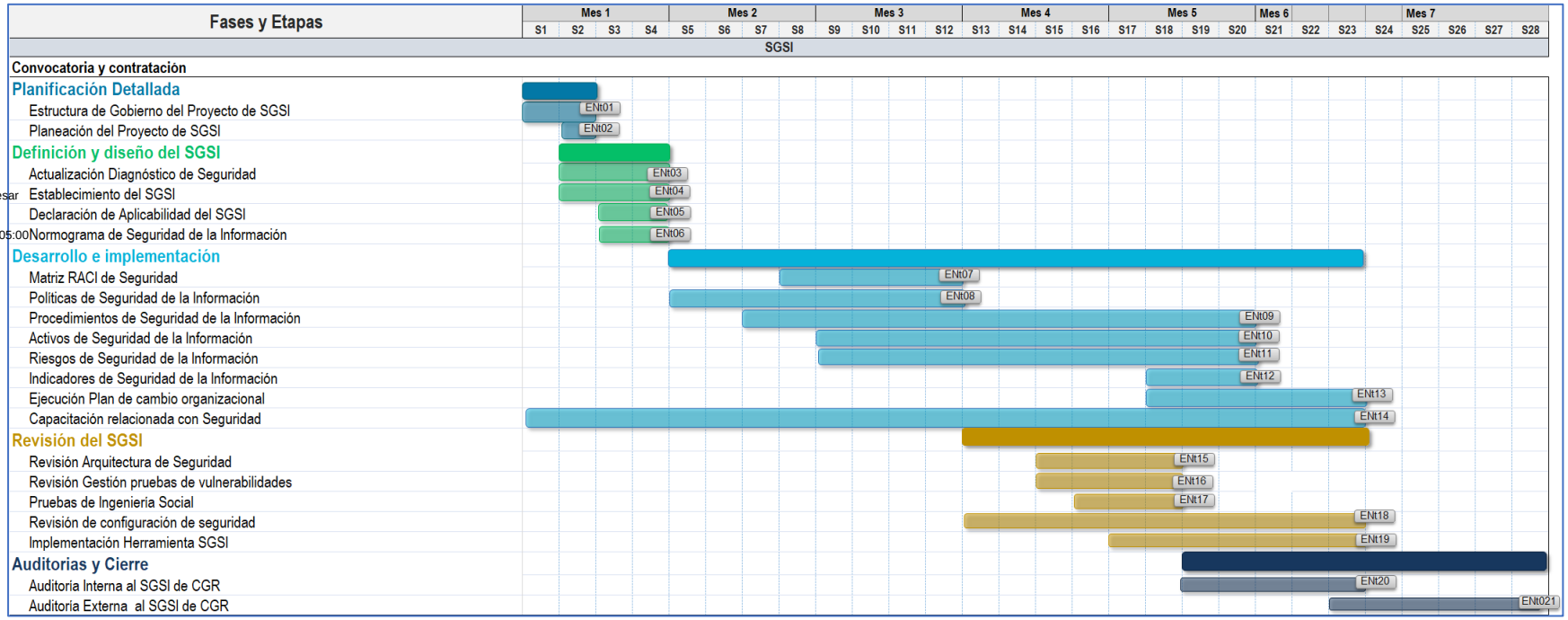


Ilustración 3 – Cronograma de ejecución

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

8. RECURSOS Y FACILIDADES PARA PROVEER POR LA ENTIDAD CONTRATANTE

La firma consultora deberá contar con su propio equipo de cómputo, licencias y las herramientas necesarias para el desarrollo de su servicio.

9. PERFIL DE LA FIRMA CONSULTORA

a) Experiencia General

Contar con experiencia cuya sumatoria sea igual o superior a USD$250.000 realizada en los últimos ocho (8) años anteriores a la fecha de la presentación de la oferta comercial, relacionadas con servicios de consultoría en Seguridad de la Información.

b) Experiencia Específica

Contar con un mínimo de tres (3) y un máximo de cinco (05) contratos que cumplan con los siguientes requerimientos:

- El objeto y/o las obligaciones principales deben ser en: Diseño y/o Diagnóstico y/o desarrollo y/o implementación de Sistemas de Gestión de Seguridad de la Información.
- La sumatoria de los contratos debe ser igual o superior a USD $200.000.
- Haberse iniciado en los últimos ocho (8) años anteriores a la fecha de presentación de la expresión de interés.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Notas con respecto a la presentación de las expresiones de interés.
1) Experiencia general: si el servicio contratado está en ejecución (no ha concluido), precisar si cuenta con entregables o productos relacionados a servicios de consultoría en Seguridad de la Información, especificando el correspondiente monto ejecutado a la fecha de la presentación de expresión de interés.
2) Experiencia específica: si el servicio contratado está en ejecución (no ha concluido), precisar si cuenta con entregables o productos relacionados a Diseño y/o Diagnóstico y/o desarrollo y/o implementación de Sistemas de Gestión de Seguridad de la Información, especificando el correspondiente monto ejecutado a la fecha de la presentación de expresión de interés.

c) Perfil del Equipo Consultor (Personal Clave)

El Proveedor presentará en su propuesta el siguiente personal clave que será materia de evaluación:

- **Rol: Gerente de proyecto**

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Formación Académica	• Título profesional universitario de Ingeniería de Sistemas, Informática, Electrónica, Eléctrica, Telecomunicaciones, Industrial o profesiones afines o el equivalente en el país de origen. • Posgrado en Gestión de Proyectos de Ingeniería y/o Gerencia de Proyectos y/o Preparación y evaluación de Proyectos y/o Gerencia integral de Proyectos y/o Ingeniería de Software y/o Desarrollo y Gerencia Integral de proyectos y/o Gerencia de Mercadeo y/o Telecomunicaciones y/o Teleinformática.
Certificaciones	• Certificado como Project Management Professional (PMP) deseable • Auditor Líder en la última versión de la ISO 27001 publicada por la ISO.org
Experiencia	• Experiencia General: Experiencia profesional de diez (10) años

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

	• Experiencia especifica: Gerente de proyecto de al menos 5 proyectos relacionados con Seguridad de la Información.
Cantidad	01

- **Rol: Consultor Líder de Seguridad de la Información**

Formación Académica	• Título profesional universitario de Ingeniería de Sistemas, Informática, Electrónica, Eléctrica, Telecomunicaciones, Industrial o profesiones afines o el equivalente en el país de origen. • Maestría en Seguridad de la Información o Seguridad Informática.
Certificaciones	• Certified Information Systems Security Professional CISSP vigente • Implementador Líder en la última versión de la ISO 27001 publicada por la ISO.org • Certified Data Privacy Solutions Engineer (CDPSE) vigente • EC-Council Certified Incident Handler vigente • ITIL 4 Managing Professional vigente
Experiencia	• Experiencia General: Experiencia profesional de quince (15) años. • Experiencia específica: diez (10) años de experiencia específica en roles y/o actividades como Oficial de Seguridad de la Información o Especialista de Seguridad o Consultor en Seguridad de la Información. • Participación en al menos (10) proyectos relacionados con el diseño, desarrollo e implementación de Sistemas de Gestión de Seguridad de la Información.
Cantidad	• 01

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

- **Rol: Consultor Senior en Seguridad de la Información**

Formación Académica	• Título profesional universitario de Ingeniería de Sistemas, Informática, Electrónica, Eléctrica, Telecomunicaciones, Industrial o profesiones afines o el equivalente en el país de origen.
Certificaciones	• Implementador Líder en la última versión de la ISO 27001 publicada por la ISO.org • Certified Data Privacy Solutions Engineer (CDPSE) vigente • ITIL 4 Managing Professional vigente
Experiencia	• Experiencia General: Experiencia profesional de ocho (8) años • Experiencia específica: cinco (5) años de experiencia específica en roles y/o actividades como consultor en seguridad de la información. • Mínimo cinco (5) proyectos de Sistemas de Gestión de Seguridad de la Información.
Cantidad	• 01

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

- **Rol: Consultor Auditor en Seguridad de la Información**

Formación Académica	• Título profesional universitario de Ingeniería de Sistemas, Informática, Electrónica, Eléctrica, Telecomunicaciones, Industrial o profesiones afines o el equivalente en el país de origen.
Certificaciones	• Auditor Líder en la última versión de la ISO 27001 publicada por la ISO.org

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

Experiencia	• Experiencia General: Experiencia profesional de ocho (8) años • Experiencia específica: cinco (5) años de experiencia específica en roles y/o actividades como consultor en seguridad de la información y/o especialista en sistemas de gestión y/o especialista en gestión de calidad y/o auditorias de sistemas de gestión • Mínimo tres (3) proyectos relacionados con sistemas de gestión de seguridad.
Cantidad	• 01

El equipo de trabajo anterior corresponde al equipo base; sin embargo, la firma consultora puede incluir personal adicional al anterior si así lo considera necesario.

ACREDITACIÓN

- La experiencia del personal se acreditará con cualquiera de los siguientes documentos: (i) Copia simple de contratos y su respectiva conformidad o (ii) Constancias o (iii) Certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal clave propuesto.
- El título profesional requerido será verificado con el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria – SUNEDU o el equivalente en su país de origen.
- En caso el título profesional requerido no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida o el equivalente en su país de origen.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Nota: La experiencia será contabilizada a partir de la obtención del grado académico de bachiller.

10. OTRAS OBLIGACIONES DE LA FIRMA CONSULTORA

- Si el personal de la Firma Consultora reside fuera del Perú, durante la ejecución del proyecto, la firma consultora debe al menos contemplar siete (7) viajes o visitas en total, con una duración de al menos 3 días cada visita, a las instalaciones de la CGR en la ciudad de Lima. Se plantea la siguiente distribución: una (1) visita para la fase de Descubrimiento y Análisis, tres (3) visitas durante la fase de Diseño, dos (2) visitas durante la ejecución de la Implementación y una (1) visita durante la realización de la auditoría externa. Solo en caso corresponda, se requerirán más visitas por ejemplo si se requiere realizar el levantamiento de no conformidades, elaborar planes de acción o realizar una nueva auditoría y se requiera su participación física.
- Si el personal reside en el Perú, el trabajo presencial, en tiempo y horario, debe ser coordinado con la CGR.
- Para visitar las instalaciones de la Contraloría General de la República, se debe cumplir con todos los elementos de bioseguridad necesarios para su protección, a fin de prevenir el contagio del COVID 19.
- Al inicio del proyecto acordar con la CGR las plantillas y los criterios de aceptación de los entregables del proyecto.
- Para los procesos y procedimientos y demás documentación que se construyan para el Sistema de Gestión de Seguridad de la Información (SGSI) se deben seguir las indicaciones, guías y lineamientos de la CGR.

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

11. FORMA Y CONDICIONES DE PAGO

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

Los pagos bajo este servicio se efectuarán contra la presentación de los entregables señalados en los presentes términos de referencia y de acuerdo con el cronograma establecido, al cual se deberá adjuntar el respectivo recibo.

La Firma Consultora es responsable de atender todas las obligaciones tributarias que surjan producto de la consultoría. Cada uno de los pagos a la firma consultora se realizará dentro de los quince (15) días siguientes a la emisión de la conformidad del servicio, por parte de la Subgerencia de Gobierno Digital.

El pago se realizará de acuerdo con el siguiente detalle:

Producto	Entregable	Contenido	Porcentaje de pago del monto total contratado
Producto 1 (Gestión del proyecto de SGSI)	Ent01	Plan de gestión del proyecto	No se realizará un pago por el desarrollo y recibo a satisfacción de este entregable
	Ent02	Plan de gestión del cambio organizacional para el proyecto	No se realizará un pago por el desarrollo y recibo a satisfacción de este entregable
Producto 2 (Diseño e implementación del SGSI)	Ent03	Documento de Diagnóstico de Seguridad	9%
	Ent04	Documento de establecimiento del SGSI	
	Ent05	Documento de la Declaración de Aplicabilidad (SoA)	
	Ent06	Documento de Normograma de Seguridad	
	Ent07	Documento de la organización de seguridad	10%
	Ent08	Política General del SGSI de la CGR, y Políticas Específicas de Seguridad	
	Ent09	Procedimientos de Seguridad	32%
	Ent10	Documento con la definición de la Gestión de Activos	
	Ent11	Documentos acordados para la Gestión de los Riesgos de Seguridad	
	Ent12	Indicadores del SGSI	
	Ent13	Documento con las evidencias de la ejecución del Plan de cambio organizacional.	15%
	Ent14	Documento con las evidencias de la ejecución de los cursos como se solicitaron	
Producto 3 (Revisión del SGSI)	Ent15	Documento con las recomendaciones generales y específicas de la revisión de la Arquitectura de Seguridad.	7%
	Ent16	Informe con las recomendaciones para mejorar la gestión del cierre de las vulnerabilidades	

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

Producto	Entregable	Contenido	Porcentaje de pago del monto total contratado
	Ent17	Informe con los resultados de las pruebas de ingeniería social	
	Ent18	Informe Revisión de configuración de componentes de seguridad	10%
	Ent19	Documento de instalación de la herramienta del SGSI[13]	
Producto 4 (Evaluación del SGSI)	Ent20	Documento de la Auditoría Interna del SGSI	17%
	Ent21	Documento de la Auditoría Externa del SGSI	

12. COORDINACIÓN, SUPERVISIÓN Y CONFORMIDAD

La firma consultora deberá reportar, informar y coordinar sus actividades con los responsables designados por la Subgerencia de Gobierno Digital de la CGR, quienes realizarán la supervisión de las actividades de la firma consultora y estarán encargados de dar la conformidad junto con el Subgerente de Gobierno Digital de la CGR a los productos presentados.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

13. PENALIDADES Y GARANTIAS

13.1. PENALIDADES

La aplicación de penalidades por retraso injustificado en la atención del servicio requerido y las causales para la resolución del contrato, serán aplicadas según contrato.

En caso de retraso injustificado del inicio de la prestación, la Entidad aplicará automáticamente una penalidad por mora, por cada día de atraso, hasta por un monto máximo equivalente a diez por ciento (10%) del monto contractual.

En el caso de retraso injustificado en el soporte y suscripción de licenciamiento para los 5 años, la entidad aplicará automáticamente una penalidad por mora, por cada día de atraso, hasta por un monto máximo equivalente a diez por ciento (10%) del monto pagado por el soporte y suscripción.

13.2. GARANTÍAS

Las siguientes obligaciones se alinean a las políticas de contratación de la CGR y de los procesos de BID:

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Durante la contratación y ejecución: la firma consultora debe cubrir los riesgos derivados del incumplimiento del contrato. La garantía puede cubrir todos o algunos de los siguientes amparos según las condiciones del objeto del contrato, según las políticas de contratación del BID:

- Buen manejo y correcta inversión del anticipo asignado por la CGR para la instalación, soporte y suscripción del licenciamiento de las herramientas adquiridas como parte de este contrato, con vigencia de cinco (5) años.

[13] Se aclara que el pago total anticipado de la herramienta realizado por la CGR incluye: Evidencia de la configuración de la herramienta de SGSI: Entrega de licenciamiento de la herramienta del SGSI a nombre de la CGR (modalidad SaaS), 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, Diseño y documentación correspondiente, Documentación relacionada con la asistencia del fabricante y proveedor de la herramienta, para el periodo contratado.

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

- Devolución del pago anticipado.
- Cumplimiento del contrato.
- Soporte por cuatro (4) meses para absolver las consultas y/o aclaraciones que le sean requeridas por el área usuaria respecto del contenido de sus entregables.

Posteriores a la ejecución: En esta fase se cubren los Riesgos que se presenten con posterioridad a la terminación del contrato con la firma consultora, conforme a las políticas de contratación del BID:

- La firma consultora es responsable hasta por un (1) año más, desde otorgada la conformidad de los entregables, de absolver las consultas y/o aclaraciones que tenga la CGR, respecto a los contenidos de sus entregables.
- Para el caso de la certificación ISO 27001, en el caso de que no se obtenga la misma, la firma consultora deberá trabajar en coordinación con la CGR en la subsanación de posibles No conformidades u observaciones y en caso corresponda, preparar el plan de acción, hacer el seguimiento de este, hasta el logro de la certificación del SGSI de la CGR ante el ente certificador. Asimismo, deberá asumir los gastos necesarios en caso se requiera contratar una nueva auditoría.
- Calidad y correcto funcionamiento de las herramientas adquiridas como parte del contrato.
- Soporte técnico y actualizaciones[14] sobre las herramientas que adquiere la Contraloría General de la República como parte de la ejecución de este contrato, de manera tal que se logre mantener la vigencia tecnológica del producto y recibir soporte técnico por parte del fabricante de manera oportuna, logrando garantizar el correcto funcionamiento de producto y brindando la operatividad requerida por los usuarios. Para esto, la firma consultora debe entregar a la CGR un documento donde se indique el nombre del producto adquirido, el número de licencias, la fecha de inicio y final de validez de las licencias, el esquema de soporte con el fabricante, los canales de comunicación y escalamiento de problemas asociados con las herramientas adquiridas.

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

14. DERECHOS DE PROPIEDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

La Firma Consultora 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 la firma consultora; el mismo que a mérito de los presentes Términos de Referencia, 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, la firma consultora no podrá revelar ninguna información confidencial o de propiedad de la CGR relacionada con los servicios, con el contrato que se generé o las actividades u operaciones de la CGR. Toda la información a la que la Firma Consultora 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 de la firma consultora, a menos que la CGR otorgue mediante pronunciamiento escrito la autorización correspondiente.

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

15. ANEXOS

Anexo A. Capacitación y Transferencia de Conocimiento para SGSI

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

[14] El periodo contratado se contabiliza a partir del día siguiente a la instalación y configuración de la herramienta.

Firmado digitalmente por
HUERTAS SALAZAR Raul Cesar
FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por
BALBUENA RODRIGUEZ Ricardo
Gerardo FAU 20131378972
soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por
BAZÁN FLORES Erik Ulises
FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00

ANEXO A. CAPACITACIÓN Y TRANSFERENCIA DE CONOCIMIENTO PARA SGSI

ANEXO CAPACITACIONES Y TRANSFERENCIAS DEL CONOCIMIENTO A CONTEMPLAR

(*) Es una aproximado ya que depende del plan que genere cada proveedor de cara al proyecto

PRODUCTO	TIPO	FASE	TEMA	HORAS (*)	CANTIDAD DE	GRUPO DE INTERÉS	OBSERVACIONES
Sistema de Gestión de la Seguridad de la Información	CAPACITACIÓN	Implementación	Interpretación de la Norma ISO 27001 y 27002	mínimo 8 horas	300	Según alcance del SGSI - Trabajadores de las unidades orgánicas incluidos en el	CURSO DE CONOCIMIENTO CON CERTIFICACIÓN DE PARTICIPACIÓN
Sistema de Gestión de la Seguridad de la Información	CAPACITACIÓN	Implementación	Auditor Interno en ISO 27001	mínimo 32 horas	60	Trabajadores seleccionados para ser auditories internos	CURSO DE CONOCIMIENTO CON CERTIFICACIÓN DE PARTICIPACIÓN
Sistema de Gestión de la Seguridad de la Información	CAPACITACIÓN	Implementación	Auditor Líder en ISO 27001	mínimo 40 horas	10	Trabajadores seleccionados para ser auditores lideres	CURSO DE CONOCIMIENTO CON CERTIFICACIÓN DE PARTICIPACIÓN + VOUCHER DE EXAMEN DE CERTIFICACIÓN
Sistema de Gestión de la Seguridad de la Información	CAPACITACIÓN	Implementación	Implementación Protección de Datos Personales	mínimo 40 horas	200	Según defina la CGR	CURSO DE CONOCIMIENTO CON CERTIFICACIÓN DE PARTICIPACIÓN
Sistema de Gestión de la Seguridad de la Información	CAPACITACIÓN	Implementación	Implementador Líder ISO 27001	mínimo 40 horas	80	Según defina la CGR	CURSO DE CONOCIMIENTO CON CERTIFICACIÓN DE PARTICIPACIÓN
Sistema de Gestión de la Seguridad de la Información	CAPACITACIÓN	Implementación	Gestor de Riesgos en Seguridad ISO 31000	mínimo 40 horas	200	Según defina la CGR	CURSO DE CONOCIMIENTO CON CERTIFICACIÓN DE PARTICIPACIÓN
Sistema de Gestión de la Seguridad de la Información	CAPACITACIÓN	Implementación	Gestor de Riesgos en Seguridad ISO 27005	mínimo 40 horas	50	Según defina la CGR	CURSO DE CONOCIMIENTO CON CERTIFICACIÓN DE PARTICIPACIÓN
Sistema de Gestión de la Seguridad de la Información	CAPACITACIÓN	Implementación	Gestor en Ciberseguridad ISO 27032	mínimo 40 horas	50	Según defina la CGR	CURSO DE CONOCIMIENTO CON CERTIFICACIÓN DE PARTICIPACIÓN
Sistema de Gestión de la Seguridad de la Información	CAPACITACIÓN	Implementación	Gestor Líder de Incidentes de Seguridad ISO 27035	mínimo 40 horas	50	Según defina la CGR	CURSO DE CONOCIMIENTO CON CERTIFICACIÓN DE PARTICIPACIÓN
Sistema de Gestión de la Seguridad de la Información	CAPACITACIÓN	Implementación	Auditor en Continuidad del Negocio ISO 22301	mínimo 40 horas	60	Según defina la CGR	CURSO DE CONOCIMIENTO CON CERTIFICACIÓN DE PARTICIPACIÓN

Firmado digitalmente por HUERTAS SALAZAR Raul Cesar FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 12:06:28 -05:00

Firmado digitalmente por BALBUENA RODRIGUEZ Ricardo Gerardo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 10-05-2023 12:49:04 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 08-05-2023 11:50:01 -05:00