Informe de Estudios Previos
Para la Consultoría de Implementación Gobernanza en Ciberseguridad

La administración pública, con el objetivo de cumplir con las funciones esenciales del Estado, lleva a cabo la actividad contractual, lo que hace trascendental la etapa precontractual. En esta etapa se realizan todas las actuaciones previas a la formalización del contrato, que incluyen las fases de planificación y preparación, entre otras, de conformidad con el artículo 62 y siguientes del Reglamento de aplicación de la Ley 340-06. Esto tiene como finalidad garantizar la correcta ejecución de los procesos de selección, un mejor aprovechamiento de los recursos y una mayor eficiencia en la ejecución de los contratos.

Dentro de la fase de planificación y preparación, se establece que todo procedimiento de contratación debe estar sustentado en estudios previos, de conformidad con políticas, manuales, guías u orientaciones normativas dictadas por la Dirección General de Contrataciones Públicas o las regulaciones especiales aplicables al objeto contractual.

El objetivo del presente informe es presentar los resultados de los estudios previos realizados por el Departamento de Ciberseguridad, que serán el punto de partida para el diseño del procedimiento a realizar para la contratación de los servicios de **Consultoría de Implementación Gobernanza en Ciberseguridad**, en cumplimiento con lo establecido en el Reglamento de aplicación de la Ley 340-06 sobre Compras y Contrataciones de Bienes, Servicios y Obras, aprobado mediante el Decreto No. 416-23, y el Manual General de Procedimientos Ordinarios de Contratación Pública, aprobado por la Dirección General de Contrataciones Públicas.

En este sentido, se pretende definir de forma detallada la necesidad a atender, el objeto del contrato, sus características y especificaciones técnicas, así como las particularidades del mercado, el costo estimado y otros aspectos mínimos que deben determinarse respetando los principios de igualdad y libre competencia, para el correcto diseño del procedimiento que será realizado por la entidad para satisfacer la necesidad y lograr los objetivos propuestos.

Luego de varias gestiones de levantamiento de información y consultas de las informaciones disponibles, del análisis del proceso anterior y de la validación de las condiciones de disponibilidad de dichos servicios y productos en el mercado, así como del análisis de la necesidad que se pretende satisfacer, presentamos a continuación los siguientes resultados.

Identificación de la necesidad y justificación del proceso

La Tesorería de la Seguridad Social (TSS) es una entidad autónoma y descentralizada del Estado, adscrita al Ministerio de Trabajo, dotada de personalidad jurídica y patrimonio propio, conforme el Artículo 28 de la Ley 87-01 crea el Sistema Dominicano de Seguridad Social (SDSS) modificada por la Ley 13-20 que fortalece la Tesorería de la Seguridad Social (TSS) y la Dirección General de Información y Defensa del Afiliado (DIDA).

La Tesorería de la Seguridad Social (TSS) desempeña un papel fundamental en la gestión eficiente de los recursos destinados a garantizar la seguridad y bienestar de la población y tiene a su cargo el proceso de recaudo, distribución y pago de las cotizaciones del Sistema Dominicano de Seguridad Social (SDSS), así como del Sistema Único de Información y Recaudo (SUIR).

La Tesorería de la Seguridad Social definió en su Plan Estratégico Institucional 2021-2024 los siguientes ejes estratégicos: Experiencia del usuario, fortalecimiento institucional y crecimiento y

desarrollo. Dentro de cada uno de estos ejes, se contemplan acciones que van encaminadas al fortalecimiento de la cultura de ciberseguridad.

La Tesorería de la Seguridad Social conforme a su Plan Estratégico Institucional (PEI), ha considerado dentro del marco del fortalecimiento institucional, optimizar sus operaciones lo que incluye la realización de actividades que buscan robustecer la seguridad de la información, cuyas actividades presupuestadas están contenidas en el Plan Anual de Compras y Contrataciones (PACC), la adquisición del servicio de **Consultoría de Implementación Gobernanza en Ciberseguridad,** los cuales son fundamentales para continuar implantando las políticas que rijan una cultura en ciberseguridad.

El objeto de la presente convocatoria constituye la Contratación de servicios de Empresa para la definición de un plan que defina Estrategias de Seguridad de la Información enfocadas en Ciberseguridad, con un enfoque moderno, actualizado y funcional, así como también definir el Modelo de Gobierno que permita gestionar dicho plan y las iniciativas propuestas el área de Dirección de Normas, Cumplimiento y Ciberseguridad, de la Tesorería de la Seguridad Social (TSS) de acuerdo con las condiciones fijadas en el presente Pliego de Condiciones.

La contratación de los servicios de **Consultoría de Implementación Gobernanza en Ciberseguridad,** permitirá a la institución mantener una cultura en ciberseguridad actualizada que garantice la prevención de ataques cibernéticos y una gestión oportuna en potenciales incidentes de ciberseguridad, por medio de la concientización del personal, toma de decisiones y adquisición de herramientas de gestión en ciberseguridad, lo que contribuirá a un ambiente ciberseguro y confiable desde el punto de vista de las partes interesadas. Cuando una institución proyecta una imagen de gestión correcta en ciberseguridad, las personas tienden a confiar más en sus servicios y productos, y esto es relevante ya que la credibilidad es esencial para construir relaciones a largo plazo con los usuarios y otras partes interesadas.

Identificación del objeto del contrato, su naturaleza, características y sus especificaciones

Se requiere contratar los servicios de **Consultoría de Implementación Gobernanza en Ciberseguridad**, según las especificaciones detalladas debajo.

Ítem	Rubro	Descripción	Cantidad	Unidad de medida	Especificaciones
1	80101507	Consultoría de Implementación Gobernanza en Ciberseguridad	1	Servicio	*Ver especificaciones debajo.

Especificaciones técnicas del servicio:

Para la Consultoría de Implementación Gobernanza en Ciberseguridad los marcos mínimos de referencia serán los siguientes: Norma **ISO 27001:2022** sobre **sistemas de gestión de la seguridad de la información (SGSI)**; Marco de Seguridad Cibernética **NIST CSF 2.0**; Los Controles Críticos de Seguridad en su octava versión **CIS Controls V8**; Norma **ISO 33052** sobre Tecnología de la Información; Norma **ISO 33072** sobre Modelo de Evaluación de Procesos (PAM).

La misma requiere que abarque las siguientes actividades:

I. **Primera etapa: Identificar el nivel actual de seguridad vs marcos de referencia.**

- Establecer el contexto detallado de la organización (TSS) sobre el cual desarrollará la identificación del nivel actual de seguridad.
- Identificar los requerimientos regulatorios de seguridad establecidos en las diferentes regulaciones aplicables a la organización.
- Definir los marcos de referencia y estándares de seguridad aplicables a la organización, estableciendo la declaración de aplicabilidad de cada uno de ellos.
- Identificar el nivel actual de seguridad implementando en la organización considerando de manera enunciativa, mas no limitativa, siguientes dominios:
    - Gobierno de seguridad, incluyendo el marco normativo
    - Procesos de seguridad, considerando los primarios de acuerdo con las mejores prácticas.
    - Estructura organizacional y segregación de funciones
    - Controles tecnológicos implementados y su nivel de efectividad
    - Controles de acceso físico implementados
    - Controles de acceso lógico implementados, modelo de autenticación, operación ABC.
    - Metodologías de desarrollo seguro y manejo de código.

- Identificar el nivel actual de cumplimiento contra cada uno de los objetivos, controles, requerimientos u otros establecidos en las regulaciones, marcos de referencia y estándares seleccionados.
- Establecer el nivel actual de madurez y cumplimiento de seguridad AS-IS vs los marcos de referencia y estándares seleccionados.

II. Segunda etapa: Definir el nivel deseado de seguridad de la información para la organización, así como desarrollar el modelo de gobierno de seguridad a ser implementado.

Durante esta etapa las actividades mínimas a realizar comprenden las siguientes:

- Establecer el nivel de madurez de seguridad de la información deseado y alcanzable TO-BE por la organización en el corto, mediano y largo plazo. Dicho nivel de considerar los siguientes niveles:
    - General
    - Por marco de referencia
    - Por control, proceso, procedimiento, objetivo de control.
    - Benchmarks vs organizaciones similares en la región y globales.
- Definir y desarrollar de manera detallada el modelo de gobierno requerido para poder alcanzar el nivel de madurez deseado.
- Desarrollar la arquitectura de seguridad de alto y medio nivel acorde con el nivel de seguridad establecido.
- Definir la matriz de controles de seguridad a implementar con el nivel de efectividad requerido y señalando a que mejor práctica hacen referencia.
- Generar un reporte del nivel de brecha existente entre el estado actual de la seguridad y el estado deseado.
- Informe del Análisis FODA de la TSS en Seguridad de la Información

III. Tercera etapa: Desarrollar el Plan Estratégico de Seguridad de la Información a ser implementado

Durante esta etapa las actividades mínimas a realizar comprenden las siguientes:

- Establecer la estructura general del plan estratégico de seguridad alineado al PEI TSS 2025-2028.
- Definir las iniciativas de implementación que cubran los requerimientos establecidos en el modelo de gobierno de seguridad, la arquitectura definida y la matriz de controles aplicables, alineado al PEI TSS 2025-2028, y bajo el formato de planilla de productos de POA TSS.
- Detallar el siguiente nivel de los controles de seguridad que deberán de ser desarrollados e implementados.
- Desarrollar el marco normativo de seguridad aplicables (políticas y procesos)
- Integrar el documento de Plan Estratégico de Seguridad de la Información, considerando el nivel de madurez objetivo, el modelo de gobierno, la arquitectura de seguridad definida y los controles a implementar. El plan debe contener el detalle de las iniciativas, el esfuerzo requerido para la implementación de las mismas, el cronograma de implementación y la prioridad de implementación, así como la estimación de la inversión.

    - Identificar los logros que persigue la institución en un plazo determinado, ya sea a corto, mediano o largo plazo, deben ser específicos, medibles, realistas, oportunos y cónsonos con las normativas legales vigentes, y alineado al PEI TSS 2025-2028.
    - Definir los indicadores para medir el desempeño institucional. (eficacia, eficiencia, economía y calidad).
    - Identificación de Ejes y objetivos estratégicos. Formalización del Cuadro de Mando de la Estrategia (KPIs/Resultados esperados. Agrupación de KPIs por Línea Estratégica). Análisis de riesgos estratégicos
    - Definición de supuestos/ identificación de riesgos. Definir los acontecimientos que se pudieren presentar, para las diferentes categorías de objetivos. Incluyendo las recomendaciones para la prevención de los riesgos y las medidas pertinentes que pudieren mitigar los supuestos planteados.
    - Definición de los estándares a partir de los cuales será evaluado el éxito del plan. Así, los colaboradores sabrán exactamente cuáles son las expectativas que la institución tiene sobre ellos. Definir resultado esperado del Plan y de cada eje, objetivo o indicador establecido.

Todas las actividades descritas anteriormente deberán realizarse con Sesiones multidisciplinarias de mesas de trabajo guiadas para la creación del contenido estratégico del plan. A su vez estar sustentadas y entregadas a la TSS por el oferente adjudicado en minutas de reuniones en físico y escaneadas con las respectivas firmas en formato PDF, y por informes que deberán estar en formato digital editable y en físico, así como materiales de apoyo impreso y digitales.

El Plan Estratégico que presente el consultor, deberá abarcar mínimo un periodo de cuatro (4) años. Presentando los objetivos y las actividades a desarrollar para el logro de cada uno de ellos, tomando en cuenta el aporte de cada una de las unidades operativas y órganos decisivos internos de la institución. Además, deberá incluir las propuestas de las políticas a implementar, con miras al cumplimiento de los objetivos planteados.

Aplicación de metodología OKR o metodología similar, enfocada en la creación de parámetros e indicadores que dejan ver la ejecución de una estrategia y el cumplimiento de estándares predefinidos. Debe incluir metas a mediano y largo plazo.

ENTREGABLES

Entregables (Primera Etapa) mínimos para la identificación de la situación actual:

1. Documento de contexto (organización, estructura y regulatorio)
2. Matriz indicando los procesos y activos considerados en el proyecto
3. Matriz de impactos de seguridad presentes
4. Documento de requerimientos operativos de seguridad de la organización
5. Matriz de nivel de madurez actual vs los marcos de referencia establecidos en esta licitación.
6. Reporte de nivel actual de seguridad AS-IS
7. Reporte de benchmark vs organizaciones similares

Entregables (Segunda Etapa) para la identificación de la situación deseada:

1. Documento del estado deseado y requerido de seguridad de la información (TO-BE) con la justificación explícita del porque se define ese nivel deseado utilizando mejores prácticas y benchmarks.
2. Documento con el modelo de gobierno de seguridad definido y desarrollado para la organización
3. Arquitectura general de seguridad basada en modelo OSA u otro similar
4. Matriz general de controles de seguridad aplicables y su referencia a regulaciones y marcos de referencia (declaración de aplicabilidad).
5. Documento de brecha existente entre el AS-IS y el TO-BE
6. Documento con la definición de las iniciativas sugeridas para llegar al estado deseado TO-BE y que representa cada una de ellas en esfuerzo de inversión económica, personas, procesos, etc., para la organización, así como una sumatoria total de dichas iniciativas.
7. Roadmap a corto, mediano y largo plazo con las iniciativas para llegar al estado deseado TO-BE y plan de trabajo sugerido.

Entregables (Tercera Etapa) para el plan estratégico de seguridad:

1. Plan Estratégico Director de Seguridad (corto, mediano y largo plazo) alineado al PEI TSS 2025-2028
2. Presentación de consolidado PE preliminar al Comité Ejecutivo.
3. Selección de contenido relevante para medios de comunicación interna y externa.
4. Arquitectura específica de seguridad (para los principales dominios)
5. Matriz detallada de controles de seguridad y su referencia a los marcos referidos.
6. Marco normativo de seguridad

Todos los productos serán propiedad de la Entidad Contratante, quien tiene el derecho de publicarlos y hacerlos disponibles públicamente.

Los técnicos o profesionales que estarán asignados a la auditoría deben en conjunto tener, al menos, las siguientes certificaciones:

- CISSP
- CISM
- CRISC
- Auditor ISO 27001
- ISO 31000 Risk Manager

- COBIT Foundation (al menos versión 5.
- ITIL Foundation (al menos versión 4).
- TOGAF Foundation (al menos versión 9).

El oferente/proponente a participar deberá contar con la certificación vigente en los siguientes sistemas de gestión para sus procesos de consultoría:

- ISO 9001-2015
- ISO 20000-1-2011
- ISO 27001-2008
- ISO 31001-2008

El número de visitas queda a consideración del oferente.

Todas las actividades descritas anteriormente deberán estar sustentadas y entregadas a la TSS por el oferente/proponente adjudicado en minutas de reuniones en físico y escaneadas con las respectivas firmas en formato PDF, y por informes que deberán estar en formato digital editable y en físico, así como materiales de apoyo impreso y digitales.

La empresa que resulte adjudicataria deberá:

1. Elaborar el plan de desarrollo de los servicios y el modelo de gobierno del proyecto.
2. Elaborar las guías de seguimiento de control del proyecto.
3. Programar las visitas, entrevistas y la revisión de controles actuales.
4. Creación de los informes, reportes y entregables.

Plazo y Lugar de Trabajo

La Convocatoria se hace sobre la base de un plazo para la ejecución de los trabajos de cuatro (04) meses contados a partir de la suscripción del contrato, con un cronograma estimado a nivel de cada producto, actividad o logro de objetivos.

El Adjudicatario realizará el trabajo con sus propios recursos (equipos, bienes, materiales, personal), la TSS no correrá con pagos de dietas, parqueos, traslados, llamadas, o cualquier otro gasto relacionado con la auditoría y de los auditores asignados. En caso de ser necesario, el proveedor se compromete a permitir que la Tesorería de la Seguridad Social realice cualquier revisión o registro de los equipos que ingresen físicamente a la Institución.

El Adjudicatario se compromete a firmar el Compromiso de Confidencialidad, para poder requerir las informaciones necesarias para la elaboración su trabajo.

Resultados o Productos Esperados.

Los productos o resultados que debe entregar el proponente que resulte adjudicatario son los siguientes:

Entregables mínimos para la identificación de la situación actual:

8. Documento de contexto (organización, estructura y regulatorio).
9. Matriz indicando los procesos y activos considerados en el proyecto.
10. Matriz de impactos de seguridad presentes.
11. Documento de requerimientos operativos de seguridad de la organización.
12. Matriz de nivel de madurez actual.
13. Reporte de nivel actual de seguridad AS-IS.

Entregables para la identificación de la situación deseada (TO-BE):

14. Documento del estado deseado y requerido de ciberseguridad de la información (TO-BE).
15. Documento con el modelo de gobierno de ciberseguridad definido y desarrollado para la organización.
16. Arquitectura general de ciberseguridad basada en modelo OSA u otro similar.
17. Matriz general de controles de ciberseguridad aplicables y su referencia a regulaciones y marcos de referencia, identificando los artículos específicos que nos aplican.
18. Políticas y procedimientos necesarios para la correcta ejecución en materia de ciberseguridad.
19. Documento de brecha existente entre el AS-IS y el TO-BE.

Entregables para el plan estratégico de ciberseguridad:

20. Plan Estratégico en ciberseguridad (corto, mediano y largo plazo).
21. Arquitectura específica de ciberseguridad (para los principales dominios).
22. Matriz detallada de controles de ciberseguridad.
23. Marco normativo de ciberseguridad.
24. Objetivos propuestos en ciberseguridad.

Coordinación, Supervisión e Informes

El proponente que resulte adjudicatario deberá coordinar sus actividades con José Luna, Asesor de la Dirección de Normas, Cumplimiento y Ciberseguridad de la Tesorería de la Seguridad Social y laborará junto al personal técnico y profesional de la TSS designado.

Duración del Servicio

El tiempo total del servicio de consultoría solicitado tendrá una duración máxima de cuatro (04) meses contados a partir de la suscripción del contrato.

Las particularidades del mercado, en cuanto a cómo y en cuáles plazos se ofrece ese bien, se presta el servicio o se ejecuta la obra

Los bienes y servicios requeridos por la entidad contratante se encuentran disponibles en el mercado local, y es ofrecido por proveedores que pueden ser personas físicas y jurídicas a nivel nacional, sin mayores complicaciones a la hora de prestarlo y el acceso a los materiales necesarios para la correcta ejecución de lo que se pretende contratar.

La ejecución del bien se llevará a cabo en el domicilio de la entidad contratante, indicadas a continuación:

Ítem	Localidad TSS	Dirección
1	Torre	Av. Tiradentes #33, Ens. Naco, SD, Distrito Nacional.
2	Gustavo Mejía Ricart	Gustavo Mejía Ricart #52, Ens. Naco, Santo Domingo, Distrito Nacional.
3	Plaza Naco	Av. Tiradentes #44, Ens. Naco, SD, Distrito Nacional.
4	Puerto Plata	Calle Beller # 95, Puerto Plata
5	San Francisco de Macorís	Calle Salcedo Plaza Galería 56, 4to. Nivel. SFM.R.D
6	Bávaro	Av. Punta Cana, Plaza Reynoso, Local No. 2

Análisis de oferta y demanda de los bienes y servicios requeridos.

Hemos identificado que en el mercado existen varios proveedores que pueden ofrecer dichos servicios en el territorio de la República Dominicana.

Por la naturaleza del proceso, se requiere realizar una presentación del esquema general de como seria desarrolladas las actividades a realizar y la experiencia de trabajos similares ejecutados.

Es necesario realizar visitas a las instalaciones de la entidad contratante para fines de levantamiento previo a la ejecución de lo contratado por parte del oferente que resulte adjudicatario del proceso. Además, en la propuesta técnica el oferente debe demostrar el cumplimiento de las especificaciones técnicas descritas en este informe de estudios previos.

Como servicios y condiciones adicionales, se requiere:

Condiciones de pago

- El pago será realizado en tres cuotas conforme se vayan recibiendo los entregables, cuya gestión de pago se iniciará una vez recibidos conforme por la Dirección de Normas, Cumplimiento y Ciberseguridad, o quien este designe en su representación. La empresa adjudicataria, deberá emitir una factura con Comprobante Gubernamental.

Hito	Descripción	Porcentaje
1	Un primer pago referente al anticipo, una vez emitido el certificado de registro de contrato por la Contraloría General de la República.	20%
2	Un segundo pago al recibido conforme de todos los entregables mínimos de la primera y segunda etapa (Situación actual- Estado deseado)	40%
3	Un tercer pago al recibido conforme de todos los entregables mínimos de la tercera etapa (Modelo de Gobierno y Plan estratégico)	40%

- El pago se realizará dentro de los treinta (30) días laborales siguientes a la fecha de vencimiento de la factura.
- En cada factura podrán ser solicitadas certificaciones de la DGII y TSS a los fines de gestionar el pago.
- La empresa adjudicataria deberá mantenerse en todo momento al día con sus obligaciones fiscales y de seguridad social, para poder recibir el pago correspondiente. En ese sentido, si por el no cumplimiento de estas obligaciones por parte del adjudicatario la Tesorería se ve imposibilitada de recibir los servicios objeto de la presente contratación, el contrato podrá ser rescindido dando pie a la adjudicación de la empresa que haya quedado en segundo lugar o a un nuevo proceso.
- Los pagos se harán por transferencia bancaria a la cuenta que el proveedor tenga registrada en DIGECOG, por lo que para recibir los pagos el suplidor debe encontrarse registrado como beneficiario en la Dirección General de Contrataciones Públicas y tener cuenta registrada. Esta cuenta debe ser en pesos dominicanos.
- La Tesorería de la Seguridad Social realiza retención del Impuesto Sobre la Renta de acuerdo con las Normas Legales Vigentes de la Dirección General de Impuestos Internos.
- Por parte de la entidad contratante, la unidad coordinadora y ejecutora será la Dirección de Normas, Cumplimiento y Ciberseguridad, bajo la responsabilidad de **José Alberto Luna Peña**, asesor.

El costo estimado del bien, obra o servicio a contratar, que determine el presupuesto de la contratación e identifique la partida presupuestaria a afectar.

El costo estimado para la contratación de los servicios de **Consultoría de Implementación Gobernanza en Ciberseguridad** es **RD$5,100,000.00,** en cuya virtud, de conformidad con el umbral establecido mediante la Resolución No. PNP-01-2024 emitida por la Dirección General de Contrataciones Públicas (DGCP), la forma idónea para satisfacer la necesidad es mediante un proceso de compra por montos debajo del umbral o compra directa, de conformidad con el artículo 45 del Reglamento de aplicación de la Ley 340-06 sobre Compras y Contrataciones de Bienes, Servicios y Obras, aprobado mediante Decreto No. 416-23, el cual se caracteriza por ser un procedimiento simple y ágil, al tiempo que se garantiza la transparencia y eficiencia, en cumplimiento de los procedimientos establecidos.

Determinación del contrato

En cuanto a la determinación del tipo de contrato a celebrar, se espera llevar a cabo un contrato de servicios que contenga el objeto, detalle de los ítems, condiciones y tiempo de entrega, forma de pago, entre otros aspectos relevantes, así como la garantía ofrecida por el proveedor de los servicios adjudicados. La adjudicación será por ítem.

En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, Capital de la República Dominicana, a los ocho (8) días del mes de agosto del año dos mil veinticuatro (2024).---

José Alberto Luna Peña
Asesor Dirección de Normas, Cumplimiento y Ciberseguridad