ESPECIFICACIONES TÉCNICAS

Contratación de los Servicios de Consultoría de Implementación Gobernanza en Ciberseguridad

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).

Se requiere que la propuesta 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 implementado 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, de acuerdo con los dominios establecidos en las diferentes referencias.
    - Controles de acceso físico implementados
    - Controles de acceso lógico implementados, modelo de autenticación, operación ABC, Control de cuentas privilegiadas, otros.
    - 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 con respecto a la seguridad de información, incluyendo los componentes de ciberseguridad. (eficacia, eficiencia, economía y calidad).
    - Identificación de Ejes y objetivos estratégicos de seguridad. Formalización del Cuadro de Mando de la Estrategia (KPIs/Resultados esperados. Agrupación de KPIs por Línea Estratégica). Análisis de riesgos de seguridad estratégicos
    - Definición de supuestos/ identificación de riesgos de seguridad. 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 considerando la estrategia a corto, mediano y largo plazo. 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 Plan Estratégico 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.

Todas las actividades descritas anteriormente deberán estar sustentadas y entregadas a la TSS por el oferente/proponente adjudicado en minutos 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 número de visitas queda a consideración del oferente.

CERTIFICACIONES DE LA EMPRESA Y PERSONAL PROPUESTO

El oferente debe indicar en su propuesta lo siguiente:

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 20000-1-2018
- ISO 27001-2022

COMPROMISOS

El oferente en su propuesta técnica debe indicar por escrito expresamente que se encuentra de acuerdo con el compromiso de entregar, en caso de resultar adjudicatario, lo siguiente:

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.

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 auditoria y de los auditores asignados. En caso de ser necesario, el proveedor se compromete a permitir que la Tesorería de la Seguridad Sociales 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 del 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:

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.
6. Reporte de nivel actual de seguridad AS-IS.

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

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

Entregables para el plan estratégico de ciberseguridad:

1. Plan Estratégico en ciberseguridad (corto, mediano y largo plazo)
2. Arquitectura especifica de ciberseguridad (para los principales dominios)
3. Matriz detallada de controles de ciberseguridad.
4. Marco normativo de ciberseguridad.
5. Objetivos propuestos en ciberseguridad.

INFORMES

En la contratación del servicio de consultoría**, los estudios, informes y material que se generen en la ejecución serán en todo momento de propiedad de la Tesorería de la Seguridad Social (TSS)**. Los responsables de su custodia no podrán utilizarlos ni proporcionar o difundir dicho material total o parcialmente; solo en caso de que se justifique su entrega a la autoridad competente, previa autorización formal y escrita de la entidad contratante.

Además de los productos, se entregarán las presentaciones, metodologías e instrumentos utilizados en la consultoría, como

también hojas de cálculo en los casos que así lo ameriten. Todos los informes se entregarán en formato digital, exceptuando el informe de cierre que deberá presentarse también en copia impresa.

Los informes en formato Word estarán escritos en idioma español, habrá un plazo de siete (7) días hábiles para que la emisión de comentarios de parte de la Tesorería de la Seguridad Social y un plazo de cuatro (4) días laborables para el consultor incorporar las modificaciones o sugerencias, a partir de los comentarios presentados.

Aspectos Generales

Toda la información que sea facilitada al oferente para iniciar los trabajos, así como la generada en el marco de la contratación será de carácter confidencial. El oferente deberá entregar a la Tesorería de la Seguridad Social toda la información de respaldo de los documentos, incluyendo las hojas y archivos electrónicos elaborados.

El oferente y sus relacionados no podrán divulgar ninguna información relacionada con la Tesorería de la Seguridad Social, por ser consideradas como CONFIDENCIALES, sin su consentimiento previo por escrito. En igual sentido, no podrán ser divulgados los documentos e informes generados a raíz de esta contratación. El Adjudicatario se compromete a firmar el Compromiso de Confidencialidad, así como todos sus colaboradores que participen en la consultoría, para poder requerir las informaciones necesarias para la ejecución de los servicios, es decir, aquellas que hayan sido calificadas como confidenciales

El Adjudicatario realizará el trabajo con sus propios recursos (equipos, bienes, materiales, personal), la TSS no correrá con pagos de dietas, traslados, llamadas, o cualquier otro gasto relacionado con la auditoría y de los auditores asignados. En caso de ser necesario, el oferente 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, en cada visita

La Entidad Contratante no se compromete a ofrecer espacios físicos al oferente adjudicado para la ejecución de los servicios a ser brindados en virtud del presente proceso. El hecho que los oferentes que no se familiaricen debidamente con los detalles y condiciones bajo las cuales serán ejecutados los trabajos, no se considerará como argumento válido para posteriores reclamaciones.

La Entidad Contratante suministrará, cuando sea necesario, los permisos pertinentes para efectuar las visitas correspondientes y designará un personal quien acompañará al representante del oferente adjudicado en todo momento, mientras dure la visita.

La supervisión y coordinación de las actividades será responsabilidad del Asesor de Ciberseguridad o quien designe la TSS.

Plan Estratégico (Contenido mínimo requerido):

- Índice. Lista de los títulos que permite la ubicación del contenido en el documento.
- Presentación/Introducción. Sección inicial para contextualizar el contenido y desarrollo del documento.
- Equipo Directivo de la Institución. Lista de los nombres y cargos del personal que lidera la institución.
- Equipo de coordinación. Lista de los nombres y cargos del personal que lidera el proyecto.
- Equipo de elaboración. Lista de nombres y cargos que trabajaron en la recopilación y redacción del documento, así como todo lo relacionado a su elaboración.
- Glosario de definiciones. Catálogo de palabras con definiciones que permitirá la compresión del documento.
- Responsabilidades/Funciones de la Institución (Dentro de la normativa)

Diagnóstico Contextual
• Análisis del Marco Normativo asociado
• Análisis Cualitativo y Cuantitativo de los Problemas
• Priorización de los Problemas
• Construcción del Árbol de Problemas

Marco Institucional
• Análisis FODA y definición de Estrategias centrales

Diseño Marco Estratégico
• Construcción de Resultados
• Construcción Indicadores de Resultados
• Establecimiento Metas de Resultados

• Priorización estratégica
• Ejes Estratégicos
• Diseño de Productos Estratégicos
• Construcción de Indicadores de Productos
• Valoración y Administración de Riesgos
• Costeo del Plan Estratégico
• Identificación de ideas de proyectos estratégicos
• Estrategias de Financiamiento

Seguimiento y monitoreo del Plan
• Mecanismos de Seguimiento
• Monitoreo

Evaluación del Plan
• Evaluación

Formatos de diagramación del Plan

Tipografías: Gilroy family
Tamaños de fuente:
Títulos: Gilroy-extrabold (20.4 pt)
Subtítulos: Gilroy-bold (mayúsculas) (13.2 pt)
Cuerpo de texto: Gilroy-regular (13.2 pt)
Márgenes: Superior: 0.91 | Izquierdo: 0.95 | Inferior: 0.71 | Derecho: 0.95
Colores:
Cuerpo de texto: gris (hexadecimal #58595B)
Títulos: azul oscuro (hexadecimal # 1B449C)
Texto destacado: gris oscuro (hexadecimales #555556 / #3B4252)
Subtítulos: azul claro (hexadecimal #008FBE)
Bullets: gris oscuro (hexadecimal #3B4252)
Banco de imágenes de referencia: Pexels y Freepick
Tratamiento a la máxima autoridad: Henry Sahdalá, tesorero de la Seguridad Social; tesorero Henry Sahdalá; tesorero.

Uso de la marca basado en el Manual de Identidad Corporativa, así como los templates de presentación o plantillas mencionadas, que sería entregado al adjudicatario.