Nombre del Servicio:

Contratación de los servicios de diseño e implementación de un Sistema de Gestión de Seguridad de la Información basado en los requisitos de la norma ISO 27001:2022, para la Superintendencia de Bancos de la República Dominicana.

1. Antecedentes

La Superintendencia de Bancos es una entidad pública de Derecho Público con personalidad jurídica propia. Tiene su domicilio en su oficina principal de Santo Domingo, Distrito Nacional, Capital de la República Dominicana, pudiendo establecer otras oficinas dentro del territorio nacional.

La Superintendencia de Bancos (SB) como ente supervisor de las entidades de intermediación financiera y cambiaria según lo establecido en la Ley 183-02, ha diseñado un plan estratégico 2021-2024 mediante el cual se propone: "Ser una institución referente nacional e internacionalmente, reconocida por la calidad de su supervisión y el acompañamiento que brinda a los usuarios de los servicios financieros, respaldada por un personal altamente calificado y la excelencia en su gestión", y para alcanzar la visión se han identificado seis ejes estratégicos que engloban los objetivos estratégicos e iniciativas que durante el período 2021-2024 la SB se propone ejecutar.

Uno de estos ejes estratégicos es el de Eficiencia y Fortalecimiento Institucional, el cual le permitirá a la SB aumentar la efectividad y calidad de la gestión institucional con un enfoque orientado a resultados, la mejora continua, la continuidad de las operaciones, la seguridad de la información propia y de sus clientes y la sostenibilidad institucional.

Implementar un sistema de gestión de seguridad de la información es un hito de relevante importancia en la Superintendencia, como parte del fomento de un enfoque de organización segura, resiliente y comprometida con mantener la seguridad de la información utilizada en sus operaciones y actividades. En consonancia con el compromiso asumido por la alta dirección en la declaración de misión institucional de ser referente nacional e internacional.

En la actualidad la SB dispone de un sistema de gestión de calidad y de riesgos en desarrollo, con niveles de responsabilidad definidos y con un marco y proceso para la gestión de riesgos documentado. Este sistema incluye lo siguiente: (i) Matrices de riesgos de los principales procesos de apoyo y misionales; y (ii) listado de controles preventivos, detectivos y compensatorio. (iii) Planes de tratamiento en ejecución para los riesgos dentro de los niveles no aceptados de acuerdo con las políticas internas de gestión de riesgos.

En función de lo anterior la SB se dispuso a realizar el diseño e implementación del sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022, como siguiente paso para lograr fortalecer la capacidad de resiliencia organizacional. En consecuencia, la SB requiere contratar una empresa especializada en el diseño e implementación del sistema de gestión de seguridad de la información basado en ISO 27001:2022, para la realización de los trabajos necesarios para que la SB disponga del referido servicio en todos sus procesos críticos y de apoyo.

2. Descripción del servicio

2.1. Objetivo y Alcance del servicio requerido.

El objetivo es contratar los servicios de una empresa consultora con experiencia comprobable, para el diseño, implementación y auditoría del sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 y experiencia en implementación de sistemas de gestión integrados, con un alcance en todos sus procesos críticos y los de apoyo a estos procesos que formen parte de los requisitos exigidos por la norma.

El oferente debe considerar dentro del alcance del proyecto las siguientes actividades/procesos, los cuales deben formar parte de su oferta técnica y económica:

- Capacitar al inicio del proyecto al personal (TDO, Riesgos, Auditoría Interna, Seguridad de la Información y otras áreas) que participará en el proyecto en el estándar ISO 27001:2022 e ISO 27002:2022. Estas capacitaciones deben comprender:
  - Capacitación de interpretación e implementación del estándar ISO 27001 al inicio del proyecto para que el equipo de la SB que estará participando en la implementación.
  - Capacitación sobre la metodología de riesgo ajustada que se utilizará para la identificación y análisis de riesgos de seguridad de la información.
  - Capacitación de auditor de ISO 27001 para el equipo de Auditoría Interna.
  - Generación de material de capacitación sobre el marco normativo y gestión de la seguridad para los usuarios de la SB.
  - Entrenamiento para los responsables de la capacitación interna
- Diagnosticar el estado actual de la seguridad de la información en la institución.
- Analizar y valorar el proceso de gestión de riesgos y gestión de calidad actual en términos de alineamiento e integración con el Sistema de Gestión de de Seguridad de la Información.
- Evolucionar el modelo actual de gestión de riesgo para que considere el riesgo tecnológico y de seguridad de la información de la SB.
- Elaborar el cronograma de trabajo sobre las actividades para la ejecución del diseño e implementación del SGSI.
- Realizar una actualización del análisis sobre el contexto de la organización con una visión de seguridad de la información, donde se revise y desarrolle lo siguiente:
  i. Contexto interno y externo.
  ii. Misión, visión y valores
  iii. Necesidades, expectativas y riesgos identificados para las partes interesadas
  iv. Requerimientos regulatorios locales e internacionales con respecto a la seguridad de la información aplicables a la institución.
  v. Evaluación del análisis de riesgo tecnológico y de seguridad de la información ejecutado por la SB.
  vi. Definición y generación del enunciado de alcance del sistema de gestión de seguridad de la información, tomando en consideración el enfoque a la integralidad de diferentes normas ISO.

- Planificar el sistema de gestión de seguridad de la información, incluyendo las siguientes actividades:

  i. Identificación de los procesos críticos y de apoyos al SGSI.
  ii. Identificación de la información sensible que existe en la organización.
  iii. Alineación y revisión de la política de seguridad de información.
  iv. Alineación del comité, gobierno y responsabilidades del SGSI.
  v. Definición de los objetivos del SGSI.
  vi. Generación de la matriz de declaración de aplicabilidad de los controles establecidos en el anexo A del ISO27001:2022 y su alineación a la guía de práctica del ISO 27002:2022.

- Diseñar los elementos estratégicos, de apoyo y operativos al SGSI, como son:

  i. Elaboración y/o actualización de la información documentada del marco normativo, técnico y de operación de obligado cumplimento en un Sistema de Gestión de Seguridad de la Información.

     - Estrategias de Atención y Respuesta a Riesgos (Plan de Tratamiento de Riesgos)

- Matriz de controles de seguridad aplicables
- Marco de políticas de seguridad
- Marco de procesos de seguridad
- Validación del comité de seguridad
- Validación e integración de formatos de documentación de seguridad de información según el estándar definido para ISO9001
- Validación y documentación de alto nivel de la arquitectura de seguridad

ii. Validación y alineación del programa de Concientización y capacitación del personal de la SB en torno a Seguridad de la Información.
iii. Programa de Análisis de Riesgos y Seguimiento al Plan de Tratamiento de Riesgos (PTR).

- Diseñar los requisitos para la evaluación de desempeño y mejora del SGSI, basado en los siguientes lineamientos:

i. Establecimiento y ejecución de un proceso de auditorías internas de seguridad de la información e integración al proceso existente de gestión de no conformidades.
ii. Integración de un esquema de seguimiento y medición de los procesos con las prácticas de seguimiento en la institución y aquellas establecidas para la gestión en el ISO 27001:2022 como medición de la dirección, revisión de efectividad, etc.
iii. Validación y documentación de los indicadores de seguridad y riesgos y su forma de medir y dar seguimiento en el SGSI.
iv. Estructura de control documental alineada a la establecida en el sistema actual ISO 9001.
v. Definición del marco de evolución para aumentar el alcance del SGSI.

Nota:

Dentro del diseño de los puntos mencionados se deben incluir los levantamientos necesarios para la generación y redacción de la información documentada, matrices de controles, arquitecturas, escenarios y otras actividades relacionadas alineados al Sistema de Gestión de la Calidad actual basado en la Norma ISO 9001:2015. Estas actividades estarán siendo realizadas por el personal dedicado facilitado por el oferente.

JP

El alcance de este proyecto de dividirá en 3 etapas:

i. Etapa 1: Diagnóstico del estado actual del SGSI, plan de cierre de brechas de seguridad de información y plan de tratamiento de riesgos, así como la declaración de aplicabilidad, generación del marco normativo, alineación del comité de seguridad y diseño del modelo de gestión.
ii. Etapa 2: Implementación y auditoría interna del sistema de gestión de seguridad de la información, de cara al cumplimiento de los requisitos exigidos por la norma ISO 27001:2022 y 27002:2022.

Etapa 3: Etapa post certificación ISO 27001:2022 por la empresa certificadora y posterior a concluir con las 2 etapas. Dicha etapa post certificación se incluye para definir las actividades y planes de acción que deben realizarse para mantener el SGSI y su certificación.

2.2. Cronograma de entrega del servicio requerido:

El proveedor debe entregar un cronograma preliminar que contenga cada una de las etapas del proyecto, incluyendo la planificación y levantamiento de informaciones.

Como base para la elaboración de este cronograma preliminar, el proveedor debe considerar:

- Concluir cada etapa en un plazo no mayor a lo siguiente:
  i. Etapa 1, cuatro (4) meses (Enero 2023 – Abril 2023)
  ii. Etapa 2, máximo cuatro (4) meses (Mayo 2023 – Agosto 2023)
  iii. Etapa 3, 1 mes luego de la certificación

- El cronograma preliminar debe contener la secuencia de implementación de las diferentes etapas y sus actividades.

Una vez firmado el contrato, la reunión de inicio del proyecto (kick-off) debe realizarse en un plazo no mayor a cinco (5) días laborables; el cronograma definitivo de implementación deberá estar definido en un plazo no mayor a siete (7) días laborables a partir de dicha reunión de inicio del proyecto (kick-off).

2.3. Especificaciones técnicas del servicio requerido:

Se requieren los servicios de diseño e implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2022 para los procesos críticos, los procesos estratégicos y de apoyo de la SB relacionados a los requisitos exigidos por la norma. Esta implementación debe estar totalmente integrada con otros normas y sistemas de gestión ya implementados en la SB y dejarla preparada para su integración con otras normas y sistemas de gestión que se encuentren en desarrollo en la institución.

Se requiere el diseño e implementación de todas las actividades y/o documentos necesarios para lograr establecer el SGSI, en materia de lo siguiente:

- **Análisis de brechas y riesgos identificados en diagnóstico.** Debe realizarse un análisis cualitativo y de brechas sobre los hallazgos encontrados en el diagnóstico. Así mismo, debe de revisarse y validarse el análisis de riesgos de seguridad ejecutado por la SB. Estos análisis se deben presentar en un informe indicando sus resultados y recomendaciones sobre las brechas y riesgos para lograr el cumplimiento de los requisitos exigidos por la norma ISO 27001:2022. Deberá considerarse la alineación a la metodología actual de riesgos existente en la SB.

- **Cronograma de implementación.** El cronograma debe incluir todas las actividades necesarias para lograr la implementación del SGSI con estimación básica de tiempo y correlación/dependencia de entre las mismas.
- **Reporte Análisis de Contexto y apoyo en actualización del PEI y POA de la SB.** Analizar y elaborar un reporte sobre el contexto interno y externo de la SB y sus partes interesadas con miras a cumplir los requisitos de la norma ISO 27001:2022. Esto debe ser integrado con el análisis de contexto ya establecido para otros sistemas de gestión implementados y dejarlo preparado para su integración con otros análisis de contexto de sistemas de gestión que se encuentren en desarrollo

- **Información documentada respecto a la identificación del alcance del Sistema de Gestión de Seguridad de la Información.** Reporte o documento que valide la determinación y el enunciado del alcance en el SGSI. Esto debe ser integrado con documentación sobre alcance de sistemas de gestión implementados y dejarlo preparado para su integración con documentación sobre alcance de otros sistemas de gestión que se encuentren en desarrollo.

- **Identificación de procesos críticos.** Levantamiento/actualización del mapa de procesos de la SB, e identificación del inventario de procesos bajo alcance para incluir referencia en lista maestra disponible para el control de la documentación.

- **Declaración de aplicabilidad.** Generación de matriz de aplicabilidad y exclusión justificada de los controles establecidos en el Anexo A de la Norma ISO 27001:2022 y la ISO 27002:2022.

- **Política, objetivos e indicadores de seguridad de la información.** Diseñar la política, objetivos e indicadores de seguridad, acorde con los propósitos establecidos, incluyendo el compromiso de cumplir los requisitos aplicables y de mejora continua. Esta política debe ser realizada junto a los lideres de equipo de la SB y en conformidad con los criterios exigidos por la norma ISO 9001 de gestión de Calidad

- **Matriz de riesgos y oportunidades.** Determinar y analizar los riesgos y oportunidades que puedan afectar a la conformidad de los procesos y la capacidad de seguridad de la información.

- **Plan de capacitaciones y concientización de seguridad de la información.** Validar y alinear el plan de capacitaciones y concientización de seguridad de la información para los colaboradores de la SB dentro del alcance del SGSI. Este plan debe considerar todas las posiciones y colaboradores que interactúen con la información contemplada en el SGSI (Ej: TDO, Riesgos Operativos, Auditoría, Seguridad de la Información), así como proponer el contenido y temas, como tipos de capacitaciones sugeridas y material de concientización, entre otros.

- **Propuesta de la estructura para la administración del sistema de gestión de seguridad de la información.** Elaborar una propuesta sobre la estructura organizacional para la administración del SGSI, esta propuesta debe incluir nombre de las posiciones, descripciones de puestos, ubicación dentro de la estructura general y sus procesos para lograr que el SGSI sea sostenible en el tiempo.

- **Propuesta para alinear (en caso necesario) la estructura del comité de seguridad**. Elaborar una propuesta sobre la estructura organizacional, roles y posiciones que deben de participar en el comité de seguridad de información incluyendo una matriz RACI y la descripción de las funciones y responsabilidades del mismo. Con respecto al órgano de gobierno, debe alinearse con las políticas de conformación de comités..

- **Requerimientos e insumos para el plan de comunicaciones del Sistema de Gestión de Seguridad de la Información.** Definir los requisitos y canales para el desarrollo del plan de comunicaciones del SGSI, así como el contenido de este, garantizando su aplicación y entendimiento en las partes interesadas.

- **Información documentada del marco normativo de seguridad de la información (manuales, políticas, matrices de control, protocolos, planes, formatos).** Revisar los formatos y contenido de la documentación controlada y verificar el nivel de cumplimiento en relación con los requisitos exigidos por la norma; actualizar en caso de ser necesario. En adición, documentar todos los procesos críticos (manuales, políticas, procedimientos, etc.), así como las matrices de controles necesarios para la implementación y funcionamiento eficaz del SGSI. Sobre este punto, se debe incluir la revisión y si es necesario, el diseño, del procedimiento para el control de los documentos y sus versiones, por si es necesario considerar algún elemento particular en cumplimiento con la ISO 27001, además de los exigidos por la ISO 9001.

- **Fichas de procesos e indicadores de seguridad.** Revisar, integrar con los sistemas de gestión ya implementados, y si es necesario levantar y elaborar, las fichas de procesos e indicadores de seguridad para el seguimiento, medición, análisis y evaluación del SGSI, de acuerdo con los requisitos de la norma.

- **Auditoría interna para evaluar la implementación del SGSI.** Realizar la auditoría interna previo a la auditoria externa de la empresa certificadora. El objetivo de esta auditoría es garantizar la implementación del SGSI y determinar el plan de acciones correctivas. Se debe incluir la revisión, integración con los sistemas de gestión ya implementados, y si es necesario el diseño, del procedimiento y criterios de auditoría interna y para mantener el SGSI y garantizar la mejora continua, por si es necesario considerar algún elemento particular en cumplimiento con la ISO 27001, además de los exigidos por la ISO 9001. El oferente deberá contar con expertos en auditorías internas del SGSI,

para garantizar el correcto funcionamiento e implementación dentro de la institución. El oferente deberá capacitar a un equipo interno de SB para que puedan realizar las auditorías anuales requeridas de forma posterior a la certificación.

- **Auditoría de 2ª parte.** Realizar una auditoría por parte del oferente con un auditor certificado emulando la auditoría de certificación que permita identificar cualquier desviación.

- **Acompañamiento en el proceso de auditoría de certificación.** El oferente deberá acompañar a la SB durante todo el proceso de certificación en el estándar ISO 27001:2022 y realizar cualquier ajuste que surja como observación del auditor de la casa certificadora que permita el logro de dicha certificación.

El oferente debe contemplar en su propuesta, todas las actividades adicionales que se requieran para lograr la implementación del SGSI en la SB y su metodología de trabajo debe estar basada en lo siguiente:

i. La mejora de los procesos existentes. El equipo consultor debe aprovechar las iniciativas anteriores de la institución y buscar oportunidades de mejora al desempeño de los procesos.
ii. Participación. El equipo consultor debe trabajar de manera activa con el dueño del proceso y sus colaboradores con el objetivo de transferir el conocimiento.
iii. Personalización. La propuesta debe adaptarse a las necesidades particulares de la SB. No se deben imponer métodos ni técnicas, las soluciones de basan en el consenso de todas las partes interesadas.
iv. Planificación. El proceso de implementación debe regirse por el tiempo específico indicando en el punto 2.2 de este documento. El equipo consultor debe ofrecer seguimiento permanente para asegurar la planificación adecuada de cada actividad.
v. Mejora continua. El sistema de gestión debe desarrollarse como una acción permanente de mejora.
vi.

El oferente debe contemplar en su propuesta, una etapa post certificación ISO 27001:2022 por la empresa certificadora y posterior a concluir con las 2 etapas. Dicha etapa post certificación se incluye para definir las actividades y planes de acción que deben realizarse para mantener el SGSI y su certificación.

3. Requisitos al oferente, tanto para su selección o si resulta adjudicatario de los servicios:

- El oferente debe poseer su Registro de Proveedor del Estado (RPE) en estado activo; además, deberá estar al día en el pago de sus impuestos.
- El oferente local podrá tener una alianza estratégica con una compañía extranjera siempre y cuando exista un contrato firmado entre ambas compañías.
- Los oferentes deben tener más de 10 años de experiencia demostrable en implementación de sistemas de gestión de de seguridad de la información, preferiblemente en el sector bancario.Los oferentes deben presentar al menos **cinco (5) implementaciones exitosas del SGSI ISO 27001:2013** a clientes diferentes; al menos **una (1)** de estas implementaciones exitosas deben ser de instituciones públicas (nacionales o internacionales) y **una adicional (1)** en una institución financiera. Las implementaciones deben tener un alcance similar o superior a lo requerido y se medirán por la certificación alcanzada de la norma.
- El oferente debe presentar al menos **cinco (5) cartas de referencia** de clientes diferentes con los datos de las empresas donde se realizaron consultorías de implementación exitosas. La Superintendencia a través de su equipo pericial podrá indagar sobre los trabajos realizados y el éxito y calidad de las implementaciones trabajadas.
- Los oferentes deben poseer personal certificado al menos como auditores o implementadores ISO 27001:2013.
- Los oferentes deberán contar con la certificación ISO 9001:2015 e ISO 27001:2013 en sus procesos consultivos.

- Los oferentes deberán garantizar que la implementación y auditoría interna de ISO27001:2022 se logrará en un lapso no mayor a ocho (8) meses.
- Los oferentes deben presentar su **metodología y plan de trabajo (ver sección 2.2)** que especifique un esquema de planificación, análisis, diseño y verificación que permita implementar todos los requisitos exigidos por la norma ISO 27001:2022, incluyendo los siguientes aspectos:

    - Dividir el plan de trabajo en las 3 etapas definidas.
    - Especificar los resultados esperados en cada una de las etapas y el tiempo de duración de cada etapa.
    - Descripción de como realizarán la implementación, su metodología, procedimientos y herramientas que utilizarán.
    - Organigrama del equipo destinado al proyecto.
    - Especificar el equipo de trabajo indicando los nombres, roles y perfil profesional de los especialistas que se asignarán a cada etapa del proyecto
    - Plan de comunicación, seguimiento y entrega de informes que contenga actas de reuniones, registros de incidencias y riesgos, informes sobre el estado del proyecto, puesta en marcha, entrega de reportes, entre otros.

  En esta metodología y plan de trabajo el oferente deberá describir paso a paso como irá ejecutando la implementación del SGSI basado en la Norma ISO 27001:2022 en la Superintendencia de Bancos. Además, debe identificar qué apoyo requiere del personal de la SB para el traspaso del conocimiento y en sentido general el éxito del proyecto.

- Los oferentes deberán presentar el **cronograma de trabajo** propuesto en formato Gantt en donde se pueda apreciar: (i) las distintas tareas e hitos del proyecto; (ii) fecha de inicio y finalización de cada tarea, así como también predecesoras; (iii) recursos humanos del oferente y de la SB; (iv) ruta crítica; (v) entre otros. Este cronograma deberá estar presentado en formato de hoja de cálculo (MS-Excel), MS-Project y PDF.
- Los oferentes deberán contemplar en su propuesta todo el personal necesario para cumplir con las fechas de la implementación del SGSI ISO 27001:2022.
- El oferente se compromete a que, en caso de existir situaciones de inconductas en su equipo de trabajo, deberá reportarlas a la SB. La empresa consultora sustituirá a la persona del conflicto, por un personal de igual o mejor competencia técnica.
- La selección del personal que trabajará en el proyecto de implementación de parte del oferente debe ser tal que permita trabajar de forma paralela en las distintas áreas funcionales de las diferentes etapas a implementar de manera que puedan lograrse los objetivos tanto en términos de fecha del proyecto como calidad de los entregables.
- El oferente adjudicado debe documentar con minutas e informes todas las actividades y reuniones que se realizan. Debe llevar el control de cambios del proyecto con las distintas aprobaciones.
- Una vez iniciado los trabajos de consultoría, el oferente adjudicatario, no podrá hacer ningún reclamo de estos, indicando desconocimiento de las responsabilidades enumeradas en estos términos de referencia, así como cualquier otro soporte del proceso y/o documento presentado en la oferta.

4. Requisitos al personal de la empresa:

- Gerente o Líder del Proyecto:
    - Debe poseer una experiencia **mínima de cinco (5) años** en implementaciones de sistemas de gestión de seguridad de la información.
    - Debe haber dirigido al menos cinco **(5) implementaciones exitosas** del SGSI ISO 27001:2013 las cuales debe demostrar en el formulario de experiencia del personal con sus soportes.
    - Debe estar certificado al menos como auditor líder ISO 27001:2013

- Capacidad y Experiencia del personal del equipo del Proyecto:
  - Dentro de los miembros del equipo del proyecto o dentro del equipo identificado para trabajar en la consultoría debe existir (deben completar el formulario de currículo del personal y experiencia del personal del oferente):
    - Mínimo **UN (1) consultor senior** especialista en implementación del SGSI ISO 27001:2013. Este consultor deberá diseñar y proponer actividades para lograr el cumplimiento de los requisitos de la norma. Deberá servir de guía durante los levantamientos de información de los procesos para cada uno de los puntos que son requeridos por la norma de calidad. Dirigir y planificar la auditoría interna del sistema de gestión durante su implementación.
    - **UN (1) consultor senior especialista en riesgo tecnológico** con certificación CRISC o ISO 31000. Este consultor será responsable de la evaluación del análisis de riesgo de seguridad, la identificación de los mismos y la generación del plan de tratamiento de riesgos.
    - **UN (1) consultor senior especialista en controles de seguridad con certificación CISSP**. Este consultor será responsable de la generación de la declaración de aplicabilidad describiendo la justificación de la exclusión de los controles que así se defina y detallando los controles de seguridad que deberán de ser implementados.
    - **UN (1) ingeniero de procesos** especialista en levantamiento, diseño y documentación de procesos. Responsable de realizar los levantamientos de procesos para la redacción de la información documentada, el diseño de diagramas de flujos y todas las actividades relacionadas al proyecto. Deberá dar el seguimiento correspondiente para las actividades y tareas del plan de trabajo para cumplir con los tiempos establecidos.
    - Mínimo **UN (1) auditor en ISO 27001:2013** UN (1) especialista en auditorias de seguridad de la información y planes de acciones correctivas para garantizar la implementación del sistema.

- El personal del oferente debe estar debidamente identificado, portar carné de empleado que identifique al personal de la empresa, según las políticas de seguridad establecidas para los visitantes, proveedores y contratistas.

JP

5. Forma de pago

Se otorgará un 20% de anticipo luego de la presentación de la Garantía de Buen Uso de Anticipo y firma del contrato. El resto de los pagos se realizarán aplicando el siguiente esquema, según los entregables completados:

Hito	Documentación requerida	Pago (como porcentaje del monto de la oferta)
Anticipo: Pagado posterior a la presentación de la garantía de buen uso de anticipo y firma de contrato	Garantía de buen uso del anticipo y Contrato Firmado	20%
Hito para Pago (1): Concluida todas las actividades de la Etapa 1 Diagnostico del estado actual del SGSI en la SB, plan de cierre de brechas de seguridad de información y plan de tratamiento de riesgos, así como la declaración de aplicabilidad, generación del marco normativo, alineación del comité de seguridad y diseño del modelo de gestión.	Factura por un monto de 20% del monto de la oferta y Acta de Aceptación de Avance debida firmada por los Representantes de la SB y el Representante del Oferente Adjudicado.	20%
Hito para Pago (2): Concluida todas las actividades de la Etapa 2 (incluyendo la auditoría interna y acciones correctivas).	Factura por un monto de 20% del monto de la oferta y Acta de	20%

	Aceptación de Avance debida firmada por los Representantes de la SB y el Representante del Oferente Adjudicado.	
Aceptación Conforme: Una vez alcanzada la certificación oficial por la empresa certificadora y en sus 2 etapas, deberá entregar un informe final post certificación indicando los planes de acción y actividades para mantener el SGSI.	Factura por un monto de 50% del monto de la oferta y Acta de Aceptación de Avance debida firmada por los Representantes de la SB y el Representante del Oferente Adjudicado	40%

Cada pago será realizado en no más de 30 días de haber presentado la factura con la documentación requerida.

Los Representantes de la SB para fines de aceptación conforme de los avances del proyecto de implementación serán el Director de Seguridad de la Información, Subdirector de Seguridad de la Información, Encargado de la División de Operaciones de Seguridad de la Información y la Encargada de División de Transformación y Desarrollo Operacional (TDO).

El oferente debe considerar que el monto de la oferta no debe presentar/incluir ITBIS, y que con cada pago de factura presentada se realizaran las retenciones establecidas en el código tributario.

JP

6. Criterios de Evaluación Técnica

Ítem	Descripción	Cumple / No Cumple
1	**Presentar el Formulario de Oferta Técnica. Debe incluir la descripción del servicio ofertado y sus funcionalidades. Incluir catálogo que soporten la descripción técnica.** Diseño, implementación y auditoria del sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022, con un alcance en todos sus procesos críticos y los de apoyo a estos procesos que formen parte de los requisitos exigidos por la norma.	
2	**Presentar el Formulario de Experiencia del oferente en proyectos similares**, (SNCC.D.049). El oferente debe deben presentar al menos **cinco (5) implementaciones exitosas del SGSI ISO 27001:2013** a clientes diferentes; **una (1)** de estas implementaciones exitosas deben ser de instituciones públicas local o internacional y **una adicional (1)** de estas implementaciones exitosas deben ser de instituciones financieras local o internacional. Las implementaciones deben tener un alcance similar o superior a lo	

	requerido y se medirán por la certificación alcanzada de la norma. Como soporte a este formulario debe presentar Certificados de Aceptación Conforme, cartas de recepción definitiva de trabajos similares, o copia de contratos de trabajo similares. Los oferentes deberán contar con la certificación ISO 9001 e ISO 27001:2013 en sus procesos consultivos. El oferente debe debe tener experiencia comprobable, para el diseño, implementación y auditoria del sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013 y experiencia en implementación de sistemas de gestión integrados Los oferentes deben tener más de 10 años de experiencia demostrable en implementación de sistemas de gestión de de seguridad de la información, preferiblemente en el sector bancario. Los oferentes deberán contar con la certificación ISO 9001:2015 e ISO 27001:2013 en sus procesos consultivos.	
3	**Cartas de referencia de los trabajos.** El oferente debe presentar al menos **cinco (5) cartas de referencia** de clientes diferentes con los datos de las empresas donde se realizaron consultorías de implementación exitosas. La Superintendencia a través de su equipo pericial podrá indagar sobre los trabajos realizados y el éxito de las implementaciones trabajadas. Las cartas deben estar timbradas, tener la información de la empresa y contactos que permitan al equipo pericial de la superintendencia hacer cualquier evaluación que entiendan de lugar.	
4	**Experiencia profesional (SNCC.D.048 y SNCC.D.045).** La empresa oferente debe presentar los formularios indicados para detallar la experiencia profesional de su personal principal destinado al proyecto (experiencia del personal principal y Currículo de estos) el cual deberá cumplir con lo exigido en estos términos de referencia. El personal propuesto en la oferta debe ser el mismo que forme parte del proyecto de consultoría. A estos formularios deben anexar los soportes y evidencias que demuestren lo indicado en el formulario (i.e. CV). Gerente o Líder del Proyecto: Debe poseer una experiencia de mínimao de cinco (5) años en implementaciones de sistemas de gestión de seguridad de la información. Debe haber dirigido al menos cinco (5) implementaciones exitosas del SGSI ISO 27001:2013 las cuales debe demostrar en el formulario de experiencia del personal con sus soportes. Debe estar certificado al menos como auditor líder ISO 27001:2013 Equipo: **Mínimo UN (1) Consultor senior especialista en implementación del SGSI ISO 27001:2013.** **Un (1) Consultor senior especialista en riesgo tecnológico con certificación CRISC o ISO 31000** **Un (1) Consultor senior especialista en controles de seguridad con certificación CISSP.** **Un (1) Ingeniero de procesos especialista en levantamiento, diseño y documentación de procesos** **Mínimo UN (1) auditor en ISO 27001:2013 UN (1) especialista en auditorias de seguridad de la información y planes de acciones correctivas para garantizar la implementación del sistema.**	
5	**Metodología y Plan de Trabajo.** El oferente debe presentar un documento o propuesta formal descriptiva que desglose su metodología de trabajo para el Diseño e Implementación del Sistema de Gestión de Seguridad de la Información, basado en ISO 27001:2022 e ISO 27002:2022. Este plan de trabajo debe contemplar e incluir de forma detallada lo exigido en estos términos de referencia y sus anexos. En la presentación de este plan el oferente deberá: i. Dividir el plan de trabajo en las 3 etapas definidas.	

	ii. Especificar los resultados esperados en cada una de las etapas y el tiempo de duración de cada etapa. iii. Descripción de como realizarán la implementación, su metodología, procedimientos y herramientas que utilizarán. iv. Organigrama del equipo destinado al proyecto. v. Especificar el equipo de trabajo indicando los nombres y roles de los especialistas que se asignarán a cada etapa del proyecto vi. Plan de comunicación y entrega de informes que contenga actas de reuniones, registros de incidencias y riesgos, informes sobre el estado del proyecto, puesta en marcha, entrega de reportes, entre otros. El oferente debe considerar que el plan debe describir paso a paso como irá ejecutando la implementación del SGSI en la Superintendencia de Bancos, además de identificar qué apoyo requiere del personal de la SB para el traspaso del conocimiento y en sentido general el éxito del proyecto.	
6	**Carta de certificación** como auditor líder en ISO 27001:2013.	
7	**Certificado de empresa en ISO27001:2013 e ISO** 9001:2015 para sus procesos de consultoría.	
8	**Borrador de Acuerdo de Servicio (SLA)** que contenga lo indicado en estos términos de referencia.	
9	Certificado de personal en CISSP	
10	Certificado de personal en ISO31000	

Juan Daniel Pujols	James Pichardo
Subdirector de Seguridad de la Información	Director de Seguridad de la Información
Firma:	Firma: