PROCESO DE GIRO ESPECÍFICO DEL NEGOCIO
DEL BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL - BIESS

"SUSCRIPCIÓN Y SERVICIO DE SOPORTE DE SOFTWARE PARA CONTROL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN"

Unidad Requirente
SUBGERENCIA DE RIESGOS / DIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

OCTUBRE-2025

ÍNDICE

1. BASE LEGAL

1.1. NORMATIVAS RELACIONADAS AL OBJETO DE CONTRATACIÓN

1.1.1. CODIFICACIÓN DE LAS NORMAS DE LA SUPERINTENDENCIA DE BANCOS

LIBRO I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO, TÍTULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS CAPÍTULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO.

El presente requerimiento se sustenta en el cumplimiento del libro I "Normas de control para las entidades de los sectores financieros público y privado", título IX "De la gestión y administración de riesgos", capítulo V "Norma de control para la gestión del riesgo operativo" de la Codificación de las Normas de la Superintendencia de Bancos, el cual señala:

> Sección II.- Administración del riesgo operativo, Artículo 9.- "En razón de que la administración del riesgo operativo constituye un proceso continuo y permanente; y, para una gestión efectiva del riesgo, las entidades controladas deben conformar bases de datos centralizadas, que permitan registrar, ordenar, clasificar y disponer de información sobre los riesgos y eventos de riesgo operativo incluidos los de orden legal, de seguridad de la información, servicios provistos por terceros y de continuidad del negocio, el efecto cuantitativo de pérdida producida y estimada, así como, la frecuencia y probabilidad, y otra información que las entidades controladas consideren necesaria y oportuna, para que se pueda estimar las pérdidas atribuibles a este tipo de riesgo. La administración de la base de datos es responsabilidad de la unidad de riesgo operativo."

LIBRO I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO, TÍTULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS CAPÍTULO I.- NORMA DE CONTROL PARA LA GESTIÓN INTEGRAL Y ADMINISTRACIÓN DE RIESGOS DE LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO

El presente requerimiento se sustenta en el cumplimiento del marco normativo de la Norma de Riesgos Integrales de la Superintendencia de Bancos, Segunda Disposición General, del CAPÍTULO I.- NORMA DE CONTROL PARA LA GESTIÓN INTEGRAL Y ADMINISTRACIÓN DE RIESGOS DE LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO, de la Resolución SB-2021-2263 de 28 de diciembre de 2021, que señala:

> *"Las entidades controladas deben disponer de un sistema informático capaz de proveer a la administración y a las áreas involucradas, toda la información necesaria para identificar, medir, controlar* / mitigar y monitorear las exposiciones de riesgo que están asumiendo, y apoyar en la toma de decisiones oportunas y adecuadas."

1.1.2. ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

EGSI v.3. ACUERDO Nro. MINTEL-MINTEL-2024-0003 emitido por el MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN, establece la recomendación en el numeral 1.36.- "*Cumplimiento de políticas, reglas y normas de seguridad de la información*":

> *"El nivel jerárquico superior, propietarios de servicios, productos o información deben identificar cómo revisar que se cumplan los requisitos de seguridad de la información definidos en la política*

de seguridad de la información. Las políticas específicas del tema, las reglas, los estándares y otras reglamentaciones aplicables. Se deben considerar herramientas automáticas de medición y generación de informes para una revisión periódica eficiente."

1.1.3. ESTATUTO ORGÁNICO POR PROCESOS

El numeral 10.3.3. del Estatuto Orgánico por Procesos del BIESS señala que la misión de la Dirección de Seguridad de la Información es "*Asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, y confiabilidad de la información generada y administrada por la institución, garantizando los niveles de seguridad de la misma*". Por lo que dentro de sus atribuciones y responsabilidades está:

- *"Diseñar y proponer al Subgerente de Riesgos, las estrategias, políticas, procedimientos, metodologías y manuales para el sistema de Gestión de Seguridad de la Información, de acuerdo con los lineamientos que fije el Directorio, el Comité de Riesgos y la Superintendencia de Bancos"*.

- *"Cumplir y hacer cumplir las disposiciones de los organismos de control y el ente regulador, en lo referente a Seguridad de la Información".*

1.1.4. POLÍTICA SEGURIDAD INFORMACIÓN

TÍTULO III: POLÍTICAS ESPECIALES
CAPÍTULO IV: CONTROL DE ACCESOS

Art.5 Políticas Específicas. -
5.1.1 **Roles y responsabilidades de seguridad de la información:** El BIESS definirá las funciones y responsables de las actividades de la seguridad de la información, que permitan establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información.
5.1.2 **Separación de funciones:** Mantener una adecuada segregación de funciones para reducir los riesgos de error o fraude, con el fin de reducir las oportunidades de alteración a las propiedades de la información o mal uso de la información.
5.1.14 **Control de acceso:** Establecer un procedimiento para el control de accesos a la información que considere la concesión, administración de usuarios y perfiles para el registro, eliminación y modificación de la información, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude; así como, la revocación de usuarios, tanto de aplicativos, software base, red, dispositivos de seguridad perimetral, bases de datos, entre otros. También se deberá controlar el acceso de los proveedores a la información del BIESS, durante la prestación de sus servicios. Concluida la vigencia del contrato, los accesos deberán ser eliminados.
5.4.2 **Derechos de acceso privilegiado:** La asignación de derechos de acceso deberá estar restringido y controlado mediante un proceso formal de autorización. 5.4.3 Restricción de acceso a la información: El acceso a la información será limitado y gestionado de acuerdo a la normativa de control de acceso definida por la institución.

1.2. REGLAMENTO PARA LAS CONTRATACIONES DE GIRO ESPECÍFICO DEL NEGOCIO DEL BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL – BIESS

1.2.1. DE LAS BASES DEL CONCURSO

***"Art. 5. - Definiciones**. - Para efectos de la aplicación del presente reglamento, se tendrán en cuenta las siguientes definiciones: **(…) 5.2 Bases del concurso**: Documento que contiene las características técnicas y condiciones requeridas para la contratación, parámetros de evaluación, las obligaciones contractuales, el cronograma, la forma de presentación de ofertas; y, demás particularidades de la contratación. (…) **5.6 Fase preparatoria**: Incluye la elaboración y/o modificación del Plan Operativo Anual - POA; informe de necesidad; informes técnicos de ser el caso, estudio de mercado para definir el presupuesto referencial; bases del concurso (…) **5.10 Mejor oferta:** Oferta que brinde al BIESS, las mejores condiciones en los aspectos técnicos, económicos y legales, sin que el precio más bajo sea el único parámetro de selección. En todo caso, los parámetros de evaluación deberán constar obligatoriamente en las bases del concurso."*

*"**Art. 27. - Bases del concurso**. - Para la contratación de adquisición de bienes y servicios, incluidos los de consultoría, el área requirente elaborará y aprobará las bases del concurso, tomando en cuenta los siguientes aspectos:*

1. *Deberán ser claras, completas e inequívocas; no deben presentar ambigüedades, ni contradicciones entre las mismas, que propicien o permitan diferentes interpretaciones.*
2. *Las áreas requirentes conjuntamente con la Dirección de Riesgo Operativo identificarán los bienes y servicios provistos por terceros que soportan los procesos críticos del negocio; de igual manera determinarán y evaluarán los riesgos a los que se expone el BIESS al contratar servicios provistos por terceros para determinar los factores y condiciones de mitigación a considerar en las bases de concurso.*
3. *El área requirente deberá observar y cumplir con todos los requisitos establecidos en las normas de control para la gestión del riesgo operativo vigente, emitidas por la Superintendencia de Bancos y demás normativa interna, particularmente en los que soportan los procesos críticos del BIESS, debiendo incorporar en las bases del concurso, los parámetros y procesos que aseguren la evaluación, calificación y selección de los proveedores; así como las condiciones requeridas para la prestación del servicio y las obligaciones del contratista, que se trasladarán a las cláusulas contractuales como obligaciones de las partes.*
4. *El área requirente, deberá establecer el proceso que asegure el control y monitoreo de los servicios contratados, mediante la evaluación, gestión y vigilancia de éstos, a fin de garantizar que se cumplan en todo momento con los niveles mínimos de servicio acordados y demás cláusulas establecidas en el contrato. La información utilizada para el monitoreo de los servicios contratados debe ser obtenida por la entidad controlada de manera independiente de aquella que proporcione el proveedor, para lo cual podrá utilizar los mecanismos técnicos que considere pertinentes, que le permita confirmar el cumplimiento de las condiciones contractuales.*
5. *Las Bases del concurso, deberán contener por lo menos, pero sin limitarse a: (…)*

Las bases del concurso, incluirán cualquier otra condición exigida por la Superintendencia de Bancos, o demás normativa que rige al sistema financiero, de acuerdo al objeto de contratación; y, serán aprobadas por el titular del área requirente; y, revisadas por las áreas técnicas que correspondan.

Las bases del concurso no podrán afectar el trato igualitario que se le debe dar a todos los participantes, ni establecer diferencias arbitrarias entre éstos.

***27.1 Consideraciones particulares de las bases del concurso:** En cumplimiento de las disposiciones exigidas por la Superintendencia de Bancos, las áreas requirentes con el acompañamiento de las áreas*

técnicas deberán incorporar en las Bases del concurso, las disposiciones vigentes exigidas por el ente de control (…)".

1.2.2. DE LA MODALIDAD DE CONTRATACIÓN

La modalidad será de selección, ya que se cuenta con varios proveedores en el mercado, el presupuesto referencial es superior al resultado de multiplicar el monto del Presupuesto Inicial del Estado por el coeficiente 0,0000002.

2. CARACTERÍSTICAS TÉCNICAS Y CONDICIONES REQUERIDAS PARA LA CONTRATACIÓN

2.1. CONVOCATORIA:

Se convoca a las personas naturales, jurídicas, en asociación o consorcios; cuya actividad económica se encuentre relacionada directamente al objeto de contratación, legalmente capaces para contratar, debidamente calificadas por la Superintendencia de Bancos, a que presenten sus ofertas para la "SUSCRIPCIÓN Y SERVICIO DE SOPORTE DE SOFTWARE PARA CONTROL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN".

2.2. ANTECEDENTES:

Mediante Informe No. BIESS-INF-SRIE-068-2025 de 15 de abril de 2025, el Subgerente de Riesgos; emitió la justificación y evaluación técnica de la contratación de la suscripción y servicio de soporte de software para control del sistema de gestión de seguridad de la información, mediante el cual fundamenta que el proceso cumple con las condiciones exigidas en el reglamento para las contrataciones de giro específico del negocio.

Con memorando No. BIESS-SRIE-2025-0213-MM, de 25 de abril de 2025, el Subgerente de Riesgos, solicitó la aprobación de la determinación de la contratación de la suscripción y servicio de soporte de software para control del sistema de gestión de seguridad de la información, por Giro Específico del Negocio; y, conforme sumilla inserta en la hoja de ruta del sistema documental Quipux; el Gerente General dispuso: *"autorizado, continuar con el proceso según corresponda."*

El Banco del Instituto Ecuatoriano de Seguridad Social (BIESS) es una institución financiera pública con autonomía administrativa, técnica y financiera, cuya finalidad es la administración eficiente de los recursos previsionales y de la Seguridad Social. Su misión es proporcionar servicios financieros con un enfoque de banca de inversión, garantizando rentabilidad y contribuyendo al desarrollo económico del país.

Sus funciones principales consisten en facilitar servicios financieros a favor de los afiliados y pensionistas del IESS a través de créditos hipotecarios, prendarios y quirografarios, así como también, operaciones de redescuento de cartera hipotecaria de instituciones financieras.

El BIESS a la presente fecha ha realizado la gestión de levantamiento de activos de la información y riesgos de seguridad de la información, así como el establecimiento de las políticas, metodologías,

procesos y procedimientos que conforman el sistema de gestión de seguridad de la información, por lo que es necesario regularlo en un proceso de automatización de la información que mantiene el banco relacionado a sus activos de la información y que es requerido por disposición normativa emitida por la Superintendencia de Bancos.

La dirección de seguridad no ha realizado compras de herramientas que permitan automatizar el proceso y seguimiento del SGSI, actualmente el proceso ha sido manejar en un archivo Excel, lo que genera carga operativa, posible falla o error en el ingreso y realizar varias iteraciones para la validar que los campos no han sido modificados por los usuarios, lo que presenta falta de efectividad en la gestión y reproceso. Adicionalmente se generan informes trimestrales al comité de seguridad de la información sobre el avance del mismo, a través de más de 14 informes en los que se presentan el estado e indicadores de avance, lo cual no muestra de forma amigable y un adecuado seguimiento por parte de la dirección y cuerpo colegiado.

A la presente fecha el banco mantiene 815 activos de información, obtenidos de levantamiento de información reportado por cada una de las áreas del BIESS, de los cuales 318 se consideran críticos y deberán evaluarse acorde a la metodología y gestión de riesgos.

El banco para la implementación del SGSI, definió en la declaración de aplicabilidad la implementación y seguimiento de 93 controles, la herramienta permitirá automatizar y dar seguimiento adecuado de la efectividad y madurez del sistema de gestión de seguridad de la información.

2.3. OBJETIVOS:

Contratar una herramienta informática para la gestión de gobierno, riesgos y cumplimiento en términos de seguridad de la información que soporte el cumplimiento del Sistema de Gestión de Seguridad de la Información del BIESS y de la normativa vigente relacionada.

2.4. ALCANCE:

La contratación de la “SUSCRIPCIÓN Y SERVICIO DE SOPORTE DE SOFTWARE PARA CONTROL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN”, contempla la suscripción de una solución informática, para automatizar el control del sistema de gestión de seguridad de la información, que permita centralizar la información de los activos de la información y sus riesgos, generar consultas y reportes para seguimiento, monitoreo, que aporten al objetivo institucional “Incrementar la eficiencia y eficacia Institucional “, y optimizar la gestión de seguridad de la información a nivel nacional.

Deberá contar de los siguientes módulos:

- Suscripción - Módulo 1 de Gobierno (que incluya la gestión de seguimiento de normativa, interna y externa; la planificación estratégica y nuevas implementaciones en términos de seguridad de la información).
- Suscripción - Módulo 2 de Gestión de Riesgos (que incluya el ciclo completo de gestión de riesgos de seguridad de la información apalancado en la ISO27005 y en la metodología de riesgos del BIESS, que incluya el inventario, clasificación y riesgos de seguridad de la información, así como la gestión de incidentes y vulnerabilidades).

- Suscripción - Módulo 3 de Gestión de Cumplimiento que incluya el monitoreo de indicadores de seguridad de la información, revisiones para medir el desempeño y oportunidades de mejora, informes y reportes de cumplimiento y la gestión sobre revisiones independientes.
- Soporte Local – 15 Horas de soporte para la carga de información de seguimiento, monitoreo e inventario de activos del BIESS a la herramienta informática.

2.5. METODOLOGÍA DE TRABAJO:

Para la ejecución de los servicios contratados, el BIESS designará un Administrador del Contrato para la ejecución del contrato, durante todo el tiempo que dure el plazo contractual.
El Contratista informará al Administrador del Contrato los nombres y niveles de escalamiento del equipo de trabajo, quienes coordinarán con el Administrador del Contrato, todos los requerimientos del Banco y establecerá los cronogramas de ejecución que sean pertinentes y necesarios.

2.5.1. PRESTACIÓN DEL SERVICIO:

El Contratista deberá atender las necesidades del BIESS, respecto a la suscripción y servicio de soporte de software para control del sistema de Gestión de Seguridad de la Información conforme las siguientes actividades

a) Activación de la suscripción

- El proveedor procederá con la activación de la suscripción al día siguiente de la suscripción del contrato.
- Brindará acceso al sistema, asignando las credenciales de administración principal de la herramienta a la persona designada por el Administrador del Contrato.

Entregables:
- Documento que confirme la activación de la suscripción del software.
- ID de Cuenta y credencial del administrador principal.

b) Reunión inicial

- Reunión entre el administrador del contrato con el proveedor para definir cronograma con un plazo máximo de 90 días, que incluya la evaluación de riesgos del servicio contratado, transferencia de conocimientos, configuración e integración para carga inicial de información.

Entregable:

- Cronograma acordado entre las partes.

c) Transferencia inicial de conocimientos a gestores de usuarios y administradores de la herramienta

- El Administrador del Contrato convocará a los analistas de seguridad de la información del BIESS involucrados, al evento de transferencia de conocimientos respecto a la administración de la herramienta y gestores de usuarios, conforme al cronograma definido en el punto 2.

- El proveedor realiza sesiones de manera virtual para entrenar en la administración de la herramienta y gestión de accesos.

Entregable:

- Documento que acredite la transferencia de conocimientos efectuada por parte del proveedor, debidamente suscrito entre el representante del proveedor, el administrador del contrato y los analistas de seguridad de la información.

d) Configuración inicial

- El proveedor participa en la configuración de la herramienta, creación de cuentas de usuarios y en el establecimiento de permisos, junto con el administrador del contrato.
- El proveedor establece la configuración y adecuación de las interfaces para carga de información y lo valida con el administrador del contrato.
- El proveedor brinda soporte respecto a la información del BIESS que permita la compatibilidad con la herramienta para la carga de la información.

Entregable:

- Informe de configuración y carga inicial suscrito entre el proveedor y el administrador del contrato.

e) Transferencia de conocimientos a usuarios

- El administrador del contrato convocará a los propietarios de los activos de información y/o sus delegados para que participen en el evento de transferencia de conocimientos en el uso de la herramienta.
- El proveedor realiza la transferencia de conocimientos de manera virtual a usuarios finales designados por el BIESS.

Entregable:

- Documento que acredite la transferencia de conocimientos efectuada por parte del proveedor, debidamente suscrito entre el representante del proveedor, el administrador del contrato y las personas a quienes se transfirieron los conocimientos.

2.5.2. CONTROL Y MONITOREO DEL SERVICIO

El administrador del contrato para asegurar el control y monitoreo de los servicios contratados, lo realizará a través de actas de entrega y órdenes de trabajo con el fin de dar cumplimiento en todo momento con la implementación y los niveles mínimos de servicio acordados y demás cláusulas establecidas en el contrato.

La Dirección de Seguridad de la Información en sus informes de gestión trimestrales informará sobre la disponibilidad, uso que se da al software para control del sistema de gestión de seguridad de la información.

2.6. INFORMACIÓN QUE DISPONE EL BIESS:

El BIESS proporcionará al proveedor lo siguiente:

- Metodología de gestión de riesgos de seguridad de la información: Es un documento que contiene las características particulares que utiliza el BIESS para gestionar los riesgos de seguridad de la información.
- Metodología de activos de información: Es un documento que contiene las particularidades para el levantamiento del inventario de activos de información y para clasificarlos conforme a su sensibilidad y criticidad.
- Política y Reglamento de seguridad de la Información: Son documentos que contienen disposiciones y lineamientos para el BIESS en términos de seguridad de la información, que se utilizará para el monitoreo de su cumplimiento.
- Archivos en Excel de activos de información: Contiene el detalle de todos los activos de información del BIESS, así como su clasificación.
- Archivos en Excel de gestión de riesgos: Contiene la estructura de gestión de riesgos de seguridad de la información; así como un listado de amenazas, vulnerabilidades y criterios utilizados para categorizar el riesgo, criterios para medir la efectividad de los controles establecidos.

2.7. PRODUCTOS O SERVICIOS ESPERADOS:

A continuación, el resumen de los servicios esperados:

ÍTEM	DESCRIPCIÓN DEL SERVICIO	CANTIDAD	UNIDAD	CARACTERÍSTICAS DEL SERVICIO
1	Suscripción y servicio de soporte de software para control del Sistema de Gestión de Seguridad de la Información. Suscripción por 2 años; Acceso concurrente para 15 usuarios; 15 horas de soporte 8x5.	**1**	**UNIDAD**	Aplicativo Web en la nube. Acceso concurrente para 15 usuarios. Suscripción por 2 años. Soporte 8x5. Horas de soporte 15.

Detalle y características del servicio, correspondiente:

ÍTEM	BIEN /SERVICIO	CANTIDAD	UNIDAD	CARACTERÍSTICAS TÉCNICAS
1	Suscripción - Módulo 1 de Gobierno (que incluya la gestión de seguimiento de normativa, interna y externa; la planificación estratégica y nuevas implementaciones en términos de seguridad de la información).	**1**	UNIDAD	Aplicativo Web al 100% para acceso a través de un navegador estándar Chrome, Edge, Firefox, con actualizaciones automáticas. Debe permitir el acceso concurrente para 15 usuarios. Suscripción por 2 años. Soporte 8x5. SLA con tiempos de respuesta, que forme parte anexo al contrato. Transferencia de conocimientos por parte de un especialista del contratista.
2	Suscripción - Módulo 2 de Gestión de Riesgos (que	**1**	UNIDAD	Aplicativo Web al 100% para acceso a través de un navegador estándar

	incluya el ciclo completo de gestión de riesgos de seguridad de la información apalancado en la ISO27005 y en la metodología de riesgos del BIESS, que incluya el inventario, clasificación y riesgos de seguridad de la información, así como la gestión de incidentes y vulnerabilidades).			Chrome, Edge, Firefox, con actualizaciones automáticas. Debe permitir el acceso concurrente para 15 usuarios. Suscripción por 2 años. Soporte 8x5 SLA con tiempos de respuesta, que forme parte anexo al contrato. Transferencia de conocimientos por parte de un especialista del contratista.
3	Suscripción - Módulo 3 de Gestión de Cumplimiento que incluya el monitoreo de indicadores de seguridad de la información, revisiones para medir el desempeño y oportunidades de mejora, informes y reportes de cumplimiento y la gestión sobre revisiones independientes.	**1**	UNIDAD	Aplicativo Web al 100% para acceso a través de un navegador estándar Chrome, Edge, Firefox, con actualizaciones automáticas. Debe permitir el acceso concurrente para 15 usuarios. Suscripción por 2 años. Soporte 8x5 SLA con tiempos de respuesta, que forme parte anexo al contrato. Transferencia de conocimientos por parte de un especialista del contratista.
4	Soporte Local - Horas de soporte para la carga de información de seguimiento, monitoreo e inventario de activos del BIESS a la herramienta informática.	**15**	HORAS	Soporte Local - Por requerimiento, presencial o virtual, SLA con tiempos de respuesta como anexo al contrato. Horario de atención 8x5.

A) Suscripción a un software en la nube para control del sistema de gestión de seguridad de la información

El Software debe cumplir con las siguientes especificaciones técnicas generales:

- Funcionalidad para conectarse con directorio activo.
- Capacidad de almacenamiento de al menos 100GB.
- Permitirán la elaboración de perfiles de usuarios de tal manera que un usuario tenga acceso a lo exclusivamente necesario para su gestión en términos de seguridad de la información.
- Permitirán la generación de reportes para monitoreo de las pistas de auditoria que se generan sobre las actividades de los usuarios.
- Disponer de manuales que contenga documentos técnicos y de usuario, en formato impreso o digital, que guíen de manera efectiva el uso de la herramienta.

- Deben ser parametrizables los criterios para evaluación de activos y riesgos acorde a las metodologías utilizadas por la institución.
- Permitan la creación de indicadores de gestión e indicadores de riesgos para cada módulo.
- Permitan que los reportes o informes sean parametrizables para colocar la información que amerita incorporar en ellos.
- Transferencia de conocimientos de al menos 8 horas en todas las opciones y menús de la herramienta informática.

El software deberá contar con las siguientes funcionalidades:

- Gobierno Corporativo (que incluya la gestión de seguimiento de normativa, interna y externa; la planificación estratégica y nuevas implementaciones en términos de seguridad de la información
- Gestión de Riesgos (que incluya el ciclo completo de gestión de riesgos de seguridad de la información que incluya el inventario, clasificación y riesgos de seguridad de la información, así como la gestión de incidentes y vulnerabilidades), para lo cual el proveedor deberá remitir un documento con la confirmación de que la metodología utilizada por el software está basada en alguna de las normas antes indicadas
- Gestión de Cumplimiento que incluya el monitoreo de indicadores de seguridad de la información, revisiones para medir el desempeño y oportunidades de mejora, informes y reportes de cumplimiento y la gestión.

El Gobierno Corporativo debe cumplir con las siguientes características técnicas:

- Tenga precargadas como mínimo la normativa vigente de seguridad de la información para lo cual el proveedor deberá remitir un documento con la confirmación de que la ISO fue cargada.
- Permita la carga o el registro de la normativa del BIESS
- Permita la carga o el registro del Plan de Seguridad de la Información
- Permita que se registre la gestión realizada por cada punto de todas las normativas y el Plan de Seguridad de la Información.
- Alerte anticipadamente por correo electrónico las actividades por cumplirse.
- Genere reportes gráficos ejecutivos y reportes detallados sobre el nivel de madurez, cumplimiento y efectividad del SGSI (Sistema de Gestión de Seguridad de la Información)
- Integrar el seguimiento a nuevos proyectos o implementaciones en términos de SI.
- Debe mantenerse pistas de auditoría de las actividades realizadas sobre este módulo, desde el aplicativo se debe acceder al log y generar reportes en formato pdf. Las pistas de auditoria deben contener al menos el usuario, la dirección ip, la fecha de la actividad, el detalle de las acciones realizadas.
- Debe manejar históricos por periodos de tal manera que la información de periodos anteriores de evaluación, pueda consultarle a través de reportes y no sea modificable, el periodo (ej. Trimestral, semestral, anual) debe ser parametrizable
- Generar un Dashboard ejecutivo con gráficos e indicadores.

La Gestión de Riesgos debe contemplar las siguientes características técnicas:

- Permita registrar el inventario de activos de información, actualizarlos, añadirlos o eliminarlos, que contengan el nombre del proceso, subproceso, área, cargo responsable, nombre responsable, código activo, nombre activo, ubicación del activo,
- Clasificar esa información y gestionar los riesgos de los activos de información conforme la normativa interna aprobada basada en amenazas y vulnerabilidades.
- Disponer de opciones para el registro y mantenimiento de amenazas y vulnerabilidades.
- La gestión de riesgos debe permitir la medición de los riesgos tanto inherente como residual, bajo criterios de riesgos y cálculos parametrizables.
- Debe permitir el registro de controles vigentes y controles propuestos o planes de acción con el cálculo de la efectividad y eficacia de estos, así como aplicar acciones correctivas a esos controles.
- La gestión de riesgos debe permitir la parametrización del apetito de riesgo y el cálculo del riesgo, cálculo de la efectividad del control.
- Además, debe permitir el registro y tratamiento a incidentes y vulnerabilidades relacionados a seguridad de la información
- Debe generar reportes sobre el mapa de riesgo del BIESS en términos de seguridad de la información.
- Debe permitir el registro de incidentes, desde el registro, la investigación, actas de reuniones, acciones de contención, planes de acción y solución. Es deseable que la solución disponga de un workflow para la gestión de incidentes en todas sus fases.
- Reportes ejecutivos y detallados sobre la gestión de riesgos, incidentes y vulnerabilidades de seguridad de la información.
- Los controles deben validarse de manera automática frente a los controles establecidos en la normativa cargada.
- Bajar archivos en formato Excel y pdf sobre el contenido completo del inventario de activos, la clasificación, riesgo y planes de acción, así como gráficas del estado de la gestión.
- Dispondrá de una opción para la gestión de proveedores en la cual se registrará a los proveedores que se expondrán a revisión y además generará un checklist propicio para evaluar al proveedor en términos de medidas de seguridad de la información implementadas por ellos y las medidas pendientes por implementar, estableciendo una calificación automática por ítem y promedio por proveedor que me determine el riesgo que tendríamos al mantenerlo con el resultado obtenido. La calificación por ítem estará determinada de manera automática por la criticidad de la medida, y será parametrizable en tanto el BIESS desee cambiarla. Por cada ítem, la herramienta debe permitir cargar el/los documentos que sustenten el cumplimiento. El checklist debe ser generado en formato pdf y Excel, tanto la estructura vacía como llena.
- Emitir alertas anticipadas de actividades por vencer.
- Debe gestionar KRI para seguridad de la información, tanto de los resultados como el mantenimiento de los KRI vigentes.
- Debe mantenerse pistas de auditoría de las actividades realizadas sobre el inventario, clasificación y gestión de riesgos, desde el aplicativo se debe acceder al log y generar reportes

en formato pdf. Las pistas de auditoria deben contener al menos el usuario, la dirección ip, la fecha de la actividad, el detalle de las acciones realizadas.

- Debe manejar históricos por periodos de tal manera que la información de periodos anteriores de evaluación, pueda consultarle a través de reportes y no sea modificable, el periodo (ej. Trimestral, semestral, anual) debe ser parametrizable.

La Gestión de Cumplimiento debe contemplar las siguientes características técnicas:

- Permita el registro de observaciones emitidas por instancias de control con sus respetivos planes de acción.
- Emita alertas anticipadas sobre planes o actividades por vencer.
- Generar reportes ejecutivos y detallados sobre la gestión ante observaciones de instancias de control.
- Debe mantenerse pistas de auditoría de las actividades realizadas sobre este módulo, desde el aplicativo se debe acceder al log y generar reportes en formato pdf. Las pistas de auditoria deben contener al menos el usuario, la dirección ip, la fecha de la actividad, el detalle de las acciones realizadas.
- Debe manejar históricos por periodos de tal manera que la información de periodos anteriores de evaluación, pueda consultarle a través de reportes y no sea modificable, el periodo (ej. trimestral, semestral, anual) debe ser parametrizable
- Generar un dashboard con indicadores de gestión o desempeño e indicadores de gestión.

B) Soporte de software para control del sistema de gestión de seguridad de la información

- Los requerimientos deben ser atendidos en horario laboral, 8 horas al día de lunes a viernes, en el horario de 8h00 a 17h00.

C) Controles de Seguridad en la Nube

- El servicio ofertado deberá cumplir una disponibilidad del centro de datos del 99.8% de disponibilidad y buenas prácticas de seguridad de la información, protección de manejo de información personal y controles de seguridad en servicios en nube, avalada por una entidad certificadora.
- Los centros de procesamiento de datos principal y/o alterno, deben haber sido implementados siguiendo el estándar ANSI-TIA-942 o superior y contar como mínimo con la certificación TIER III o su equivalente para diseño, implementación y operación y así garantizar la disponibilidad de los servicios brindados;
- El proveedor de servicios debe contar, para los servicios ofertados, como mínimo, con certificación ISO 27001 en seguridad de la información, así como, la implementación de los controles establecidos en los estándares ISO 27017 (controles de seguridad para servicios en la nube).

2.8. DEFINICIÓN DE PRESUPUESTO REFERENCIAL:

Del resultado del Estudio de Mercado se ha definido que el presupuesto referencial para esta contratación es de USD $39.065,33 (TREINTA Y NUEVE MIL SESENTA Y CINCO con 33/100 dólares de los Estados Unidos de América), más IVA, desglosados de la siguiente manera:

ítem	Descripción	Cantidad	Unidad de medida	Precio Unitario	Subtotal
1	Suscripción y servicio de soporte de software para control del Sistema de Gestión de Seguridad de la Información. Suscripción por 2 años; Acceso concurrente para 15 usuarios; 15 horas de soporte 8x5.	1	U	$39.065,33	$39.065,33
				SUBTOTAL (SIN IVA):	$39.065,33

2.9. PLAZO DE EJECUCIÓN:

El plazo de ejecución para esta contratación es de 730 días calendario, a partir de la activación de la suscripción por parte del proveedor.

2.10. FORMA Y CONDICIONES DE PAGO:

El BIESS pagará al contratista el 100% contra entregar del documento de activación de la suscripción al software y verificación de acceso por parte del administrador del contrato, posterior a la suscripción del acta entrega recepción a entera satisfacción del BIESS.

El/la contratista(s), deberán entregar los siguientes informes al Administrador del Contrato:

- Documento de activación de la suscripción por parte del proveedor
- Acta Entrega Recepción definitiva
- Pre factura.

2.11. GARANTÍAS:

Las garantías se solicitarán previo a la celebración del contrato de conformidad a la normativa vigente.

- **Garantía Técnica*:***

El proveedor emitirá una garantía técnica sobre la parametrización y carga de información, trasferencia de conocimiento, buen funcionamiento de la herramienta y el cumplimiento de buenas prácticas de seguridad de la información y tecnológicas del servicio en la nube contratado y del centro de datos del servicio contratado, la cual permanecerá vigente durante la ejecución del contrato.
El proveedor garantizará que el software en la nube mantendrá actualizado en sus últimas versiones estables y se contará con soporte 8x5, durante la ejecución del contrato.

2.12. RIESGOS ASOCIADOS A LOS SERVICIOS PROVISTOS POR TERCEROS:

Se ha procedido a levantar la matriz de riesgos asociados a los servicios provistos por terceros, misma que consta suscrita en conjunto con la Dirección de Riesgos Operativo. En la misma se determina y evalúan los riesgos a los que el Banco se expone al contratar este objeto de contratación.

3. CONDICIONES PARTICULARES DE LA CONTRATACIÓN

3.1 OBLIGACIONES DEL CONTRATISTA:

- Dar cumplimiento cabal a las condiciones establecidas en las bases del concurso.
- El contratista prestará todas las facilidades para la revisión y seguimiento del servicio prestado por parte del BIESS, así como de los auditores externos y la Superintendencia de Bancos.
- Si el contratista realiza una actividad económica sujeto a reporte a la Unidad de Análisis Financiero y Económico, deberá presentar el Certificado de Cumplimiento de la UAFE en la ejecución contractual.
- El CONTRATISTA, debe guardar confidencialidad absoluta sobre la información que el BIESS entregue para la ejecución del contrato.
- El canal oficial de comunicaciones entre el CONTRATISTA y el/la Administrador/a de Contrato será a través de documentos escritos, firmados y en castellano. Comunicaciones, actas de reunión, cronogramas, remitidos a través de correos electrónicos; en los casos que amerite, los documentos se firmarán electrónicamente.
- Transferencia de conocimientos del servicio contratado y entrega de toda la documentación que soporta el proceso o servicio.
- Todos los servicios deben efectuarse en estricto cumplimiento de las bases del concurso. En caso de que cualquier dimensión y/o especificación no hubiera sido establecida, si el CONTRATISTA no pudiera obtenerla directamente de las bases del concurso, la solicitará al/la Administrador/a del Contrato.
- Los sueldos y salarios del personal del contratista deben ser pagados por la contratista sin que esto implique costos adicionales para el BIESS.
- Implementación ISO 27018 (protección de información personal en la nube) u otras similares que aplique conforme el servicio ofertado.

3.2 OBLIGACIONES ADICIONALES DEL CONTRATISTA:

a) Confidencialidad de la Información

El Contratista y/o cualquiera de sus colaboradores quedan expresamente prohibidos de reproducir o publicar la información que llegue a su conocimiento, en razón de que es considerada confidencial y no divulgable. El incumplimiento de esta obligación será causal para dar por terminado el contrato y quedará a criterio de la parte afectada el iniciar las acciones correspondientes por daños y perjuicios.

El Contratista y el personal involucrado en la prestación del servicio tienen que suscribir el Acuerdo de Confidencialidad elaborado por la Dirección de Seguridad de la Información del BIESS.

Durante la ejecución del servicio el contratista se compromete a cumplir la Política, Reglamento, Manual e Instructivos de Seguridad de la Información del BIESS.

El proveedor del servicio deberá notificar al administrador del contrato cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de dos (2) días contados a partir de la fecha en la que tenga conocimiento de ella.

El proveedor se compromete a dar cumplimiento a la Ley Orgánica de Protección de Datos Personales vigente dentro del ámbito de competencias del servicio prestado.

El contratista se compromete a devolver toda la información del BIESS, al finalizar el contrato.

b) Plan de Contingencia y Continuidad del Negocio:

NO APLICA

c) Derechos de propiedad intelectual:

Los documentos, informes y productos brindados como parte de las actividades de la contratación serán de propiedad del Banco del Instituto Ecuatoriano de Seguridad Social; sin embargo, de ello se reconocerán en los documentos que fueren del caso, los créditos pertinentes que correspondan al CONTRATISTA .

d) Etapa de transición

NO APLICA

e) Cumplimiento normativo interna:

El Contratista deberá cumplir con la normativa interna del Banco relacionada a la norma expedida por la Superintendencia de Bancos, aplicable en función del servicio a ser contratado, contenida en la normativa interna.

El presente requerimiento se sustenta en el cumplimiento del libro I “Normas de control para las entidades de los sectores financieros público y privado”, título IX “De la gestión y administración de riesgos”, capítulo V “Norma de control para la gestión del riesgo operativo” de la Codificación de las Normas de la Superintendencia de Bancos, el cual señala:

Sección II.- Administración del riesgo operativo, Artículo 9.-
“En razón de que la administración del riesgo operativo constituye un proceso continuo y permanente; y, para una gestión efectiva del riesgo, las entidades controladas deben conformar bases de datos centralizadas, que permitan registrar, ordenar, clasificar y disponer de información sobre los riesgos y eventos de riesgo operativo incluidos los de orden legal, de seguridad de la información, servicios provistos por terceros y de continuidad del negocio, el efecto cuantitativo de pérdida producida y estimada, así como, la frecuencia y probabilidad, y otra información que las entidades controladas consideren necesaria y oportuna, para que se pueda estimar las pérdidas atribuibles a este tipo de riesgo. La administración de la base de datos es responsabilidad de la unidad de riesgo operativo.”

El presente requerimiento también se sustenta en el cumplimiento del marco normativo de la Norma de Riesgos Integrales de la Superintendencia de Bancos, Segunda Disposición General, del CAPÍTULO I.- NORMA DE CONTROL PARA LA GESTIÓN INTEGRAL Y ADMINISTRACIÓN DE RIESGOS DE LAS

ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO, de la Resolución SB-2021-2263 de 28 de diciembre de 2021, que señala:

"Las entidades controladas deben disponer de un sistema informático capaz de proveer a la administración y a las áreas involucradas, toda la información necesaria para identificar, medir, controlar / mitigar y monitorear las exposiciones de riesgo que están asumiendo, y apoyar en la toma de decisiones oportunas y adecuadas."

Adicionalmente, el presente requerimiento se sustenta en el cumplimiento del marco normativo establecido en el Esquema Gubernamental de Seguridad de la Información (EGSI) para las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). La recomendación del numeral 1.36.- "*Cumplimiento de políticas, reglas y normas de seguridad de la información*", del EGSI v.3. del ACUERDO Nro. MINTEL-MINTEL-2024-0003 emitido por el MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN, señala:

"El nivel jerárquico superior, propietarios de servicios, productos o información deben identificar cómo revisar que se cumplan los requisitos de seguridad de la información definidos en la política de seguridad de la información. Las políticas específicas del tema, las reglas, los estándares y otras reglamentaciones aplicables. Se deben considerar herramientas automáticas de medición y generación de informes para una revisión periódica eficiente."

f) Equipo de la Contraparte calificado para brindar el servicio en los niveles requeridos:

El Contratista, al inicio de la ejecución del contrato deberá entregar el listado del equipo de contraparte técnica y/o administrativa al Administrador del Contrato para la oportuna ejecución del servicio.

g) ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN

Las condiciones que el sistema debe contar respecto de aspectos de seguridad de la información incluyendo ciberseguridad, se encuentran contemplados en el apartado 2.7 de este documento.

h) TRANSFERENCIA DE CONOCIMIENTO

El Contratista, en el término de 15 días posterior que se cuente con el acceso al sistema, deberá realizar la transferencia de conocimiento del uso del sistema de módulos para la gestión de cuentas de usuario y perfiles de acceso que será utilizado por el BIESS, misma que será coordinada con el Administrador de contrato.

i) COMPUTACIÓN EN LA NUBE

El SOFTWARE PARA CONTROL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, no se encuentra establecido como crítico para el BIESS, en función de ello, posterior a la contratación, el administrador del contrato emitirá un informe y requerirá otro a la Coordinación Jurídica, un informe respecto a la identificación de los riesgos operativos asociados al servicio, los cuales serán analizados para gestionar su mitigación sea que aplique o no al servicio, conforme a:

"*Para el caso de contratación de servicios de infraestructura, plataforma y/o software, en la nube tanto con proveedores nacionales o extranjeros; las entidades controladas deberán disponer conforme el servicio contratado: Un informe técnico, uno de seguridad de la información y uno legal, emitido por el personal de la entidad controlada en función de sus competencias, en los cuales, se haya identificado los riesgos operativos asociados al servicio y la gestión respectiva.*"

En un plazo máximo de 15 días de suscrito el contrato se deberá contar con el informe técnico, informe legal.

El análisis de riesgos del servicio contratado, será realizado por la Dirección de Seguridad de la Información en un plazo máximo de 15 días de suscrito el contrato entre las partes y para ello:

- El proveedor prestará las facilidades y brindará las respuestas para la ejecución de la identificación de los riesgos en el servicio.
- La Dirección de Seguridad de la Información efectuará el análisis de riesgos al servicio de computación en la nube, conforme es requerido por la normativa de la Superintendencia de Bancos.
- El proveedor indicará documentadamente los controles que tiene vigentes para mitigar los riesgos identificados en el servicio.

Entregables a los 15 días:

- Informe preliminar de la dirección de seguridad de la información de los riesgos identificados.
- Informe del proveedor sobre los controles que tienen respecto a los riesgos identificados por la Dirección de Seguridad de la Información del BIESS.

Entregables a los 30 días:

- Informe final de seguridad de la información con el detalle de los riesgos identificados y los controles aplicados.
- Plan de tratamiento remitidos por parte del proveedor acorde metodología de riesgos de SI del BIESS con el fin de mitigar los riesgos del servicio contratado (si los tuviere)

El proveedor deberá entregar sustentos de lo siguiente:

- Para los centros de procesamiento de datos principal y/o alterno, deben haber sido implementados siguiendo el estándar ANSI-TIA-942 o superior y contar como mínimo con la certificación TIER III o su equivalente para diseño, implementación y operación y así garantizar la disponibilidad de los servicios brindados.

- Para los servicios ofertados, como mínimo:
  - Certificación ISO 27001 en seguridad de la información.
  - Implementación de los controles establecidos en los estándares ISO 27017 (controles de seguridad para servicios en la nube),
  - Implementación ISO 27018 (protección de información personal en la nube) u otras similares que aplique conforme el servicio ofertado.

j) ACUERDO DE NIVELES DE SERVICIO

A continuación, se encuentran las características del nivel de servicio (SLA) que el contratista deberá brindar al BIESS.

El Contratista deberá disponer de al menos los siguientes métodos para brindar soporte, ayuda y para mantener una comunicación fluida hacia la Institución y durante la vigencia del contrato no podrá interrumpirse:

- Líneas telefónicas conmutadas y celulares.
- Correos electrónicos para soporte técnico y para soporte operativo y funcional.
- Personal para soporte técnico.
- Soporte y ayuda de chat a través de WhatsApp.
- Soporte técnico y operativo a través de conexión remota mediante la utilización de Microsoft Teams u otros programas similares.

Posterior a la resolución del evento el contratista deberá entregar un informe técnico, dentro de los diez (10) días laborables siguientes a la atención, en el cual se contemple los siguientes datos:

a) Fecha / Hora de Notificación.
b) Fecha / Hora de Solución
c) Numero de Atención acorde a la hoja de servicio.
d) Diagnóstico y estado actual de la herramienta.
e) Detalle de las tareas realizadas como parte del soporte.
f) Conclusiones y recomendaciones.

Por el incumplimiento de los tiempos establecidos en los acuerdos de nivel de servicio (SLA), el BIESS sancionará al proveedor con una penalidad correspondiente al % detallado en el siguiente cuadro, en función al valor de cada hora, por cada hora o fracción de hora de atraso.

Niveles de criticidad	Tiempo máximo de respuesta	Tiempo máximo de solución	Factor	Penalidades
SLA – SOPORTE EN LA "SUSCRIPCIÓN Y SERVICIO DE SOPORTE DE SOFTWARE PARA CONTROL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. **El Nivel de Servicio se lo definirá de la siguiente manera: Alto, Medio, Bajo.**				
1- Alto	2 horas	24 horas	1/1000	**Si el tiempo tomado para la solución es mayor a 24 horas en horario laborable, la penalidad será del 1 por 1000 por hora de retraso, del valor del contrato.**
2- Medio	4 horas	48 horas	1/1000	**Si el tiempo tomado para la solución es mayor a 48 horas en horario laborable, la penalidad será del 1 por 1000 por hora de retraso, del valor del contrato.**
3- Bajo	**12 horas**	**72 horas**	**1/1000**	**Si el tiempo tomado para la solución es mayor a 72 horas en horario laborable, la penalidad será del 1 por 1000 por día de retraso, del valor del contrato.**

k) Informes de Auditoria Externa aplicable al servicio a ser contratado

NO APLICA

3.3 OTRAS CONDICIONES CONTRACTUALES EXIGIDAS POR LOS ENTES DE CONTROL:

No aplica, para los servicios del objeto de contratación no involucran la consideración de este apartado.

3.4 OBLIGACIONES DEL CONTRATANTE Y ADMINISTRADOR DE CONTRATO:

- Designar al administrador del contrato.
- Dar solución a las peticiones y problemas que se presenten en la ejecución del contrato, en un término no mayor a 5 días contados a partir de la petición escrita formulada por el contratista.
- Suscribir las actas de entrega recepción de los bienes/servicios recibidos, siempre que se haya cumplido con lo previsto en la ley para la entrega recepción; y, en general, cumplir con las obligaciones derivadas del contrato.
- El administrador de contrato aplicará la Metodología de Control y Monitoreo de los servicios contratados, conforme al numeral 2.4.2 de la Metodología de Trabajo.
- Brindar facilidades de acceso a los diferentes entes de control, así como a la auditoría interna, y externa, para la revisión y seguimiento de la contratación efectuada que incluye la documentación generada en las distintas etapas del proceso de contratación; misma que se encontrará publicada en la página web institucional; y, mantendrá un expediente, según corresponda.

3.5 MULTAS Y PENALIZACIONES:

De las multas. - En los casos de incumplimiento de las obligaciones contractuales por parte del contratista, se aplicará por cada día de retraso en la ejecución, una multa que en ningún caso será inferior al 1 x 1.000 del valor del contrato.

De las penalidades. - De acuerdo a la naturaleza del objeto de contratación, se aplicarán las penalidades determinadas por incumplimiento en los acuerdos de niveles de servicio.

3.6 VIGENCIA DE LA OFERTA:

Conforme el numeral 33.1 del artículo 33 del Reglamento para las Contrataciones de Giro Específico del Negocio del Banco del Instituto Ecuatoriano de Seguridad Social – BIESS: *"Las ofertas se entenderán vigentes hasta la fecha de la suscripción del contrato".*

3.7 SUBCONTRATACIÓN:

No aplica

4. PARÁMETROS Y METODOLOGÍA DE EVALUACIÓN DE LAS OFERTAS

Para realizar la evaluación de la capacidad del servicio solicitado, la instalación y/o soporte e historial de desempeño, capacidad logística, instalaciones y recursos humanos, según sea el caso; los oferentes deberán acreditar documentadamente el cumplimiento de los siguientes requisitos:

4.1 METODOLOGÍA CUMPLE / NO CUMPLE:

Para la verificación del cumplimiento de los requisitos mínimos, se empleará la metodología cumple/no cumple.

4.1.1. INTEGRIDAD DE LA OFERTA

El BIESS verificará la presentación de los formularios previstos en las bases del concurso, que se encuentre debidamente firmado y completos conforme a los formatos establecidos.

4.1.2. EXPERIENCIA DE EL/LOS PARTICIPANTE/S:

EXPERIENCIA ESPECÍFICA MÍNIMA DEL OFERENTE

Tipo	Descripción	Temporalidad	Valor del monto mínimo $	Número de proyectos similares	Monto Mínimo por Contrato $
Experiencia Específica	Experiencia en la prestación del servicio de suscripción y servicio de soporte de software para el control del Sistema de Gestión de Seguridad de la Información	Últimos 5 años	$1.200,00	Al menos 3	$400,00

Para acreditar la experiencia especifica el oferente deberá presentar tres o más contratos/facturas que sumados alcancen el valor del monto mínimo de USD 1.200,00 (Mil doscientos con 00/100 dólares de los Estados Unidos de América); si son contratos del Sector Público deberá presentar el Contrato y el Acta Entrega Recepción parcial/definitiva, si son contratos del sector privado deberán presentar facturas o un certificado del cliente que indique la recepción a satisfacción, los cuales deberán contar con la siguiente información: objeto del contrato/factura, monto, plazo de entrega. Se validará únicamente la experiencia de los contratos/facturas ejecutados parcial o totalmente hasta antes de la presentación de la oferta.

4.1.3. PERSONAL TÉCNICO, RECURSO HUMANO, EQUIPO DE TRABAJO / RECURSOS:

- **Personal técnico**

No.	Función/Cargo	Cantidad	Nivel de estudio	Descripción	Medio de Verificación
1	Ingeniero en Sistemas	1	Tercer nivel con titulo	Título de tercer nivel, en sistemas o redes o computación o telecomunicaciones o informática	Se deberá adjuntar copia del título académico registrado en el Senescyt. Si es una persona extranjera, se debe avalar el título en el país de origen de fuentes fidedignas.

El BIESS se reserva el derecho de verificar la información de los títulos obtenidos tanto en la página del Ministerio de Educación y/o la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT), la misma que deberá ser validada por la Comisión de Contratación.

- **Equipo Mínimo**

No aplica

4.1.4. EXPERIENCIA DEL PERSONAL TÉCNICO:

No.	Descripción	Tiempo	Número de Proyectos	Monto de Proyectos
1	Deberá acreditar experiencia acumulada en: conocimiento del software a suscribirse	1 año	Al menos 1 proyecto	$1.200,00

Deberán incluir en su oferta la HOJA DE VIDA del técnico, adjuntando los certificados que acrediten la experiencia requerida en el último año, mismo que deben especificar como mínimo:

- Nombre o razón social.
- Nombre de quien expide o firma la certificación (con logo, dirección y números de contacto de la empresa).
- Señalar la experiencia en el cargo.
- Tiempo de experiencia.
- Fecha de expedición de la certificación.

- Monto del proyecto

Se evaluará únicamente el monto ejecutado sin considerar el IVA, siempre que cumpla con el monto mínimo requerido.

Cada anexo o documentación de respaldo que se adjunte, y que hayan sido suscritos o emitidos por un tercero con firma manuscrita, deberán ser digitalizados, y este documento será firmado electrónicamente por el oferente. Esta firma implicará la declaración de que todos los documentos presentados son auténticos, exactos y veraces, y que, el oferente se hace responsable de los mismos dentro de los controles posteriores que se puedan realizar.

4.1.5. OFERTA ECONÓMICA

Al corresponder este a un proceso de selección, la Dirección de Seguridad de la Información incluye este parámetro para que sea sujeto a puntaje.

4.1.6. ANÁLISIS DE ÍNDICES FINANCIEROS:

Los índices financieros constituirán información de referencia respecto de los participantes en el procedimiento y en tal medida, su análisis se registrará conforme el detalle a continuación:

Índice	Indicador solicitado	Observaciones
Solvencia	mayor o igual a 1,0	(Activo corriente / Pasivo corriente) Adjuntar Declaración del Impuesto a la Renta del año inmediato anterior
Endeudamiento	menor a 1,5	(Pasivo Total / Patrimonio neto) Adjuntar Declaración del Impuesto a la Renta del año inmediato anterior

Los factores para su cálculo estarán respaldados en la correspondiente declaración de impuesto a la renta del ejercicio fiscal inmediato anterior y/o los balances presentados al órgano de control respectivo, que deberá adjuntar a la oferta.

El incumplimiento de los indicadores mínimo solicitados en las bases del concurso, serán causal de rechazo de la oferta.

4.1.7. OTRO(S) PARÁMETRO(S) EXIGIDOS POR LOS ENTES DE CONTROL:

Otros parámetros	Descripción	Medio de comprobación
– **Certificación ISO 27001 en seguridad de la información.**	Certificado vigente	Copias simples de certificado ISO 27001
– **Implementación de los controles establecidos en los estándares ISO 27017 (controles de seguridad para servicios en la nube),**	Cumplimiento de controles	Carta emitida por el proveedor del centro de datos que mantiene implementado los controles
– **Implementación ISO 27018 (protección de información personal en la nube) u otras similares que aplique conforme el servicio ofertado.**	Cumplimiento de controles	Carta emitida por el proveedor del centro de datos que mantiene implementado los controles

4.2 METODOLOGÍA POR PUNTAJE:

Aquellas ofertas que cumplan integralmente con los requisitos mínimos pasarán a la etapa de evaluación de ofertas por puntaje, caso contrario serán descalificadas por cuanto los requisitos mínimos constituyen parámetros de cumplimiento obligatorio.

Se han definido los siguientes parámetros de calificación.

PARÁMETRO SUJETO A PUNTAJE	DESCRIPCIÓN DE LA METODOLOGÍA DE EVALUACIÓN	PUNTAJE
Experiencia Específica	No se otorgará puntaje a la experiencia específica mínima requerida, por ser de cumplimiento obligatorio. Para que la experiencia especifica presentada sea susceptible de calificación por puntaje, ésta deberá ser mayor a la establecida como requisito mínimo. El valor total de la experiencia especifica solicitada adicional al requisito mínimo que será puntuada, no podrá superar el valor del presupuesto referencial del procedimiento de contratación multiplicado por un factor de 1,25. Se otorgará el máximo puntaje a la o las ofertas que presenten como experiencia específica adicional el monto más alto y, a las demás ofertas se asignará un puntaje directamente proporcional.	10
Experiencia del personal técnico	No se otorgará puntaje al tiempo mínimo de experiencia requerida, por ser de cumplimiento obligatorio. **Puntaje máximo a otorgarse a:** **Ingeniero en Sistemas:** 2 puntos por cada año adicional al requisito mínimo hasta llegar a un máximo de 10 puntos.	10
Oferta económica	La oferta económica se evaluará aplicando un criterio inversamente proporcional; a menor precio, mayor puntaje.	80
	TOTAL	100

5. CRONOGRAMA

El cronograma que regirá el proceso será el siguiente:

No.	Concepto	Fecha máxima	Hora
1	Fecha publicación página web	24/10/2025	19:00
2	Fecha límite para preguntas	27/10/2025	17:00
3	Fecha límite de respuestas y aclaraciones	28/10/2025	19:00
4	Fecha límite de recepción de oferta	31/10/2025	15:00
5	Fecha de apertura oferta	5/11/2025	19:00
6	Solicitar Convalidación de Errores	6/11/2025	19:00
7	Respuesta a la Convalidación de Errores	7/11/2025	17:00
8	Evaluación de oferta	10/11/2025	19:00
9	Fecha estimada de Adjudicación	17/11/2025	19:00

6. FORMA DE PRESENTACIÓN DE OFERTAS

Las ofertas deberán ser presentadas de manera física, dentro del plazo establecido en el cronograma del proceso de contratación, en la siguiente dirección: ciudad de Quito, Av. Amazonas y Unión Nacional de Periodistas, Plataforma Financiera Gubernamental, Piso 2, Dirección de Servicios Generales, Contratación y Compras Públicas. Se presentará un sobre único el cual contendrá la siguiente ilustración:

SUSCRIPCIÓN Y SERVICIO DE SOPORTE DE SOFTWARE PARA CONTROL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Señor(es)
BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL – BIESS
Presente.-

PRESENTADA POR: _____

RUC. _____

PERSONA DE CONTACTO: _____

No se tomarán en cuenta las ofertas entregadas en otro lugar o después del día y hora fijados para su entrega-recepción.

7. DEBIDA DILIGENCIA – POLÍTICA CONOZCA A SU PROVEEDOR

Los Formularios de Perfil Conozca a su Proveedor deberán ser presentados solo por el **OFERENTE FINALISTA DEL PROCESO**, **PREVIO A LA ADJUDICACIÓN**, según corresponda (persona natural o jurídica).

El OFERENTE deberá llenar y presentar el formulario que le corresponda más la documentación de respaldo solicitada, dentro del término de 5 días, a partir de la fecha de solicitud por parte de la Coordinación Administrativa.

Adicionalmente si EL OFERENTE es persona jurídica, deberá presentar el formulario CONOZCA A SU PROVEEDOR según corresponda (persona natural o jurídica) **de los socios y/o accionistas cuya participación sea igual o superior al 6 % del capital suscrito y pagado de la empresa**.

(ANEXOS FORMULARIO CONOZCA A SU PROVEEDOR Persona Jurídica y FORMULARIO CONOZCA A SU PROVEEDOR Persona Natural).

8. FORMULARIOS DE LA OFERTA

ANEXOS

FIRMA DE RESPONSABILIDAD:

NOMBRES Y APELLIDOS	CARGO	FIRMA
Elaborado por: José Eduardo Ortega Yánez	**Especialista de Seguridad de la Información**	Firmado electrónicamente por: JOSE EDUARDO ORTEGA YANEZ Validar únicamente con FirmaEC
Revisado por: Mery Paulina Suárez León	**Directora de Seguridad de la Información**	Firmado electrónicamente por: MERY PAULINA SUAREZ LEON Validar únicamente con FirmaEC
Revisión técnica por: Fabian Dario Quito Carrion	**Coordinador de Tecnología**	Firmado electrónicamente por: FABIAN DARIO QUITO CARRION Validar únicamente con FirmaEC
Aprobado por: Luis Fernando Ruiz Estrella	**Subgerente de Riesgos encargado**	Firmado electrónicamente por: LUIS FERNANDO RUIZ ESTRELLA Validar únicamente con FirmaEC