1. ANTECEDENTES

El Banco del Instituto Ecuatoriano de Seguridad Social - BIESS, es una institución financiera pública del Instituto Ecuatoriano de Seguridad Social, creada mediante ley, publicada en el Suplemento del Registro Oficial No. 587 de 11 de mayo del 2009; y, tiene personería jurídica propia y de carácter público, con finalidad social, con autonomía técnica, administrativa y financiera.

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 con sus activos de la información y que es requerido por disposición normativa emitida por la Superintendencia de Bancos.

La Dirección de Seguridad de la Información, no ha realizado compras de herramientas que permitan automatizar el proceso y seguimiento del Sistema de Gestión de Seguridad de la Información SGSI, actualmente el proceso se lo lleva en un archivo Excel, lo que genera una alta carga operativa, posibles fallas o errores en el ingreso de información y realizar varias iteraciones para la validación 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 para el 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 deben evaluarse acorde a la metodología y gestión de riesgos.

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.

Mediante 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."*

2. BASE LEGAL

A continuación, se detalla la base legal relacionada a este proceso de contratación:

REGLAMENTO PARA LAS CONTRATACIONES POR DE GIRO ESPECÍFICO DEL NEGOCIO DEL BIESS

"Art. 25.- Informe de Necesidad. – Previo a iniciar un procedimiento de contratación, el área requirente elaborará un informe que contenga un análisis técnico, funcional y legal amparado en la norma expresa de la Superintendencia de Bancos."

NORMATIVA ADICIONAL O ESPECIFICA AL OBJETO DE CONTRATACION

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."*
>
> Sección VII.- Servicios provistos por terceros, artículo 23, numeral 6.-
> "*b) Los centros de procesamiento de datos principal y/o alterno, contratados en la nube tanto con proveedores nacionales o extranjeros, 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;*
> *c) El proveedor de servicios en la nube tanto con proveedores nacionales o extranjeros, 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), ISO 27018 (protección de información personal en la nube) u otras similares que aplique conforme el servicio ofertado;*"

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."*

CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN

El Artículo 146 del parágrafo primero del software y bases de datos, Sección V Disposiciones especiales sobre ciertas obras, de la Sección V, señala:

"*Localización de datos.- Cuando las entidades del sector público contraten servicios de software u otros que impliquen la localización de datos, deberán hacerlo con proveedores que garanticen que los datos se encuentren localizados en centros de cómputo que cumplan con los estándares internacionales en seguridad y protección conforme las siguientes reglas:*

a) Los datos relacionados con seguridad nacional y sectores estratégicos se deben encontrar en centros de cómputo ubicados en territorio ecuatoriano;
b) Los datos de relevancia para el Estado que no se encuentren contenidos en el literal a) de este artículo se deben encontrar de forma preferente en centros de cómputo ubicados en territorio ecuatoriano o en países con normas de protección de datos iguales o más exigentes que los establecidos en el Ecuador; y,
c) Los datos que no se encuentren contenidos en los literales a y b del presente artículo se deben encontrar de forma indistinta en centros de cómputo ubicados en territorio ecuatoriano o extranjero."

El numeral 10.3.3. del Estatuto Orgánico por Procesos del Banco del Instituto Ecuatoriano de Seguridad Social – 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 la de *"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".

3. ANÁLISIS TÉCNICO, FUNCIONAL Y LEGAL DE LA NECESIDAD

A fin de dar cumplimiento normativo a lo establecido en el numeral artículo 9, sección 2, capítulo V, título IX, libro I, codificación de las normas de la Superintendencia de Bancos; así como al numeral 1.36 cumplimiento de políticas, reglas y normas de seguridad de la información, EGSI v.3, acuerdo Nro. MINTEL-MINTEL-2024-0003 del Ministerio de Telecomunicaciones y de la Sociedad de la Información.

El BIESS requiere la contratación de la SUSCRIPCIÓN Y SERVICIO DE SOPORTE DE SOFTWARE PARA CONTROL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, servicio en la nube enfocado a reforzar el Sistema de Gestión de Seguridad de la Información.

La Dirección de Seguridad de la Información, no ha realizado compras de herramientas que permitan automatizar el proceso y seguimiento del Sistema de Gestión de Seguridad de la Información SGSI, actualmente el proceso se lo lleva en un archivo Excel, lo que genera una alta carga operativa, posibles fallas o errores en el ingreso de información y realizar varias iteraciones para la validación 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 para el 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.

El BIESS para la implementación del SGSI, ha definido en la declaración de aplicabilidad, la implementación y seguimiento de 93 controles. La herramienta requerida permitirá automatizar y dar seguimiento adecuado de la efectividad y madurez del sistema de gestión de seguridad de la información.

Con la disponibilidad del software el BIESS podrá atender de manera adecuada las necesidades funcionales de:

a) Efectuar seguimiento del cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI) para que la gestión sea efectiva y eficiente, proporcionando al jerárquico superior, comités y auditoria informes de manera oportuna sobre el estado del SGSI.
b) Registrar las disposiciones normativas y verificar el cumplimiento respectivo.

c) Registrar y gestionar los riesgos de seguridad de la información conforme la metodología del BIESS, y monitorear indicadores de riesgo.

d) Registrar hallazgos de auditorías y observaciones de revisiones realizadas por organismos de control.

e) Efectuar seguimiento al cumplimiento normativo, planes de acción, hallazgos, KRIs y reportes, que servirán de insumo para la generación de informes gerenciales en la toma de decisiones del jerárquico superior y comités.

Por lo expuesto del cumplimiento normativo, la Dirección de Seguridad de la Información requiere contar con una herramienta en la nube:

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 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).	**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.
3	Suscripción - Módulo 3 de Gestión de Cumplimiento que incluya el monitoreo de	**1**	UNIDAD	Aplicativo Web al 100% para acceso a través de un navegador estándar Chrome, Edge, Firefox, con actualizaciones automáticas.

	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.			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.

- **Beneficio**

  El BIESS al llegar a contar con la SUSCRIPCIÓN Y SERVICIO DE SOPORTE DE SOFTWARE PARA CONTROL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, podrá beneficiarse de:

  - Dar cumplimiento de la normativa.
  - Alertar oportunamente sobre la ruta crítica de la gestión de seguridad de la información en el BIESS para la toma de decisiones del Jerárquico Superior en las áreas de su competencia.
  - Brindar al Jerárquico Superior un mecanismo para gestionar sus riesgos de seguridad de la información de manera amigable, fiable, automatizado y consolidado; así como brindarles reportes del estado de su gestión en términos de seguridad de la información.
  - Mejora continua en el establecimiento de controles orientados a proteger la información del BIESS en los distintos medios, físicos o digitales en los cuales se localice.
  - Otorgar al BIESS una visión general sobre el estado del sistema de Gestión de Seguridad de la Información para la toma de decisiones oportunas.
  - Determinar la magnitud de exposición del BIESS en términos de seguridad de la información.

Por lo expuesto y considerando la imperante necesidad del BIESS, canalizado a través de la Dirección de Seguridad de la Información, se requiere la contratación de SUSCRIPCIÓN Y SERVICIO DE SOPORTE DE SOFTWARE PARA CONTROL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, en razón de que se beneficiará a la institución para la aplicación de mejores prácticas de seguridad de la información y proveerá a la

Dirección de Seguridad de la Información una solución para la gestión del gobierno, riesgo y cumplimiento que permita la toma de decisiones relacionadas a la protección de los activos de información.

4.1. IDENTIFICACIÓN DEL/OS SERVICIO/S QUE SOPORTAN PROCESOS CRÍTICOS

El proceso es crítico:

SI		NO	X

El servicio de "SUSCRIPCIÓN Y SERVICIO DE SOPORTE DE SOFTWARE PARA CONTROL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN" permitirá realizar el seguimiento y monitoreo al cumplimiento del Sistema de Gestión de Seguridad de la Información, que no forma parte de un servicio que el BIESS brinde en su giro normal del negocio, por lo cual no está orientado a soportar un proceso especifico del negocio, y en tal sentido se identifica como NO CRÍTICO. Considerando que el software manejará una base de datos que contendrá información relacionada al estado de gestión en términos de seguridad de la información, pudiéndose determinar vulnerabilidades a ser explotadas, en tal sentido, la información es catalogada como "CONFIDENCIAL".

El servicio es continuo:

SI	X	NO	

El servicio que brindará el software es provisto para utilizarlo al interior del BIESS con la finalidad de verificar el estado del sistema de gestión de seguridad de la información y para regularizar o normar puntos pendientes como parte del seguimiento y monitoreo constantes.

4. CONCLUSIÓN

Con base en el análisis realizado se concluye que la **SUSCRIPCIÓN Y SERVICIO DE SOPORTE DE SOFTWARE PARA CONTROL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN** es necesario para cumplir con los objetivos institucionales y cumple con las condiciones para una contratación de Giro Específico de Negocio.

5. RECOMENDACIÓN

Se recomienda dar inicio al proceso de contratación SUSCRIPCIÓN Y SERVICIO DE SOPORTE DE SOFTWARE PARA CONTROL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN de conformidad a la normativa vigente.

6. FIRMAS 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: Paulina Suárez	Directora de Seguridad de la Información	Firmado electrónicamente por: MERY PAULINA SUAREZ LEON Validar únicamente con FirmaEC
Aprobado por: César Bolívar Estrella Jaramillo	Subgerente de Riesgos	Firmado electrónicamente por: CESAR BOLIVAR ESTRELLA JARAMILLO Validar únicamente con FirmaEC