Superintendencia de Seguros
República Dominicana

PROTOCOLO PARA LA APROBACIÓN DE EMPRESAS DE TERCERIZACIÓN

1. DESCRIPCIÓN GENERAL.

Establecer los requisitos que deberán cumplir las empresas interesadas en operar como Plataformas de Tercerización de Seguros, a los fines de presentar sus credenciales técnicas, legales y operativas para la obtención de la autorización de operación que las habilite a ofrecer servicios de intermediación tecnológica y comercio electrónico a las aseguradoras debidamente autorizadas, garantizando su integración formal, segura y supervisada al ecosistema del Sistema de Remisión de Información de Seguros (SIRISE).

El objetivo es integrar a los proveedores tecnológicos que acrediten cumplimiento verificable bajo el estándar SOC 2 Tipo II o su equivalente que evidencie la efectividad de los controles de seguridad, demostrando no solo el diseño adecuado de controles, sino su efectividad operativa sostenida en el tiempo, conforme a los criterios de seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad.

En consecuencia, los proveedores deberán evidenciar:

- Implementación efectiva de controles de acceso basados en roles y autenticación multifactor.
- Monitoreo continuo de infraestructura y registros de auditoría.
- Gestión formal de riesgos y respuesta a incidentes documentada.
- Políticas de continuidad del negocio y recuperación ante desastres probadas periódicamente.
- Protección criptográfica de la información en tránsito y en reposo.
- Procesos estructurados de gestión de cambios y control de vulnerabilidades.
- Evaluaciones independientes realizadas por firma auditora autorizada, que certifiquen la operación efectiva de los controles durante un período mínimo de evaluación.

Garantizando que la innovación tecnológica incorporada al sector asegurador opere bajo un marco de control interno robusto, auditable y alineado a estándares internacionales de aseguramiento y confianza.

1.1. BASE LEGAL.

El presente protocolo se fundamenta en un marco jurídico robusto que garantiza la validez de las operaciones digitales y la facultad supervisora de la SIS:

- Facultad Supervisora (Ley No. 146-02 sobre Seguros y Fianzas): Otorga a la SIS la facultad de autorizar, regular, supervisar y fiscalizar las operaciones de todas las entidades que intervienen en el mercado asegurador, asegurando el cumplimiento de sus obligaciones técnicas y financieras.

- Mandato de Remisión de Información (Resolución No. 01-2024): Establece la obligatoriedad de remitir información veraz y oportuna al ente regulador.

- Validez Jurídica Digital (Ley No. 126-02 de Comercio Electrónico y Firmas Digitales): Provee el marco legal para que las pólizas, fianzas y contratos emitidos digitalmente tengan plena fuerza probatoria, utilizando recursos tecnológicos como Firmas Digitales seguras y certificadas para garantizar la integridad y no repudio de los documentos.

- Protección del Usuario (Ley No. 172-13 de Protección de Datos Personales): Obliga a las personas a implementar controles estrictos para garantizar la privacidad, confidencialidad y seguridad de los datos sensibles de los asegurados que transitan por sus sistemas.

- Gestión de Riesgos (Ley 147-02, sobre Gestión de Riesgos en la República Dominicana) Esta Ley establece la obligación de gestionar riesgos en todos los ámbitos, incluyendo el tecnológico. En la era digital, la infraestructura es parte esencial del sistema nacional de gestión de riesgos.

- Libre Acceso a la Información Pública (Ley 200-04, sobre Libre Acceso a la Información Pública y su Reglamento de aplicación No. 130-05). Esta Ley es una norma de transparencia, pero su cumplimiento es eminentemente tecnológico en la era digital. Sin sistemas seguros, organizados y auditables, no es posible garantizar el libre acceso a la información pública.

- Estrategia Nacional de Ciberseguridad (Decreto No. 313-22 sobre Estrategia Nacional de Ciberseguridad 2021-2030). Este decreto convierte la ciberseguridad en una obligación estratégica nacional. No se limita a proteger sistemas; establece un marco de gobernanza, prevención, monitoreo y respuesta que impacta directamente la arquitectura tecnológica de las instituciones públicas y sectores regulados.

- Notificación de Incidentes de Ciberseguridad (Decreto No. 685-22 de Notificación Obligatorio de Incidentes e Intercambio de Inteligencia de Amenazas). Este decreto transforma la ciberseguridad en una obligación operativa verificable. No basta

con tener políticas; se requieren capacidades técnicas reales de detección, respuesta y notificación. No es solo una norma administrativa; impone obligaciones técnicas concretas a las instituciones públicas y sectores críticos.

1.2. ALCANCE DE LA AUTORIZACIÓN.

La autorización otorgada mediante el presente documento faculta a la empresa solicitante para operar como un proveedor tecnológico habilitado dentro del ecosistema regulado de seguros. La autorización de operación permite la prestación de servicios de intermediación digital, procesamiento de transacciones y cumplimiento normativo a las aseguradoras y reaseguradoras autorizadas.

Los servicios comprendidos dentro de este alcance, respecto de los cuales la plataforma deberá remitir información a la SIS de manera obligatoria e integral, lo establecido a continuación:

A. Servicios de Comercio Electrónico y/o Gestión de Pólizas:

- Gestión completa del ciclo de vida del producto asegurador: cotización, suscripción, emisión, renovación, cancelación y modificaciones (endosos).
- Entrega segura de documentos contractuales (pólizas, certificados, fianzas) en formato digital (PDF) y firmados digitalmente cuando aplique.

B. Servicios de Procesamiento de Pagos en Línea (Pasarela de Pagos):

- Habilitación de mecanismos para el recaudo digital de primas (tarjetas de crédito/débito, transferencias bancarias), garantizando la liquidación transparente de fondos hacia las aseguradoras.
- Cumplimiento estricto de los estándares de seguridad para transacciones financieras (PCI-DSS) y prevención de lavado de activos.
- Estos mecanismos y estándares aplican exclusivamente a las empresas que realicen procesamiento de pagos en línea.

C. Servicios de Consulta y Validación de Datos:

- Provisión de interfaces para la consulta del estatus de pólizas, vigencia de marbetes y autenticidad de fianzas por parte de los usuarios finales y beneficiarios.
- Interconexión para la validación de identidad de clientes y datos de vehículos o bienes asegurados entre otros.

D. Servicios de Remisión de Información Regulatoria (Resolución 01-2024):

- Centralización de toda la información transaccional generada en la plataforma.

- Actuación como Agente de Remisión Delegado, presentando o enviando los datos operativos, financieros y estadísticos directamente a la Superintendencia de Seguros a través del SIRISE (Vía API), conforme a la Resolución 01-2024.

E. Servicios de Supervisión y Auditoría:

- Acceso directo y privilegiado para la Superintendencia de Seguros a herramientas de monitoreo, dashboards de control y extracción de reportes para la fiscalización continua de las operaciones.

2. PROCEDIMIENTO DE EVALUACIÓN.

Para garantizar un proceso de evaluación ágil, transparente y objetivo, se regirá por una metodología de revisión de la documentación que deberá ser remitida en formato física o digital a través del correo infosirise@sis.gob.do, sin perjuicio de que la SIS pueda requerir documentos físicos cuando lo considere necesario, bajo la determinación de criterios habilitantes y de las inspecciones realizadas por técnicos de la SIS.

2.1 Organización del Expediente

El comité evaluador dispondrá de hasta treinta (30) días laborables para emitir la aprobación o negación de la solicitud, contados a partir de la recepción del expediente.

2.1.1 Carta de Solicitud:

Firmada por el representante legal, solicitando formalmente la autorización para operar como empresa de tercerización conectada al SIRISE.

2.1.2 Documentación Corporativa:

- Registro Mercantil actualizado, emitido por la Cámara de Comercio y Producción correspondiente.
- Asamblea General que establezca el representante legal de la entidad, y los documentos constitutivos de la misma.
- Certificación emitida por la Dirección General de Impuestos Internos de Registro Nacional de Contribuyente (RNC).

2.1.3 Requisitos Técnicos

Estos se someten a evaluación técnica bajo la modalidad de Cumplimiento Verificable. Cada criterio será evaluado cualitativamente para determinar si la plataforma posee las condiciones mínimas de seguridad y funcionalidad para operar.

2.2 Categorización de Requisitos

Para fines de evaluación, únicamente se considerarán los criterios directamente vinculados a los servicios tecnológicos objeto de autorización, especialmente aquellos que impliquen procesamiento de datos sensibles, integración con sistemas institucionales o exposición a riesgos cibernéticos relevantes. Cada hallazgo será clasificado conforme a la siguiente escala:

No	Clasificación	Escala de Color	Tiempo	Significado
1	Crítico (CR)	Rojo	Rechazado	Riesgo inaceptable o incumplimiento de requisito obligatorio. Su existencia impide la aprobación o continuidad del servicio hasta su total subsanación.
2	Alto (A)	Naranja / Amarillo fuerte	De acuerdo a las disposiciones del Comité Evaluador	Riesgo significativo con potencial impacto en la seguridad, disponibilidad o cumplimiento normativo. Debe corregirse con carácter prioritario.
3	Medio (M)	Amarillo	De acuerdo a las disposiciones del Comité Evaluador	Riesgo moderado que requiere plan de acción formal. No bloquea inmediatamente la autorización, pero exige seguimiento y verificación de mejora.
4	Bajo (B)	Verde	De acuerdo a las disposiciones del Comité Evaluador	Riesgo menor, observación de mejora o requisito formal. No representa amenaza inmediata, pero debe ser atendido dentro del plazo establecido.

2.3 Resultados de la Evaluación

Con base en la revisión de la documentación y de los requisitos tecnológicos presentados por el solicitante, el Comité Evaluador emitirá uno de los siguientes dictámenes:

2.3.1 Aprobación: Autorización Definitiva

Se otorgará **Autorización Definitiva** cuando:

- Cumpla con el 100% de los requisitos clasificados.
- No presente observaciones pendientes que comprometan la seguridad, continuidad operativa o supervisión regulatoria.

La autorización definitiva tendrá una vigencia de tres (3) años, renovable previa evaluación técnica y regulatoria por parte de la SIS. Esta podrá ser revocada por: fallas graves de seguridad, uso indebido de datos y incumplimiento de algún requisito del SIRISE.

2.3.2 Habilitado Provisional: Autorización Provisional

Se otorgará **Autorización Provisional** cuando:

- Cumpla con el 100% de los requisitos Críticos (CR).
- Presenta incumplimientos en requisitos clasificados como Medio (M), y Bajo (B) ya que no representan riesgo sistémico o vulnerabilidad crítica.
- Deben presentar un plan de adecuación formal, viable y calendarizado, con responsables designados y compromisos verificables de subsanación.
- Al finalizar el plazo de adecuación, el comité evaluador ejecutará la Segunda Evaluación Técnica (Reevaluación) específicamente sobre los puntos pendientes.

Se emitirá Autorización Provisional, permitiendo la operación del servicio. La empresa deberá subsanar los hallazgos dentro del plazo otorgado. El incumplimiento del plan aprobado podrá dar lugar a la revocación automática de la habilitación provisional y la empresa deberá reiniciar el proceso de solicitud presentando nueva documentación y sometiéndose a una nueva evaluación integral.

En caso de que la solicitud cumpla con el 100% de los requisitos Críticos (CR) e incumpla uno o más de los requisitos clasificados Alto (A), deberá presentar un plan de adecuación formal, viable y calendarizado, con responsables designados y compromisos verificables. La Comisión requerirá que el solicitante subsane en el plazo determinado los hallazgos encontrados. En caso de que el solicitante no subsane las correcciones indicadas, se procederá al rechazo de la solicitud, y el solicitante deberá iniciar una nueva solicitud de habilitación.

2.3.3 Rechazado

Procederá el rechazo de la solicitud cuando:

- Incumpla uno o más requisitos clasificados como Críticos (CR).
- Se detecten vulnerabilidades graves de seguridad, deficiencias estructurales en la arquitectura tecnológica, ausencia de controles esenciales o documentación técnica insuficiente.
- Se evidencie imposibilidad técnica o jurídica para garantizar la integridad, confidencialidad, disponibilidad o supervisión del servicio.

La empresa deberá iniciar el proceso de solicitud presentando nueva documentación y sometiéndose a una evaluación integral.

2.4 Matriz de Evaluación Técnica

La presente Matriz de Evaluación Técnica establece los criterios de clasificación de hallazgos identificados durante el proceso de revisión técnica y de ciberseguridad.

Los requisitos se organizan por áreas de control y se valoran conforme a su nivel de criticidad, impacto en la seguridad de la información, continuidad operativa y cumplimiento normativo.

Los plazos de las adecuaciones iniciarán desde que el Comité notifique a la empresa del resultado de la evaluación de su solicitud.

2.5 Matriz de requisitos de interoperabilidad y de GRC

Garantizar que la plataforma tecnológica implemente una arquitectura centralizada, interoperable y auditable, que permita la gestión integral de la información bajo un modelo de Gobernanza, Riesgo y Cumplimiento (GRC), asegurando compatibilidad con los sistemas institucionales y estándares de seguridad

No.	Requisitos	**Clasificación/ Riesgo**	**Tiempo**	**Medio de Verificación**	**Criterio de Aceptación**
1	Núcleo GRC (System of Record)	**Crítico (CR)**	Rechazado	Documentación técnica y diagrama	La plataforma deberá operar bajo un modelo de System of

				detallado de arquitectura	Record, centralizando la totalidad de la data transaccional y documental relevante, garantizando integridad, trazabilidad y disponibilidad para fines de consulta, auditoría o remisión regulatoria.
2	Interoperabilidad mediante APIs seguras	**Crítico (CR)**	Rechazado	Validación técnica de endpoints y documentación API	Deberá existir especificación técnica formal de las APIs (REST/JSON u otro estándar interoperable), incluyendo mecanismos de autenticación, autorización, cifrado en tránsito (TLS 1.2 o superior) y control de acceso basado en roles.
3	Repositorio seguro de información	**Alto (A)**	De acuerdo a las disposiciones del Comité Evaluador	Pruebas técnicas y evidencias de controles implementados	El sistema deberá implementar mecanismos integrales de protección de datos (cifrado en reposo, control de versiones, segregación de

					entornos, políticas de retención y respaldo), conforme a reglas de negocio definidas y estándares de seguridad aplicables.
4	Descripción técnica del Software GRC	**Alto (A)**	De acuerdo a las disposiciones del Comité Evaluador	Documento formal de arquitectura, mapa de servicios y endpoints	La arquitectura deberá estar claramente definida (diagramas lógicos y físicos), con descripción de módulos, flujos de datos y compatibilidad técnica con SIRISE u otros sistemas regulatorios.
5	Dashboard y módulo de reportería independiente	**Medio (M)**	De acuerdo a las disposiciones del Comité Evaluador	Documentación funcional y demostración operativa	El sistema deberá contar con capacidades de visualización, análisis y exportación de datos que permitan consultas independientes, generación de reportes regulatorios y trazabilidad de eventos.

2.6 Matriz de Requisitos Técnicos Normativos de Calidad

Garantizar la trazabilidad de los procesos, la mejora continua, la gestión estructurada del riesgo y la satisfacción del cliente, mediante la adopción de sistemas formales de gestión y estándares internacionales verificables.

No.	Requisitos	Clasificación	Tiempo	Medio de Verificación	Criterio de Aceptación
1	Certificación SOC 2 Tipo II vigente o su equivalente	**Alto (A)**	De acuerdo a las disposiciones del Comité Evaluador	Informe oficial del auditor independiente y carta de atestación	Evidencia de evaluación independiente sobre la efectividad operativa de los controles relacionados con seguridad, disponibilidad, confidencialidad, integridad del procesamiento y privacidad, incluyendo gestión de no conformidades y control documental continuo.
2	Plan de Gestión de la Seguridad de la Información (SGSI)	**Medio (M)**	De acuerdo a las disposiciones del Comité Evaluador	Documento formal del plan y evidencias de ejecución	Implementación de un sistema estructurado de gestión de riesgos tecnológicos, monitoreo de controles técnicos, gestión de vulnerabilidades y revisión periódica de incidentes de seguridad.

3	Plan de Gestión de la Continuidad del Negocio (BCP)	**Medio (M)**	De acuerdo a las disposiciones del Comité Evaluador	Documento del plan, resultados de pruebas y simulacros	Existencia de análisis de impacto al negocio (BIA), estrategias de recuperación definidas (RTO/RPO), pruebas periódicas documentadas y evidencia de capacidad operativa ante escenarios disruptivos.
4	Plan basado en el Sistema de Gestión de la Calidad (QMS)	**Bajo (B)**	De acuerdo a las disposiciones del Comité Evaluador	Manual de calidad y registros de seguimiento	Implementación de procesos documentados que permitan trazabilidad, medición de desempeño, gestión de no conformidades y aplicación de mecanismos de mejora continua.
5	Plan basado en Sistema de Gestión Antisoborno	**Bajo (B)**	De acuerdo a las disposiciones del Comité Evaluador	Política formal, matriz de riesgos y evidencias de cumplimiento	Implementación de controles internos orientados a prevenir prácticas indebidas, incluyendo mecanismos de denuncia, debida diligencia de terceros y monitoreo de cumplimiento ético.

2.7 Matriz de Requisitos Técnicos de Seguridad de la Información y Ciberseguridad

Garantizar la protección integral de los datos sensibles, la infraestructura tecnológica y los servicios digitales, conforme al Régimen de Seguridad y Ciberseguridad Institucional (RSCI) y estándares internacionales aplicables.

No.	Requisitos	Clasificación	Tiempo	Medio de Verificación	Criterio de Aceptación
1	Arquitectura de Seguridad y Alta Disponibilidad	**Crítico (CR)**	Rechazado	Evaluación técnica de arquitectura, diagramas lógicos/físicos y pruebas de resiliencia	Infraestructura con alta disponibilidad (HA), redundancia geográfica o lógica, balanceo de carga y mecanismos de recuperación automática ante fallas.
2	Plan de Continuidad del Negocio y Recuperación ante Desastres (BCP/DRP)	**Crítico (CR)**	Rechazado	Documento formal del plan, resultados de pruebas y simulacros	Existencia de BIA documentado, definición de RTO y RPO, procedimientos de recuperación tecnológica, responsables designados y evidencia de pruebas periódicas exitosas.
3	Protección e Integridad de Datos (en tránsito y en reposo)	**Crítico (CR)**	Rechazado	Evidencia técnica de configuración, políticas de cifrado y	Cifrado obligatorio en tránsito mediante TLS 1.2 o superior;

				pruebas de seguridad	cifrado en reposo mediante AES-256 o estándar equivalente; gestión segura de llaves criptográficas; cumplimiento con los criterios de seguridad establecidos en SOC 2 Tipo II o su equivalente
4	Autenticación Multifactor (MFA)	**Crítico (CR)**	Rechazado	Evidencia técnica de implementación y pruebas de acceso	Implementación obligatoria de MFA para accesos administrativos, cuentas privilegiadas, integraciones críticas y plataformas de supervisión.
5	Protección de Datos y Privacidad	**Crítico (CR)**	Rechazado	Políticas formales, registros de respaldo y pruebas de restauración	Existencia de políticas de respaldo periódico, cifrado de copias, almacenamiento seguro, pruebas de restauración verificables y cumplimiento de principios de minimización y confidencialidad de datos.
6	Segregación de Ambientes Tecnológicos	**Crítico (CR)**	Rechazado	Documentación de arquitectura y verificación	Separación lógica o física entre entornos de Desarrollo

	(DEV, QA, PROD)			técnica de entornos	(DEV), Pruebas (QA) y Producción (PROD), con controles de acceso diferenciados y prohibición de uso de datos reales en ambientes no productivos sin anonimización.
7	Personal Técnico Certificado y Gestión de Privilegios	**Alto (A)**	De acuerdo a las disposiciones del Comité Evaluador	Certificaciones, perfiles de cargo y matriz de control de accesos	Evidencia de competencias técnicas en seguridad y administración de sistemas; aplicación del principio de mínimo privilegio (Least Privilege) y revisión periódica de accesos.

2.8 Funcionalidad de Negocio

Garantizar la validez jurídica de las operaciones digitales, la trazabilidad integral de los procesos, la transparencia en la gestión de información y la capacidad de supervisión efectiva por parte de la autoridad reguladora.

No.	Requisitos	Clasificación	Tiempo	Medio de Verificación	Criterio de Aceptación
1	Gestión Integral del Ciclo de Vida del Proceso de Negocio	**Crítico (CR)**	Rechazado	Documentación técnica del sistema, diagramas de flujo y pruebas funcionales	El sistema deberá documentar y automatizar el ciclo completo del proceso de

					negocio: captura y validación de datos, reglas de negocio, procesamiento, almacenamiento seguro, auditoría y remisión de información a la SIS. Debe garantizar trazabilidad, registro de eventos (logs) y control de versiones.
2	Pasarela de Pagos con Cumplimiento Normativo	Alto (A)	De acuerdo a las disposiciones del Comité Evaluador	Certificación PCI-DSS vigente o contrato con proveedor certificado	Evidencia de cumplimiento del estándar PCI-DSS (propio o a través del proveedor de pasarela), cifrado de transacciones, segregación de datos financieros y mecanismos antifraude.
3	Dashboard de Supervisión para la SIS	Alto (A)	De acuerdo a las disposiciones del Comité Evaluador	Demostración funcional y documentación técnica	Implementación de un módulo de supervisión que permita a la SIS acceso seguro, visualización en tiempo real, exportación estructurada de datos (CSV/Excel/API) y generación de reportes

					regulatorios (BI básico).
4	Plan de Atención y Soporte a Usuarios (SLA)	Medio (M)	De acuerdo a las disposiciones del Comité Evaluador	Documento formal de soporte y acuerdos de nivel de servicio	Estructura de soporte escalonado (N1, N2, N3), definición de tiempos de respuesta y resolución (SLA), canales formales de atención (correo, mesa de ayuda, teléfono) y mecanismos de registro y seguimiento de incidencias.

3. PUNTO DE CONTACTO

Para la canalización de consultas técnicas, aclaraciones sobre los términos de referencia y el seguimiento al estatus de evaluación de los expedientes, los solicitantes deberán dirigirse por la vía electrónica, utilizando la dirección de correo infosirise@sis.gob.do.