SuperTransporte

ANEXO TÉCNICO - ALIADO TECNOLÓGICO SARLAFT - RMS

Requisitos para Aliados Tecnológicos

Superintedencia de Transporte

Versión 1.0

Mayo 27 de 2026.

1. TABLA DE CONTENIDO

2. OBJETIVO

Establecer los requisitos mínimos para el proceso de autorización de Aliados Tecnológicos para interoperar con el Módulo de Supervisión SARLAFT dispuesto en el Sistema Inteligente Nacional de Supervisión al Transporte (SINST – VIGIA 2).

3. ALCANCE

El presente Anexo Técnico aplica a todas las personas jurídicas que deseen acreditarse como aliados tecnológicos autorizados para interoperar con el Módulo de Supervisión SARLAFT dispuesto en el Sistema Inteligente Nacional de Supervisión al Transporte (SINST – VIGIA 2).

4. REQUISITOS FUNCIONALES DE LA PLATAFORMA TECNOLÓGICA ALIADO TECNOLÓGICO SARLAFT - RMS.

La plataforma tecnológica debe contar con las siguientes funcionalidades mínimas:

4.1 Módulo de Seguimiento de Tareas (relacionado con SARLAFT y RMS) en Tiempo Real.

La plataforma debe permitir el seguimiento continuo y en tiempo real de todas las actividades de relacionadas con el funcionamiento del SARLAFT y RMS. El Aliado Tecnológico deberá cumplir con los siguientes requisitos:

- Dashboard principal con visualización del estado general de cumplimiento.
- Indicadores de progreso por actividad, área, responsable y período.
- Actualización automática del estado de las actividades de mitigación relacionadas a SARLAFT y RMS sin necesidad de recargar la página.
- Filtros y vistas personalizables según las necesidades del usuario.
- Trazabilidad completa de las acciones realizadas sobre cada actividad relacionadas con el SARLAFT y RMS (historial de cambios).
- Capacidad de asignar y reasignar actividades relacionadas a SARLAFT y RMS a diferentes responsables.

4.2 Sistema de Alertas y Recordatorios.

La plataforma debe contar con un sistema robusto de notificaciones que garantice el cumplimiento oportuno. Se requiere:

- Alertas automáticas por correo electrónico para cada actividad próximas a vencer.
- Notificaciones dentro de la plataforma (in-app) en tiempo real.
- Configuración flexible de tiempos de alerta (días previos al vencimiento).
- Escalamiento automático de alertas según niveles de criticidad.
- Recordatorios programables y recurrentes.
- Consolidado diario o semanal de actividades relacionadas con el SARLAFT y RMS pendientes para supervisores.

4.3 Gestión de Evidencias

El sistema debe permitir la gestión integral de las evidencias documentales que soportan el cumplimiento:

- Carga de documentos en múltiples formatos (PDF, Word, Excel, imágenes).
- Organización jerárquica de documentos por categoría, período y tarea.
- Búsqueda avanzada de documentos por metadatos y contenido.
- Vinculación de evidencias con tareas específicas.
- Previsualización de documentos sin necesidad de descarga.
- Límites de almacenamiento claramente definidos por cliente.

4.4 Reportes y Métricas

La plataforma debe generar reportes e indicadores que permitan evaluar el estado del cumplimiento:

- Reportes de cumplimiento por período (mensual, trimestral, anual).
- Indicadores clave de desempeño (KPIs) configurables.
- Gráficos y visualizaciones interactivas del estado de cumplimiento.
- Exportación de reportes en formatos estándar (PDF, Excel).
- Reportes comparativos entre períodos.
- Métricas de productividad por responsable y área.
- Generación de informes para presentación ante entes de control.

4.5 Gestión de Roles y Permisos

El sistema debe implementar un modelo de control de acceso basado en roles (RBAC):

- Definición de roles predeterminados (Administrador, Supervisor, Operador).
- Creación de roles personalizados según necesidades de la entidad.
- Asignación granular de permisos por módulo y funcionalidad.
- Segregación de funciones para garantizar independencia en la gestión.
- Auditoría de accesos y cambios en permisos.
- Gestión de múltiples empresas/sedes desde una única cuenta administradora.

4.6 Interfaz de Usuario

El Aliado Tecnológico debe describir las características de usabilidad de su plataforma, incluyendo: diseño responsivo para acceso desde dispositivos móviles, cumplimiento de políticas de accesibilidad según lineamientos de MinTIC, disponibilidad en idioma español, y experiencia de usuario intuitiva que minimice la curva de aprendizaje.

4.7 Gestión del Riesgo LA/FT/FP

El Aliado Tecnológico deberá disponer de funcionalidades que permitan apoyar la implementación, operación y monitoreo del SARLAFT y RMS por parte del sujeto obligado, incluyendo como mínimo:

- Consulta de listas vinculantes para Colombia.
- Screening automático de contrapartes.
- Integración con fuentes externas de información para debida diligencia.
- Gestión y actualización de perfiles de riesgo.

- Segmentación de factores de riesgo.
- Parametrización de señales de alerta.
- Monitoreo de operaciones y eventos relevantes.
- Identificación de operaciones inusuales.
- Registro de decisiones del Oficial de Cumplimiento.
- Generación de indicadores y reportes de riesgo.
- Conservación de trazabilidad de las evaluaciones realizadas.

5. REQUISITOS DE ARQUITECTURA TECNOLÓGICA

El Aliado Tecnológico debe presentar documentación detallada de la arquitectura de su solución:

5.1 Marco de Referencia de Arquitectura

Indicar el framework de arquitectura utilizado para el diseño de la solución (TOGAF, Zachman, etc.) y justificar su selección.

5.2 Descripción de Componentes

Proporcionar descripción detallada de los componentes tecnológicos que conforman la plataforma: frontend, backend, base de datos, servicios de integración, colas de mensajería, caché, entre otros.

5.3 Diagramas de Arquitectura

Presentar los siguientes diagramas técnicos:

- Diagrama de contexto del sistema.
- Diagrama de componentes.
- Diagrama de despliegue.
- Diagrama de integración (APIs, servicios web).
- Diagrama de seguridad.

5.4 Integración de Datos

Describir la estrategia de integración de datos, incluyendo: protocolos utilizados (REST, SOAP, GraphQL), formatos de intercambio (JSON, XML), mecanismos de sincronización y APIs disponibles para integración con sistemas externos.

5.5 Escalabilidad y Rendimiento

Explicar cómo la arquitectura soporta el crecimiento en usuarios y transacciones, incluyendo: estrategias de escalamiento horizontal/vertical, uso de balanceadores de carga, implementación de caché y CDN, y métricas de rendimiento garantizadas.

5.6. Especificación de integración del Módulo SARLAFT y ambiente de pruebas

La Superintendencia de Transporte pondrá a disposición de los aspirantes a Aliado Tecnológico, desde la apertura del proceso de autorización y como documento referenciado del presente Anexo, la especificación técnica de integración del Módulo SARLAFT del sistema SINST – VIGIA 2, la cual contendrá como mínimo: (i) el diccionario de datos con la definición, tipo, longitud y obligatoriedad de cada campo; (ii) el catálogo de servicios web disponibles,

descrito mediante un estándar abierto de especificación legible por máquina —tal como OpenAPI (Swagger) para servicios REST, WSDL para servicios SOAP o SDL para GraphQL, según corresponda al estilo de servicio—, con sus métodos, mecanismo de autenticación y la estructura de los mensajes de solicitud y respuesta; (iii) las reglas de validación y las causales de rechazo; (iv) los estados del reporte y los códigos de error; y (v) la periodicidad y demás parámetros técnicos del reporte. Asimismo, la Superintendencia dispondrá de un ambiente de pruebas (sandbox) que reproduzca el comportamiento del ambiente productivo, disponible para los aspirantes durante las etapas de preparación y de pruebas en ambiente controlado, con el fin de permitir el desarrollo y la verificación de la integración con anterioridad a la evaluación técnica.

La especificación de servicios web se publicará en un formato estándar, abierto e interoperable que permita su procesamiento automatizado y la generación de clientes y validadores, con el fin de reducir la ambigüedad de la integración y los tiempos de desarrollo. Parágrafo segundo. La especificación de integración y el ambiente de pruebas se mantendrán actualizados y su versión vigente será publicada por la Superintendencia. Cualquier modificación se sujetará a las reglas de gestión del cambio previstas en este Anexo.

6. REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

6.1 Gestión de Acceso

El Aliado Tecnológico debe describir los mecanismos de control de acceso implementados:

- Autenticación segura (contraseñas robustas, políticas de complejidad).
- Autenticación multifactor (MFA) disponible.
- Soporte para autenticación federada (OpenID Connect, OAuth 2.0, SAML).
- Gestión de sesiones y timeout de inactividad.
- Bloqueo de cuentas por intentos fallidos.

6.2 Cifrado de Datos

Detallar las medidas de cifrado implementadas:

- Cifrado de datos en tránsito mediante TLS 1.2 o superior (certificados SSL).
- Cifrado de datos en reposo para información sensible.
- Gestión segura de claves de cifrado.

6.3 Auditoría y Monitoreo

- Describir las capacidades de auditoría y monitoreo de seguridad:
- Registro de eventos de seguridad (logs de acceso, cambios de configuración).
- Monitoreo de actividades sospechosas.
- Alertas de seguridad automatizadas.
- Retención de logs según políticas definidas.

7. REQUISITOS DE INFRAESTRUCTURA

El Aliado Tecnológico debe documentar la infraestructura tecnológica que soporta la plataforma:

7.1 Ambiente de Hospedaje

- Tipo de hospedaje (nube pública, privada, híbrida, on-premise).
- Proveedor de nube utilizado (AWS, Azure, GCP, etc.) si aplica.
- Ubicación geográfica de los centros de datos.
- Certificaciones del centro de datos (Tier III, Tier IV, SOC 2).

7.2 Niveles de Servicio Service Level Agreement (SLA)

Definir los acuerdos de nivel de servicio garantizados:

Métrica	Valor Mínimo	Observaciones
Disponibilidad del servicio	99.5%	Mensual
Tiempo de respuesta - Crítico	2 horas	Sistema no disponible
Tiempo de respuesta - Alto	8 horas	Funcionalidad afectada
Tiempo de respuesta - Medio	24 horas	Incidencia menor
Tiempo de respuesta - Bajo	48 horas	Consulta o mejora

7.3 Personal Técnico

El Aliado Tecnológico debe contar con personal con conocimientos tecnológicos en arquitecturas SOA y/o microservicios, debidamente certificado o con título profesional avalado por instituciones de educación superior autorizadas en Colombia.

8. PLAN DE CONTINUIDAD DEL NEGOCIO

8.1 Matriz de Riesgos

El Aliado Tecnológico debe entregar una matriz de riesgos que identifique los riesgos asociados a la solución tecnológica, incluyendo: descripción del riesgo, probabilidad de ocurrencia, impacto potencial, nivel de riesgo resultante, medidas de mitigación, responsable de la mitigación y estado de implementación.

8.2 Plan de Recuperación de Desastres

Documentar la estrategia de respaldo y recuperación incluyendo:

- Tipos de respaldo utilizados (completo, incremental, diferencial).
- Frecuencia de los respaldos y justificación.
- Ubicación de almacenamiento de respaldos (preferiblemente en zona geográfica diferente).
- Tiempo objetivo de recuperación (RTO) y punto objetivo de recuperación (RPO).
- Procedimientos documentados de recuperación paso a paso.

8.3 Plan de Contingencia

Entregar un plan de contingencia que describa:

- Procedimientos de activación del plan.
- Roles y responsabilidades durante una contingencia.
- Procedimientos de comunicación con clientes afectados.
- Pruebas periódicas del plan (mínimo cada 6 meses).

8.4. Portabilidad y entrega de datos y evidencias ante suspensión, revocación o terminación

En caso de suspensión, revocación o terminación de la autorización del Aliado Tecnológico, o de cese de la prestación del servicio por cualquier causa, el Aliado garantizará la portabilidad de la información y entregará a cada sujeto obligado, en un formato estructurado, interoperable y de uso común, la totalidad de los datos, documentos, soportes y evidencias digitales que hubiere gestionado por su cuenta, así como los registros de trazabilidad asociados, sin pérdida, alteración ni retención indebida. El Aliado Tecnológico informará de manera previa a la Superintendencia de Transporte y a los sujetos obligados afectados, con una antelación no inferior a treinta (30) días calendario, sobre cualquier circunstancia que afecte la continuidad del servicio, salvo en los eventos de suspensión o revocación dispuestos por la Superintendencia, en los cuales la notificación a los vigilados se efectuará de forma inmediata. Durante el plazo de transición, el Aliado mantendrá disponibles los datos y evidencias y prestará la colaboración necesaria para la migración hacia el reporte directo o hacia otro Aliado Tecnológico autorizado, de modo que se garantice el cumplimiento oportuno de las obligaciones de reporte por parte del sujeto obligado. Parágrafo. La suspensión o terminación de la autorización del Aliado Tecnológico no exime al sujeto obligado de sus deberes de reporte; las obligaciones de portabilidad, entrega y notificación aquí previstas tienen por finalidad asegurar que dicho cumplimiento no se vea afectado por causas atribuibles al Aliado.

9. SOPORTE TÉCNICO

El Aliado Tecnológico debe garantizar un servicio de soporte técnico con las siguientes características mínimas:

9.1 Modelo de Atención

- Descripción de los niveles de atención (Nivel 1, 2, 3).
- Flujo de escalamiento de incidencias.
- Personal asignado al soporte.

9.2 Canales de Atención

- Sistema de tickets para registro y seguimiento de incidencias.
- Correo electrónico de soporte.
- Línea telefónica o chat en línea.
- Base de conocimientos y documentación de autoayuda.

9.3 Horarios de Atención

Indicar claramente los horarios de atención del soporte técnico, diferenciando entre horario regular y atención de emergencias fuera de horario si aplica.

9.4 Métricas y Monitoreo

Describir las herramientas y métricas utilizadas para monitorear el rendimiento del servicio de soporte: tiempo promedio de respuesta, tiempo de resolución, satisfacción del cliente, entre otros.

10. REFERENCIAS Y EXPERIENCIA EN MATERIA DE ADMINISTRACIÓN DE RIESGOS LA/FT/FP

10.1 Proyectos Anteriores

Detallar proyectos tecnológicos similares completados, incluyendo: tipo de proyecto, alcance, tecnologías utilizadas y resultados obtenidos.

10.2 Casos de Éxito

Acreditar experiencia de mínimo de 05 años en sistemas de gestión de riesgos LA/FT/FP, como SAGRILAFT, SARLAFT, SIPLAFT, etc.

10.3 Referencias de Clientes

Incluir referencias de clientes actuales que puedan respaldar la calidad de los servicios prestados (nombre de contacto, cargo, teléfono y correo electrónico, previa autorización del cliente).

10.4 Tiempo de Implementación

Indicar el tiempo estimado para la implementación completa de la solución en una entidad vigilada, incluyendo las fases del proyecto y entregables de cada fase.