# ANEXO TECNICO - ALIADOS TECNOLOGICOS

## 1. INTRODUCCIÓN

El presente documento tiene como objetivo definir los aspectos tecnológicos y operativos que deben cumplir los aspirantes a ser autorizados como aliados tecnológicos, con el fin de apoyar a los sujetos obligados en el reporte de información requerida por la Superintendencia de Transporte en el marco de la inspección, vigilancia y control del sector transporte. Asimismo, establece las condiciones tecnológicas y operativas necesarias para garantizar la interoperabilidad con el Sistema Inteligente Nacional de Supervisión al Transporte (SINST – VIGIA 2).

Es importante mencionar que el procedimiento descrito en el presente anexo no genera costos directos o indirectos para los aspirantes a ser autorizados como aliados tecnológicos.

## 2. ACTORES ESTRATÉGICOS DEL SISTEMA

<table>
<tr><th colspan="2">Actores Estratégicos</th><th>Roles</th></tr>
<tr><td colspan="2">Superintendencia de Transporte (ST)</td><td>− Administrador del SINST<br>− Proveedor de los servicios Web – del Sistema Inteligente Nacional de Supervisión al Transporte (SINST – VIGIA 2).</td></tr>
<tr><td rowspan="2">Aliados tecnológicos (AT)</td><td>Proveedores Tecnológicos (PT)</td><td>Proveedor tecnológico de los sujetos obligados encargados de consumir y reportar a través de los servicios web la información requerida por los diferentes módulos del Sistema Inteligente Nacional de Supervisión al Transporte (SINST – VIGIA 2).</td></tr>
<tr><td>Organismos administradores del programa de seguridad en la operación del transporte (OAPSOT)</td><td>Organismos administradores del programa de seguridad en la operación del transporte encargados de consumir y reportar a través de los servicios web el resultados de las pruebas de alcoholimetría, sustancias psicoactivas, exámenes médicos generales de aptitud física y el programa de seguridad en la operación del transporte en el sistema.</td></tr>
</table>

## 3. PROCESO DE AUTORIZACIÓN PARA EL REPORTE DE INFORMACIÓN A TRAVÉS DE SERVICIOS WEB POR PARTE DE LOS ALIADOS TECNOLÓGICOS DE LOS SUJETOS OBLIGADOS.

Los aspirantes a ser aliados tecnológicos de los sujetos obligados deberá acreditar el cumplimento del siguiente procedimiento:

### 3.1 ETAPA # 1 SOLICITUD INICIAL

Los aspirantes a ser aliados tecnológicos deberán registrar la solicitud Inicial en el Sistema Inteligente Nacional de Supervisión al Transporte (SINST – VIGIA 2) y seguir los siguientes pasos:

- Ingresar al enlace web https://transformaciondigital.supertransporte.gov.co)
- Ingresar a la modulo “Solicitud aliado tecnológico”
- Diligenciar la información de la sección “Datos del aliado tecnológico”
- Diligenciar la información de la sección “Datos del representante legal”
- Adjuntar los documentos solicitados en la sección “Carga de documentos”
- Aceptar términos y condiciones - Hacer clic en el botón “Solicitar”

En la sección “Carga de documentos”, se deberá acreditar y cargar los siguientes documentos:

- **Experiencia**: Los aliados tecnológicos deberán contar con más de 3 años de experiencia acreditada en la prestación de servicios de gestión, desarrollo, implementación, administración, mantenimiento y despliegue de soluciones tecnológicas utilizando servicios web. Esta experiencia debe ser verificable a través de referencias de proyectos y/o contratos que demuestren su trayectoria y solidez en el ámbito tecnológico relacionado con proyectos similares.

- **Propiedad Intelectual y Patente:** Los aliados tecnológicos deberán poseer la propiedad intelectual y patentes del software ofrecido o, en su defecto, ser un distribuidor autorizado. Se deberá presentar la documentación correspondiente que acredite la titularidad o la autorización de distribución del software, garantizando así la legalidad y originalidad del producto suministrado.

El Sistema Inteligente Nacional de Supervisión al Transporte (SINST – VIGIA 2) enviara las credenciales de acceso ( usuario y contraseña) al correo electrónico del representante legal registrado.

### 3.2 ETAPA # 2 – INFORMACION COMPLEMENTARIA

Los aspirantes a ser aliados tecnológicos deberán ingresar al módulo de aliados tecnológicos del Sistema Inteligente Nacional de Supervisión al Transporte (SINST – VIGIA 2), indicar el o los módulos al cual aspira a ser autorizado, así como preparar y cargar los documentos que acrediten el cumplimiento de los siguientes ítems:

### 3.2.1 CERTIFICADOS LEGALES

Presentación de los documentos que acrediten la legalidad y existencia de la empresa, como:

- **Certificado de Cámara de comercio:** es un documento donde se visualice claramente la información de existencia y representación legal actualizada, su representante legal, dirección, objeto social, teléfono de contacto, correo electrónico, no mayor a 30 días.

- **RUT (Registro Único Tributario):** Es el registro necesario para cumplir con obligaciones tributarias. Incluye información sobre el tipo de contribuyente, régimen tributario, y otros detalles fiscales, no mayor a 30 días.

- **Certificado de Antecedentes Judiciales de Representante Legal:** Es un documento que demuestra la ausencia de antecedentes judiciales del representante legal de la empresa, no mayor a 30 días.

### 3.2.2. DESCRIPCIÓN DE SOLUCIÓN

- **Objetivos y Beneficios:**Indicar el nombre de su solución y explique los objetivos que persigue tu solución y cómo beneficiaría a la Superintendencia de Transporte y a los vigilados, en términos de eficiencia, automatización, mejora de procesos.

- **Funcionalidades Clave:**Describir las funcionalidades específicas que ofrece su solución, detallando cómo abordarían las necesidades y requisitos de la Superintendencia de Transporte.

- **Interfaz de Usuario:** Suministrarla información sobre la interface y la experiencia de usuario (Ux/Ui) y cómo los usuarios designados por los vigilados de la Superintendencia de Transporte interactuarán con ella. Según las políticas de accesibilidad emitidas por MinTIC.

- **Integración de Datos:** Explicar su estrategia de datos, e indica cómo se realizara la transferencia y la sincronización de datos entre su solución y los sistemas de la Superintendencia de Transporte.

- **Seguridad y Cumplimiento:** Detallar las medidas de seguridad que serán implementadas para proteger los datos de los vigilados y cómo su solución cumplirá con las regulaciones y políticas de seguridad de la información de la Superintendencia de Transporte.

- **Escalabilidad y Rendimiento:** Describir cómo su solución manejará la carga de información y cómo podrá escalar para proveer una mayor capacidad al momento de producirse un incremento en el volumen de transacciones.

- **Mantenimiento y Soporte:** Explicar cómo se realizará el mantenimiento continuo y el soporte técnico para garantizar el funcionamiento óptimo de la solución, utilizando los concepto de integración y despliegue continuo (CI/CD).

- **Tiempo de Implementación:** Indicar cuánto tiempo tomará implementar completamente la solución y desplegarla en ambiente productivo para un vigilado.

- **Caso de Uso :** Proporcionar las referencias concretas de éxitos en su solución y cómo esos casos de uso podrían aplicarse a la Superintendencia de Transporte.

- **Arquitectura TI:** Proporcionar el detalle de la Arquitectura TI diseñada para la solución, incluyendo cómo se comunicará con el sistemas provisto por la Superintendencia de Transporte.

- **Marco de Referencia de la Arquitectura:** Framework de Arquitectura utilizado para el diseño de la arquitectura implementada.

- **Descripción de Componentes:** Proporcionar una descripción detallada de los componentes tecnológicos clave que componen el sistema o la solución.

- **Diagramas de Arquitectura:** Presentar visualmente la estructura, las relaciones y las interacciones entre los componentes clave de la arquitectura. Los diagramas deben proporcionar una representación gráfica de cómo se organizan y se conectan los diferentes elementos dentro la solución tecnológica. Debe contener diagrama de contexto, diagrama de componentes¸ diagrama de despliegue, diagrama de integración y diagrama de seguridad.

#### 3.2.2.1. CONSIDERACIONES DE INTEGRACIÓN Y COMPATIBILIDAD

Describir los aspectos relacionados con la integración de diferentes sistemas, aplicaciones y componentes, así como en garantizar la compatibilidad entre los mismo.

- **Plan de Migración y Despliegue:** Describir cómo se llevará a cabo la transición de la arquitectura existente a la nueva arquitectura propuesta, así como los pasos y consideraciones para implementar y desplegar la solución tecnológica, en caso que se presente.

### 3.2.2.1. CONSIDERACIONES DE SEGURIDAD

Describir los componentes que forman parte de la arquitectura y estén orientados a la seguridad de la aplicación y a la prevención y protección contra amenazas.

- **Gestión de acceso:** Explicar cómo controla y gestiona el acceso a los sistemas y datos sensibles. Mencione si utiliza autenticación federada mediante protocolos Open ID o Auth2, si utiliza autenticación multifactor (MFA) y cómo gestiona los roles y permisos de usuario.

- **Cifrado:** Detallar cómo implementará el cifrado de datos al momento de la transmisión para proteger la información del vigilado. Mencione si utiliza certificados SSL o cualquier otra forma de cifrado.

### 3.2.2.2. CONSIDERACIONES DE RENDIMIENTO Y ESCALABILIDAD

Describir los componentes que forman parte de la arquitectura y estén orientados al rendimiento y la escalabilidad:

- **Balanceador de Carga:** Detallar cómo esta implementado el balanceador de carga para distribuir la carga de manera uniforme entre múltiples servidores o nodos.

- **Caché y Memoria:** Detallar cómo se gestiona el caché de datos y la utilización eficiente de la memoria para reducir la carga en los recursos.

- **Arquitectura de Red:** Detallar la arquitectura de red que se utilizará para garantizar un rendimiento óptimo, como redundancia, segmentación y ancho de banda.

- **Capacidad de Almacenamiento:** Describir los componentes que se encargan de gestionar el almacenamiento de datos.

### 3.2.2.3. CONSIDERACIONES DE MANTENIMIENTO Y SOPORTE

Describa los componentes que forman parte de la arquitectura y estén orientados al mantenimiento y soporte:

- **Gestión de Versiones:** Describir los componentes y herramientas para la gestión y control de versiones del software y sus componentes.

- **Integración y Despliegue Continuo:** Describir los componentes y herramientas para la integración y el despliegue continuó (CI/CD) para la reparación de bugs y nuevas funcionalidades.

### 3.2.2.4. SEGURIDAD DE DATOS

- **Políticas de Seguridad:** Describir las políticas y procedimientos que su empresa ha establecido para garantizar la seguridad de los datos. Esto podría incluir políticas de acceso, uso de los datos, gestión de credenciales de acceso, entre otras.

- **Auditorías y Monitoreo:** Explicar cómo supervisa y audita sus sistemas en busca de actividades sospechosas o no autorizadas. Describa las herramientas y prácticas de monitoreo que utilizas.

- **Certificacion:** Acredite la certificación sobre sistemas de gestión de seguridad de la información y calidad de la información conforme a algunas de las siguientes normas ISO/IEC 27001 o ISO/IEC 39000 o Certificación Internacional PCI DSS, sobre sistemas de gestión de seguridad de la información para los procesos, documentos y servicios. Si para la fecha de presentación de la solicitud como aliado tecnológico ante la Oficina TIC de la Superintendencia de Transporte, no se cuenta con alguna de estas certificaciones, deberá manifestarse el compromiso de aportarla a más tardar dentro de los doce (12) meses siguientes a la notificación de la autorización como aliado tecnológico; término dentro del cual registrar en el Sistema Inteligente Nacional de Supervisión al Transporte (SINST – VIGIA 2) la certificación correspondiente, como requisito necesario para interoperar.

### 3.2.3. REFERENCIAS Y EXPERIENCIA

- **Descripción de Proyectos Anteriores:** Detallar de proyectos tecnológicos anteriores que hayas completado, incluyendo información sobre el tipo de proyecto, el alcance, las tecnologías utilizadas y los resultados obtenidos.

- **Casos de Éxito:** Detallar los sasos específicos en los que la solución tecnológica haya tenido un impacto positivo en los clientes. Proporcionar detalles sobre cómo tu tecnología resolvió problemas y mejoró procesos.

- **Referencias de Clientes:** Presentar las referencias de clientes anteriores que puedan respaldar la calidad de los servicios y soluciones tecnológicas.

- **Cargos y Roles:** Presentar el organigrama, roles y responsabilidades.

- **Tecnologías y Herramientas Utilizadas:** Detallar las tecnologías, herramientas y enfoques utilizados en proyectos anteriores para mostrar su experiencia en el ámbito tecnológico.

- **Equipo y Experiencia del Personal:** En caso de contar con un equipo que cuente con experiencia relevante, mencione sus antecedentes y contribuciones a los proyectos anteriores.

- **Premios o Reconocimientos:** En caso de que su empresa cuente con premios o reconocimientos por su trabajo en proyectos tecnológicos, asegúrese de mencionarlos.

- **Evolución a lo Largo del Tiempo:** Si ha trabajado con clientes a largo plazo y ha evolucionado sus soluciones en el tiempo, esto puede demostrar la capacidad de adaptación y mejora continua.

### 3.2.4. INFRAESTRUCTURA TECNOLÓGICA

- Allegar la documentación y los soportes, identificando la infraestructura tecnológica requerida, para garantizar la continuidad de la prestación del servicio. Incluyendo las condiciones y niveles de servicio, la tipificación de los posibles incidentes de acuerdo la parte del proceso involucrada, estableciendo una clasificación por nivel de criticidad e indicando los tiempos de respuesta (máximo, mínimo y promedio) para solucionarlos.

- Contar con personal que cuenta con conocimientos tecnológicos en Arquitecturas SOA y/o Microservicios, para ello, el interesado en obtener la autorización como aliado tecnológico debe tener vinculado personal con título profesional avalado por instituciones educativas de grado superior autorizadas por autoridad competente en Colombia.

- Realizar satisfactoriamente las pruebas tecnológicas del software para la recolección de información que demuestren el adecuado funcionamiento de los servicios que presta como aliado tecnológico.

### 3.2.5. PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO

### 3.2.5.1. Analisis y Evaluaciones de Riesgos:

Identificar y abordar los riesgos específicos asociados a la solución tecnológica. A continuación, se presenta una estructura sugerida para este apartado, explicar cómo realiza evaluaciones regulares de riesgos de seguridad y cómo ajusta sus medidas en función de los resultados.

- **Matriz de riesgos:** Diligenciar la Matriz de Riesgos, la información debe ser clara, organizada y debe permitir una visualización rápida de los riesgos identificados, sus niveles de riesgo y las acciones propuestas para su mitigación. A continuación, la estructura sugerida para la matriz de riesgo:

| Matriz de Riesgo - Formato | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| N° | Riesgo | Probabilidad | Impacto | Exposición al Riesgo | Nivel de Riesgo | Medidas de Mitigación | Responsable de Mitigación | Estatus de Mitigación | Efectividad de Mitigación | Comentarios Adicionales | Prioridad de Acción |
| 1 | | | | | | | | | | | |
| 2 | | | | | | | | | | | |
| 3 | | | | | | | | | | | |
| 4 | | | | | | | | | | | |
| 5 | | | | | | | | | | | |

A continuación, se describen las columnas propuestas para el formato de la matriz de riesgos: ***N°;*** número de identificación único para cada riesgo. ***Riesgo;*** descripción concisa y clara del riesgo específico asociado con la solución. ***Probabilidad;*** estimación de la probabilidad de que el riesgo ocurra, utilizando la escala baja, media o alta. ***Impacto;*** evaluación del impacto potencial en caso de que el riesgo se materialice, utilizando la escala baja, media o alta. ***Exposición al Riesgo;*** resultado del cálculo de la exposición al riesgo multiplicando la probabilidad por el impacto. ***Nivel de Riesgo;*** clasificación del riesgo en categorías como bajo, moderado o alto según la exposición al riesgo. ***Medidas de Mitigación;*** descripción detallada de las estrategias y medidas para reducir la probabilidad y/o el impacto del riesgo. ***Responsable de Mitigación;*** persona o equipo asignado para implementar y monitorear las medidas de mitigación. ***Estatus de Mitigación;*** estado actual de la implementación de las medidas de mitigación (planificado, en progreso, completado). ***Efectividad de Mitigación;*** evaluación de la efectividad de las medidas de mitigación implementadas. ***Comentarios Adicionales;*** espacio para observaciones adicionales o detalles relevantes sobre cada riesgo y su mitigación. ***Prioridad de Acción;*** indicación de si se requiere una acción inmediata (alta prioridad) o si se puede abordar en etapas posteriores (baja prioridad).

### 3.2.5.2. Estrategia de respaldo de infraestructura tecnologica

- **Plan de Recuperacion de Desastres:** Entregar un Plan de Recuperación de Desastres donde se explique en detalle cual será su estrategia de respaldo y recuperación de la infraestructura tecnológica. Ofreciendo detalles sobre cómo se planificarán, implementarán y administrarán los procedimientos de respaldo.

Especifique:

- ***Tipos de Respaldo;*** enumerando los tipos de respaldo que se utilizarán, como respaldo completo, incremental, diferencial, entre otros.

- ***Frecuencia de Respaldo;*** definición de con qué frecuencia se realizarán los respaldos (diarios, semanales, mensuales, etc.). Justificación de la elección de la frecuencia en función de la criticidad de los datos y la capacidad de recuperación.

- ***Mecanismos de Respaldo;*** descripción de las herramientas y tecnologías que se utilizarán para llevar a cabo los respaldos, como software de respaldo, servicios en la nube, entre otras.

- **Ubicación de Almacenamiento de Respaldo;** indicación de dónde se almacenarán los respaldos, ya sea en dispositivos locales, servidores remotos o en la nube.

- **Seguridad de los Respaldos;** descripción de las medidas de seguridad que se implementarán para proteger los respaldos, como cifrado, autenticación y control de acceso.

- ***Roles y Responsabilidades;*** identificación de las personas o equipos responsables de ejecutar los procedimientos de respaldo. Asignación de responsabilidades claras en caso de una situación de contingencia.

- ***Actualización y Mantenimiento;*** explicación de cómo se mantendrá actualizada y revisada la estrategia de respaldo a medida que cambien los sistemas y las tecnologías.

- ***Documentación de Procedimientos;*** referencias a la documentación detallada de los procedimientos de respaldo, incluyendo instrucciones paso a paso.

Esta información deberá estar contenida en un documento que será actualizado por lo menos una vez cada año, y será implementado cada 6 meses en un ambiente controlado para verificar su efectividad, los resultados obtenidos deben ser entregados a la entidad en un informe.

- **Correccion de vulnerabilidades:** Detallar cómo mantendrá los sistemas actualizados con los últimos parches de seguridad y actualizaciones que permitan la corrección de las vulnerabilidades detectadas en la solución.

### 3.2.5.3. Plan de Contingencia

Entregar un Plan de Contingencia donde se describa en detalle cual será su estrategia de contingencia en caso de interrupciones en el servicios prestado. Ofreciendo detalles sobre cómo se planificarán, implementarán y administrarán los procedimientos de hacer efectivo el plan de contingencia.

Especifique:

- ***Procedimientos de Recuperación;*** explicación detallada de cómo se llevará a cabo la recuperación de la infraestructura a partir de los respaldos. Inclusión de pasos específicos para restaurar sistemas y datos en caso de una interrupción del servicio.

- ***Pruebas de Recuperación;*** detalle sobre cómo se llevarán a cabo las pruebas regulares de recuperación para verificar la efectividad de los procedimientos y los respaldos, en caso de contar previamente con esta información, o se han hecho procesos de recuperación anteriores, por favor aporte la evidencia.

- ***Roles y Responsabilidades;*** identificación de las personas o equipos responsables de ejecutar los procedimientos de recuperación. Asignación de responsabilidades claras en caso de una situación de contingencia.

- ***Procedimientos de Comunicación;*** descripción de cómo se notificará al personal y a las partes interesadas en caso de una situación de contingencia y cómo se coordinarán las acciones.

- ***Documentación de Procedimientos;*** referencias a la documentación detallada de los procedimientos de recuperación, incluyendo instrucciones paso a paso.

Esta información deberá estar contenida en un documento que será actualizado por lo menos una vez cada año, y será implementado cada 6 meses en un ambiente controlado para verificar su efectividad, los resultados obtenidos deben ser entregados a la entidad en un informe.

### 3.2.5.4. Mesa de Ayuda

El Aliado tecnológico debe garantizar la prestación del servicio a sus clientes, como mínimo debe contar con una mesa de ayuda que cuente con las siguientes características, detallándolas en el respectivo documento, características como:

- ***Modelo de Atención;*** descripción de Niveles de Atención, Cantidad de Personal, Flujo de Atención (Atención Inicial, Escalación y Resolución

Intermedia, Escalación a Especialistas o Supervisores, Revisión de Alta Gerencia).

- ***Metodología;*** *gestión de tickets* - plataforma de gestión de tickets para registrar, *acuerdo de niveles de servicios* - plataforma de gestión de tickets para registrar, asignar y dar seguimiento a todas las solicitudes.

- ***Multicanalidad;*** indicar cuales son los canales de atención.

- ***Automatización;*** indicar el nivel de automatización en el proceso para la asignación de incidencia, enrutamiento basado en palabras clave y respuestas automáticas.

- ***Base de Conocimientos;*** información accesible para los clientes y los agentes de soporte puede ayudar a resolver problemas comunes sin la necesidad de interactuar directamente con el equipo de soporte.

- ***Agentes Especializados;*** personal capacitado y especializado en las funcionalidades de la solución.

- ***Tiempos de Respuesta;*** indicar los tiempos de respuesta de acuerdo con la criticidad de las incidencias reportadas.

- ***Horarios;*** indicar disponibilidad en horarios que se adapten a las necesidades de los clientes.

- ***Monitoreo y Análisis;*** herramientas a utilizar para monitorizar el rendimiento y analizar métricas clave, como tiempo de respuesta, tiempo de resolución y satisfacción del cliente.

- ***Seguridad;*** procedimientos para la seguridad de los datos y la privacidad de los clientes, especialmente al comunicarse a través de canales virtuales.

#### 3.2.5.5. Requerimientos especiales

Los aspirantes a ser aliados tecnológicos clasificados como Organismos administradores del programa de seguridad en la operación del transporte (OAPSOT) deberán acreditar el cumplimiento de los lineamientos, instrucciones y demás disposiciones definidas por el Ministerio de Transporte en las resoluciones 2734 de 2018, 2222 de 2002, 4222 de 2002, circulares 20234000000837, 20244000000047, 20244000000127, así como la resolución 9597 de 2024 de la Superintendencia de Transporte y demás normativas vigentes.

### 3.3 ETAPA # 3 REVISIÓN SOLICITUD

La Superintendencia de Transporte en un periodo máximo de 30 días hábiles revisará e informará a través del Sistema Inteligente Nacional de Supervisión al

Transporte (SINST – VIGIA 2) el resultado de la validación, la cual podrá tener los siguientes resultados:

- **Estado Rechazada:** Motivo de no cumplimiento con las respectivas observaciones para ser validada y/o corregida y/o actualizada por parte del aspirante a ser aliado tecnológico.

- **Estado Aprobado**: Aceptada y fecha de reunión técnica. (sujeto a disponibilidad del equipo de profesionales de la Superintendencia de Transporte)

### 3.4 ETAPA # 4 REUNIÓN TÉCNICA

En periodo máximo de 30 días hábiles la Superintendencia de Transporte informará las consideraciones técnicas asociadas al consumo de los servicios web, estructura de datos, esquema de seguridad y demás aspectos técnicos. Asimismo, se entregarán las credenciales de seguridad, servicios web, parámetros de entrada y resultados esperados en ambiente de pruebas para el consumo de los servicios web y programación de la reunión técnica de evaluación del aplicativo.

### 3.5 ETAPA # 5 PRUEBAS EN AMBIENTE CONTROLADO

Los aspirantes a aliados tecnológicos en un periodo máximo de 30 días hábiles deberán realizar las validaciones y consumos de los servicios web del o los módulos al cual aspira a ser autorizado en el ambiente de pruebas de la Superintendencia de Transporte, así como preparar un informe denominado “plan de pruebas” el cual deberá contener como mínimo con los siguientes datos:

- Nombre y versión del aplicativo
- Nombres, apellidos, cargo, email y teléfono del líder técnico
- Modulo
- Caso de Uso
- Nombre del Servicio Web
- Fecha de la realización de pruebas
- Parámetros (Datos de entrada)
- Resultado obtenido

### 3.6 ETAPA # 6 EVALUACIÓN TÉCNICA EN AMBIENTE CONTROLADO

Los aspirantes a ser aliados tecnológicos deberán presentar el plan de pruebas y realizar las pruebas del aplicativo en conjunto con el equipo técnico de la Superintendencia de Transporte, la reunión técnica y el resultado de las pruebas serán grabadas y documentadas. El aspirante a aliados tecnológicos recibirá a través del Sistema Inteligente Nacional de Supervisión al Transporte (SINST – VIGIA 2) el resultado de la evaluación, la cual podrá tener los siguientes resultados:

- **Estado Rechazada Evaluación Técnica:** Motivo de no cumplimiento de la evaluación.

- **Estado Aprobado Evaluación Técnica**: Asignación de las credenciales de seguridad, URL de los servicios web, autorización por cada módulo, vigencia y aprobación para el consumo en ambiente productivo.

### 3.7 ETAPA # 7 PUESTA EN OPERACIÓN

La Superintendencia de Transporte publicará en su página web el listado de aliados tecnológicos con autorización vigente para realizar la interoperabilidad con el Sistema Inteligente Nacional de Supervisión al Transporte (SINST – VIGIA 2) a través de Servicios Web.

## 4. CONDICIONES DE AUTORIZACIÓN PARA LOS ALIADOS TECNOLÓGICOS

En desarrollo de lo dispuesto en el presente anexo técnico, los aliados tecnológicos con autorización vigente por la Superintendencia de Transporte deberán cumplir dentro de sus políticas y procedimientos las siguientes obligaciones:

- Disponer de la infraestructura tecnológica necesaria para los despliegues del aplicativo de software, así como de los procedimientos y controles requeridos que permitan la gestión de la información conforme con las condiciones derivadas de los criterios de seguridad de la información.

- Disponer de un equipo de mesa de ayuda que gestione las incidencias y errores al momento de consumir los servicios web por parte del aplicativo de software. (disponer como mínimo de canales de atención por correo electrónico, teléfono, plataforma para realizar reuniones virtuales y la definición de un responsable de mesa se ayuda)

- Al momento de consumir los servicios web por parte del aplicativo de software se debe garantizar que este se encuentre libre de software malicioso.

- Disponer y mantener en operación la infraestructura tecnológica y aspectos asociados (protocolos, servicios, aplicaciones, usuarios, equipos, entre otros) requeridos para el adecuado consumo de los servicios web.

- Utilizar e implementar de acuerdo con su capacidad e infraestructura las mejores prácticas sobre los estándares mínimos de seguridad dispuestos en la norma Colombiana NTC-ISO/IEC 27001. Para ello se sugiere, por ejemplo, mecanismos de monitoreo del consumo y disponibilidad del aplicativo de software que consumirá los servicios web.

- Disponer de planes de contingencia y continuidad debidamente documentados que garanticen la disponibilidad del servicio y la operación, los planes de contingencia y continuidad deben tener al menos los siguientes componentes:

    - **Análisis y evaluación de riesgos:** Mantener actualizada y documentada la solución tecnológica, así como los procesos que se consideran críticos para el funcionamiento de este sistema.

    - **Estrategia de respaldo de la infraestructura tecnológica:** definir diferentes alternativas y estrategias de respaldo de la infraestructura tecnológica en aras de garantizar la disponibilidad del servicio. Además, deberá corregir las vulnerabilidades detectadas en los procesos críticos identificadas en el análisis de riesgos.

    - **Plan de contingencia:** definir e implementar los procedimientos y planes de acción que permitan la ejecución del plan de contingencia.

        i. Cada 6 meses se deberá generar informe con los resultados obtenidos.
        ii. El plan de contingencia debe revisarse y actualizarse por lo menos una vez al año, verificando nuevos riesgos en la plataforma tecnológica que soporta el sistema y tomando las acciones necesarias que permitan la continuidad y disponibilidad de la operación.

- Mantener y suministrar sin ningún tipo de restricciones técnicas la información estadística de consumo de los servicios web, para tal fin deberá disponer como mínimo de los siguientes datos:

    - Código Operador (número único asignado por la Superintendencia de Transporte)
    - Tipo Identificación (Tipo identificación - sujetos obligados)
    - Número de Identificación (Sujetos obligados.)
    - Modulo
    - Fecha consumo servicio web (DD/MM/YYYY)
    - Parámetros entrada
    - Resultado

- Suministrar la estadística de consumo de los servicios web por parte aplicativo de software y deberá suministrar como mínimo con los siguientes datos:

    - Sujetos obligados
    - Modulo
    - Vigencia (año)

- Mes
- Número de consultas realizadas
- Número de consultas exitosas
- Número de consultas fallidas
- Tiempo de respuesta promedio.

- Informar y mantener debidamente actualizados, los procedimientos necesarios para atender de manera segura y eficiente a los sujetos obligados en todo momento, en particular cuando se presenten situaciones especiales tales como: fallas en los sistemas, restricciones en los servicios o mantenimientos programados, entre otros.

- Suministrar a los usuarios, información clara, completa y oportuna a las personas naturales y jurídicas vigiladas por la Superintendencia de Transporte.

- Garantizar la confidencialidad de la información y contar con políticas de seguridad.

- Contar con mecanismos que garanticen la trazabilidad de consumos de los servicios por parte aplicativo de software. (log de auditoria)

## 5. AUDITORIAS

El aplicativo de software será auditado al menos una vez al año una vez iniciada su operación, con el fin de verificar el cumplimiento de los aspectos relacionados con la prestación del servicio, la seguridad de la información y la confidencialidad. También se evaluará la continuidad de la autorización del aliado tecnológico.

Estas auditorías se realizarán conforme al cronograma que adopte la Superintendencia de Transporte, los costos directos e indirectos serán asumidos por el aliado tecnológico y la selección del auditor estará a cargo de la Superintendencia de Transporte.

## 6. APOYO TECNOLOGICO Y OPERATIVO

Los aliados tecnológicos con autorización vigente por la Superintendencia de Transporte deberán presentar informes de operación, mejoras operativas y avances tecnológicos, con el fin de fortalecer los procesos de vigilancia y control. Estos informes deberán presentarse en mesas técnicas que defina, convoque, lidere y coordine la Superintendencia de Transporte en el mes de junio y diciembre de cada año.

Adicionalmente, los aliados tecnológicos con autorización vigente por la Superintendencia de Transporte deberán disponer del personal técnico, operativo y

de apoyo en aras de brindar asistencia técnica y acompañamiento a la Superintendencia de Transporte en la implementación de mejoras, controles operativos, revisión documental y proyectos especiales, en el marco de la vigilancia y control. La Superintendencia será responsable de liderar, gestionar, coordinar, definir los planes de trabajo y realizar el seguimiento de estas actividades. Los costos directos e indirectos del apoyo técnico y operativo serán asumidos por el aliado tecnológico.