Monitorización de Comportamiento e ITS

Implicaciones Éticas y Legales de la IA
Máster en Inteligencia Artificial Aplicada

1. Análisis de Comportamiento

El análisis de comportamiento desempeña un papel crucial en la detección y respuesta a amenazas en el mundo de la ciberseguridad. En la era digital, las organizaciones, tanto públicas como privadas, manejan vastas cantidades de datos a diario. La identificación manual de amenazas en estos enormes volúmenes de información se ha vuelto prácticamente imposible. A su vez, los ciberataques modernos han evolucionado para emplear tácticas sigilosas y mantener un perfil bajo, lo que dificulta su detección mediante los métodos tradicionales de seguridad informática.
En respuesta a estos desafíos, la inteligencia artificial (IA) se ha convertido en una herramienta invaluable en la lucha contra las amenazas cibernéticas. En lugar de depender únicamente de la detección de acciones de malware conocidas, la IA se enfoca en identificar patrones de comportamiento anómalos. Esto permite la detección de amenazas previamente desconocidas o variantes de malware que podrían pasar desapercibidas por sistemas de seguridad basados en firmas.

1.1. Herramientas de Análisis de Comportamiento

En respuesta a esta necesidad, han surgido diversas herramientas y sistemas, tanto comerciales como de código abierto, que se especializan en el enfoque de detección de amenazas basado en el comportamiento. A continuación, se enumeran algunas de las herramientas más destacadas:

- Darktrace: Darktrace utiliza algoritmos de aprendizaje automático y técnicas de IA para detectar, responder y mitigar amenazas en tiempo real, basándose en patrones de comportamiento anómalo. Su "Enterprise Immune System" aprende y establece lo que podría considerarse como un "estado normal" en la red y detecta desviaciones de esta norma.

- Vectra: Vectra se especializa en la detección de amenazas en tiempo real utilizando IA. Se centra en detectar comportamientos maliciosos dentro del tráfico de red y proporciona una visión detallada de las cadenas de ataque en curso, lo que permite a los equipos de seguridad responder de manera ágil.

- CrowdStrike Falcon: CrowdStrike es conocida por sus soluciones de protección de endpoints. Su plataforma Falcon utiliza técnicas basadas en el comportamiento para detectar y prevenir amenazas que otros sistemas basados en firmas podrían pasar por alto.

- Cylance: CylancePROTECT es una solución de protección de endpoints que utiliza modelos de IA para identificar y bloquear malware basándose en sus características y comportamientos, en lugar de en firmas conocidas.

- Gurucul: Ofrece soluciones de Análisis de Comportamiento de Usuarios y Entidades (UEBA) que utilizan algoritmos de aprendizaje automático para detectar amenazas internas, fraudes y accesos no autorizados.

- Wazuh: Se trata de una plataforma de código abierto para la detección de amenazas, gestión de vulnerabilidades y monitorización de la integridad. Utiliza reglas y decodificadores para analizar eventos de seguridad y detectar comportamientos anómalos.

- Snort: Aunque es más conocido como un sistema de detección y prevención de intrusiones (IDPS), Snort ha evolucionado para incorporar capacidades basadas en comportamiento. La comunidad Snort desarrolla y comparte nuevas reglas que pueden detectar comportamientos anómalos.

- ELK Stack (Elasticsearch, Logstash, Kibana): Aunque ELK en sí misma no es una herramienta de detección basada en el comportamiento, se puede configurar con complementos y reglas específicas para realizar análisis de comportamiento de logs y eventos.

1.2. Aprendizaje Automático en el Análisis de Comportamiento

Los sistemas de IA que operan bajo el modelo de Aprendizaje Automático para el Análisis de Comportamiento se entrenan utilizando grandes conjuntos de datos que contienen tanto comportamientos legítimos como maliciosos. A través del aprendizaje supervisado, la IA puede aprender a clasificar y detectar actividad anómala. A medida que procesa más datos, estos sistemas mejoran su precisión mediante el aprendizaje no supervisado y el aprendizaje por refuerzo.

Algunas soluciones de ciberseguridad modernas han incorporado el aprendizaje automático en sus capacidades para mejorar la detección y respuesta ante amenazas. Estas herramientas utilizan el aprendizaje automático para aprender y adaptarse a nuevas amenazas estudiando patrones y comportamientos en los datos. A continuación, se mencionan algunas soluciones notables:

- Endgame: Esta plataforma utiliza el aprendizaje automático para la protección de endpoints, la detección de amenazas y la respuesta. Se enfoca en detectar técnicas y tácticas de ataque sin depender únicamente de firmas conocidas.

- PatternEx: Es una solución de Análisis de Comportamiento de Usuarios y Entidades (UEBA) que utiliza el aprendizaje automático. Analiza grandes volúmenes de datos para identificar patrones que sugieren actividades maliciosas.

- SentinelOne: Es una solución de protección de endpoints que utiliza el aprendizaje automático para detectar, clasificar y responder a comportamientos maliciosos y anómalos.

- Kaspersky Machine Learning for Anomaly Detection (MLAD): Diseñado para sistemas industriales, MLAD de Kaspersky utiliza el aprendizaje automático para detectar desviaciones en la operación de máquinas industriales.

- Splunk: Aunque Splunk es principalmente una herramienta de análisis de datos y SIEM (gestión de eventos e información de seguridad), tiene capacidades que permiten a los usuarios implementar modelos de aprendizaje automático para identificar patrones y anomalías en grandes volúmenes de datos.

2. Intelligent Transport Systems

Los ITS son un conjunto de tecnologías, aplicaciones y sistemas que se utilizan para mejorar la eficiencia, seguridad, calidad y sostenibilidad de los sistemas de transporte y la movilidad en general. Estos sistemas utilizan la información, la comunicación y la automatización para gestionar y optimizar el flujo de tráfico, la infraestructura de transporte y los servicios relacionados con el mismo.

2.1. Objetivos de los ITS

Los ITS tienen varios objetivos clave, que incluyen:

- Mejorar la seguridad vial, reduciendo accidentes y mitigando sus efectos.

- Optimizar la eficiencia del transporte, reduciendo la congestión del tráfico y mejorando los tiempos de viaje.

- Reducir el impacto ambiental al disminuir las emisiones de gases de efecto invernadero y mejorar la gestión del tráfico.

- Mejorar la calidad del servicio de transporte público y la experiencia del usuario.

- Facilitar la toma de decisiones informadas para conductores, operadores de transporte y autoridades.

2.2. Coches conectados

Hay tres niveles de conectividad en vehículos:

- Telemática: la telemática se refiere a la capacidad de un vehículo para comunicarse de manera remota, recopilar datos y compartir información a través de una conexión en línea. Los sistemas de telemática en un vehículo pueden recopilar información sobre el rendimiento del vehículo, la ubicación, las condiciones del tráfico, el estado del motor y otros datos relevantes. Esta información se puede transmitir a una plataforma en la nube para su análisis y procesamiento, lo que permite a los fabricantes de automóviles y a los propietarios de flotas realizar un seguimiento del rendimiento y programar el mantenimiento de manera más eficiente. Los servicios de telemática también pueden incluir funciones de asistencia en carretera, seguimiento de vehículos robados, actualizaciones de software a través de la nube y más.

- Vehículo a Todo (V2X): vehículo a Todo (V2X) se refiere a la comunicación entre vehículos (V2V) y la comunicación entre vehículos e infraestructura (V2I). La comunicación V2V permite que los vehículos se comuniquen entre sí para intercambiar información importante, como la velocidad, la posición, las condiciones del tráfico y las advertencias de seguridad. La comunicación V2I implica la interacción entre vehículos y la infraestructura de tráfico, como semáforos, señales de tráfico y sistemas de gestión del tráfico. Esto puede mejorar la seguridad y la eficiencia del tráfico. V2X también puede incluir la comunicación entre vehículos y peatones (V2P) y otros elementos del entorno (V2E), como edificios y dispositivos IoT (Internet de las cosas) en las ciudades inteligentes.

- Infoentretenimiento en el Vehículo: la conectividad para infoentretenimiento en el vehículo se refiere a la capacidad de un automóvil para proporcionar acceso a servicios y contenido en línea dentro del vehículo. Esto incluye funciones como la reproducción de música en streaming, navegación basada en Internet, acceso a aplicaciones de redes sociales, contenido multimedia y más. Los sistemas de infoentretenimiento en el vehículo pueden estar equipados con interfaces de usuario avanzadas, pantallas táctiles, comandos de voz y pueden sincronizarse con dispositivos móviles a través de Bluetooth o tecnologías similares. Los vehículos modernos suelen ofrecer una variedad de aplicaciones y servicios conectados que mejoran la experiencia del conductor y los pasajeros, al proporcionar entretenimiento, información y conectividad en tiempo real.

2.3. Coches autónomos

Un coche autónomo, también conocido como vehículo autónomo o vehículo sin conductor, es un tipo de vehículo que tiene la capacidad de desplazarse de manera automatizada sin la necesidad de intervención humana constante. Estos vehículos utilizan una combinación de sensores, cámaras, radares, sistemas de procesamiento de datos, inteligencia artificial y algoritmos para percibir su entorno, tomar decisiones de conducción y controlar todas las funciones necesarias para operar de manera segura. Los coches autónomos se diseñan para mejorar la seguridad vial, reducir la congestión del tráfico y proporcionar una experiencia de conducción más eficiente y cómoda.

A continuación, se describen las áreas de control y sistemas involucrados en un coche autónomo:

- Control de Tren Motriz: este sistema controla la propulsión del vehículo, la velocidad y el frenado. En un coche autónomo, el control del tren motriz puede ajustarse automáticamente para adaptarse a las condiciones del tráfico y al estado de la carretera. Los sistemas de tren motriz eléctrico o híbrido son comunes en vehículos autónomos para lograr una mayor eficiencia energética.

- Control del Chasis: el control del chasis incluye la gestión de la dirección, la suspensión y otros sistemas relacionados con la estabilidad del vehículo. Los vehículos autónomos pueden ajustar la dirección y la suspensión de manera dinámica para mantener una conducción suave y segura.

- Control por los Usuarios: los sistemas de control por los usuarios permiten a los pasajeros o conductores interactuar con el vehículo a través de interfaces de usuario. Esto puede incluir la entrada de destinos en sistemas de navegación, la configuración de preferencias de confort y el acceso a funciones de seguridad.

- Control de Entretenimiento a Bordo/Información: este sistema ofrece entretenimiento y acceso a información para los ocupantes del vehículo. Puede incluir pantallas táctiles, sistemas de audio, conexión a Internet y aplicaciones que brindan música, películas, noticias y más. Los sistemas de infoentretenimiento también pueden integrar la navegación en tiempo real y la información sobre el tráfico.

- Control de Comunicaciones: los vehículos autónomos se conectan a través de redes inalámbricas para comunicarse con otros vehículos (V2V) y con la infraestructura de tráfico (V2I). Esto permite compartir información importante, como señales de tráfico, alertas de seguridad y actualizaciones de tráfico en tiempo real.

- Sistemas de Diagnóstico y Mantenimiento: llos vehículos autónomos pueden incorporar sistemas de diagnóstico avanzados que monitorean el estado del vehículo y los componentes en tiempo real. Esto permite identificar y abordar problemas de mantenimiento antes de que se conviertan en problemas graves, mejorando la confiabilidad y la seguridad.

2.4. Niveles de automatización según la SAE (Sociedad de Ingenieros Automotrices)

La Sociedad de Ingenieros Automotrices (SAE) ha establecido una clasificación de los niveles de automatización de los vehículos que se conoce comúnmente como "Niveles de Automatización SAE". Esta clasificación describe el grado de automatización de un vehículo, desde vehículos con cero automatización (donde el conductor es responsable de todas las tareas de conducción) hasta vehículos completamente autónomos que no requieren intervención humana en ninguna circunstancia. Los cinco niveles establecidos son:

- Nivel 0: Sin Automatización (No Automatizado)

  En este nivel, el conductor es responsable de todas las tareas de conducción. No hay asistencia automática en la conducción, y el vehículo no cuenta con sistemas avanzados de asistencia al conductor.

- Nivel 1: Asistencia al Conductor

  En este nivel, el vehículo puede asistir al conductor en ciertas tareas, como el control de velocidad o la dirección, pero el conductor debe supervisar activamente la conducción. Algunos ejemplos de sistemas de Nivel 1 incluyen el control de crucero adaptativo y la asistencia en la dirección.

- Nivel 2: Automatización Parcial

El vehículo es capaz de realizar ciertas tareas de conducción, como la aceleración, la frenada y la dirección, pero el conductor debe permanecer alerta y supervisar el entorno. Aunque el vehículo asume más responsabilidad en la conducción, el conductor debe estar preparado para intervenir en cualquier momento. Ejemplos de sistemas de Nivel 2 incluyen algunas implementaciones avanzadas de control de crucero adaptativo y sistemas de asistencia al estacionamiento.

- Nivel 3: Automatización Condicional

  En el Nivel 3, el vehículo puede realizar la mayoría de las tareas de conducción en circunstancias normales, pero el conductor debe estar listo para intervenir si es necesario. El conductor puede distraerse mientras el vehículo controla la conducción, pero se espera que retome el control si se le solicita. El nivel 3 permite una "conducción autónoma" limitada en ciertas situaciones.

- Nivel 4: Automatización Alta

  En este nivel, el vehículo es capaz de operar de forma autónoma en la mayoría de las condiciones y circunstancias, pero puede requerir que el conductor tome el control en situaciones excepcionales o en áreas específicas. El conductor no necesita supervisar constantemente la conducción, pero el vehículo tiene limitaciones geográficas o situacionales. El nivel 4 permite un alto grado de automatización, pero no es completamente autónomo en todas las circunstancias.

- Nivel 5: Automatización Completa

  En el Nivel 5, el vehículo es completamente autónomo y no requiere la presencia de un conductor humano. Puede operar en todas las condiciones y en cualquier lugar sin restricciones geográficas o situacionales. En este nivel, no hay necesidad de un volante, pedales ni controles para el conductor, ya que el vehículo se encarga de todas las tareas de conducción.

Es importante destacar que la mayoría de los vehículos autónomos en desarrollo actualmente se encuentran en los niveles 2 o 3, con un despliegue limitado de sistemas de nivel 4 en ciertos entornos controlados. La consecución de vehículos de nivel 5 completamente autónomos sigue siendo un objetivo a largo plazo que requiere superar numerosos desafíos técnicos, de seguridad y regulatorios.

2.5. Tipos de usuarios contemplados por el estándar

El estándar se refiere a cuatro tipos de usuarios que son relevantes en el contexto de vehículos autónomos y sistemas de conducción automatizada:

- Conductor: este es el usuario que realiza en tiempo real las tareas de la conducción dinámica, ya sea en su totalidad o en parte. En el caso de un vehículo autónomo, el conductor puede ser una persona que está presente en el vehículo pero no está realizando activamente tareas de conducción, ya que el vehículo se encarga de la

mayoría de las funciones de conducción. También puede referirse a un "conductor remoto" que controla el vehículo de forma remota, como en el caso de sistemas de conducción autónoma a distancia.

- Pasajero: este tipo de usuario es alguien que se encuentra en el vehículo, pero no tiene ningún papel en la operación del mismo. El pasajero es un observador o viajero en el vehículo y no interviene en las decisiones de conducción ni en el control del vehículo.

- Usuario preparado para Intervenir: este usuario asume la tarea de respaldo durante la conducción autónoma. Aunque el vehículo puede estar operando de manera autónoma en ciertas circunstancias, se espera que el usuario preparado para intervenir esté listo para asumir la conducción en cualquier momento. Esta persona debe estar atenta y lista para tomar el control si surge una situación inesperada o problemática.

- Gestor, Preparador o "Despachador" del Vehículo: este usuario se encarga de verificar que el sistema de conducción automatizada esté disponible y en condiciones correctas para funcionar. Es responsable de la preparación del vehículo antes de la operación autónoma, garantizando que todos los sistemas estén funcionando adecuadamente y que el vehículo cumpla con los requisitos de seguridad. El gestor también puede ser responsable de configurar rutas, horarios y otros aspectos logísticos de la operación del vehículo autónomo.

Estos tipos de usuarios son importantes para comprender cómo se implementan y operan los vehículos autónomos y los sistemas de conducción automatizada. Cada tipo de usuario tiene un papel específico en la interacción con el vehículo y puede ser relevante en diferentes etapas de la operación, desde la preparación hasta la intervención en situaciones críticas. La consideración de estos usuarios es esencial para garantizar una operación segura y eficiente de los vehículos autónomos.

2.6. Peligros de la automatización de vehículos

Los peligros de la automatización de vehículos pueden agruparse en varias categorías:

- Pérdida de activos de IT

    - Pérdida de información en la nube: la automatización de vehículos puede depender de sistemas de almacenamiento en la nube para el acceso a datos y actualizaciones. La pérdida de información en la nube puede ser perjudicial.

    - Pérdida de integridad de información sensible: si la información sensible se ve comprometida o alterada, podría tener graves consecuencias en la seguridad de los vehículos y la privacidad de los usuarios.

    - Daños causados por terceros: la presencia de vehículos automatizados podría atraer a hackers y actores maliciosos que intenten dañar o tomar el control de estos sistemas.

    - Conflictos de registros digitales (DRM): la gestión de derechos digitales (DRM) es importante para proteger la propiedad intelectual. Los conflictos en los registros DRM pueden llevar a problemas legales y de seguridad.

    - Filtración de información: la fuga de información puede exponer datos confidenciales o secretos comerciales a personas no autorizadas.

- Amenazas físicas

    - Inyección de fallas/glitching: los atacantes pueden intentar inyectar fallas o glitches en los sistemas de vehículos automatizados para causar mal funcionamiento o incluso accidentes.

    - Canal lateral: los ataques de canal lateral se refieren a la obtención de información a través de canales secundarios, como la radiación electromagnética emitida por dispositivos electrónicos.

    - Acceso a puertos de depuración de hardware (HW): si los puertos de depuración de hardware no están adecuadamente protegidos, podrían permitir el acceso no autorizado a sistemas críticos.

- Actividad maliciosa/abuso

    - Negación de servicio: los ataques de denegación de servicio pueden paralizar la operación de vehículos automatizados, lo que podría ser peligroso en situaciones de tráfico.

    - Actividad maliciosa de código/software: el malware dirigido a sistemas de vehículos automatizados puede causar daños, robo de datos o control no autorizado.

    - Manipulación de hardware y software: la manipulación de componentes o software de vehículos automatizados puede poner en riesgo la seguridad.

    - Manipulación de información: cambiar información en tiempo real, como señales de tráfico, puede llevar a accidentes.

    - Acceso no autorizado a sistemas/red de información: obtener acceso no autorizado a sistemas de vehículos automatizados puede permitir el control malicioso.

    - Compromiso de información confidencial: la exposición de información confidencial puede dañar la seguridad y la privacidad de los usuarios.

    - Fraude de identidad: el robo de identidad puede llevar a la autorización no deseada y al acceso a sistemas.

    - Abuso de información almacenada: el uso indebido de información almacenada en vehículos automatizados puede tener implicaciones de privacidad.

    - Uso no autorizado de administración de dispositivos y sistemas: si se abusa de los privilegios de administración, se pueden tomar medidas perjudiciales.

    - Uso no autorizado de software: la ejecución de software no autorizado puede tener consecuencias peligrosas.

    - Abuso de autorización: utilizar autorizaciones de manera indebida puede llevar a comportamientos maliciosos.

    - Software malicioso: la presencia de malware puede comprometer la seguridad y el funcionamiento de los vehículos automatizados.

    - Actividad remota (ejecución): los ataques remotos pueden controlar vehículos automatizados sin autorización.

- Fallas/malfunciones

    - Fallas/malfunciones de dispositivos o sistemas: las fallas en componentes críticos pueden llevar a accidentes o mal funcionamiento.

    - Fallas/disrupciones en el suministro de energía: la pérdida de energía puede dejar los sistemas inoperables.

    - Errores de software: los errores de programación pueden causar comportamientos inesperados o peligrosos.

    - Fallas/malfunciones de partes de dispositivos: incluso pequeñas fallas en componentes pueden tener consecuencias importantes.

    - Fallas/disrupciones en enlaces de comunicación: la pérdida de comunicación puede dificultar la toma de decisiones seguras.

    - Fallas/disrupciones en la fuente de alimentación principal: la falta de energía puede detener completamente la operación de los vehículos.

- Interrupción de red

    - Apagón de red: la interrupción de la red puede afectar la comunicación y la operación de los vehículos automatizados.

- Daños no intencionales (accidentales)

    - Filtración o compartición de información: la divulgación no intencionada de datos puede comprometer la seguridad.

    - Administración errónea de dispositivos y sistemas: los errores humanos pueden causar problemas en la operación.

    - Uso de información de una fuente no confiable: la toma de decisiones basada en información inexacta puede ser peligrosa.

    - Cambio no intencionado de datos en un sistema de información: errores en la entrada de datos o en el software pueden tener consecuencias no deseadas.

    - Diseño y planificación inadecuados o falta de adaptación: la falta de planificación puede llevar a problemas de seguridad y eficiencia.

- Amenazas avanzadas persistentes

    - Escucha/Espionaje/Secuestro: los actores persistentes avanzados pueden espiar y secuestrar comunicaciones y sistemas.

2.7. Buenas prácticas

Estas prácticas son esenciales para garantizar la seguridad, la conformidad con la regulación y la gestión de riesgos en la implementación de sistemas de IA y monitorización de comportamiento.

- Política y estándares (adherencia a la regulación / responsabilidad): Es esencial establecer políticas y estándares que se adhieran a la regulación vigente y definan claramente las responsabilidades en la monitorización de comportamiento y el uso de IA.

- Medidas organizativas generales (equipo de seguridad + SGSI): Formar un equipo de seguridad competente y establecer un Sistema de Gestión de Seguridad de la Información (SGSI) que garantice la integridad y confidencialidad de los datos.

- Medidas organizativas de desarrollo seguro: Integrar prácticas de desarrollo seguro desde el inicio del proceso de diseño e implementación de sistemas de IA y monitorización de comportamiento.

- Medidas organizativas de seguridad durante todo el ciclo de vida: Considerar la seguridad en todas las etapas del ciclo de vida de los sistemas, desde la concepción hasta el retiro.

- Medidas técnicas: Implementar medidas técnicas sólidas para proteger los datos y los sistemas, como firewalls, sistemas de detección de intrusiones y cifrado de datos.

- Auditoría de seguridad: Realizar auditorías periódicas para evaluar la efectividad de las medidas de seguridad implementadas y garantizar el cumplimiento de los estándares.

- Protección de las comunicaciones: Asegurar que las comunicaciones entre los sistemas estén protegidas contra intrusiones y accesos no autorizados.

- Criptografía: Utilizar la criptografía para proteger datos confidenciales y garantizar la privacidad de los usuarios.

- Protección de datos del usuario: Cumplir con las leyes de protección de datos y garantizar que la información del usuario se maneje de manera segura y ética.

- Identificación, autenticación y autorización: Implementar sistemas de identificación sólidos, autenticación segura y autorización adecuada para controlar el acceso a los sistemas y datos.

2.8. RIS (River Information Services)

Los "Servicios de Información para la Navegación Interior" (RIS, por sus siglas en inglés) son un concepto en el que los servicios de información en la navegación fluvial respaldan la gestión del tráfico y el transporte en la navegación interior, incluyendo interfaces con otros modos de transporte. La Directiva 2005/44/CE sobre servicios armonizados de información fluvial en las vías navegables interiores de la Unión Europea (en adelante, referida como la Directiva RIS) requiere que los Estados miembros implementen los RIS de acuerdo con ciertos estándares. Se espera que los RIS mejoren la seguridad, la eficiencia y la amigabilidad ambiental de la navegación interior. La Unión Europea ha adoptado un enfoque global que abarca el desarrollo de políticas, un marco legal, apoyo a la investigación y desarrollo, y el seguimiento de la implementación de la legislación.

La Directiva RIS se refiere a cuatro tecnologías clave: el Sistema Electrónico de Visualización e Información de Cartas Fluviales Interiores (Inland ECDIS), Avisos a los Navegantes (NtS), Identificación Automática de Buques en Navegación Interior (AIS) y Reporte Electrónico Internacional (ERI). Estas tecnologías se basan en estándares técnicos y operativos que fueron inicialmente definidos y son continuamente actualizados por Grupos de Expertos en RIS. La Directiva RIS exige a los Estados miembros implementar los RIS de acuerdo con estos estándares. Una contribución importante al proceso de estandarización ha sido la adopción por parte de la Comisión Europea de regulaciones técnicas para Inland ECDIS, Avisos a los Navegantes (NtS), Seguimiento y Rastreo de Buques (VTT) y Reporte Electrónico Internacional (ERI).

La estandarización y su armonización en los países europeos tienen como objetivo cumplir mejor los objetivos de los RIS de la siguiente manera:

1. Mejora de la seguridad en puertos y ríos interiores.

2. Mejorar la eficiencia de la navegación interior: optimizar la gestión de recursos de la cadena de transporte acuático permitiendo el intercambio de información entre buques, esclusas, puentes, terminales y puertos.

3. Uso mejor y más eficaz de la infraestructura de vías navegables interiores: proporcionando información sobre el estado de las vías navegables.

4. Protección del medio ambiente: proporcionar información sobre tráfico y transporte para un proceso eficiente de reducción de calamidades.

5. Mejor integración del transporte por vías navegables interiores en las cadenas de suministro multimodales a través de información precisa y oportuna para apoyar la gestión del transporte.

Los servicios incluidos en el concepto de RIS son, por ejemplo:

- Información sobre calles para planificar, ejecutar y monitorear viajes por parte de capitanes de embarcaciones y administradores de flotas, que incluye datos geográficos, hidrológicos, meteorológicos y relacionados con el tráfico.

- Servicios de información de tráfico que proporcionan información sobre las posiciones de los buques para permitir la planificación táctica o estratégica.

- La gestión del tráfico, que tiene como objetivo optimizar el uso de la infraestructura y facilitar la navegación segura, especialmente en centros RIS, así como en esclusas y puentes.

- Servicios de reducción de calamidades (CAS) que registran los buques y sus datos de transporte al comienzo de un viaje y actualizan los datos durante el viaje para proporcionar información inmediata en caso de accidentes.

- Información para la gestión del transporte, que incluye tiempos estimados de llegada (ETA) proporcionados por capitanes de embarcaciones y administradores de flotas basados en información de calles, así como información sobre la gestión de carga y flota.

- Estadísticas y servicios aduaneros: el RIS mejora y facilita la recopilación de datos estadísticos sobre las vías navegables interiores en los Estados miembros.

- Tasas navegables y tasas portuarias: los datos de viaje de los barcos se pueden utilizar para calcular automáticamente las tarifas e iniciar el proceso de facturación.