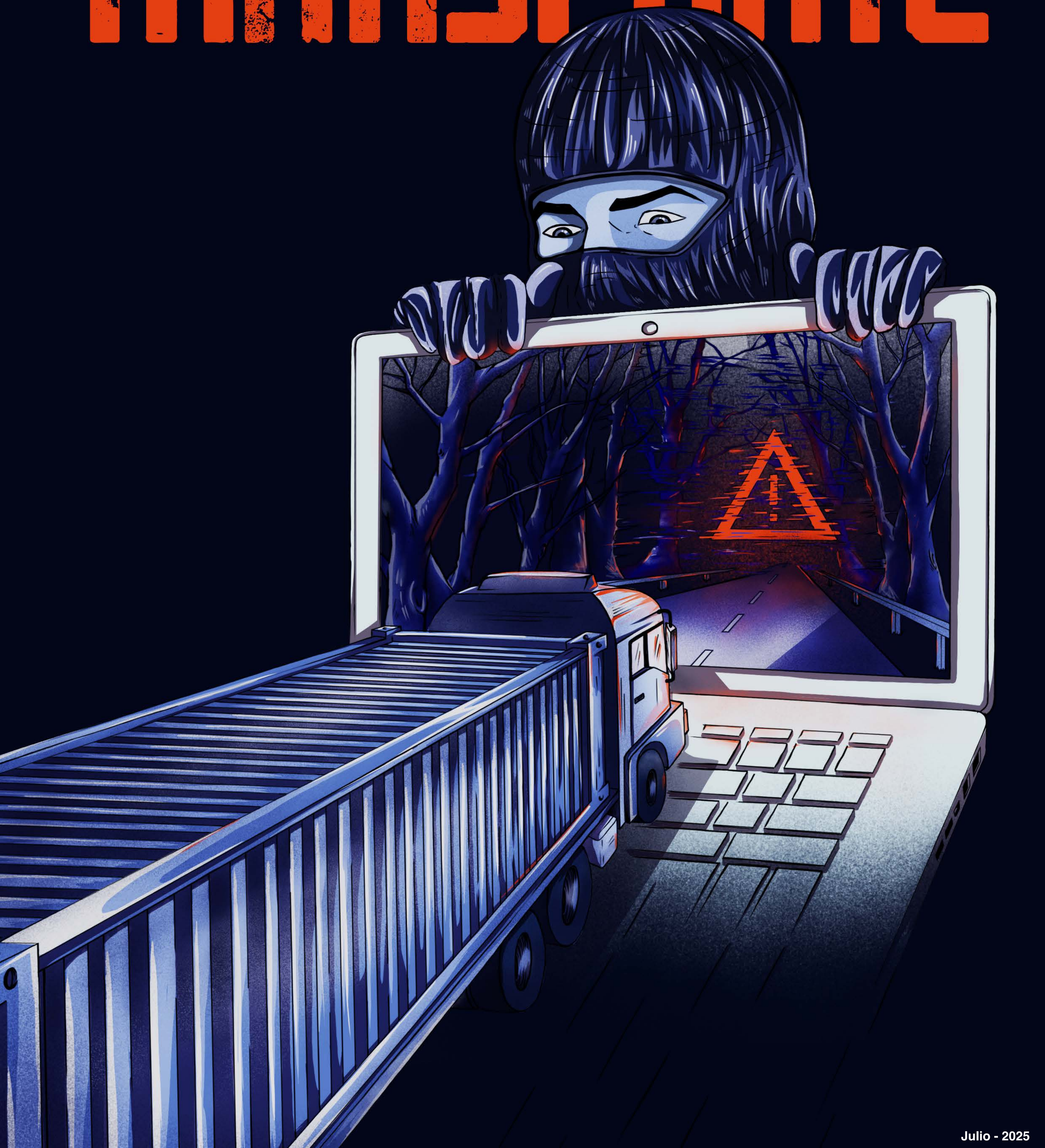
KERBEROS
MANAGING GENERAL AGENCY

ATAQUES AL SECTOR
TRANSPORTE



Julio - 2025

Ciberseguridad en el Sector Transporte

Avances, Riesgos y Amenazas Emergentes

La digitalización y automatización de procesos han transformado radicalmente al sector transporte, posicionando a las tecnologías de la información (TI) y las tecnologías operativas (TO) como ejes fundamentales de su evolución. Desde la gestión de flotas en tiempo real hasta la operación de terminales automatizadas, la convergencia tecnológica ha potenciado la eficiencia, la trazabilidad y la experiencia del usuario. Sin embargo, este progreso también ha ampliado exponencialmente la superficie de ataque, exponiendo a las organizaciones a riesgos cibernéticos cada vez más sofisticados y disruptivos.

Transformación Digital del Sector Transporte

En las últimas décadas, múltiples avances han impulsado una escalabilidad sostenida en las operaciones logísticas, de carga y transporte de pasajeros:

Tecnificación de procesos

El uso de herramientas para almacenar, procesar y consolidar grandes volúmenes de datos ha generado eficiencias clave en la cadena operativa, permitiendo una toma de decisiones más ágil y precisa.

Integración de nuevas tecnologías

Soluciones como inteligencia artificial, IoT, blockchain o sistemas autónomos se han convertido en piezas clave de la infraestructura del sector. No obstante, muchas organizaciones priorizan la productividad y rentabilidad, dejando la seguridad como un componente secundario.

Interconexión entre múltiples actores

La interoperabilidad entre compañías, proveedores y clientes ha permitido superar barreras geográficas y operativas, facilitando ecosistemas complejos de información, pero también generando múltiples puntos vulnerables de acceso para los atacantes.y rentabilidad, dejando la seguridad como un componente secundario.

Nuevas Vulnerabilidades y Riesgos Emergentes

La evolución de las tecnologías ha sido acompañada de una sofisticación proporcional en los riesgos cibernéticos. El informe de amenazas 2024 de ENISA posiciona al transporte como el segundo sector más atacado de Europa, superando a banca y finanzas, y sólo por detrás del sector público. Los ciberataques en este sector pueden generar disrupciones críticas con consecuencias financieras, operativas y reputacionales de gran magnitud.

Entre los principales riesgos que enfrenta el sector, destacan:

Protección y privacidad de los datos

El sector gestiona volúmenes masivos de datos sensibles y personales. Una fuga de esta información no solo puede implicar sanciones regulatorias, sino también demandas de terceros y pérdida de confianza.

Interrupción de operaciones

Los ataques a infraestructuras críticas, como sistemas de rastreo o logística, pueden paralizar por completo las operaciones. Las consecuencias incluyen pérdidas económicas directas, gastos en recuperación, y afectación de la continuidad del negocio.

Impacto reputacional

Los incidentes de ciberseguridad afectan la percepción del cliente. Una organización vulnerable puede perder usuarios frente a competidores más confiables, incluso si estos no cuentan con diferencias sustanciales en la oferta de valor.

Uso de tecnologías obsoletas (EOL):

La dependencia de sistemas sin soporte del fabricante incrementa la exposición. Esto exige la implementación de medidas compensatorias robustas y el diseño de planes de migración tecnológica.

Dependencia de terceros

La subcontratación de servicios tecnológicos o logísticos introduce riesgos adicionales. Una vulnerabilidad en un proveedor puede escalar rápidamente a toda la cadena, generando un efecto dominó.

Incidentes Relevantes a Nivel Global

Diversos ciberataques recientes han evidenciado la fragilidad del sector transporte ante amenazas digitales:

2025 — **Miatech (EE.UU.)**

Empresa de soluciones tecnológicas para aviación, afectada por exfiltración de datos sensibles de pasajeros.

2023 — **Puertos de Santos (Brasil)**

Ataque de ransomware atribuido a LockBit paralizó el agendamiento de contenedores por más de 36 horas.

2023 — **Puerto de Nagoya (Japón)**

Ransomware detuvo operaciones por varios días, generando pérdidas significativas.

2023 — **KNP Logistic (Canadá)**

Compromiso de sistemas críticos por falta de MFA. La compañía quebró meses después.

2023 — **DP World (Australia)**

Exploit sobre Citrix Bleed detuvo la operación portuaria, afectando 30.000 contenedores y robando datos de empleados.

2022 — **Servientrega (Colombia)**

Ciberataque con robo de credenciales sin MFA, cifrado de CRM y paralización de operaciones por 48 horas.

Estos casos evidencian un patrón común: interrupciones críticas del negocio y exposición masiva de datos personales, afectando no solo a las empresas atacadas, sino también a todo su ecosistema de clientes, aliados e inversionistas.

Conclusión:
Una Prioridad Estratégica

El transporte, columna vertebral del comercio global, se ha convertido en un objetivo prioritario para los cibercriminales, tanto con fines económicos como políticos. La creciente dependencia de tecnologías interconectadas ha traído eficiencia, pero también ha creado complejidades de seguridad difíciles de gestionar sin una estrategia integral.

El **costo promedio de una violación de datos en este sector supera los USD 4,4 millones** según el Cost of a Data Breach Report 2024 de IBM. Ante este panorama, se vuelve urgente implementar políticas robustas de ciberseguridad, fortalecer la gobernanza de la información, garantizar la ciberresiliencia operativa y evaluar permanentemente la exposición ante terceros.

Las organizaciones del sector transporte deben pasar de una postura reactiva a una proactiva, donde la ciberseguridad sea un pilar estratégico del negocio y no una preocupación secundaria tras un incidente. La prevención, la capacitación y la inversión en protección digital ya no son opcionales: son una condición para operar en un entorno globalizado, complejo e interdependiente.

KERBEROS

MANAGING GENERAL AGENCY

www.kerberosre.io