



Fraudes y prevención

Volumen II: Fraudes virtuales



Tabla de contenidos

Introducción	3
Tipos de Fraude	4
Phishing, skimming y email hacking	5
Suplantación de transportistas	7
Suplantación de intermediarios o fake brokers	8
Fraude en plataformas digitales de carga	9
Fraude documental (CMR, albaranes, licencias, seguros)	10
Empresas logísticas ficticias	11
Fraude en facturación o pagos	12
Protocolo transversal de prevención	13
Soluciones Eurowag	14
Conclusión	17





Introducción

El fraude virtual se ha convertido en una amenaza creciente para el transporte y la logística. La suplantación de identidades, la manipulación de correos y documentos, las empresas ficticias, el acceso no autorizado a sistemas y el fraude en pagos pueden utilizarse para desviar mercancías, obtener información sensible o provocar pérdidas económicas.

Estas modalidades suelen combinar herramientas digitales con fallos en los procesos de contratación, recogida, tránsito, entrega y facturación. Por ello, la protección efectiva no depende únicamente de una solución tecnológica, sino de aplicar controles de verificación escalonados, mantener canales de comunicación seguros y formar a las personas implicadas en cada fase de la operación.

Esta segunda guía de Eurowag desarrolla las principales modalidades de fraude virtual que afectan al transporte de mercancías por carretera en España y Europa. Para cada una se ofrecen medidas preventivas, protocolos de actuación y recomendaciones prácticas destinadas a facilitar su detección y reducir su impacto. Complementa así la primera guía dedicada al fraude físico y aporta una visión más completa de los riesgos que afectan actualmente a la cadena logística.

Este documento desarrolla, uno a uno, los fraudes más relevantes en el mercado español y europeo del transporte por carretera, y ofrece orientación operativa para prevenir, detectar y escalar incidencias.

¿Para quién es esta guía?

- Cargadores
- Conductores
- Operadores logísticos
- Departamentos de tráfico
- Compras y contratación
- Seguridad corporativa
- Dirección de operaciones

Tipos de fraude

La siguiente clasificación recoge los casos de fraude desarrollados en esta guía y los separa por el medio principal de ejecución. En la práctica, muchas bandas mezclan ambos planos – digital y físico – dentro de una misma operación, pero esta división ayuda a ordenar riesgos, controles y protocolos de prevención.

Fraudes físicos

- Uso no autorizado de tarjetas de combustible
- Robo de combustible
- Robo organizado de carga
- Recogida fraudulenta de mercancía
- Desvío presencial de la entrega
- Falsos controles o falsa autoridad
- Suplantación física del conductor o empleado
- Fraude mediante subcontratación encadenada

Fraudes virtuales

- Suplantación de transportistas
- Suplantación de intermediarios o fake brokers
- Fraude en plataformas digitales de carga
- Ciberdelincuencia logística y email hacking
- Fraude documental
- Empresas logísticas ficticias
- Fraude en facturación o pagos



1. Phishing, skimming y email hacking

En qué consiste

El phishing (suplantación de identidad), skimming (clonación de tarjetas) y email hacking (hacking de correo electrónico) son distintas modalidades de ciberdelitos y fraudes diseñados para robar información confidencial, credenciales de acceso o dinero. Aunque todos buscan comprometer tu seguridad, operan de formas muy diferentes.

El **phishing** utiliza correos, mensajes o llamadas falsas que imitan a entidades de confianza para obtener contraseñas, datos bancarios o instalar malware. El **skimming** roba datos de tarjetas mediante dispositivos ocultos en cajeros o terminales, o mediante ataques a tiendas online. El **email hacking** consiste en acceder sin autorización a una cuenta de correo para robar información, cambiar contraseñas, suplantar al usuario o estafar a sus contactos.

Medidas preventivas

- 1 Implantar autenticación multifactor (MFA) en correo y accesos sensibles, limitando los permisos al personal autorizado. (Phishing / email hacking).
- 2 Establecer doble validación humana para cambios de destino, receptor, horarios, pagos o datos bancarios. (Phishing / email hacking).
- 3 Verificar por un segundo canal cualquier instrucción sensible recibida por correo, SMS o teléfono. (Phishing / email hacking).
- 4 Formar al personal para identificar phishing, spoofing, suplantación de identidad e ingeniería social.
- 5 Reducir la exposición pública de rutas, horarios, contactos y datos operativos sensibles. (Phishing / email hacking).
- 6 Aplicar límites de gasto y alertas ante operaciones anómalas. (Skimming).
- 7 Proteger el PIN y revisar cajeros, surtidores y terminales ante posibles signos de manipulación. (Skimming).
- 8 Monitorizar las operaciones de combustible y contrastarlas, cuando sea posible, con la ruta o ubicación del vehículo. (Skimming).
- 9 No ejecutar cambios críticos basándose únicamente en un correo o mensaje, aunque parezca legítimo. (Phishing / email hacking).



Check list

- ✓ Revisar el dominio exacto del remitente. (Phishing / email hacking).
- ✓ Desconfiar de urgencias, amenazas, errores de estilo o cambios de última hora. (Phishing / email hacking).
- ✓ No abrir enlaces o archivos adjuntos sospechosos. (Phishing).
- ✓ Verificar firmas, teléfonos, IBAN y documentos antes de actuar. (Phishing / email hacking).
- ✓ Confirmar por un segundo canal cualquier cambio de destino, receptor, horario o pago. (Phishing / email hacking).
- ✓ Revisar terminales y proteger el PIN antes de utilizar la tarjeta. (Skimming).
- ✓ Comprobar repostajes o transacciones inusuales o incompatibles con la ruta. (Skimming).
- ✓ Ante cualquier discrepancia, detener la operación, comunicar la incidencia y escalarla a sistemas o seguridad.
- ✓ Conservar la trazabilidad de correos, operaciones y validaciones.



Dato o referencia estadística

ROADSEC Security Toolkit identifica el cibercrimen como uno de los principales modus operandi que facilitan el robo de mercancías. Señala expresamente el robo de datos para obtener información sobre cargas, rutas y horarios, así como la manipulación de direcciones de entrega y de las comunicaciones entre los distintos actores de la cadena logística para desviar mercancías. No se ofrece una cifra cerrada por modalidad, pero sí una consideración expresa como vector de riesgo prioritario.

[ROADSEC Security Toolkit](#)

[CETM – Suplantación de identidades para desviar cargas de alto valor](#)

[FROET – Fraude mediante suplantación de identidades](#)

[Fenadismer – Suplantación de transportistas](#)

[TT Club – Cyber Security](#)

[TT News – Fuel Fraud Protection](#)

2. Suplantación de transportistas



En qué consiste

Fraude virtual con materialización física en la recogida o el tránsito (carrier fraud). Los delincuentes copian la identidad de una empresa real de transporte o de un conductor legítimo para aceptar un porte, retirar la mercancía y desaparecer con ella. Suelen replicar nombre comercial, logos, licencias, matrículas o correos, introduciendo cambios mínimos difíciles de detectar a simple vista.

Medidas preventivas

- 1 Homologar transportistas y revisar periódicamente sus datos maestros.
- 2 Confirmar por doble canal la identidad del conductor, matrícula y teléfono operativo antes de liberar la carga.
- 3 Verificar dominio de correo, licencias, seguro y antigüedad societaria.
- 4 No aceptar cambios de conductor o vehículo por vías informales o de última hora sin revalidación completa.

Check list

- ✓ Contrastar CIF/NIF, teléfono y dominio de email con la web oficial y registros conocidos.
- ✓ Pedir copia anticipada de documentación y revisar coherencia entre empresa, conductor y vehículo.
- ✓ Confirmar con un contacto ya conocido de la empresa, no con el remitente del nuevo mensaje.
- ✓ No liberar la carga si existe la menor discrepancia en matrícula, nombre o seguro.

Dato o referencia estadística

Fenadismer señaló en 2025 que esta modalidad supone ya el 1,5% de los robos de mercancías en Europa, con datos atribuidos a TAPA. Además, TT Club informó de que el carrier fraud representó el 84% de sus reclamaciones por fraude o engaño en 2022 dentro de ese grupo de siniestros por fraude.

Links fuentes:

[Link 1](#)

[Link 2](#)



3. Suplantación de intermediarios o fake brokers

En qué consiste

Fraude virtual y documental que redirige operaciones de alto valor. El delincuente suplanta a un transitario, operador o intermediario legítimo para contratar el transporte con apariencia normal y luego desviar la carga a otro destinatario, almacén o transportista controlado por la banda.

Medidas preventivas

- 1 No confiar solo en la apariencia del correo o del membrete.
- 2 Establecer listas blancas de intermediarios verificados y contactos autorizados.
- 3 Confirmar cualquier cambio de instrucciones con el cliente por un canal independiente.
- 4 Reducir la intermediación en cargas sensibles o de valor alto.

Check list

- ✓ Validar que el correo pertenece realmente al intermediario habitual.
- ✓ Revisar si hay cambios sutiles en dominio, firmas, teléfonos o IBAN.
- ✓ Confirmar dirección de entrega y persona receptora con el cargador original.
- ✓ Escalar la operación si la tarifa, la urgencia o el procedimiento resultan anómalos.

Dato o referencia estadística

CETM alertó en 2025 de estafas de este tipo para desviar cargas de alto valor, especialmente electrodomésticos y bebidas alcohólicas. No existe un porcentaje público estable del total de casos, pero sí una alerta sectorial expresa sobre su incremento.

Links fuentes:

[Link 1](#)



4. Fraude en plataformas digitales de carga

En qué consiste

Fraude virtual de contratación en bolsas de carga y marketplaces. Se aprovechan plataformas de intercambio de cargas para publicar ofertas falsas, contratar con perfiles fraudulentos o captar servicios con documentación inconsistente. El fraude suele apoyarse en prisas, tarifas agresivas y verificación insuficiente.

Medidas preventivas

- 1 Restringir la compra o adjudicación de cargas sensibles a usuarios internos autorizados.
- 2 Reforzar la verificación documental cuando la operación proceda de una plataforma abierta.
- 3 No mover mercancía de alto valor sin validación reforzada del proveedor efectivo.
- 4 Vigilar republicaciones sospechosas de la misma carga y subcontrataciones en cadena.

>>> Check list

- ✓ Comprobar referencias, web profesional, CIF/NIF y seguro del proveedor.
- ✓ Solicitar licencia, datos del conductor y matrícula antes de asignar.
- ✓ Verificar que la empresa no use solo correos genéricos o canales informales.
- ✓ Seguir la entrega con confirmación final del destinatario.

Dato o referencia estadística

No hay un dato público único y consolidado para España. Las alertas sectoriales recientes sí describen un aumento de estafas de falsos intermediarios y operadores en entornos digitales de contratación.



5. Fraude documental (CMR, albaranes, licencias, seguros)

En qué consiste

Fraude virtual, documental y operativo. Consiste en utilizar documentos falsificados o alterados para legitimar una recogida, una entrega, una reclamación o un cambio de destino. Puede presentarse tanto en papel como en PDF o imagen enviada por email o mensajería.

Medidas preventivas

- 1 No validar documentos solo por apariencia gráfica.
- 2 Comprobar coherencia entre CMR, albarán, orden de carga, vehículo, seguro y datos societarios.
- 3 Mantener plantillas de documentos y formatos esperados por cliente y operador.
- 4 Verificar sellos, poderes y números de precinto con el departamento de soporte.

Check list

- ✓ Revisar fechas, razón social, direcciones, matrícula y teléfonos.
- ✓ Comprobar que no haya tachaduras, tipografías mezcladas o firmas dudosas.
- ✓ Confirmar el número de precinto y la orden de carga con la oficina.
- ✓ No aceptar un cambio de destino sustentado solo en un documento reenviado.

Dato o referencia estadística

No hay un número de casos homogéneo publicado para España. No obstante, el ROADSEC Security Toolkit y TT Club identifican el fraude documental y la falsificación de credenciales como uno de los principales métodos utilizados para facilitar recogidas ficticias, desviar mercancías

mediante instrucciones de entrega fraudulentas y suplantar a transportistas o empresas logísticas legítimas.

Links fuentes:

[Link 1](#)

6. Empresas logísticas ficticias

En qué consiste

Fraude virtual y societario para ganar apariencia de legitimidad. Se crean empresas pantalla o webs profesionales falsas para captar operaciones, obtener documentación, cobrar servicios o retirar mercancía. A veces se aprovechan números de licencia de terceros o identidades de sociedades inactivas.

Medidas preventivas

- 1 Analizar antigüedad de la empresa, estructura societaria y huella digital real.
- 2 Desconfiar de compañías con web reciente, poca trazabilidad y teléfonos móviles únicos.
- 3 Pedir referencias reales y comprobar su existencia fuera de la documentación remitida.
- 4 Evitar dar acceso a cargas sensibles sin un proceso formal de homologación.

Check list

- ✓ Verificar si la web y el dominio tienen trayectoria y actividad coherente.
- ✓ Comprobar sede social, permisos, seguro y referencias de clientes.
- ✓ Detectar si el interlocutor presiona para operar antes de la validación.
- ✓ Escalar cualquier incoherencia entre la empresa y la documentación del conductor.

Dato o referencia estadística

No existe una cifra pública homogénea sobre la incidencia de este fraude en España. No obstante, el ROADSEC Security Toolkit identifica el uso de empresas logísticas ficticias y recogidas fraudulentas (fictitious pick-up) como uno de los métodos empleados para la sustracción

de mercancías, mientras que TT Club incluye el carrier fraud – basado en empresas de transporte ficticias o suplantadas – entre las principales modalidades de fraude que afectan a la cadena logística.

7. Fraude en facturación o pagos

En qué consiste

Fraude dirigido a desviar pagos legítimos mediante la manipulación de facturas, cuentas bancarias o instrucciones de pago. Los ciberdelincuentes suelen acceder previamente al correo electrónico de una de las partes (cliente, proveedor, operador logístico o transitario) o suplantar su identidad para enviar una factura modificada o comunicar un supuesto cambio de cuenta bancaria. El objetivo es que el pago se realice a una cuenta controlada por los atacantes sin que ninguna de las partes detecte el fraude hasta días después.

Medidas preventivas

- 1 Verificar por un canal independiente cualquier cambio de cuenta bancaria o de instrucciones de pago.
- 2 Implantar el principio de doble validación para modificaciones de datos financieros.
- 3 Utilizar autenticación multifactor en las cuentas de correo corporativo y sistemas financieros.
- 4 Revisar periódicamente los permisos y accesos a las plataformas de facturación.
- 5 Formar al personal para detectar intentos de Business Email Compromise (BEC) y facturas manipuladas.

Check list

- ✓ Confirmar telefónicamente cualquier modificación de la cuenta bancaria del proveedor.
- ✓ Comprobar que el dominio del correo electrónico coincide exactamente con el habitual.
- ✓ Revisar importes, conceptos y datos bancarios antes de autorizar el pago.
- ✓ Establecer una segunda aprobación para pagos extraordinarios o cambios de beneficiario.
- ✓ Escalar cualquier solicitud urgente de modificación de pagos o facturación que no siga el procedimiento habitual.

Dato o referencia estadística

No existe una estadística pública homogénea en España sobre este tipo de fraude. No obstante, Europol considera el Business Email Compromise (BEC) una de las modalidades de ciberfraude con mayor impacto económico para las empresas, y TT Club recomienda

verificar por un canal independiente cualquier cambio en las instrucciones de pago o en los datos bancarios.

Links fuentes:

[Link 1](#)

[Link 2](#)

Protocolo transversal de prevención

A continuación, presentamos las prácticas imprescindibles a seguir para cada fase del transporte de mercancías por carretera.

Fase	Control	Qué valida	Acciones clave
1. Antes de contratar (Contratación)	Análisis de riesgos y controles antifraude	Que el proveedor es legítimo y cumple los requisitos de seguridad.	• Validar identidad societaria, licencias, seguro y reputación. • Confirmar canales oficiales de comunicación. • Bloquear proveedores no homologados • Evitar decisiones sin verificación.
2. Antes de cargar (Recogida)	Validación de conductor, matrícula y referencia	Que la carga sale con el operador correcto	• Confirmar conductor, matrícula, remolque y franja horaria • Definir código de liberación • Revisar coherencia documental • Asegurar que muelle y expedición aplican el protocolo
3. Durante el tránsito (Tránsito+ Paradas)	Canal único para cambios y paradas seguras	Que no hay desvíos, engaños ni exposición a robo	• Prohibir cambios por canales no oficiales • Permitir solo parkings seguros o preautorizados • Escalar comunicaciones sospechosas o falsa autoridad • Monitorizar incidencias en ruta
4. En la entrega (Entrega)	Confirmación de destinatario y ubicación	Que no hay desvío ni entrega fraudulenta	• Verificar destinatario, dirección y precintos • No descargar en puntos alternativos no validados • Registrar prueba de entrega y receptor efectivo
5. Después del incidente (Posincidente y Administración)	Análisis de causa raíz + control antifraude en pagos	Que el aprendizaje se integra y no hay desvío económico	• Preservar evidencias y reportar • Analizar fallos de control • Validar cuentas bancarias (cambios por canal independiente) • Actualizar listas negras/blancas

Soluciones antifraude Eurowag

Sólidas funciones de seguridad antifraude, gratuitas, con monitorización automatizada del sistema de detección de fraude las 24 horas.



- 1 Bloqueo de tarjetas y seguridad.
- 2 Bloquea o desbloquea tarjetas al instante a través del Portal del cliente, la app de Eurowag o SMS.
- 3 Monitorización antifraude 24/7.
- 4 Configuración de tarjetas adaptada al tipo de vehículo y a las necesidades operativas.
- 5 Códigos PIN seguros y límites de gasto definidos para cada tarjeta.

- Eurowag ofrece el **sistema de soluciones antifraude más avanzado** técnicamente para mantener tus tarjetas seguras y tu dinero en tu bolsillo.
- **Bloqueo de tarjeta** – Ya no tendrás que preocuparte por el impacto significativo del fraude en tu negocio. Protege tu empresa con más que un simple código PIN y un límite de Card Lock. El bloqueo de tarjeta es un nivel de verificación adicional para nuestras tarjetas de combustible. Cuando el Bloqueo de Tarjeta está activo, la tarjeta de combustible tiene que ser “desbloqueada” antes de que pueda ser utilizada para pagar el combustible. Para desbloquearla, puedes utilizar nuestro Portal del cliente, un SMS o la aplicación Eurowag.
- **PIN y límites** – Todas nuestras tarjetas están protegidas con un código PIN que solo tú conoces. También puedes elegir el límite de seguridad de cada tarjeta para que se corresponda con el tipo de vehículo para el que se utiliza.



Soluciones antifraude:

Fuel guard



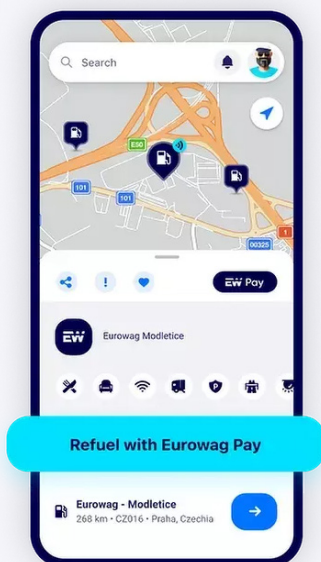
Fuel guard es la solución de Eurowag que bloquea la transacción del repostaje si la tarjeta de combustible Eurowag, el dispositivo EVA y la estación de servicio no se ubican en el mismo punto.

- **Tarifas de peaje competitivas**
 - Reduce tus costes de peaje y benefíciate de importantes descuentos al trabajar directamente con el proveedor EETS Eurowag. De este modo, se eliminan los costes adicionales derivados de intermediarios.
- **Sin costes de instalación** – El dispositivo de peaje EVA está diseñado para una configuración rápida y sencilla, sin necesidad de instalación fija y, por tanto, sin costes de instalación. Se alimenta mediante un conector de mechero, aunque también puede instalarse con cableado fijo.
- **Fácil instalación** – Olvídate de procesos de instalación complejos. La unidad EVA está lista para su uso: solo tienes que conectarla y ponerte en marcha.
- **Un único pago para todos los peajes**
 - Independientemente de dónde circules, solo realizarás un pago por periodo de facturación.
- **Solución integral** – Gestiona fácilmente todas tus facturas de peaje e informes a través del portal de clientes de Eurowag.
- **Un dispositivo, múltiples países** – Circula sin interrupciones por Alemania, Austria, República Checa, Eslovaquia, Polonia, Hungría, España, Bélgica, Portugal y otros países; una solución ideal para el transporte internacional.
- **Entrega rápida** – Recibe tu dispositivo integrado EVA directamente en tu puerta en tan solo dos días laborables.

Soluciones antifraude: Eurowag Pay

Pagos móviles para comprar combustible. Eurowag Pay hace que repostar sea más fácil, más eficiente y más seguro.

Eurowag Pay ahorra tiempo al permitir pagar desde el móvil sin colas ni tarjetas físicas, con la comodidad de un único PIN. Además, ofrece gestión remota de tarjetas y alta seguridad con control de ubicación y funciones de emergencia.



- 1 Pagos de combustible con el móvil con un alto nivel de seguridad.
- 2 Pago de combustible, AdBlue, GNL, peajes, aparcamiento y servicios adicionales.
- 3 Visibilidad total de las transacciones de toda tu flota.

Eurowag tiene la protección más fuerte del mercado

	Eurowag	Otros proveedores
PIN	●	●
Bloqueo de tarjetas	●	●
Seguro contra uso indebido de la tarjeta de combustible (o similar)	●	●
Fuel Guard (o función equivalente)	●	●
Grabaciones de CCTV (o similar)	●	●
Informe de actividad de la tarjeta (o similar)	●	●
Monitorización antifraude 24/7	●	●

● Sí ● Parcialmente ● No

Conclusión

Esta guía recoge una selección de las principales modalidades de fraude virtual que afectan al sector del transporte y la logística, identificadas a partir de la experiencia de Eurowag, de la información proporcionada por nuestros clientes, socios y colaboradores, y del análisis de las amenazas que actualmente afectan a la cadena de suministro.

Su objetivo es ofrecer al sector una herramienta de referencia con recomendaciones, buenas prácticas y protocolos orientados a prevenir los principales riesgos asociados al fraude digital, desde un enfoque práctico y preventivo. No obstante, se recomienda a cada organización adaptar estas medidas a sus procesos, sistemas tecnológicos, estructura interna y perfil de riesgo.

Esta publicación complementa la primera guía de Eurowag sobre fraude físico, proporcionando una visión más completa de las amenazas que afronta el transporte de mercancías y contribuyendo a reforzar la seguridad de toda la cadena logística frente a un entorno cada vez más digitalizado.

¡Únete a la familia Eurowag!

Si quieres saber más acerca de cómo podemos ayudar a tu empresa en la prevención de fraudes, escanea este QR.



 **+34 937 371 151**

Servicio de atención al cliente Eurowag:
De 9:00 a 18:00, días laborables.

