Transporte XXI .com

CARRETERA | 08/05/2026

Los 'hackers' llaman a la puerta del transporte

La cuestión ya no es si una empresa del sector sufrirá un ciberataque, sino cuándo, advirtió la patronal Asetrabi en una jornada sobre ciberseguridad, organizada junto a Sui Broker Correduría de Seguros.

La ciberseguridad se ha convertido en un riesgo empresarial de primer nivel para el transporte y la logística. Así se puso de manifiesto en la jornada "Ciberseguridad en el transporte: ¿Está preparada tu empresa para el próximo ciberataque?", celebrada ayer en el salón de actos de la Asociación Empresarial de Transporte de Bizkaia (Asetrabi), que preside Sonia García. El encuentro, organizado por la propia patronal, junto a Sui Broker Correduría de Seguros, reunió a un reducido grupo de empresas, una asistencia discreta que contrasta con la creciente relevancia de una amenaza llamada a ocupar un lugar cada vez más destacado en la agenda del sector.

Miguel Moral y Benjamín Pellegrini (Markel), Urtzi Vidal (Sui Broker Correduría de Seguros) y Sonia García, presidenta de Asetrabi.

La sesión tuvo como objetivo advertir de los riesgos reales a los que se enfrentan las empresas de transporte en su actividad diaria, identificar los errores más habituales y explicar cómo evitarlos, además de detallar qué cubre -y qué no- un seguro de riesgos cibernéticos. También se abordó cómo debe actuar una compañía desde el primer minuto tras sufrir un incidente.

El ponente de la jornada, Benjamín Pellegrini, Suscriptor Senior Cyber de Markel, firma especialista en seguros, subrayó que la cuestión ya no es si una empresa va a sufrir un ciberataque, sino cuándo. En este sentido, advirtió de que el transporte y la logística se encuentran en el punto de mira de la ciberdelincuencia por su papel esencial dentro de la cadena de suministro. La alta dependencia de sistemas informáticos, el acceso constante a datos, la integración con terceros y proveedores tecnológicos y la digitalización de procesos críticos amplifican la exposición del sector.

"Si la tecnología falla, el negocio se detiene", subrayó Pellegrini, que alertó del impacto que un ataque puede tener no solo en la operativa diaria, sino también en la continuidad de la empresa. La cadena de suministro digital, añadió, ha ampliado el perímetro de riesgo: "ya no es necesario ser un experto para lanzar determinados ataques y la amenaza no se limita al interior de la organización, sino que puede llegar a través de proveedores, plataformas o sistemas conectados".

Durante la jornada se aportaron datos que reflejan la magnitud del problema. España figura como el segundo país del mundo más atacado por ciberdelincuentes, solo por detrás de Estados Unidos, y en 2025 se habrían registrado unas 45.000 incidencias diarias conocidas, sin contar aquellas que no trascienden. Además, la mayor parte de los siniestros se concentra en compañías con ventas inferiores a 50 millones de euros.

Pellegrini defendió que el seguro Cyber protege a las organizaciones más allá de las pérdidas financieras, al combinar medidas preventivas y reactivas. Entre las primeras figuran escaneos de vulnerabilidad, evaluaciones de seguridad y formación específica para los equipos. Entre las segundas, la respuesta a incidentes. El paraguas de cobertura incluye daños propios, responsabilidad regulatoria y responsabilidad civil, con especial atención a la compensación por pérdida de ingresos, según el alcance de la póliza, y a la negociación en casos de extorsión cibernética con los *hackers*.

La jornada se enmarca en el acuerdo suscrito entre Asetrabi y Sui Broker Correduría de Seguros, que prevé elaborar un mapa de riesgos entre las empresas asociadas mediante auditorías personalizadas para analizar su grado de exposición y determinar si cuentan con una cobertura adecuada.