Diario del Puerto

CARRETERA

ASETRABI reúne en una jornada en Bilbao a expertos de Markel y Sui Broker para abordar los riesgos cibernéticos

La ciberseguridad gana peso estratégico en el transporte ante el auge de los ataques

Miguel Morán, responsable Centro-Norte de Markel España; Benjamín Pellegrini, suscriptor senior Cyber y Fintech/Insurtech de Markel; Urtzi Vidal, director general de Sui Broker; Sonia García, presidenta de Asetrabi, Foto J.P.

08 mayo 2026 05:20

Jaime Pinedo

Última actualización 08 mayo 2026 09:32

ASETRABI reunió ayer en Bilbao a expertos de seguros de Sui Broker y Markel para alertar al sector del transporte sobre el creciente impacto de los ciberataques y la necesidad de reforzar la prevención, la respuesta y la continuidad operativa ante un riesgo que ya es prioritario.

BILBAO. La Asociación Empresarial de Transportes de Bizkaia (ASETRABI) celebró ayer en Bilbao la jornada "Ciberseguridad en el transporte" junto a Sui Broker Correduría de Seguros y la aseguradora especializada Markel, con el fin de ayudar a las empresas a identificar riesgos digitales y mejorar su capacidad de respuesta ante incidentes cada vez más frecuentes. La sesión abordó la creciente exposición del sector a los ataques informáticos y la necesidad de entender la ciberseguridad no solo como una cuestión tecnológica, sino como un riesgo empresarial de primer nivel.

TEMAS

- Asetrabi
- Broker seguros
- Ciberseguridad en el transporte
- Correduría de seguros
- Jornada sobre ciberseguridad
- Markel
- Sui Broker

RELACIONADAS

ASETRABI y Sui Broker impulsan una jornada en Bilbao sobre ciberseguridad en el transporte

Las compañías de seguros adaptan sus polizas al incremento de actividad que se concentra en los puertos

El director general de Sui Broker, Urtzi Vidal, explicó que la iniciativa formaba parte del paquete de ventajas ofrecido a los asociados de ASETRABI y defendió la necesidad de impulsar formaciones "prácticas, interesantes y actualizadas" relacionadas con la gestión del riesgo. Vidal añadió que la correduría había planteado también la realización de auditorías objetivas sobre seguros y riesgos para que las empresas pudieran conocer "qué tiene, cuáles son sus riesgos y cómo los tiene cubiertos". En su opinión, muchas compañías del transporte "ni los conocen y, evidentemente, tampoco los tienen bien cubiertos".

> *El transporte y la logística son "objetivos prioritarios para los ciberdelincuentes por su estratégico papel en la cadena de suministro"*

El responsable Centro-Norte de Markel España, Miguel Morán, situó el ciberriesgo como "el primer riesgo" a nivel internacional y advirtió de que el transporte es un ámbito especialmente vulnerable. Morán presentó el perfil de Markel como aseguradora especializada en responsabilidad civil, líneas financieras y riesgos vinculados al transporte y la actividad "marine", una de las principales áreas de negocio del grupo a nivel internacional. Explicó además que, frente a la percepción tradicional del empresario español, centrada en incendios o explosiones, en el entorno anglosajón el principal temor empresarial ya era el ciberriesgo por su potencial devastador sobre la continuidad de la actividad.

Cuestión de supervivencia

La intervención más extensa y técnica corrió a cargo de Benjamín Pellegrini, suscriptor senior de Cyber y Fintech/Insurtech de Markel, quien alertó de que todas las empresas tienen hoy "una dependencia digital total" y recordó que la operativa empresarial depende completamente de sistemas digitales, plataformas en la nube y proveedores tecnológicos externos, por lo que "cuando la tecnología falla, el negocio se detiene".

Según dijo, las pérdidas comienzan "desde el primer momento" cuando una compañía pierde capacidad operativa por un ataque o una caída de sistemas. Pellegrini incidió en la exposición del transporte y la logística, sectores que definió como objetivos prioritarios para los ciberdelincuentes por su papel estratégico en la cadena de suministro y por los importantes flujos económicos que gestionan. Señaló que los ataques buscan intervenir en procesos críticos como el control de flotas, la gestión financiera o los sistemas operativos internos, y subrayó que el impacto no se limita a la empresa afectada, sino que se extiende a clientes, proveedores y socios.

"No es un problema de IT, es un problema de negocio, de continuidad e incluso de supervivencia", dijo.Como ejemplo, relató el caso de la empresa británica KNP, que tras sufrir un ataque derivado de "una única contraseña débil" perdió todos sus datos históricos, paralizó 500 camiones y acabó desapareciendo tras 158 años de actividad.