

Ciberseguridad Marítima:

La nueva frontera de la soberanía pesquera argentina

Estado, cámaras, gremios y trabajadores del mar quedaron convocados a construir juntos el “paraguas protector” de una cadena de valor cada vez más digital y cada vez más expuesta.

El sector pesquero argentino atraviesa una transformación tecnológica sin precedentes. Navegación digital, conectividad satelital a bordo, gestión informatizada de capturas y trazabilidad electrónica del producto configuran hoy un ecosistema hiperconectado que va de la embarcación en alta mar al consumidor final en los mercados más exigentes del mundo. Esa misma conectividad que multiplica la eficiencia y la competitividad es, al mismo tiempo, una superficie de ataque en expansión constante. Así lo planteó Capitán Jorge A. Frías, Secretario General de la AACPYPP y presidente de la FUNCESMAR en las Jornadas de Intereses Marítimos Argentinos, realizadas los días 16 y 17 de julio en Mar del Plata.

La exposición no se limitó a describir un riesgo tecnológico. Trazó una hoja de ruta con dos ejes que se entrelazan: uno político-gremial, que interpela a todos los eslabones de la cadena productiva -desde el Estado, pasando por el capitán del buque y sus tripulantes, las cámaras de armadores hasta el consumidor final-, y otro de capacitación, que desemboca en una propuesta institucional concreta: un seminario internacional que en 2027 debería producir la primera Guía de Mejores Prácticas en Ciberseguridad Marítima para el Sector Pesquero argentino y un curso especializado de Ciberseguridad Marítima para el Sector Pesquero, para ser incorporado en la Diplomatura de Capitán de Pesca.

Un ecosistema hiperconectado, un objetivo de alto valor

La llamada “**Pesca 4.0**” -sensores IoT, inteligencia artificial para optimizar rutas, *blockchain* para la trazabilidad, navegación digital- generó eficiencias notables: menores costos operativos, capturas más sostenibles, mejor trazabilidad del producto. Pero según se advirtió en la exposición, cada sensor y cada sistema automatizado es también una puerta de entrada potencial para actores maliciosos, “*los sicarios cibernéticos*”, según Frías. La digitalización de puertos y buques convirtió al ecosistema pesquero en un objetivo de alto valor.

El diagnóstico expuesto es contundente: los ataques cibernéticos al sector marítimo global crecieron un 300% entre 2019 y 2024, y la totalidad de los incidentes registrados en buques durante 2023 involucraron sistemas operativos críticos de navegación. A ese escenario se suma un factor nuevo y acelerador: el desarrollo de inteligencia artificial de frontera, cuyas capacidades -

según se señaló en la charla- están modificando el equilibrio estratégico en el ciberespacio y bajando la barrera técnica que antes frenaba a los atacantes menos sofisticados.

En el corazón del problema está la convergencia entre los **sistemas IT** (gestión comercial, comunicaciones satelitales, reportes regulatorios como el SiFIPA y el VMS, facturación, trazabilidad) y los **sistemas OT** (ECDIS, GPS/GNSS, AIS, control de máquinas y propulsión, cadena de frío, equipos de pesca). Esa convergencia es precisamente lo que habilita la eficiencia de la Pesca 4.0, pero también elimina el aislamiento que históricamente protegía a los sistemas críticos de navegación: un correo electrónico comprometido en el área administrativa puede, en una red mal segmentada, terminar afectando el control de la embarcación.

Los tres ejes: información, tecnología y personas

La exposición organizó el problema en torno a un marco de origen naval, hoy directamente aplicable al sector pesquero: información, tecnología y personas.

La **información** es el activo estratégico. Las decisiones de navegación y de captura ya no dependen solo de la observación directa del capitán, sino de un flujo continuo de datos -VMS, AIS, ECDIS, trazabilidad *blockchain*-. El riesgo, se explicó, es lo que podría llamarse “**el problema del oráculo**”: la tecnología *blockchain* garantiza que un dato no fue modificado después de registrado, pero no garantiza que ese dato haya sido verdadero al momento de ingresar. Una posición satelital falsificada puede derivar en un certificado de captura formalmente impecable y sustancialmente falso.

La **tecnología** es una espada de doble filo: cuanto más sofisticada, más frágil. Un buque tiene una vida útil de treinta años, pero su software pierde soporte en cinco o diez. Y la asimetría económica es notable: un ataque que cuesta apenas un par de cientos de dólares puede paralizar una embarcación de millones. La respuesta de mayor impacto y menor costo, se subrayó, es tan simple como segmentar las redes operativas y administrativas.

Las **personas** son el eslabón que no se puede parchear. Entre el 82% y el 95% de los incidentes exitosos comienzan con un error humano o una manipulación, no con un ataque técnico sofisticado. La paradoja del sector pesquero es que la misma conectividad satelital que acerca al tripulante con su familia lo expone las 24 horas como blanco de ingeniería social, *phishing* y chantaje. La respuesta, se planteó, no es solo tecnológica: exige formación obligatoria, principio de mínimo privilegio y una cultura de seguridad sostenida en el tiempo.

El eje político-gremial: una convocatoria a toda la cadena

Aquí es donde la propuesta despliega su primer eje. La **ciberseguridad marítima pesquera no puede ser resuelta por un solo actor**: requiere una arquitectura de responsabilidad compartida

entre el Estado, las cámaras de armadores, el sector privado exportador, los gremios, los capitanes de los buques y los trabajadores embarcados y en tierra.

En el plano normativo, la exposición identificó una brecha crítica. La Resolución MSC.428(98) de la Organización Marítima Internacional integra la gestión de riesgos cibernéticos en los sistemas de gestión de la seguridad desde enero de 2021, y resulta obligatoria para los buques de bandera argentina en aguas internacionales. La circular MSC-FAL.1/Circ.3 aporta el marco técnico para identificar sistemas críticos y definir salvaguardias. Sin embargo, la Ley 24.922 de Régimen Federal de Pesca no contiene disposiciones específicas de ciberseguridad para la flota ni para la cadena de valor. Tampoco el Acuerdo sobre Medidas del Estado Rector del Puerto contempla la dimensión cibernética del monitoreo satelital de buques. Hoy día el aporte normativo está dado por Ordenanzas de la Prefectura Naval Argentina que deberán actualizarse.

La tesis central es clara: Argentina carece hoy de un instrumento que articule de manera integrada la ciberseguridad, la actividad pesquera y la soberanía marítima. Y la manipulación de señales satelitales -el llamado “GNSS spoofing”- no es solo una amenaza a la navegación: es, según se planteó, una herramienta técnica para el blanqueo de pesca ilegal y el fraude en la certificación de origen, con implicancias directas sobre la soberanía argentina en el Atlántico Sur.

Frente a ese vacío, la convocatoria incluye a organismos nacionales (Subsecretaría de Recursos Acuáticos y Pesca, Agencia Nacional de Puertos y Navegación, Ministerios de Seguridad, Defensa y Relaciones Exteriores, Armada Argentina, Prefectura Naval, INIDEP, Consejo Federal Pesquero), a organismos internacionales (OMI, FAO, OEA, Interpol, ENISA), y al sector privado y gremial: la AACPyPP y los gremios de la pesca, las cámaras de armadores, los proveedores de sistemas de navegación y trazabilidad, las empresas de ciberseguridad marítima y las sociedades de clasificación.

El eje de capacitación: el seminario de CESMAr y sus cinco módulos

El segundo eje traduce el diagnóstico en una hoja de ruta formativa. Desde CESMAr - Centro de Estudios Superiores del Mar Argentino, con sede propuesta en Puerto Madryn y Mar del Plata- se propone organizar el Seminario Internacional de Ciberseguridad Marítima para el Sector Pesquero, de modalidad híbrida y alcance internacional, con traducción simultánea al inglés, pensado para su edición inaugural en la segunda mitad de 2027.

El seminario se estructura en cinco bloques, que recorren el ciclo completo de los tres ejes ya descriptos más la dimensión jurídica y la de formación:

1. **El panorama de amenazas en la cadena de valor pesquera** (eje información)
2. **La tecnología y la integridad de la información en la Pesca 4.0** (eje tecnología).
3. **El factor humano: vulnerabilidad y resiliencia de la tripulación** (eje personas)

4. **Gobernanza, regulación y el futuro ciber-resiliente** (aspectos jurídicos)

5. **Capacitación alineada con el Convenio Internacional sobre Normas de Formación, Titulación y Guardia para el Personal de los Buques Pesqueros (STCW-F/95)**

El producto final de ese proceso -tres días de trabajo presencial y virtual- sería una Guía de Mejores Prácticas en Ciberseguridad para el Sector Pesquero.

Un llamado sin urgencia de inversión, pero con urgencia de decisión

Uno de los mensajes centrales de la exposición apunta a desactivar una objeción previsible: la implementación de estas prácticas no requiere grandes inversiones iniciales. La higiene cibernética básica -segmentación de redes, formación del personal, protocolos mínimos de verificación de datos- genera un retorno significativo y constituye, se planteó, el punto de partida realista para la flota argentina.

Lo que sí exige la propuesta es una decisión política y gremial que integre en una única mesa de trabajo al Estado, industria y trabajadores dado que tienen un rol único e insustituible para liderar esta agenda: la oportunidad de comprometer a esa tríada en la defensa cibernética del mar argentino.

“La ciberseguridad no es un costo: es una inversión en la integridad del producto argentino en el mundo”, resumió Frías al cierre de su exposición. *“El mar no se pide prestado, se defiende. Y en el siglo XXI, defenderlo significa también defender sus datos, sus señales y su soberanía digital”.*

Nota elaborada sobre la base de la exposición "La ciberseguridad marítima en la cadena de valor del sector pesquero", presentada por el Capitán Jorge A. Frías (FUNCESMAR) y el Vicealmirante VGM (RE) Mg. Alvaro J. Martínez en las Jornadas de Intereses Marítimos Argentinos, Mar del Plata, 16 y 17 de julio de 2026.