Tomasello & Weitz
Estudio Jurídico

INFORMATIVO N° 333

MAT: Análisis del Ordinario N° 12.600/204 VRS. de la DGTM y MM.

Viña del Mar, 22 de Julio de 2025
C-029

Estimados (s) Señor(es):

A continuación les hacemos llegar un análisis del Ordinario N° 12.600/204 VRS. de la DGTM y MM., que aprueba la Circular DGTM y MM. Ord. N° 0-75/006, que establece disposiciones relativas a la implementación de medidas de seguridad de la información y protección cibernética por parte de Buques, Instalaciones Portuarias y Compañías en el marco de la gestión de riesgos cibernéticos marítimos.

1. La Circular N° 0-75/006 (en adelante, la "Circular") apunta a la implementación de un "sistema de gestión de riesgos" para enfrentar los "riesgos cibernéticos".

2. Obviamente la gestión de los riesgos cibernéticos se estima fundamental para la seguridad y protección de las operaciones de transporte marítimo que, se dice, tradicionalmente se han centrado en el ámbito físico, pero que actualmente, atendido el desarrollo cibernético y la digitalización, debe extenderse también a la gestión de los riesgos cibernéticos dentro del ámbito marítimo.

3. Para efectos de la Circular, se entiende por riesgo cibernético: *"el grado de exposición a la materialización de una amenaza (a través de un evento o incidente) que pueda causar daños a una organización, por ejemplo, fallas operacionales, de seguridad o protección del transporte marítimo al corromperse, perderse o poner en peligro la información y los sistemas"*.

4. La Circular se aplica a (a) todos los Buques de tráfico internacional sujetos al Código IGS, (b) a todas las Compañías marítimas que deban cumplir con el Código IGS y (c) a todas las Instalaciones Portuarias que den cumplimiento al Código PBIP.

5. Todos los Buques y Compañías referidas en el N° 4, deben incorporar a sus procesos un "sistema de gestión de riesgos cibernéticos".

6. Este "sistema" debe cumplir las recomendaciones de las normas ISO 27000, para la gestión de la seguridad de la información e ISO 27001/NCh-ISO/IEC 27001.

7. Todas las Compañías e Instalaciones deberán considerar, dentro de su sistema de gestión de riesgos cibernéticos, una persona responsable denominada CISO (*Chief Information Security Officer*) que será una suerte de "sujeto responsable" en estas materias.

8. El CISO está obligado a denunciar al Ministerio Público en caso que detecte actividades cibernéticas que constituyan delito, de acuerdo a la Ley N° 21.459, de 20 de junio de 2022, que establece normas sobre delitos informáticos.

9. Tratándose de Compañías y Buques, el "sistema de gestión de riesgos informáticos" deberá considerar, a lo menos, las siguientes áreas sensibles:

   - Los sistemas de puente.
   - Los sistemas de manipulación y gestión de carga.
   - Los sistemas de propulsión y gestión de las máquinas y de control de suministros eléctricos.
   - Los sistemas de servicio a los pasajeros y de organización de los mismos.
   - Las redes públicas de tripulación y pasajeros.
   - Los sistemas de comunicación.
   - Los sistemas administrativos y de bienestar de la tripulación.

10. Cuando el servicio tecnológico sea otorgado por uno o varios proveedores externos, el proveedor deberá asegurar la disponibilidad, confidencialidad e integridad a objeto de proteger la información propia y la de sus clientes.

11. Tanto para las Compañías como para los Buques, la verificación de la adecuada implementación se efectuará mediante auditorías internas o externas, que deberán realizarse de acuerdo a lo establecido en el Código IGS.

12. Tratándose de Instalaciones Portuarias, el "sistema de gestión de riesgos informáticos" deberá considerar, a lo menos, las siguientes áreas sensibles:

    - Los sistemas de control de acceso.

    - Los sistemas de servicio a los pasajeros y de organización de los mismos.

    - Los sistemas de comunicaciones en el marco de lo dispuesto en cada plan de protección marítima.

    - Los sistemas operacionales de manipulación de la carga y sus respectivos procesos.

    - Las ayudas a la navegación electrónicas, propiedad de las Instalaciones Portuarias.

    - Los sistemas de proveedores que interactúen con sistemas anteriores.

    - Cualquier otro sistema informático que interactúe con los sistemas anteriores.

13. Cuando el servicio tecnológico sea otorgado por uno o varios proveedores externos, el proveedor deberá asegurar la disponibilidad, confidencialidad e integridad a objeto de proteger la información propia y la de sus clientes.

14. Las Instalaciones Portuarias deberán incorporar, en la respectiva evaluación de protección, el proceso de gestión del riesgo informático. De igual forma, deberán incorporar los procedimientos necesarios para mitigar los riesgos detectados en la actividad de evaluación, como asimismo el procedimiento necesario para mitigar los riesgos detectados en la misma evaluación.

15. Tratándose de Instalaciones Portuarias, la evaluación de protección y el plan de protección deberán ser aprobados por la Dirección de Seguridad y Operaciones Marítimas, conforme lo establece el Código PBIP.

16. La verificación de la adecuada implementación del sistema de gestión de riesgos cibernéticos se efectuará mediante auditorías internas y los procesos de auditorías externas, serán ejecutados por los auditores dependientes de la Autoridad Marítima chilena, de acuerdo al plan anual de auditorías respectivo, que se realizarán de acuerdo a lo establecido en el Código PBIP.

17. Por último, aquellas Instalaciones Portuarias que se consideren estratégicas, deberán incorporar un "Sistema de Gestión de Riesgos Cibernéticos en el Estudio de Seguridad y Plan General de Seguridad".

18. La Circular entra en vigencia dos años después de la fecha de su publicación en el Diario Oficial, publicación que tuvo lugar el 16 de junio de 2023, razón por la cual, entendemos que esta Circular ha entrado en vigencia desde el 16 de junio de este año 2025.

Atentamente,

Leslie Tomasello Weitz
TOMASELLO Y WEITZ