

Ciberseguridad Marítima

Protegiendo la Infraestructura Crítica
del Sector Marítimo Español



El Panorama de Ciberataques



Incremento del 900%

Los ciberataques al sector marítimo se han multiplicado en los últimos 3 años.

Fuente: IBM Cost of Data Breach Report 2024



Sector Transporte: #2

ENISA clasifica el sector transporte como el segundo más atacado de Europa.

Fuente: ENISA Threat Landscape 2024



Actores Estatales

APT28, APT35 y grupos chinos intensifican ataques a puertos estratégicos europeos.

Fuente: OTAN/CCDCOE 2025



287 Días

Tiempo medio para detectar una brecha en sistemas OT marítimos.

Fuente: Informes sectoriales Lloyd's

Vulnerabilidades Críticas a Bordo



Sistemas de Navegación

GPS, ECDIS y AIS vulnerables a spoofing y jamming. Los sistemas DP también son objetivos.

Riesgo: CRÍTICO



Comunicaciones

VHF, satelital, email marítimo y sistemas GMDSS son interceptables.

Riesgo: ALTO



Control de potencia y propulsión a bordo

Los sistemas PMS que controlan propulsión y generadores pueden ser comprometidos.

Riesgo: CRÍTICO



Sistemas de Carga

Los sistemas de gestión de carga controlan estabilidad, lastre y operaciones portuarias.

Riesgo: ALTO

Riesgos en Infraestructura Portuaria



Automatización Portuaria

Grúas AGV, sistemas automatizados de manejo de carga y vehículos autónomos dependen de redes industriales.

⚠ Impacto: €50M/día



Centros de Control Integrados

Los PCC unifican operaciones, seguridad, aduanas y dirección financiera.

⚠ Impacto: Multisectorial



SCADA/ICS

Los sistemas TOS gestionan la cadena de suministro global.

⚠ Impacto: Seguridad Nacional

Casos Documentados: Puerto de Barcelona (2023), Puerto de Los Ángeles (2022), terminales petroleras en Alemania/Países Bajos (2022). El coste total supera los \$6,000M anuales.

Marco Regulatorio y Compliance



ISO 27001

Estándar Internacional de Seguridad

Estándar internacional para Sistemas de Gestión de Seguridad de la Información (SGSI). Establece los requisitos para implementar, mantener y mejorar continuamente la seguridad de la información en cualquier organización.

- ✓ Requisito para contratos públicos
- ✓ Marco de referencia internacional
- ✓ Ciclo de mejora continua

Certificación reconocida mundialmente



Requisitos IACS

E26 y E27 - 2024

A partir del 1 de julio de 2024, las nuevas construcciones deben cumplir con los requisitos unificados de la IACS:

- ✓ Se centran en la seguridad digital de los sistemas integrados de a bordo, desde la navegación hasta la propulsión
- ✓ Cubre el diseño, construcción, puesta en marcha y vida operativa del barco
- ✓ Se basa en 5 funciones clave: Identificar, Proteger, Detectar, Responder y Recuperarlo

Normativa marítima internacional



ENS Alto

Esquema Nacional de Seguridad

Marco de seguridad obligatorio para todas las entidades del sector público español y empresas que presten servicios a la Administración. El nivel ALTO es el más exigente.

- ✓ Obligatorio sector público
- ✓ Nivel ALTO - Máxima exigencia
- ✓ Auditorías periódicas

Cumplimiento legal español

Nuestra Solución Integral

01 Evaluación de Riesgos

Análisis exhaustivo de vulnerabilidades técnicas y organizativas en buques y puertos, con una tasa de cero falsos positivos.

02 Pentesting con IA

Ataques controlados potenciados por inteligencia artificial propia y la implantación de gemelos digitales para entornos críticos.

03 Formación

Programas de capacitación específicos para tripulaciones y personal portuario.

04 Monitorización 24/7

SOC especializado con detección de amenazas en tiempo real.

05 Respuesta a Incidentes

Equipo de respuesta inmediata con protocolos específicos para entornos marítimos.

06 ISO 27001

Desarrollo e implantación de SGSI adaptado al entorno marítimo.

100%

Cobertura ENS

24/7

Monitorización

Inmediata

Respuesta

Alianza Estratégica de Expertos



Altum Ingeniería y Servicios

Ingeniería Naval

- ✓ +20 años de experiencia en ingeniería naval y consultoría marítima
- ✓ Expertos en realización de análisis de riesgos en el entorno marítimo.
- ✓ Servicios para armadores, astilleros e instalaciones portuarias

Sedes: Huelva & Madrid



Hermes Security

Ciberseguridad + IA

- ✓ Startup innovadora en BIC Euronova
- ✓ IA propia que descubre fallos de seguridad
- ✓ Simulación predictiva de ataques usando gemelos digitales

Sedes: Málaga & Huelva



Objetivo 17

Consultoría Estratégica

- ✓ +30 años de experiencia en sectores clave
- ✓ Integración ISO 27001 con compliance
- ✓ Red global de partners internacionales

Sede: Madrid

Trayectoria Probada

Nuestros Clientes

+50

Proyectos Marítimos

+20

Años Experiencia

100%

Clientes Satisfechos



Navantia



Puerto de Huelva



Freire Shipyard



SPC Spain



Astilleros
Armón



Baleària



Guardia Civil



Silversun



Acciona

MOODY'S

Moody's



Gobierno de
Islandia



OVHcloud



Alibaba Cloud



BMW

¿Por Qué Elegirnos?

Propuesta de Valor Diferencial



Expertise Sectorial Único

Somos los únicos que combinamos conocimiento profundo de ingeniería naval con excelencia en ciberseguridad ofensiva predictiva.

★ Diferenciador clave frente a consultoras genéricas



Inteligencia Artificial Propia

Nuestra IA toma decisiones autónomas y descubre fallos de seguridad replicando el comportamiento de un hacker humano.

</> Desarrollada desde cero por nuestro equipo



Simulación Predictiva

Tecnología exclusiva para simular ataques en entornos virtuales idénticos a los reales, sin afectar sistemas en producción.

⚙️ Tecnología de última generación | Gemelo Digital



Compliance Integral

No solo cumplimos con ISO 27001, ENS Alto e IACS: integramos todos los requisitos en una solución eficaz.

🤝 Un único partner para todas las normativas



La Elección Inteligente para cualquier Sector

Optimización de recursos, total transparencia y resultados medibles desde el primer día.

Ciberseguridad marítima avanzada

Protejamos Juntos Nuestros Mares



Altum Ingeniería y Servicios

Daniel Santos

+34 959 283 295

daniel.santos@altum-marine.com

altum-marine.com



Hermes Security

Cristian Mateo

+34 621 373 780

cristian.mateo@hermesecurity.com

hermesecurity.com



Objetivo 17

Víctor Manuel Fuertes

+34 638 056 821

direccion@objetivo17.com

objetivo17.com

La seguridad de nuestra infraestructura marítima crítica es responsabilidad de todos.

Estamos listos para acompañarles.