


Cibersegurança Marítima



Protegendo a Infraestrutura Crítica
do Setor Marítimo

O Panorama dos Ciberataques



Aumento de 900%

Os ciberataques ao setor marítimo aumentaram significativamente nos últimos 3 anos.

Fonte: IBM Cost of Data Breach Report 2024



Setor de Transportes: #2

A ENISA classifica o setor de transportes como o segundo mais atacado da Europa.

Fonte: ENISA Threat Landscape 2024



Atores Estatais

APT28, APT35 e grupos chineses intensificam ataques a portos estratégicos europeus.

Fonte: OTAN/CCDCOE 2025



287 Dias

Tempo médio para detectar uma violação em sistemas OT marítimos.

Fonte: Relatórios setoriais da Lloyd's

Vulnerabilidades Críticas a Bordo



Sistemas de Navegação

GPS, ECDIS e AIS vulneráveis a spoofing e jamming. Os sistemas DP também são alvos.

Risco: CRÍTICO



Comunicações

VHF, satélite, e-mail marítimo e sistemas GMDSS são interceptáveis.

Risco: ALTO



Controle de Potência e Propulsão a Bordo

Os sistemas PMS que controlam propulsão e geradores podem ser comprometidos.

Risco: CRÍTICO



Sistemas de Carga

Os sistemas de gestão de carga controlam estabilidade, lastro e operações portuárias.

Risco: ALTO

Riscos na Infraestrutura Portuária



Automatização Portuária

Guindastes AGV, sistemas automatizados de movimentação de carga e veículos autónomos dependem de redes industriais.

⚠ Impacto: €50M/dia



Centros de Controle Integrados

Os PCC unificam operações, segurança, alfândega e direção financeira.

⚠ Impacto: Multissetorial



SCADA/ICS

Os sistemas TOS gerenciam a cadeia de suprimentos global.

⚠ Impacto: Segurança Nacional

Casos Documentados: Porto de Barcelona (2023), Porto de Los Angeles (2022), terminais petrolíferos na Alemanha/Países Baixos (2022). O custo total ultrapassa \$6.000M por ano.

Marco Regulatório e Compliance



ISO 27001

Padrão Internacional de Segurança

Padrão internacional para Sistemas de Gestão de Segurança da Informação (SGSI). Define os requisitos para implementar, manter e melhorar continuamente a segurança da informação em qualquer organização.

✓ Requisito para contratos públicos

✓ Referência internacional

✓ Ciclo de melhoria contínua

Certificação reconhecida mundialmente



Requisitos IACS

E26 e E27 - 2024

A partir de 1º de julho de 2024, as novas construções devem cumprir os requisitos unificados da IACS:

✓ Focam na segurança digital dos sistemas integrados a bordo, desde a navegação até a propulsão.

✓ Abrangem o projeto, construção, comissionamento e vida operacional da embarcação.

✓ Baseiam-se em 5 funções-chave: Identificar, Proteger, Detectar, Responder e Recuperar.

Normativa marítima internacional



Diretrizes da IMO

Cibersegurança para Navios e Instalações Portuárias

Estas diretrizes fornecem práticas recomendadas internacionalmente reconhecidas para reforçar a cibersegurança em operações marítimas, abrangendo navios e instalações portuárias.

✓ Riscos e Governança: Identificar e gerir vulnerabilidades.

✓ Medidas Técnicas: Proteger redes e sistemas a bordo.

✓ Resposta a Incidentes: Detectar, responder e recuperar.

Regulamentação marítima internacional

Nossa Solução Integrada

01 Avaliação de Riscos

Análise detalhada de vulnerabilidades técnicas e organizacionais em navios e portos, com taxa zero de falsos positivos.

02 Pentesting com IA

Ataques controlados potencializados por nossa inteligência artificial própria e pelo uso de gêmeos digitais em ambientes críticos.

03 Treinamento

Programas de capacitação específicos para tripulações e pessoal portuário.

04 Monitorização 24/7

SOC especializado com detecção de ameaças em tempo real.

05 Resposta a Incidentes

Equipa de resposta imediata com protocolos específicos para ambientes marítimos.

06 ISO 27001

Desenvolvimento e implementação de um SGSI adaptado ao ambiente marítimo.

100%

Conformidade Regulamentar

24/7

Monitorização

Resposta

imediate

Aliança Estratégica de Especialistas



Altum Ingeniería y Servicios Engenharia Naval

- ✓ +20 anos de experiência em engenharia naval e consultoria marítima.
- ✓ Especialistas na realização de análises de risco no ambiente marítimo.
- ✓ Serviços para armadores, estaleiros e instalações portuárias.

Sedes: Huelva & Madrid



Hermes Security Cibersegurança + IA

- ✓ Startup inovadora no BIC Euronova
- ✓ IA própria que identifica falhas de segurança
- ✓ Simulação preditiva de ataques utilizando gémeos digitais

Sedes: Málaga & Huelva



Objetivo 17 Consultoria Estratégica

- ✓ +30 anos de experiência em setores-chave
- ✓ Integração da ISO 27001 com compliance
- ✓ Rede global de parceiros internacionais

Sede: Madrid

Histórico Comprovado

Nossos Clientes

+50

Projetos Marítimos

+20

Anos de Experiência

100%

Clientes Satisfeitos



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 Que Nos Escolher?

Proposta de Valor Diferencial



Expertise Setorial Único

Somos os únicos que combinam conhecimento profundo em engenharia naval com excelência em cibersegurança ofensiva preditiva.

★ Diferencial chave em relação a consultorias genéricas



Inteligência Artificial Própria

Nossa IA toma decisões autônomas e identifica falhas de segurança replicando o comportamento de um hacker humano.

</> Desenvolvida do zero pela nossa equipe



Simulação Preditiva

Tecnologia exclusiva para simular ataques em ambientes virtuais idênticos aos reais, sem impactar os sistemas em produção.

⚙️ Tecnologia de última geração | Gémeo Digital



Compliance Integral

Não apenas cumprimos a ISO 27001 e IACS: integramos todos os requisitos em uma solução eficaz.

🤝 Um único parceiro para todas as normas



A Escolha Inteligente para Qualquer Setor

Otimização de recursos, total transparência e resultados mensuráveis desde o primeiro dia.

Cibersegurança Marítima Avançada

Protejamos Juntos os Nossos 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

A segurança da nossa infraestrutura marítima crítica é responsabilidade de todos.

Estamos prontos para acompanhar-vos.