MÁS ALLÁ DE LA CIBERSEGURIDAD: DESARROLLO DE LA RESILIENCIA DIGITAL MARÍTIMA MEDIANTE EL CONOCIMIENTO INTEGRADO DEL DOMINIO MARÍTIMO (iMDA)

PRODAR

Ciber Seguridad

Resilencia Digital Marítima

¿Cómo garantizamos la continuidad, la seguridad y la resiliencia de nuestras economías marítimas en un mundo cada vez más digital?


La Revolución Digital
ECOSISTEMAS ALTAMENTE INTERCONECTADOS
Los puertos se han convertido en
“Ecosistemas Ciber-físicos”.

THE THREAT LANDSCAPE

Riesgos cibernéticos que desafían la seguridad marítima y portuaria

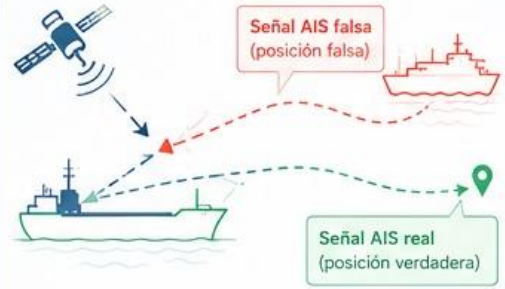
5 CIBERATAQUES QUE HAN AFECTADO PUERTOS ALREDEDOR DEL MUNDO

- **COLONIAL PIPELINE (EE. UU.) – 2021**
  Ransomware que afectó operaciones y provocó escasez de combustible.
- **PORT OF SAN DIEGO (EE. UU.) – 2022**
  Ataque de ransomware que afectó sistemas y operaciones del puerto.
- **DP WORLD (Global) – 2023**
  Interrupción de sistemas en múltiples puertos por ransomware.
- **PORT OF ANTWERP (BÉLGICA) – 2022**
  Brecha en sistemas, exposición de datos de clientes.
- **SHANGHAI PORT (CHINA) – 2020**
  Malware que afectó los sistemas internos del puerto.

Los puertos son objetivos estratégicos debido a su impacto económico global y su creciente digitalización.

6 AIS SPOOFING

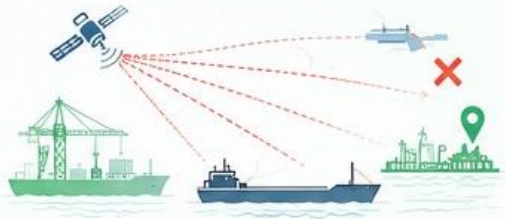
Manipulación de señales AIS para transmitir información falsa sobre la identidad, posición, rumbo o destino de un buque.



Impacto: colisiones, confusión operacional, contrabando, evasión de sanciones y amenazas a la seguridad marítima.

7 GPS JAMMING

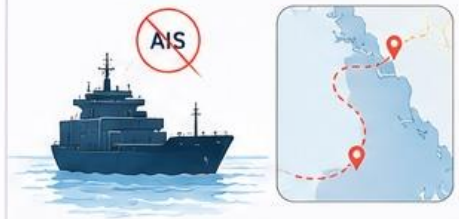
Interferencia intencional a las señales GPS para degradar o bloquear la navegación.



Impacto: pérdida de posicionamiento, encallamientos, colisiones, afectación de operaciones portuarias y sistemas sincronizados (tiempo).

8 DARK VESSELS

Buques que apagan o manipulan su AIS para operar sin ser detectados.



Impacto: actividades ilícitas (tráfico, pesca INDNR, evasión de sanciones), riesgos para la seguridad y el medio ambiente.

9 INSIDER THREATS

Empleados, contratistas o terceros con acceso legítimo que usan su privilegio para causar daño intencional o no intencional.

Impacto: robo de datos, sabotaje, interrupción de operaciones y compromiso de la seguridad de la información.

10 ATAQUES A SISTEMAS OT

Ataques dirigidos a sistemas de tecnología operacional (OT) que controlan procesos físicos en puertos y buques.

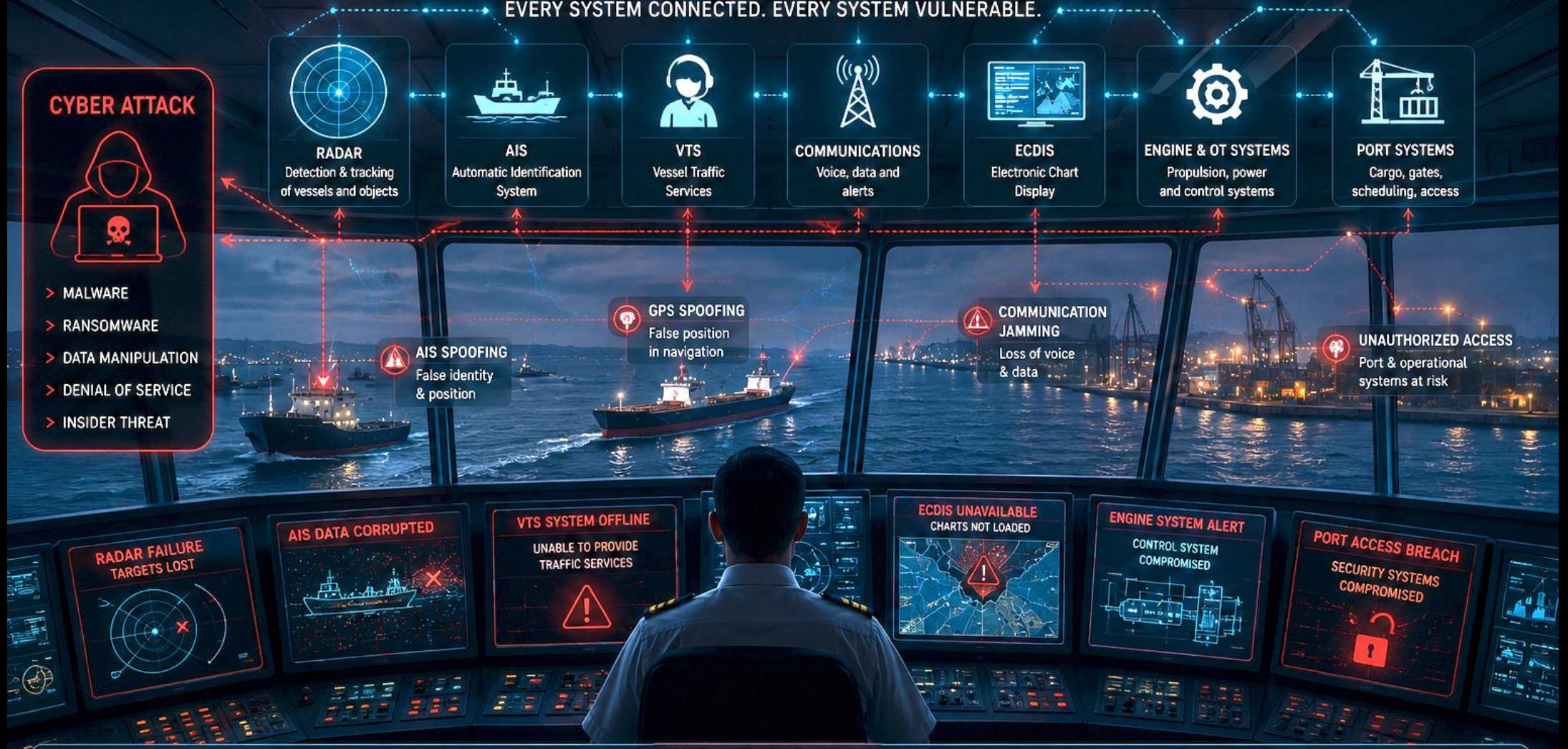
Impacto: daño físico, interrupción de operaciones, riesgos para la seguridad de las personas y el medio ambiente.

DEFENSA EN PROFUNDIDAD

- Concienciación y capacitación
- Gestión de accesos
- Monitoreo continuo y detección
- Segmentación de redes IT/OT
- Respuesta a incidentes
- Colaboración e intercambio de inteligencia

MARITIME CYBER THREATS

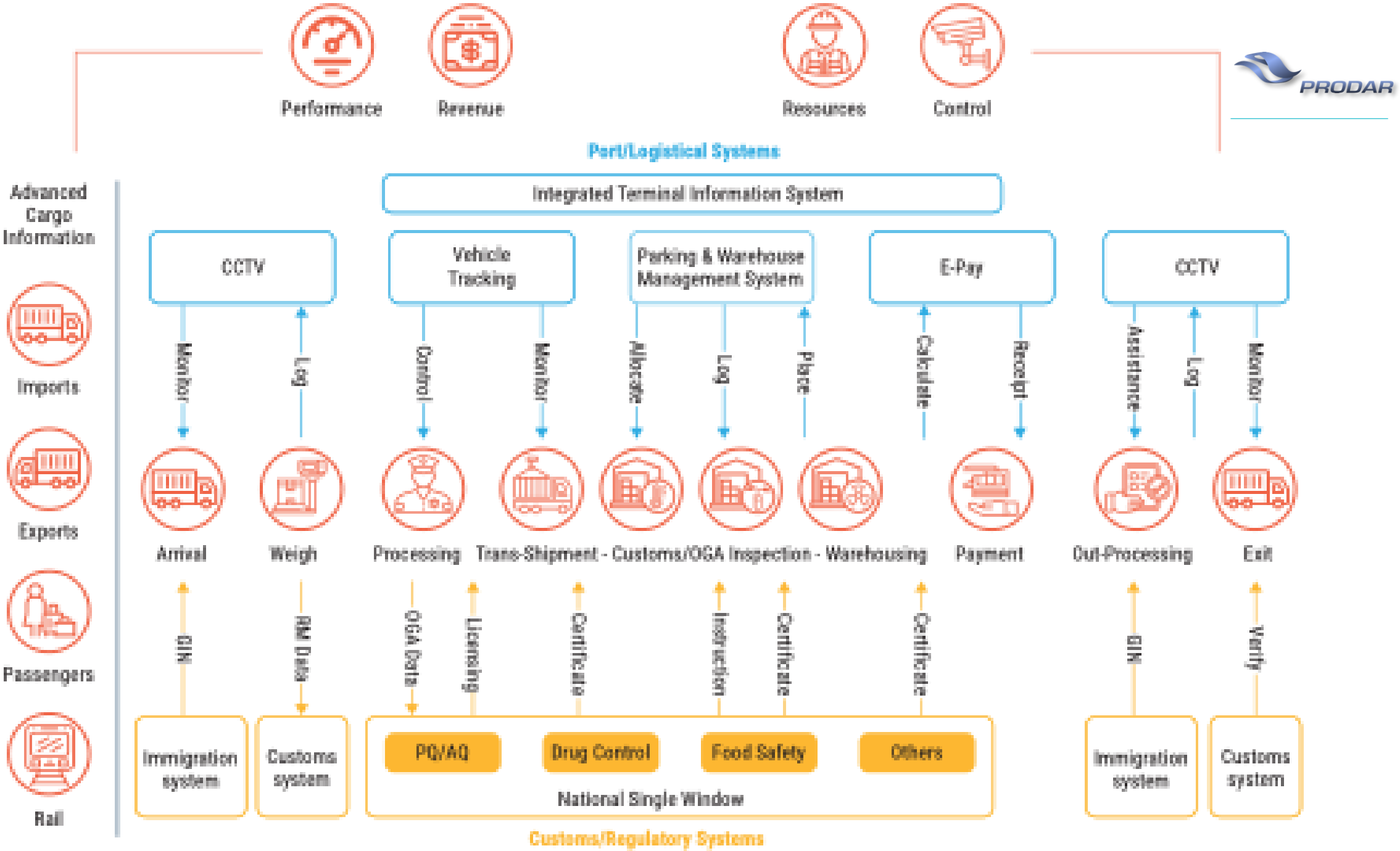
EVERY SYSTEM CONNECTED. EVERY SYSTEM VULNERABLE.



POTENTIAL IMPACT

- LOSS OF SITUATIONAL AWARENESS
- COLLISION RISK
- GROUNDING RISK
- PORT DISRUPTION & CONGESTION
- ENVIRONMENTAL DAMAGE
- ECONOMIC LOSS
- REPUTATIONAL DAMAGE
- NATIONAL SECURITY RISK

⚠ A CYBERATTACK CAN COMPROMISE THE SAFETY OF NAVIGATION, PEOPLE, ASSETS AND THE ENVIRONMENT. ⚠


Performance
Revenue
Resources
Control
PRODAR
Port/Logistical Systems
Advanced Cargo Information
Integrated Terminal Information System
CCTV
Vehicle Tracking
Parking & Warehouse Management System
E-Pay
CCTV
Monitor
Log
Control
Monitor
Allocate
Log
Place
Calculate
Receipt
Assistance
Log
Monitor
Imports
Exports
Passengers
Rail
Arrival
Weigh
Processing
Trans-Shipment - Customs/OGA Inspection - Warehousing
Payment
Out-Processing
Exit
EIR
RM Data
OGA Data
Licensing
Certificate
Instruction
Certificate
Certificate
EIR
Verify
Immigration system
Customs system
PQ/AQ
Drug Control
Food Safety
Others
National Single Window
Immigration system
Customs system
Customs/Regulatory Systems


PRODAR
Common Operational Picture
COP
VTS
GMDSS
LRIT
SAR
Fishing Vessel Monitoring
CSS
Situational Awareness - Response Coordination - Decision Making - Risk Management
National Operations & Surveillance Center

EL PAPEL DE LA
INTELIGENCIA ARTIFICIAL

- La IA no reemplaza operadores.
- La IA potencia operadores.
- La IA actúa como multiplicador de fuerza.
- Nos permite procesar volúmenes masivos de información.
- Y Acelerar la Toma de Decisiones

- Comportamientos anómalos.
- Embarcaciones oscuras.
- Manipulación de AIS.
- Actividades ilícitas.
- Riesgos de navegación.
- Incidentes de ciberseguridad.

Por ello existe una conclusión inevitable:

No existe Inteligencia Artificial confiable sin una sólida estrategia de ciberseguridad.

CONSTRUYENDO RESILIENCIA DIGITAL MARÍTIMA

La resiliencia no es una tecnología.
Es la integración de capacidades.

RECOMENDACIONES PARA AMÉRICA LATINA Y EL CARIBE

Desde nuestra experiencia regional,
proponemos cinco líneas estratégicas:

1

Adoptar una visión integral.

Integrar seguridad física, marítima y cibernética.

2

Fortalecer la gobernanza digital.

Desarrollar políticas, estándares y procedimientos comunes.

3

Implementar arquitecturas Zero Trust.

Particularmente en infraestructura crítica.

4

Desarrollar capacidades regionales.

Capacitación continua para operadores, analistas y tomadores de decisión.

5

Evolucionar hacia plataformas iMDA.

Capaces de fusionar información, generar inteligencia y apoyar decisiones estratégicas.

PRODAR

PORT CYBER MATURITY MODEL

A roadmap to cyber resilience and operational continuity across the port ecosystem

MATURITY LEVEL	1 INITIAL Ad Hoc / Reactive	2 REPEATABLE Aware / Basic	3 DEFINED Structured / Proactive	4 MANAGED Integrated / Advanced	5 OPTIMIZED Adaptive / Resilient
DESCRIPTION					
CAPABILITIES	Cybersecurity activities are informal and reactive. Limited awareness of cyber risks.	Basic cybersecurity practices are in place. Awareness of critical assets and risks.	Cybersecurity is managed and documented. Processes are standardized and proactive.	Cybersecurity is integrated into operations and decision-making. Continuous improvement.	Cybersecurity is adaptive and intelligence-driven. Resilience is built-in and continuously enhanced.
TECHNOLOGY & PRACTICES	• Limited policies or procedures • No asset inventory • Ad hoc risk management • Reactive to incidents	• Asset inventory (partial) • Basic risk assessments • Some documented policies • Incident response (basic)	• Complete asset inventory • Risk management process • Documented policies & standards • Incident response plan	• Integrated risk management • KPIs and performance metrics • Threat intelligence • Regular testing & drills	• Predictive risk management • AI-driven threat detection • Business continuity by design • Ecosystem collaboration
	Basic antivirus Perimeter firewall Limited access controls No monitoring	Firewalls & antivirus User access management Regular backups Basic log collection	Network segmentation Vulnerability management Security monitoring (SIEM) Access control (MFA)	Advanced threat detection OT/ICS security controls Security orchestration (SOAR) Continuous monitoring	AI/ML & behavioral analytics Zero Trust Architecture Digital twin & simulation Automated response
OUTCOME	High risk of disruption and operational impact	Reduced risk of incidents and service interruptions	Improved resilience and incident response	Strong cyber resilience and operational continuity	Adaptive, resilient and future-ready port

FOUNDATIONAL PILLARS (ENABLERS)

- LEADERSHIP & GOVERNANCE
- RISK MANAGEMENT & COMPLIANCE
- PEOPLE, AWARENESS & CULTURE
- TECHNOLOGY & ARCHITECTURE
- PARTNERSHIPS & INFORMATION SHARING
- CONTINUOUS IMPROVEMENT

INCREASING MATURITY → GREATER RESILIENCE → SAFER OPERATIONS → STRONGER ECONOMIES

PRODAR

MARITIME DIGITAL RESILIENCE IS NO LONGER A TECHNOLOGICAL ADVANTAGE.

IT IS A NATIONAL STRATEGIC CAPABILITY.

And probably one of the most decisive capabilities for the competitiveness, security and prosperity of our maritime nations in the coming decades.

PShield / Coastal Surveillance System / Vessel Traffic Service / Port Management and Information System / National Security / Critical Infraestructure

Contact: +1 (281) 536-4661 / edelangel@prodar.com

PRODAR

SOLUCIONES TECNOLOGICAS
Para Puertos Inteligentes

CONTACTO:
Eduardo Del Angel
edelangel@prodar.com
+1 281 536 4661