



GMV

# Servicios CERT en Puertos

---



11 de junio de 2024  
AMETIC



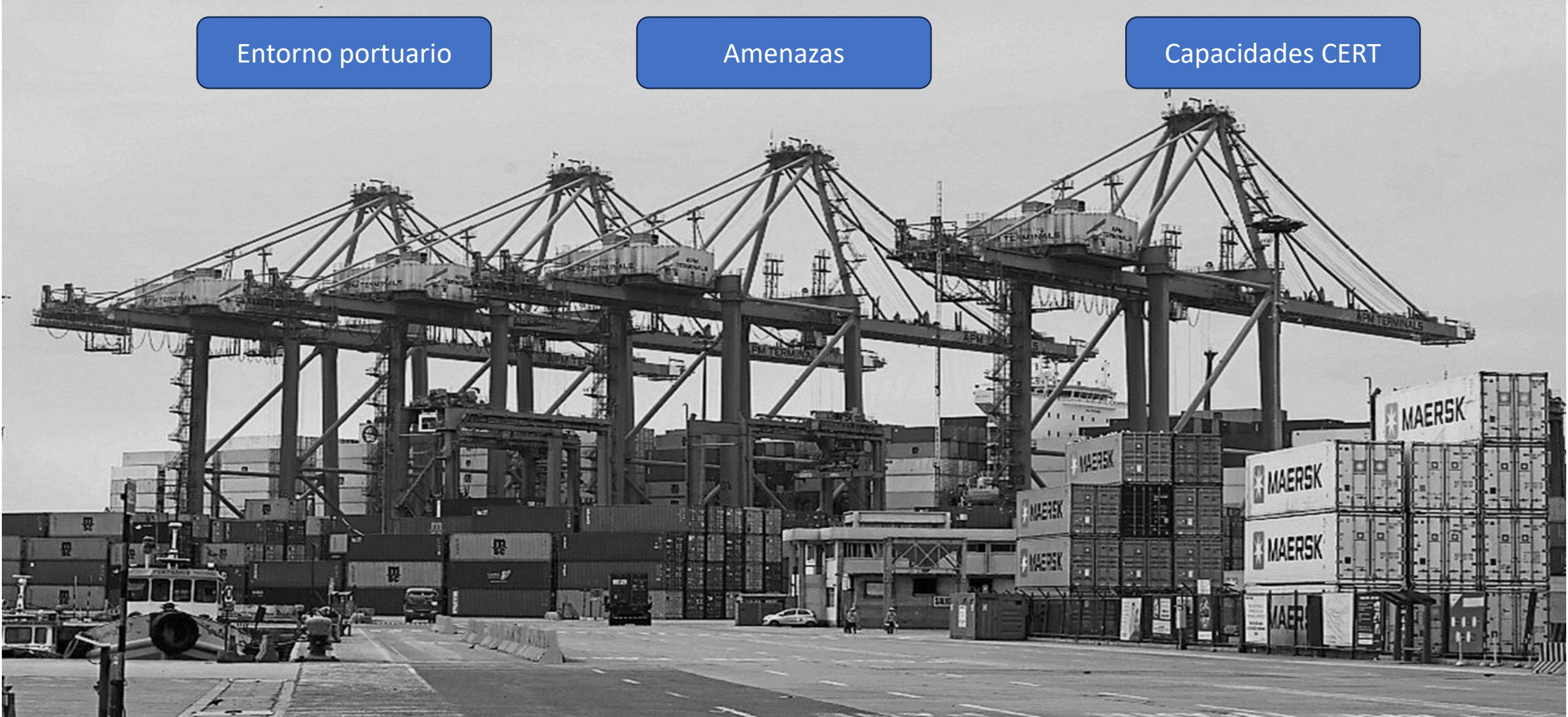
# CERT en Puertos



Entorno portuario

Amenazas

Capacidades CERT



# Entorno portuario

Pilar de la economía

● +80% COMERCIO MUNDIAL



● +100.000 BUQUES



● 175.000 EMPLEOS ESPAÑA



● 20% PIB TRANSPORTE

● +30 MILLONES CRUCERISTAS

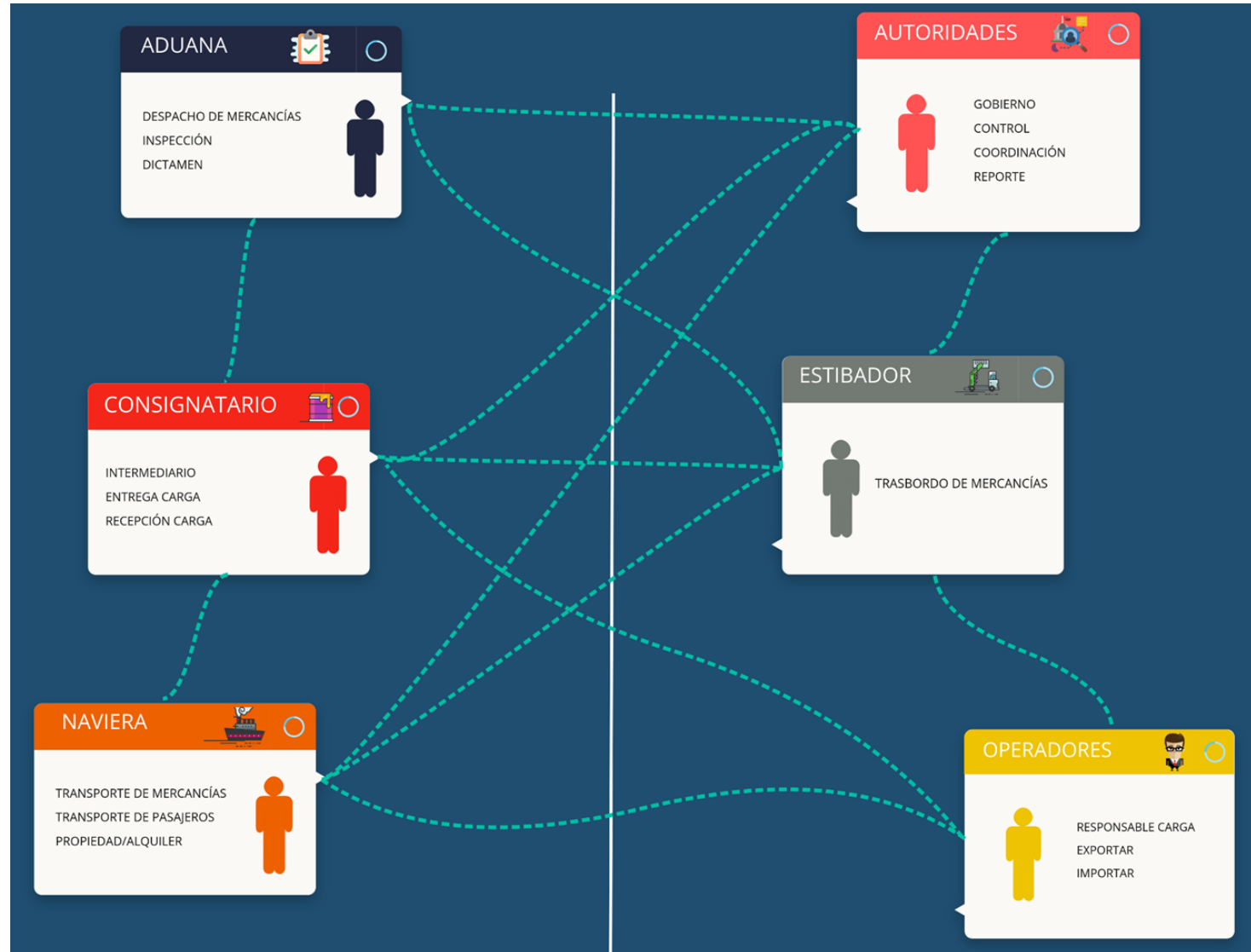


**gmv**  
INNOVATING SOLUTIONS

**Ametic**  
LA VOZ DE LA INDUSTRIA DIGITAL

# Entorno portuario

Multitud de agentes



# Entorno portuario

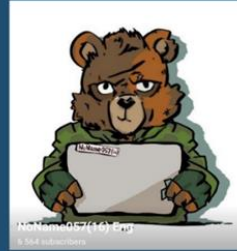
Sistemas heterogéneos



# Amenazas

Las de siempre

## Y SI OCURRIERA....



### DENEGACIÓN DE SERVICIO



### ACCESO INFORMACIÓN



### CADENA DE SUMINISTRO

**Vulnerabilidades al descubierto: más de 1.600 dispositivos de transporte marítimo susceptibles de sufrir ciberataques**

La digitalización se está acelerando en todos los sectores industriales, incluido el del transporte marítimo, en el que la automatización y la digitalización se aplican utilizando diversas tecnologías de la información y la comunicación (TIC). Sin embargo, a medida que avanza la tecnología del transporte marítimo, aumenta la preocupación por los ciberataques a los buques. En particular, los sistemas de transporte marítimo están conectados a través de redes como Internet y la comunicación por satélite. Estos sistemas son vulnerables a los ciberataques desde múltiples fuentes, lo que los convierte en una preocupación crucial en la industria de la ciberseguridad. El piratería de buques suele tener como objetivo los sistemas de transporte marítimo con vulnerabilidades expuestas en Internet, más que los ataques directos en los que los atacantes intentan acceder al buque. En este artículo, investigaremos el número de sistemas y dispositivos de transporte marítimo actualmente conectados a Internet y vulnerables a las amenazas de la piratería informática.

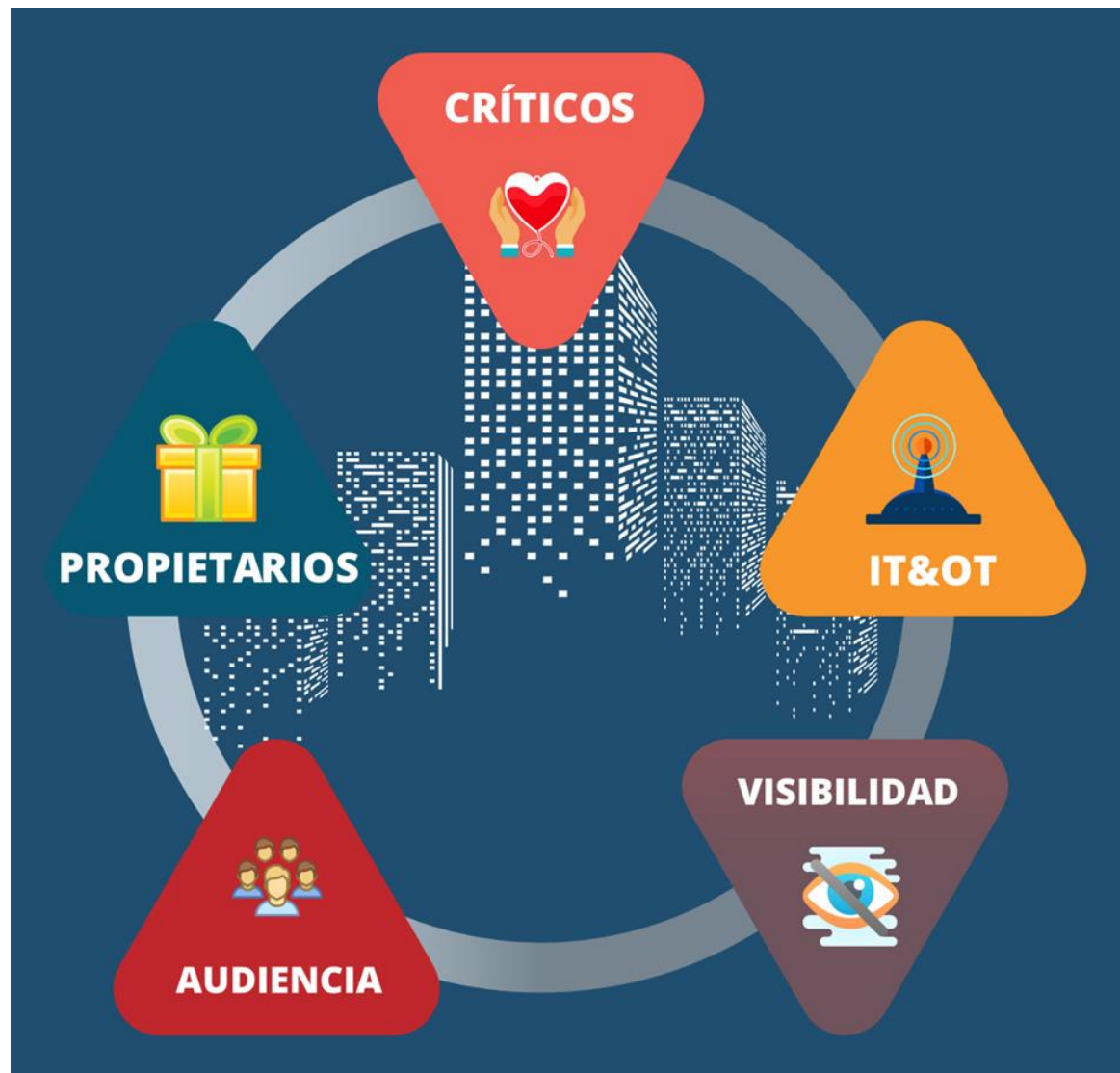


### VULNERABILIDADES DISPOSITIVOS



# Retos del CERT en este ámbito

Capacidades CERT



# Buscando lo evidente...

## Capacidades CERT

```
MALTRACKER 1.0
by gmv-cert

-----
MALTRACKER 1.0
-----
1) USE CASE 1: HUNT CRITICAL VULNERABILITIES
2) USE CASE 2: HUNT LEAKS
3) USE CASE 3: HUNT THREATS
4) USE CASE 4: TRACK INVENTORY
5) USE CASE 5: ANALYZE ATTACK
6) EXIT

MALTRACKER > Port Authority

*****
Total IP's analyzed: 53
IP's with critical vulnerabilities: 30
IP's without critical vulnerabilities: 19
IP's without validation: 4
*****
```

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/8.5.72

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:  
[Security Considerations How-To](#)  
[Manager Application How-To](#)  
[Clustering/Session Replication How-To](#)

Server Status  
Manager App  
Host Manager

Developer Quick Start  
Tomcat Setup  
First Web Application  
Beans & AAA  
JDBC Data Sources  
Examples  
Servlet Specifications  
Tomcat Versions

Managing Tomcat  
For security, access to the `manager/localhost` is restricted. Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.  
In Tomcat 8.5 access to the manager application is split between different users. [SMB Issues...](#)

Documentation  
[Tomcat 8.5 Documentation](#)  
[Tomcat Wiki](#)  
Find additional important configuration information in `$CATALINA_HOME/bin/README.txt`.  
Developers may be interested in:  
[Tomcat 8.5 Dev Database](#)  
[Tomcat 8.5 Javadocs](#)  
[Tomcat 8.5.0 Release Notes](#)

Getting Help  
**FAG and Mailing Lists**  
The following mailing lists are available:  
[tomcat-announce](#)  
Important announcements, releases, security vulnerability notifications, etc. (low volume).  
[tomcat-users](#)  
User support and discussion.  
[tomcat-dev](#)  
User support and discussion for [Apache DevList](#).  
[tomcat-jira](#)  
Development mailing list, including current messages.





# Monitorización

## Capacidades CERT




# Capacidades avanzadas


Capacidades CERT

## COBERTURA


**THREAT INTEL**




**DETT&CT**




**RED TEAM**



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Supply Chain Compromise	Control Panel Items	Security Support Provider	Access Token Manipulation	Access Token Manipulation	Input Capture	Process Policy	Logon Scripts	Input Capture	Domain Fronting	Data Compressed	Endpoint Denial of Service
Service Execution	PowerShell	AppCert DLLs	Extra Window Memory Injection	Control Panel Items	Credential Dumping	As the Host	Data from Network	Uncommonly Used Port	Data Encrypted	Network Denial of Service	
Drive-by Compromise	Regsvr32	Image File Execution Options Injection	Process Injection	LLMNR/NBT-NS Poisoning and Relay	System Owner/User Discovery	Exploitation of Remote Services	Clipboard Data	Standard Application Layer Protocol	Size Limits	Disk Content Wipe	
Spearphishing Attachment	Scheduled Task	Image File Execution Options Injection	Image File Execution Options Injection	Scripting	Brute Force	Application Window Discovery	Remote Desktop Protocol	Data from Local System	Connection Proxy	Protocol Wipe	
Exploit Public-Facing Application	Scheduled Task	Image File Execution Options Injection	Image File Execution Options Injection	Scheduled Task	Exploitation for Credential Access	Browser Bookmark Discovery	Remote File Copy	Data from Removable Media	Custom Corrupt	Exfiltration Over Alternative Protocol	
External Remote Services	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Forced Authentication	Domain Trust Discovery	Remote Services	Data Staged	Man in the Browser	Screen Capture	
Hardware Additions	Command-Line Interface	Account Manipulation	Account Manipulation	Bits Jobs	Hooking	Network Service Scanning	Replication Through Removable Media	Shared Media	Webroot	Taint Shared Content	
Replication Through Removable Media	Compiled HTML File	Appinit DLLs	Appinit DLLs	Bits Jobs	Input Prompt	Network Service Scanning	Shared Media	Video Capture			
Spearphishing Link	Dynamic Data Exchange	Authentication Package	Authentication Package	Bits Jobs	Network Sniffing	Network Share Discovery	Shared Media				
Spearphishing via Service Relationship	Execution through API	Bootkit	Bypass User Account Control	Bits Jobs	Network Sniffing	Network Sniffing	Shared Media				
Valid Accounts	Module Load	Browser Extensions	Bypass User Account Control	Bits Jobs	Network Sniffing	Network Sniffing	Shared Media				
	Exploitation for Client Execution	Change Default File Association	Order Hijacking	Code Signing	Password Filter DLL	Peripheral Device Discovery	Taint Shared Content				
	Graphical User Interface	Component Firmware	Privilege Escalation	Compiled HTML File	Private Keys						
	InstallUtil										



INNOVATING SOLUTIONS



LA VOZ DE LA INDUSTRIA DIGITAL

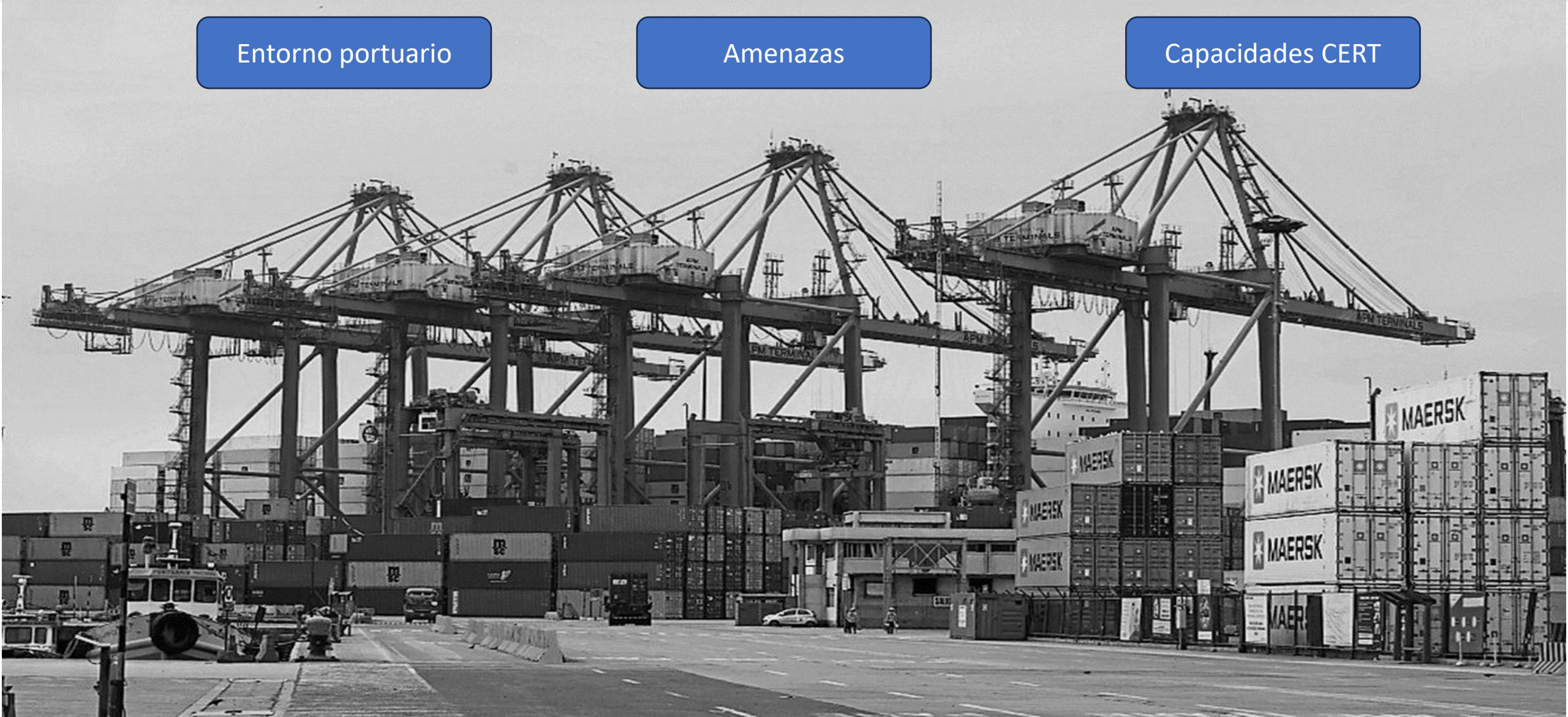
# CERT en Puertos



Entorno portuario

Amenazas

Capacidades CERT





**¡Muchas gracias!**

Para cualquier consulta o más información:

-  [www.ametic.es](http://www.ametic.es)
-  [ametic@ametic.es](mailto:ametic@ametic.es)
-  [@AMETIC\\_es](#) [#AMETIC](#)

