Sin ciberseguridad no hay Smart Ports

Rafael Company Peris

Seguridad

Ciberseguridad, Smart Ports, Transformación digital portuaria, Directiva NIS2

Cada día, miles de buques conectan puertos de todo el mundo transportando más del 80 % del comercio internacional por volumen. Detrás de cada escala existe una compleja red de sistemas digitales que coordina la llegada del buque, la asignación del atraque, la planificación de las operaciones, el movimiento de contenedores, los controles aduaneros y el transporte terrestre de las mercancías entre otros. Lo que hace apenas dos décadas dependía principalmente de infraestructuras físicas y de la coordinación entre personas, hoy se apoya en plataformas digitales, sensores iot, inteligencia artificial, redes de comunicaciones y sistemas de automatización.

Esta transformación ha convertido a los puertos en auténticos **ecosistemas ciberfísicos**. La eficiencia alcanzada gracias a la **digitalización** ha permitido reducir tiempos de escala, optimizar recursos y mejorar la trazabilidad de las mercancías. Sin embargo, también ha generado una creciente dependencia tecnológica que amplía la superficie de exposición frente a **ciberamenazas** cada vez más sofisticadas.

Los **ciberataques** ya no afectan únicamente a ordenadores o bases de datos. Pueden paralizar terminales, interrumpir operaciones logísticas, comprometer sistemas industriales o alterar servicios esenciales para el comercio internacional. En un entorno donde la disponibilidad de la información es tan importante como la disponibilidad de las infraestructuras físicas, la **ciberseguridad** ha dejado de ser una función técnica para convertirse en un **elemento estratégico de la gestión portuaria**.

La Unión Europea ha respondido a esta evolución mediante un conjunto de iniciativas que refuerzan la protección de las infraestructuras críticas, entre las que destacan la **Directiva NIS2**, la **Directiva sobre Resiliencia de las Entidades Críticas (CER),** el **Cyber Resilience Act** y el **Reglamento de Inteligencia Artificial**. Todas ellas reflejan una misma realidad: la seguridad del sistema portuario europeo depende cada vez más de su capacidad para anticipar, resistir y recuperarse de incidentes que combinan **dimensiones físicas** y **digitales**.

Este artículo analiza cómo la transformación digital está redefiniendo la **ciberseguridad en los puertos europeos,** cuáles son las principales amenazas que afronta el sector y por qué la protección del ciberespacio se ha convertido en un requisito indispensable para garantizar la continuidad de unas infraestructuras críticas de las que depende buena parte de la economía mundial.

La revolución digital de los puertos

Durante siglos, la **competitividad de un puerto** estuvo determinada por factores físicos como la profundidad de sus dársenas, la longitud de los muelles, la capacidad de almacenamiento o la calidad de sus conexiones terrestres. Aunque estos elementos continúan siendo esenciales, la transformación digital ha incorporado un nuevo componente que resulta igual de determinante: la capacidad para **gestionar información** de forma **rápida**, **segura** y **eficiente**.

Los **puertos modernos** ya no son únicamente espacios donde se transfieren mercancías entre el transporte marítimo y terrestre. Son **plataformas logísticas** altamente conectadas en las que confluyen navieras, terminales, autoridades portuarias, agentes consignatarios, operadores ferroviarios, aduanas, cuerpos de seguridad y un amplio ecosistema de proveedores tecnológicos. La coordinación entre todos ellos depende, en gran medida, de **sistemas digitales** que permiten intercambiar información en tiempo real y optimizar la toma de decisiones.

La evolución hacia el concepto de **Smart Port** ha acelerado este proceso. Tecnologías como el Internet de las Cosas (IoT), la inteligencia artificial, el análisis masivo de datos,

las redes privadas 5G, los gemelos digitales o la computación en la nube están transformando la forma de gestionar las operaciones portuarias. **Sensores distribuidos** monitorizan el estado de infraestructuras críticas, **algoritmos** optimizan el tráfico interno, **plataformas digitales** facilitan la coordinación logística y **sistemas inteligentes** permiten anticipar incidencias antes de que afecten a la operativa.

Otro elemento clave en esta transformación ha sido la consolidación de los **Port Community Systems (PCS)**, plataformas que facilitan el intercambio seguro de información entre los distintos actores de la comunidad portuaria. Gracias a estos sistemas, documentos que tradicionalmente se gestionaban en papel han sido sustituidos por procesos digitales que reducen tiempos administrativos, mejoran la trazabilidad y aumentan la eficiencia de las operaciones.

Paralelamente, la **automatización de terminales** ha impulsado la incorporación de equipos conectados capaces de operar con un elevado grado de autonomía. Grúas automatizadas, vehículos guiados automáticamente (AGV), sistemas de control industrial y soluciones de mantenimiento predictivo permiten **incrementar la productividad** y **reducir costes operativos**. Sin embargo, esta evolución también implica una creciente interdependencia entre las **tecnologías de la información (IT)** y las **tecnologías operacionales (OT),** tradicionalmente gestionadas de forma independiente.

Esta convergencia constituye uno de los mayores desafíos de la ciberseguridad portuaria. Mientras los **sistemas IT** fueron diseñados para gestionar información corporativa, los **sistemas OT** controlan procesos físicos cuya disponibilidad resulta crítica para la continuidad de las operaciones. La conexión entre ambos entornos aporta importantes beneficios, pero también crea nuevas vías de acceso que pueden ser explotadas por actores maliciosos.

La digitalización también ha incrementado la dependencia de **proveedores externos de software**, **servicios en la nube** y **dispositivos conectados**. Cada nueva integración tecnológica incorpora ventajas operativas, pero también introduce nuevos riesgos asociados a vulnerabilidades, errores de configuración o compromisos en la cadena de suministro digital. La seguridad del puerto deja así de depender únicamente de sus propios sistemas y pasa a estar condicionada por un **ecosistema tecnológico** mucho más amplio.

Este cambio de escenario obliga a replantear el concepto tradicional de seguridad. Proteger el perímetro físico de las instalaciones ya no es suficiente. La verdadera **frontera de un puerto inteligente** se extiende ahora a redes de comunicaciones, plataformas digitales, sensores, dispositivos móviles y servicios distribuidos que operan dentro y fuera del recinto portuario.

En consecuencia, la **ciberseguridad** deja de entenderse como una función de soporte tecnológico para convertirse en un **elemento esencial de la continuidad operativa**. La disponibilidad de un sistema de gestión portuaria, la integridad de los datos intercambiados entre operadores o la protección de una red industrial pueden tener hoy

un impacto tan decisivo sobre la actividad del puerto como el funcionamiento de una grúa o la disponibilidad de un atraque.

La evolución hacia puertos cada vez más inteligentes no solo está transformando la forma de operar. También está redefiniendo el concepto mismo de seguridad. Comprender esta nueva realidad constituye el primer paso para afrontar un entorno en el que las amenazas ya no distinguen entre el mundo físico y el digital.

El nuevo mapa de las ciberamenazas: cuando el riesgo digital se convierte en riesgo operativo

La **digitalización** ha transformado profundamente la actividad portuaria, pero también ha modificado la naturaleza de las amenazas a las que se enfrenta el sector. Si hace apenas una década la principal preocupación era proteger la información corporativa frente al robo o la pérdida de datos, hoy el **objetivo de un ciberataque** puede ser mucho más ambicioso: interrumpir la actividad de una terminal, comprometer un sistema industrial, alterar la cadena logística o afectar al suministro de servicios esenciales.

Esta evolución responde, en gran medida, al creciente **valor estratégico de los puertos**. Como nodos fundamentales del comercio internacional y de las cadenas de suministro, concentran un elevado volumen de mercancías, infraestructuras críticas, información sensible y servicios cuya interrupción puede generar importantes consecuencias económicas y sociales. Para un ciberdelincuente, un grupo criminal organizado o incluso un actor patrocinado por un Estado, un puerto representa un objetivo de alto impacto.

Además, la **motivación de los ataques** ha cambiado. Mientras que en el pasado predominaban los incidentes orientados al robo de información, en la actualidad proliferan campañas dirigidas a **paralizar operaciones**, **extorsionar económicamente** a las organizaciones o **desestabilizar infraestructuras estratégicas**. La frontera entre la ciberdelincuencia, el espionaje industrial y las amenazas híbridas es cada vez más difusa.

Del ransomware al sabotaje operativo

El **ransomware** continúa siendo una de las principales amenazas para el sector marítimo-portuario. Este tipo de ataque cifra la información de una organización e **impide el acceso a sistemas críticos** hasta que se paga un rescate. Sin embargo, su impacto va mucho más allá de la pérdida de datos.

En un **puerto altamente digitalizado**, la indisponibilidad de plataformas de gestión documental, sistemas de planificación de terminales o aplicaciones logísticas puede provocar retrasos en las operaciones, congestión en los accesos, dificultades para coordinar el movimiento de mercancías y pérdidas económicas significativas para todos los actores de la comunidad portuaria.

Uno de los ejemplos más conocidos fue el ataque **NotPetya** sufrido por **Maersk** en 2017. Aunque la compañía no era el objetivo inicial del **malware**, la infección se propagó rápidamente por su red corporativa y afectó a cientos de aplicaciones y miles de servidores en todo el mundo. La recuperación requirió semanas de trabajo y supuso pérdidas estimadas en cientos de millones de dólares. Más allá del impacto económico, el incidente evidenció hasta qué punto una gran organización logística podía quedar prácticamente paralizada por un ciberataque.

Casos más recientes, como los incidentes sufridos por **DP World Australia** en 2023 o el **Puerto de Nagoya** ese mismo año, confirman que estas amenazas continúan evolucionando. En ambos casos, las operaciones portuarias experimentaron **interrupciones relevantes** que afectaron al movimiento de mercancías y obligaron a activar procedimientos de contingencia para restablecer la actividad.

Estos episodios demuestran que la ciberseguridad ya no puede medirse únicamente por el número de equipos comprometidos o por el volumen de información afectada. Su verdadero impacto debe evaluarse en función de las consecuencias sobre la **continuidad de las operaciones**.

La cadena de suministro digital: el eslabón más débil

La creciente **interconexión** entre organizaciones ha convertido la cadena de suministro digital en uno de los principales vectores de riesgo.

Un puerto mantiene conexiones permanentes con navieras, terminales, transitarios, autoridades aduaneras, proveedores de software, empresas de mantenimiento, operadores logísticos y numerosos servicios externos. Cada una de estas relaciones implica el **intercambio de información** y, en muchos casos, la **interconexión de sistemas**.

Esta realidad genera un escenario donde la **seguridad del conjunto** depende del nivel de protección del eslabón más vulnerable.

Los ataques dirigidos contra **proveedores tecnológicos** se han multiplicado en los últimos años porque permiten comprometer simultáneamente a múltiples organizaciones utilizando un único punto de acceso. Este tipo de amenazas obliga a ampliar la visión tradicional de la ciberseguridad. Ya no basta con proteger la infraestructura propia; resulta imprescindible evaluar el **riesgo asociado a terceros**, establecer requisitos de seguridad para proveedores y supervisar continuamente las relaciones de confianza existentes dentro del ecosistema digital.

La convergencia entre IT y OT: una nueva superficie de ataque

Otra de las características que definen la evolución de las amenazas es el creciente interés por los **sistemas industriales**.

Durante muchos años, las **tecnologías operacionales (OT)** permanecieron aisladas de las redes corporativas y, en consecuencia, presentaban una exposición limitada frente a ciberataques. Sin embargo, la digitalización de las operaciones ha favorecido una integración progresiva entre los **entornos IT** y **OT** para mejorar la eficiencia, facilitar el mantenimiento remoto y optimizar la gestión de los activos.

Aunque esta convergencia aporta importantes ventajas operativas, también incrementa significativamente la **superficie de ataque**.

Grúas automatizadas, sistemas de control de accesos, redes eléctricas, estaciones de suministro energético, instalaciones de combustible o infraestructuras de comunicación forman parte de un entorno donde un **incidente cibernético** puede tener consecuencias físicas inmediatas. La manipulación de estos sistemas no solo compromete la información, sino que puede afectar directamente a la seguridad de las personas y a la continuidad de las operaciones.

Esta realidad exige **estrategias específicas de protección** para los **entornos OT**, diferentes de las aplicadas tradicionalmente a las redes corporativas.

Nuevas amenazas para un puerto conectado

El panorama de riesgos continúa ampliándose con la incorporación de nuevas tecnologías.

La utilización de sistemas de navegación y posicionamiento por satélite ha incrementado la preocupación por los ataques de **interferencia (jamming)** y **suplantación de señal (spoofing)**, capaces de alterar la información de posicionamiento utilizada por embarcaciones y determinados servicios portuarios.

Del mismo modo, el creciente empleo de **inteligencia artificial** plantea un **doble desafío**. Por una parte, ofrece capacidades avanzadas para detectar anomalías, identificar patrones de comportamiento y mejorar la respuesta frente a incidentes. Por otra, facilita que los atacantes automaticen campañas de phishing, desarrollen códigos maliciosos con mayor rapidez o generen contenidos falsos cada vez más difíciles de identificar.

Las **amenazas híbridas** añaden una dimensión adicional a este escenario. La combinación de ciberataques con campañas de desinformación, sabotaje físico o presión geopolítica pone de manifiesto que la protección de los puertos trasciende el ámbito estrictamente tecnológico y forma parte de la seguridad económica y estratégica de la Unión Europea.

Una cuestión de continuidad operativa

Todos estos ejemplos conducen a una misma conclusión: el principal riesgo ya no reside únicamente en sufrir un ciberataque, sino en la **capacidad de mantener la actividad** cuando este se produce.

La experiencia demuestra que ninguna organización puede garantizar una **protección absoluta** frente a un entorno de amenazas en constante evolución. Por ello, el verdadero **reto** consiste en reducir la probabilidad de éxito de los ataques, detectar los incidentes de forma temprana, responder con rapidez y recuperar la operativa con el menor impacto posible.

Este cambio de perspectiva explica por qué la **ciberseguridad** ha pasado a ocupar un lugar prioritario en las estrategias de gestión de infraestructuras críticas. La cuestión ya no es únicamente proteger sistemas informáticos, sino asegurar el funcionamiento continuo de unos servicios esenciales sobre los que se sustenta buena parte del comercio internacional.

Europa responde: un nuevo marco para proteger las infraestructuras críticas

La creciente digitalización de los puertos y el incremento de las ciberamenazas han llevado a la **Unión Europea** a replantear su **estrategia de protección de las infraestructuras críticas**. La ciberseguridad ya no puede abordarse únicamente desde una perspectiva tecnológica; requiere un enfoque integral que combine gobernanza, gestión del riesgo, cooperación y continuidad operativa.

En este contexto surge la **Directiva NIS2**, aprobada en 2022, que sustituye a la anterior Directiva NIS y amplía de forma significativa su alcance. Más allá de introducir nuevas obligaciones regulatorias, NIS2 representa un cambio de paradigma: la ciberseguridad pasa a ser una responsabilidad estratégica de la organización y no únicamente de sus departamentos tecnológicos.

Para las autoridades portuarias, terminales y otros operadores considerados entidades esenciales o importantes, la directiva exige implantar medidas de gestión del riesgo, reforzar la seguridad de la cadena de suministro, establecer procedimientos de notificación de incidentes, desarrollar planes de continuidad y garantizar la implicación de la alta dirección en la toma de decisiones relacionadas con la ciberseguridad.

Sin embargo, NIS2 no actúa de forma aislada. Forma parte de un ecosistema normativo más amplio que incluye la **Directiva sobre Resiliencia de las Entidades Críticas (CER)**, orientada a reforzar la protección frente a riesgos físicos y tecnológicos; el **Cyber Resilience Act (CRA)**, que establece requisitos de ciberseguridad para productos con componentes digitales; y el **Reglamento Europeo de Inteligencia Artificial (AI Act)**, que introduce obligaciones específicas para sistemas de IA de alto riesgo.

El **objetivo común** de estas iniciativas es fortalecer la autonomía estratégica europea y garantizar que las infraestructuras críticas puedan seguir prestando servicios esenciales incluso en escenarios de elevada presión tecnológica o geopolítica.

Para el sector portuario, este marco representa una **oportunidad** para avanzar hacia modelos de gestión donde la **ciberseguridad** se integra en la planificación estratégica, la continuidad del negocio y la gestión global del riesgo.

La ciberseguridad del puerto inteligente

La evolución de las amenazas obliga a replantear también la forma en que se protege un puerto. Las estrategias tradicionales, basadas en la protección del perímetro y en la separación entre tecnologías de la información (IT) y tecnologías operacionales (OT), resultan **insuficientes** para responder a un **entorno altamente interconectado**.

El puerto inteligente requiere una visión integrada de la ciberseguridad. Esto implica aplicar principios como la segmentación de redes, la autenticación robusta, la supervisión continua, la gestión de vulnerabilidades y el intercambio de inteligencia sobre amenazas. Modelos como **Zero Trust**, que parten de la premisa de que ningún usuario o dispositivo debe considerarse confiable por defecto, comienzan a incorporarse progresivamente a las arquitecturas de seguridad de las infraestructuras críticas.

La **protección de los sistemas OT** constituye otro de los **grandes desafíos**. A diferencia de los entornos IT, donde la actualización de software y la aplicación de parches forman parte de la operación habitual, muchos sistemas industriales deben priorizar la disponibilidad del servicio y cuentan con ciclos de vida mucho más largos. Esto obliga a desarrollar estrategias específicas de protección que compatibilicen la seguridad con la continuidad operativa.

La **inteligencia artificial** también está modificando la forma de gestionar la ciberseguridad. Su capacidad para analizar grandes volúmenes de información facilita la detección temprana de anomalías, la correlación de eventos y la identificación de comportamientos sospechosos. No obstante, estas mismas capacidades pueden ser utilizadas por actores maliciosos para automatizar ataques o desarrollar campañas de ingeniería social cada vez más sofisticadas, lo que exige mantener una supervisión humana y una evaluación continua de los riesgos asociados a estas tecnologías.

Junto a las soluciones tecnológicas, el **factor humano** continúa siendo uno de los elementos más importantes de la ciberseguridad. La formación del personal, los ejercicios de respuesta a incidentes, la coordinación entre organizaciones y el desarrollo de una cultura de seguridad constituyen medidas tan relevantes como la implantación de nuevas herramientas. La experiencia demuestra que la capacidad para detectar y gestionar un incidente depende tanto de las personas y los procesos como de la tecnología disponible.

En definitiva, la ciberseguridad del puerto inteligente no se construye únicamente mediante firewalls o sistemas de detección de intrusiones. Se basa en **una combinación equilibrada de tecnología**, **gobernanza**, **cooperación** y **preparación** para responder a incidentes cada vez más complejos.

Conclusiones

La **transformación digital** ha convertido a los puertos en uno de los mejores ejemplos de **infraestructura crítica ciberfísica**. La incorporación de tecnologías avanzadas ha incrementado la eficiencia y la competitividad del sector, pero también ha ampliado la superficie de exposición frente a amenazas que evolucionan con gran rapidez.

En este escenario, la ciberseguridad deja de ser un requisito tecnológico para convertirse en un **componente esencial de la gestión portuaria**. Proteger redes, sistemas industriales y plataformas digitales significa proteger la continuidad de las operaciones, la confianza de la comunidad portuaria y la estabilidad de unas cadenas logísticas de las que depende buena parte del comercio internacional.

La **respuesta europea,** materializada en iniciativas como **NIS2**, **CER**, **CRA** o **AI Act**, refleja una visión cada vez más integrada de la protección de las infraestructuras críticas. El objetivo ya no consiste únicamente en evitar incidentes, sino en desarrollar organizaciones capaces de anticiparse, responder y recuperarse con rapidez cuando estos se producen.

Para los puertos europeos, este cambio representa mucho más que un **desafío regulatorio**. Constituye una oportunidad para reforzar su competitividad, consolidar la confianza de operadores y clientes y avanzar hacia un modelo de gestión donde la seguridad forma parte del valor que ofrecen al conjunto de la cadena logística.

Durante décadas, la fortaleza de un puerto se midió por la capacidad de sus infraestructuras físicas y por la eficiencia de sus operaciones. En la **economía digital**, esa fortaleza dependerá también de su capacidad para **proteger el ciberespacio** sobre el que se sustentan esas operaciones. La ciberseguridad ha dejado de ser un elemento de soporte para convertirse en uno de los **pilares de la competitividad**, la **resiliencia** y la **sostenibilidad** del sistema portuario europeo.

Referencias bibliográficas

Agencia de la Unión Europea para la Ciberseguridad (ENISA). *ENISA Threat Landscape 2024*.

Comisión Europea. *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)*.

Comisión Europea. *Directive (EU) 2022/2557 on the resilience of critical entities (CER)*.

Comisión Europea. *Cyber Resilience Act* (Regulation (EU) 2024/2847).

Comisión Europea. *Artificial Intelligence Act* (Regulation (EU) 2024/1689).

International Maritime Organization (IMO). *Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.2)*.

United Nations Conference on Trade and Development (UNCTAD). *Review of Maritime Transport 2024*.

European Maritime Safety Agency (EMSA). *Maritime Cybersecurity Best Practices*.

European Sea Ports Organisation (ESPO). *ESPO Environmental Report and Digitalisation Papers*.

World Economic Forum. *Global Cybersecurity Outlook*.

Pharos 39.0

Valenciaport Knowledge Hub

www.pharos390.com
info@pharos390.com