WISTA Perú

EL RIESGO CIBERNÉTICO EN EL SECTOR MARÍTIMO

#MiércolesDeTI

Por Eileen Chavesta Paico

EL RIESGO CIBERNÉTICO EN EL SECTOR MARÍTIMO

El sector marítimo desempeña un papel fundamental en la economía y en la sociedad, ya que representa un gran segmento del transporte total de mercancías y pasajeros en el mundo, es así como las organizaciones marítimas facilitan las actividades de la cadena de suministro nacional e internacional.

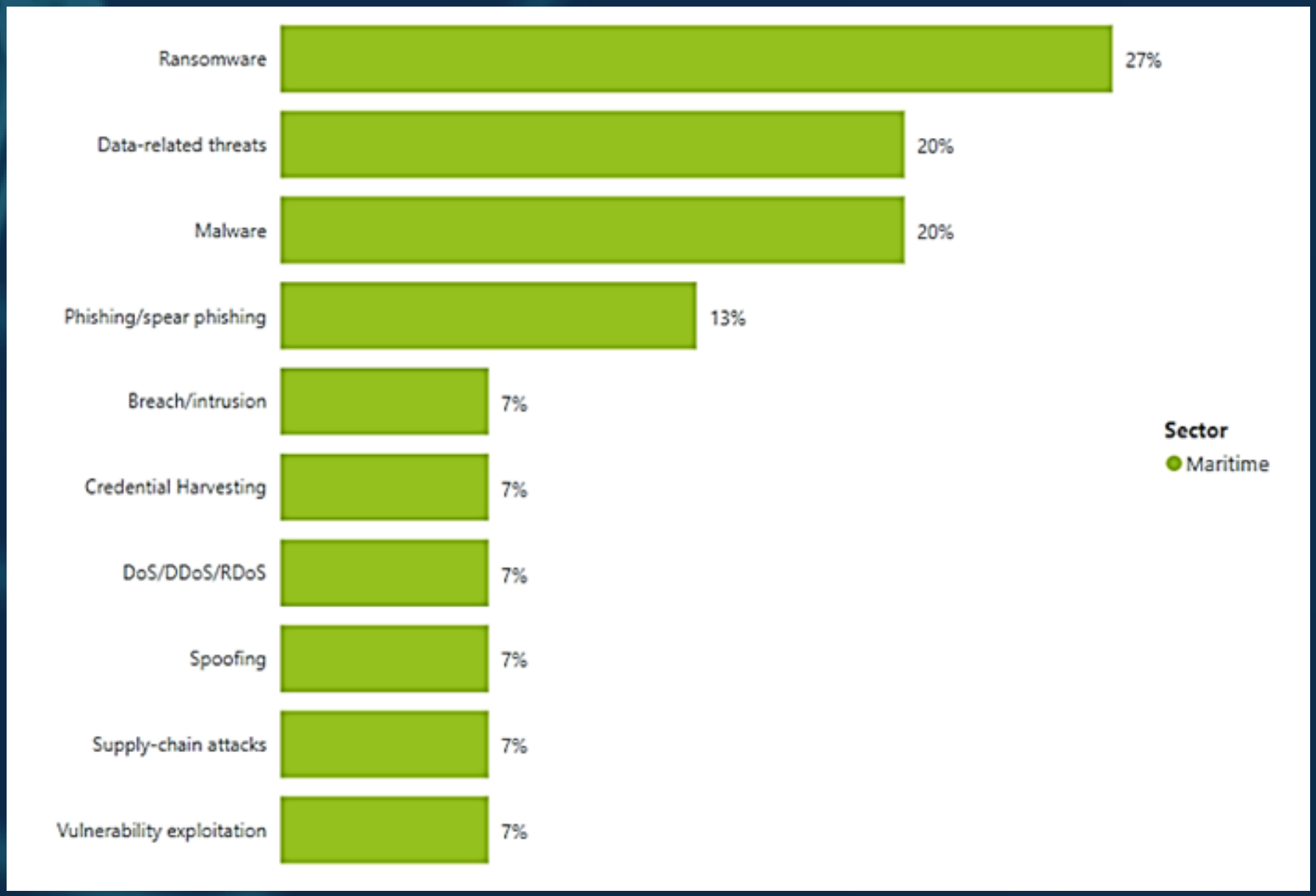
En los últimos años ha experimentado una gran transformación digital constante en sus operaciones logísticas y marítimas, adoptando nuevas tecnologías, como la implementación de sistemas comunitarios portuarios y la adopción de sistemas de ventanillas únicas marítima, ayudando a la simplificación de la información y procesamiento de estos con mayor rapidez. Por ello, el sector marítimo también se encuentra expuesto a ciberataques contra puertos y compañías navieras.

De acuerdo con el último reporte de European Union Agency for Cybersecurity (ENISA, 2023), las principales amenazas que afectan al sector marítimo, tal como se puede apreciar, son:

- Ataques ransomware.
- Amenazas relacionadas con los datos.
- Malware.
- Ataques de denegación de servicio (DoS), de denegación de servicio distribuido (DDos) y de denegación de servicio de rescate (RDos).

EL RIESGO CIBERNÉTICO EN EL SECTOR MARÍTIMO

- Suplantación de identidad.
- Ataques a la cadena de suministro.



EL RIESGO CIBERNÉTICO EN EL SECTOR MARÍTIMO

De acuerdo con la Organización de las Naciones Unidas (2021) es importante analizar los factores claves que convierten a las organizaciones marítimas en blancos atractivos para los ataques cibernéticos en todo el mundo.

Existen dos principales: la digitalización y automatización de las operaciones portuarias y marítimas, dado que cuanto más las empresas automaticen y digitalicen se vuelve más vulnerables a los ciberataques y el segundo factor es que las organizaciones marítimas son centros y depósitos de datos logísticos, esto quiere decir, que debido a la gran cantidad de información valiosa y crítica que manejan y al impacto que una interrupción en su funcionamiento podría repercutir en la economía y la seguridad de un país o región.

Entre otras razones más comunes se incluyen:

- Sabotaje: Un ciberataque puede ser utilizado para sabotear los sistemas críticos de un puerto marítimo, lo que podría tener graves consecuencias para la seguridad y el funcionamiento del mismo.
- Extorsión: Los piratas informáticos pueden realizar ciberataques para extorsionar a los puertos marítimos y exigir el pago de un rescate a cambio de no divulgar información sensible o crítica.

EL RIESGO CIBERNÉTICO EN EL SECTOR MARÍTIMO

- Robo de información: Los ciberataques también pueden tener como objetivo el robo de información valiosa, como planes de seguridad, registros de carga, datos financieros o información de clientes, entre otros.

- Espionaje industrial: Los piratas informáticos pueden ser contratados por empresas competidoras para acceder a información confidencial y secreta de los puertos marítimos y utilizarla en su propio beneficio.

- Terrorismo: Los grupos terroristas pueden realizar ciberataques a puertos marítimos como parte de una estrategia para causar daño físico o interrumpir el flujo de comercio y transporte marítimo.

Algunos ataques a las comunidades portuarias fueron:

- Mayo 2022: la Autoridad Portuaria de Londres sufrió un ataque DDoS, que desconectó temporalmente el sitio web del Puerto. Se cree que el ataque fue llevado a cabo por un grupo terrorista con fines más políticos que financieramente.

- Enero 2021: se informó que dos puertos marítimos indios fueron atacados por piratas informáticos.

EL RIESGO CIBERNÉTICO EN EL SECTOR MARÍTIMO

- Agosto 2021: la Autoridad Portuaria de Houston fue blanco de cybersecurity attack.

- Agosto 2021: la Compagnie générale de navigation sur le Lac Léman fue víctima de un ciberataque en su sitio web, "logrando" robar los datos bancarios de algunos de sus clientes.

- Junio 2021: la Autoridad de Buques de Vapor de Massachusetts tuvo un ataque de ransomware que destruyó su sitio web y provocó retrasos para los pasajeros del ferry.

- Febrero 2021: la empresa francesa de barcos Beneteau, comunicó que había sufrido una intrusión de malware en algunos de sus servidores, por lo que decidieron desconectar todos los "sistemas de información" para evitar que el malware se propague. Como consecuencia tuvieron que detener sus actividades de producción durante algunos días.

- En 2018: la naviera Cosco sufrió un ataque de ransomware que afectó sus sistemas de comunicación en Estados Unidos, Canadá y Sudamérica.

EL RIESGO CIBERNÉTICO EN EL SECTOR MARÍTIMO

- En junio 2017: el malware llamado “NotPetya” llegó q infectar las operaciones de 17 terminales portuarias globales operadas por Maersk, entre ellas las de Callao (Perú), Elizabeth, Nueva Jersey (Estados Unidos), Itajai (Brasil), Los Ángeles (Estados Unidos) y Buenos Aires (Argentina). Maersk se vio obligada a interrumpir sus operaciones a medida que el malware se extendía por los sistemas informáticos críticos y para recuperarse tuvo que modificar casi toda su infraestructura informática.

Cinco acciones para gestionar los Riesgos Cibernéticos:

The National Institute of Standards and Technology (NIST, 2022), de acuerdo al marco de ciberseguridad, sugiere integrar las siguientes cinco acciones para una gestión de riesgos cibernéticos:

- Identificar: desarrollar un entendimiento de los riesgos de sus sistemas, personas, activos, datos y capacidades.
- Proteger: implementar salvaguardias adecuadas para proteger sus servicios y operaciones críticas.
- Detectar: desarrollar medidas que permitan la detección temprana de ciber incidentes.

EL RIESGO CIBERNÉTICO EN EL SECTOR MARÍTIMO

- Responder: poner en marcha un plan de acción que sea implementado tras un incidente de seguridad cibernética.
- Recuperar: identificar acciones apropiadas para restaurar sistemas afectados por un incidente cibernético.

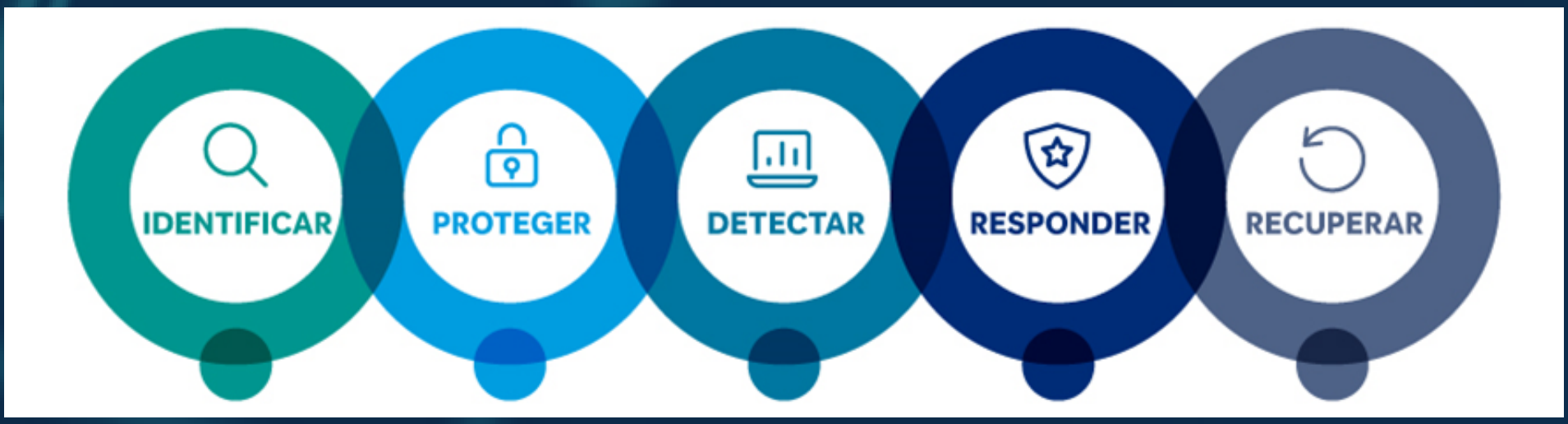


Imagen tomada de Marsh, 2022.

BIBLIOGRAFÍA

Documentos y fuentes consultadas:

- Marsh, 2022: https://www.marsh.com/pr/es/industries/marine/insights/digitalization-in-ports-and-terminals-technology-advances-bring-increased-risk.html?gclid=CjwKCAjw_YShBhAiEiwAMomsELIO64nwJKNfGMONByURQaejjrDdmhDxMxLT-tTKCb3ZjWKNnteZ5xoCayQQAvD_BwE

- ENISA, 2023: https://www.enisa.europa.eu/ licenced under CC-BY 4.0

- Centro Criptológico, 2022: https://www.ccn-cert.cni.es/gl/gestion-de-incidentes/lucia/23-noticias/274-nuevo-informe-de-enisa-qincentivos-y-obstaculos-para-el-mercado-del-seguro-ciberneticoq.html

Cualquier información o contacto a los siguientes correos: info@wistaperu.org o president@wistaperu.org

BIBLIOGRAFÍA

Documentos y fuentes consultadas:

- NIST, 2022: https://www.nist.gov/documentary-standards

- OEA, 2021: Programa de protección marítima y portuaria https://www.oas.org/es/sms/cicte/prog-proteccion-maritima.asp#:~:text=El%20Programa%20de%20Protecci%C3%B3n%20Mar%C3%ADtima,y%20marcos%20normativos%20y%20legislativos.

Cualquier información o contacto a los siguientes correos: info@wistaperu.org o president@wistaperu.org

INFORMACIÓN GENERAL

Comité de TI de WISTA Perú:

Directora:

- Mariela Gutarra.

Miembros:

- Eileen Chavesta.
- Doris Eyzaguirre.
- Krista Lucenti.
- Mirella Torres.
- Marisol Geldres.
- Pamela Saavedra.
- Mónica Esteban.

Cualquier información o contacto a los siguientes correos: info@wistaperu.org o president@wistaperu.org