MARINA

SECRETARÍA DE MARINA
ESTADO MAYOR GENERAL DE LA ARMADA
UNIDAD DE CIBERSEGURIDAD

Riesgo Cibernético Marítimo y Portuario: Visión de la SEMAR

07 de octubre de 2021

"Seguridad y defensa en el ciberespacio"

Agenda

1. Introducción
2. Desafío actual
3. Amenazas en el ciberespacio
4. Escenarios de riesgo
5. Incidentes de Ciberseguridad
6. Conclusiones

Introducción

Desafíos globales para satisfacer la necesidad humana del suministro de alimentos, provisión de servicios, energía, agua y recursos orgánicos o minerales.

Tendencias tecnológicas hacia la conectividad mundial y aprovechamiento de la navegación digitalizada, adoptando tecnologías disruptivas y de transformación.

Identificación de escenarios de riesgo cibernético, con impacto a la continuidad de las operaciones, mantenimiento de la seguridad de la vida humana en la mar, infraestructura, recursos y protección del medio ambiente marino.

Introducción

04/11/93

Código IGS

Código Internacional de Gestión de la Seguridad

16/06/17

Resolución MSC-428

Gestión de riesgos cibernéticos marítimos en Sistemas de Gestión de Seguridad

05/07/17

Circular MSC-FAL.1/Circ.3

Directrices sobre la gestión de los riesgos cibernéticos

OBJETIVOS

- Seguridad operacional del buque
- Prevención de contaminación
- Preservación de la vida humana en la mar

PREMISAS

- Necesidad de gestionar amenazas y vulnerabilidades cibernéticas
- Todos los actores marítimos deberán gestionar el riesgo cibernético
- Gestión de riesgo cibernético: Identificar, Analizar, Evaluar y Comunicar

RECOMENDACIONES DE ALTO NIVEL

- Elementos funcionales: Identificar, Proteger, Detectar, Responder, Recuperar
- Mejores prácticas: Estándares normas y marcos de trabajos

ORGANIZACIÓN MARÍTIMA INTERNACIONAL

Desafío actual

En el escenario actual se distingue la aplicación de tecnologías enfocadas a:

- Digitalización de la información
- Automatización de procesos operativos
- Conectividad entre el buque y el puerto
- Análisis de Big-Data en operaciones marítimas
- Monitoreo de motores y maquinaria
- Mantenimiento remoto de sistemas
- Buques autónomos
- Control en tierra y operaciones portuarias autónomas
- Internet de las cosas (IoT)
- Uso de servicios en la nube (cloud computing)

Amenazas en el ciberespacio

ACTORES MALICIOSOS (Estados revisionistas)

- Amenazas Persistentes Avanzadas (APT)

ACTORES MALICIOSOS (sin apoyo gubernamental)

- Ciberterroristas
- Ciberdelincuentes
- Hacktivistas

CÓDIGO MALICIOSO

- Ransomware
- Troyano
- Gusano
- Virus
- Rootkit
- Spyware
- Backdoor
- Adware

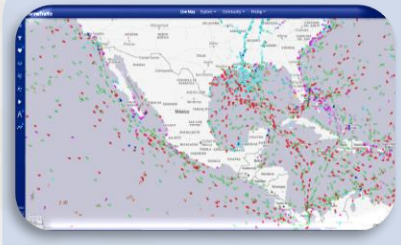
FACTOR HUMANO

- Interno descontento
- Interno Inexperto

Escenarios de riesgo cibernético

Tecnologías de Información y Comunicación

Buques



AIS

ECDIS

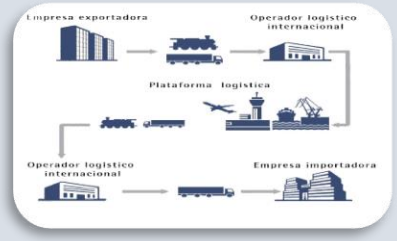
Puertos

CCTV

CONECTIVIDAD
Y SERVICIOS

Administraciones Portuarias y Aduanas

SISTEMAS DE
TRAMITE EN LINEA



SEGUIMIENTO
CADENA DE SUMINISTRO

Tecnologías de Operación

SISTEMAS DE CONTROL

SCADA

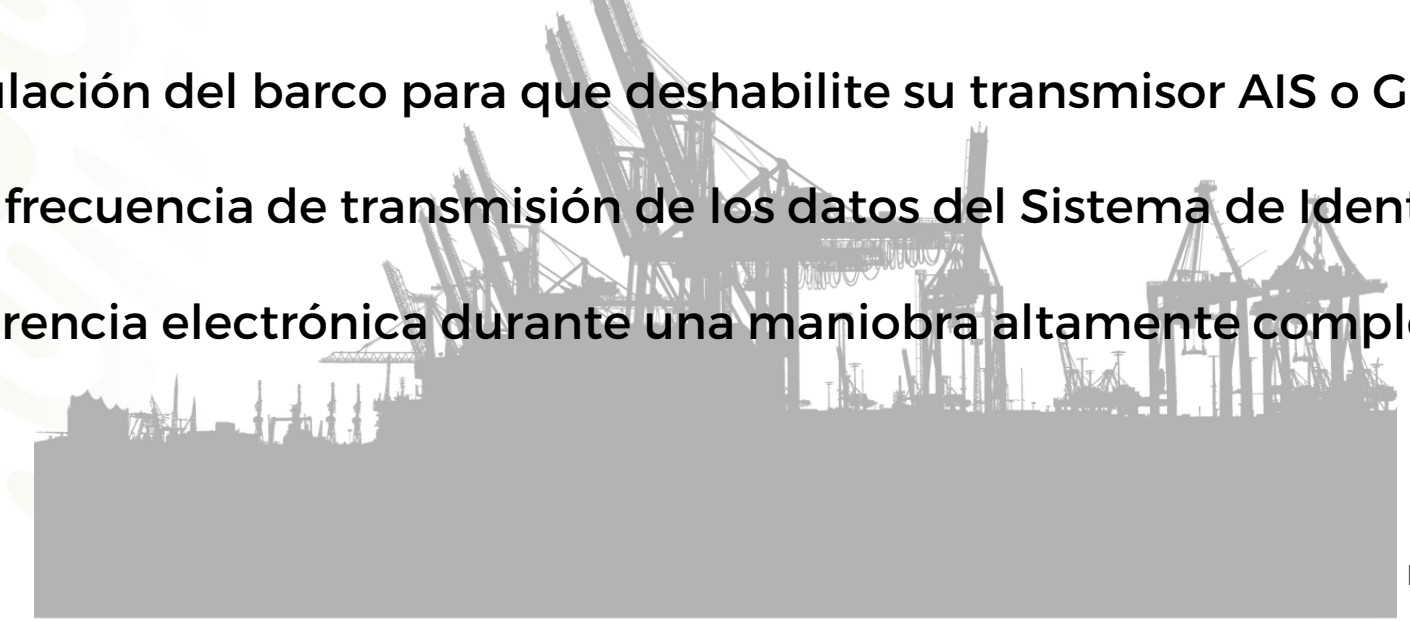
SISTEMAS DE
MONITOREO DE CARGA

SISTEMAS DE
CONTROL DE CARGA

MONITOREO DE
MOVIMIENTOS DE CARGA

Escenarios de riesgo

- Modificación de todos los detalles del barco, incluyendo nombre, posición, rumbo, velocidad y carga
- Creación de buques fantasmas en cualquier ubicación global
- Activación de una alerta de colisión falsa como consecuencia de un desajuste del rumbo
- Transmisión de información falsa de las condiciones meteorológicas
- Suplantación de identidad de las autoridades marinas
- Engañar a la tripulación del barco para que deshabilite su transmisor AIS o GPS.
- Incremento de la frecuencia de transmisión de los datos del Sistema de Identificación Automática
- Ataque de interferencia electrónica durante una maniobra altamente compleja

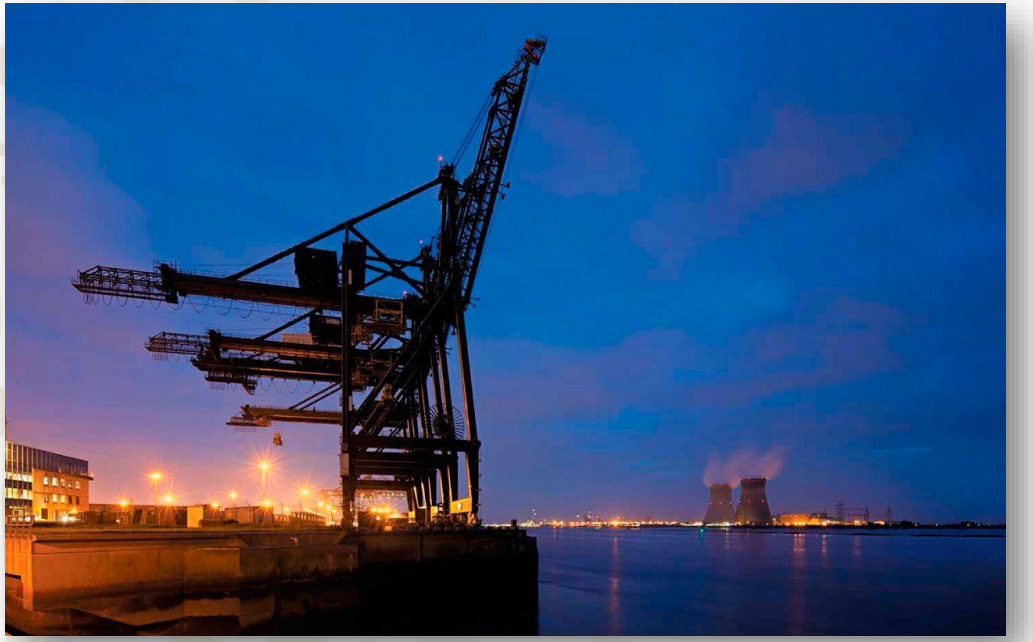


Escenarios de riesgo

Fuente: La Vanguardia. https://www.youtube.com/watch?v=HFT5qg9cxKU

Principales incidentes de ciberseguridad

Puerto de Amberes, Bélgica. 2011-2013



- El puerto fue usado para tráfico de drogas por un cartel mexicano
- A finales de 2013 se hizo público que este puerto había sido objeto de un ciberataque persistente, que había estado en curso desde junio de 2011

- Utilizando a expertos en tecnología los criminales enviaron **correos electrónicos** a trabajadores cargados con **programas maliciosos (malware)**
- Instalaron dispositivos para capturar contraseñas (Keylogger)
- Ingresaron a los **sistemas de carga** para mover y ocultar contenedores específicos que contenían contrabando

Principales incidentes de ciberseguridad

Empresa naviera Maersk, 2017

- La empresa de transporte marítimo A. P. Moller Maersk es una de las más grandes del mundo
- Sufrió **ciberataque de ransomware** que paralizó sus operaciones al cifrar la información de sus servidores
- Los problemas afectaron los puertos de Bombay (el mayor de India) y de Rotterdam (el más activo de Europa)

- El impacto se estimó entre 250 millones y 300 millones de dólares en pérdidas

Panorama Internacional de Ciberseguridad

ENERO

Correos electrónicos maliciosos contra empresas navieras Dryad y RedSkyAlliance

MARZO

Hurtigruten identificó que un actor no autorizado cifró los sistemas informáticos

ABRIL

Ciberataque que afectó a la red informática de proveedor de servicios Bourbon

JULIO

Ciberataque interrumpe las principales operaciones portuarias de Sudáfrica

SEPTIEMBRE

Ciberataque a servidores en el Puerto de Houston, Tx.

Conclusiones

El sector marítimo y portuario debe estar consciente del impacto generado por los ciberataques

Desarrollar e implementar medidas y acciones robustas de ciberseguridad a través de una estrategia

La cooperación, comunicación, coordinación y colaboración entre los actores del sector marítimo

Concientización a la comunidad marítima y portuaria

MARINA

SECRETARÍA DE MARINA

GRACIAS