Colombia mar 2023

VIII CONGRESO INTERNACIONAL DE DISEÑO E INGENIERIA NAVAL

Ciberseguridad: Un marco general en el mundo marítimo y militar

CC. Ferney Martínez Ossa
CC. Francisco Guevara Arismendy
PHD. Luis Enrique Sánchez Crespo

Gerencia de ciencia, tecnología e Innovación - COTECMAR
Universidad Castilla La Mancha

“Si piensas que la tecnología por sí misma puede resolver tus problemas de seguridad, entonces no entiendes los problemas y no entiendes la tecnología”

Bruce Schneier

HOJA DE RUTA

01

CONTEXTO

Ambientación
descripción

02

LINEAMIENTOS

Conceptos globales
Entidades públicas y privadas

03

ARC

Ámbito militar

04

POLÍTICAS

Directrices emitidas

05

CONCLUSIONES

Consideraciones Finales
Focos de investigación

06

APORTES

Espacio abierto

TRANSFORMACIÓN DIGITAL MARÍTIMA

Inteligencia artificial (IA)

Machine learning

Redes de internet de las cosas (IoT)

Analíticas avanzadas y robótica

El transporte marítimo internacional representa alrededor del

90%

del comercio mundial de mercancías

Y aún así...

Fuente:
- Kapersky Daily
- Alsum

En 2010 una plataforma de perforación marítima cambió su ubicación desde Corea del Sur a América del Sur en los sistemas de monitoreo debido al ataque de un virus informático.

Puerto de Amberes, Bélgica (2011-2013): fue víctima de un ciber ataque en 2011. Un grupo organizado de tráfico de drogas logró acceder al sistema que controlaba el movimiento y posición de los contenedores. Al parecer el control de los sistemas se vulneró hasta 2013.

En Agosto de 2011, un grupo de hackers se infiltró en los servidores de IRISL (Iranian Shipping Line) y dañó cientos de datos sobre cargamentos y fechas y lugares de entrega. Debido a esto, una gran cantidad de estos cargamentos fueron enviados a destinos equivocados.

En 2012 piratas informáticos al servicio de una organización criminal pusieron en peligro el sistema de carga controlado por la Agencia Aduanera y de Protección Fronteriza de Australia. Los delincuentes querían saber cuáles contenedores eran objeto de sospecha de las autoridades policiales y aduaneras. De esta manera podrían saber si era necesario abandonar los contenedores con cargas de contrabando.

En 2013, mientras perforaban en el Golfo de México, los trabajadores de una compañía petrolera con sede en EE. UU. cargó accidentalmente malware en el sistema informático principal del MODU. Los efectos de este ataque paralizaron la plataforma, particularmente de comunicarse con el sistema de navegación de la plataforma. Un trabajador involuntariamente introdujo archivos corruptos a través de una USB.

En 2014 se produjo el ataque Zombie Zero a la industria logística y fue descubierto en julio de ese año por la empresa TrapX2. Consistió en un ciberataque oculto dentro de una pieza de hardware; más específicamente en un escáner que contenía este malware presente en 8 compañías logísticas.

2014, Los piratas informáticos interceptan y alteran cuentas bancarias a través de correos electrónicos, lo que provoca graves pérdidas financieras. Los ataques apuntan a transacciones entre las líneas navieras y los proveedores de combustible y entre líneas navieras y astilleros.

2016, En Corea del Sur, 280 barcos tienen que regresar a puerto después de experimentar problemas con sus sistemas de navegación. Se especula que fue un ataque cibernético desde Corea del Norte pero no existen pruebas.

2017, El corredor británico Clarksons es pirateado y los atacantes exigen un rescate por los datos robados. Se robaron información confidencial y las acciones disminuyeron 5% después del incidente.

2017, Moller-Maersk sufrió una pérdida que se estima en 300 millones de dólares en lo que se considera el ataque más grande de la industria hasta el momento.

2018, El puerto de Barcelona informa de un ciberataque, que resulta ser una infección ransomwaredel Ryuk que hace secuestro de datos. Este virus solo afectó internamente los equipos de tecnología pero no se afectaron las operaciones del trafico de buques.

2019, Un petrolero cerca del puerto de Naantali en Finlandia es infectado en su servidor por ransomware. Se borra la información incluyendo el disco de respaldo. El ataque se produjo por el uso de una USB o un correo electrónico. El mismo barco se vuelve a infectar 4 meses después cerca al mismo puerto.

2020, La naviera MSC es víctima de un virus ransomware y su sede en Ginebra es cerrada durante 5 días.

2019 y 2020, El operador de cruceros Carnival Corporation & plc se ve afectado por el virus ransomware dos veces entre 2019 y 2020. Se robaron información confidencial de los clientes como los datos de las tarjetas de crédito. Se recibieron múltiples reclamos por el ataque.

2020, La Organización Marítima Internacional (OMI) sufrió un ataque cibernético sofisticado que le afectó su sitio web durante varios días.

2021, Un ataque cibernético mantuvo cerrados durante varios días los servicios informáticos de Transnet, ente que rige como autoridad de puertos, ferrovías y ductos de Sudáfrica.

2021, La naviera francesa CMA CGM ha sido víctima, otra vez, de un ciberataque a poco menos de un año desde la brecha de seguridad anterior y que afectó a los servidores periféricos de la empresa provocando problemas en su infraestructura de TI y dejándolos fuera de línea una semana.

2021, Bourbon, la naviera basada en Marsellesa de buques de suministro en alta mar, sufrió un ciberataque, el 8 y 9 de abril. Ese mismo día, otra naviera de la misma ciudad francesa, Gazocean, fue víctima de un ciberataque similar.


RESCATE BITCOINS
Maquinas
Ordenadores
Sistemas conectados a la red
300 mll euros
Cifrado y Bloqueo
Reino Unido
2017
Petya
España
Ataque a Maersk
Rusia
Naviera Maersk
80 puertos
Holanda
Francia
45.000 computadores
4.000 servidores
instalar 2.500 aplicaciones
Ucrania
Otros

Y la guerra?

Fuente:
- Kapersky Daily
- Alsum


ТРЯХА

EL RIESGO CIBERNÉTICO MARÍTIMO

Es la medida del nivel de amenaza de un activo tecnológico por una circunstancia o suceso posibles, que podrían causar fallos operacionales, de seguridad o protección del transporte marítimo al corromperse, perderse o ponerse en peligro información o sistemas.

Las motivaciones son muy variadas, por lo que ninguno de los componentes del ámbito marítimo puede ser excluido.

ESPIONAJE

Acceso no autorizado a información sensible, sujeta a propiedad intelectual, asociada a gestiones comerciales, estrategias corporativas, entre otras, con el fin de interrumpir el normal funcionamiento o causar pérdidas

ACTIVISMO

O hacktivismo (de hackeo por intereses del grupo) que buscan publicidad o generar presión en representación de una causa u objetivo

CRIMINALES

Con el propósito de obtener beneficios económicos, daño a bienes materiales, robo, tráfico de especies o personas y/o con el propósito de evadir impuestos o deberes.

TERRORISMO

Acciones orientadas a producir temor y causar interrupciones físicas y económicas.

BÉLICAS

En el contexto de conflictos entre Estados, con el propósito de interrumpir los sistemas y vías de comunicación, con el propósito de negar su acceso.

71% de todos los ataques cibernéticos están motivados económicamente

(Verizon)

Los ataques de ransomware ocurren cada **10** segundos

(Grupo de InfoSeguridad)

AMENAZAS Y RIESGOS

Los riesgos son cada vez más diversos, y los ataques más minuciosos y novedosos; amenazando su tecnología, operaciones, seguridad o protección de sus cargas o pasajeros, información o sistemas en peligro.

FILTRACIÓN

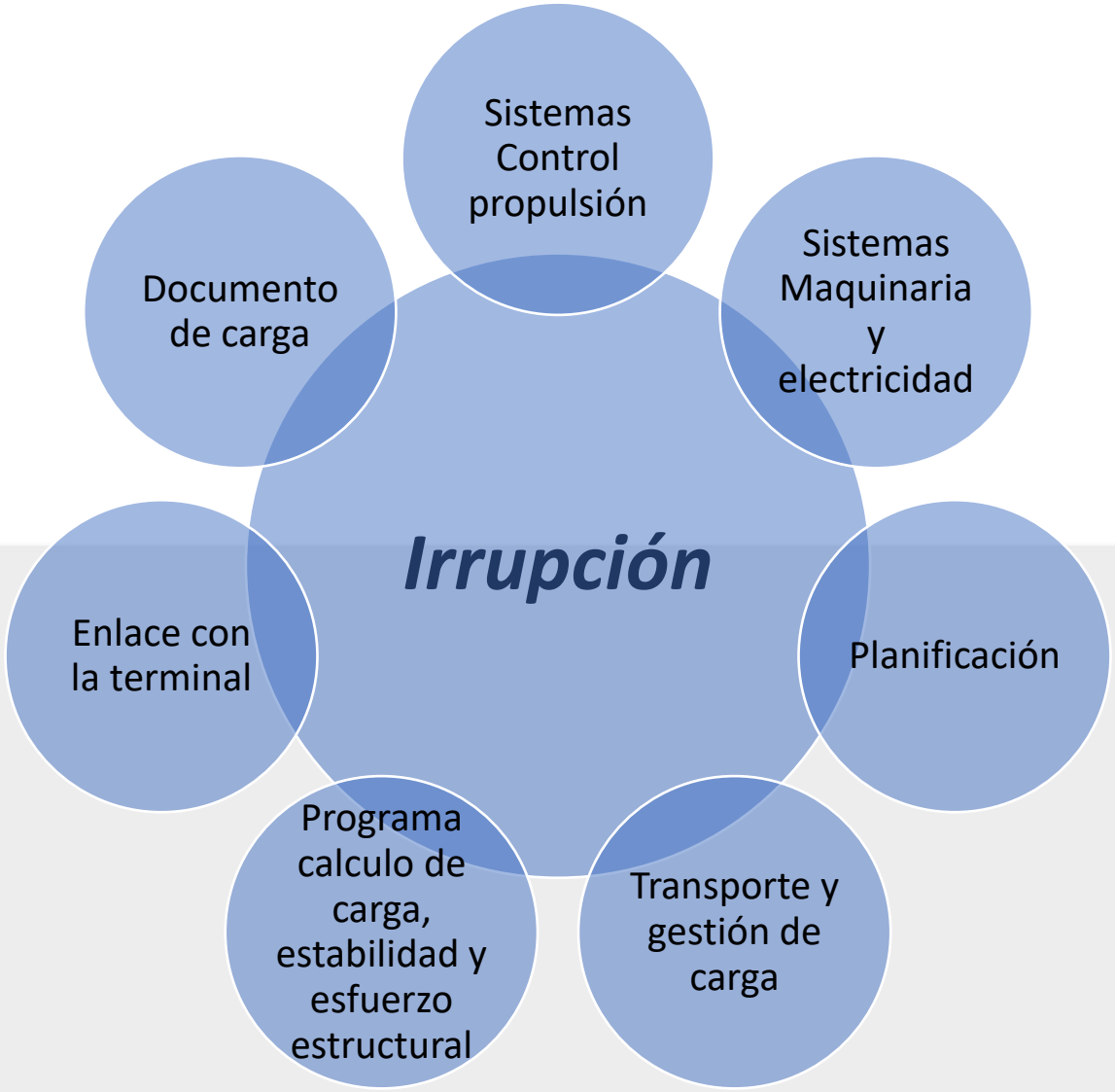
IRRUPCIÓN DE PROCESOS

PENETRACIÓN

IRRUPCIÓN EN SISTEMAS DE CONTROL DE PUENTE

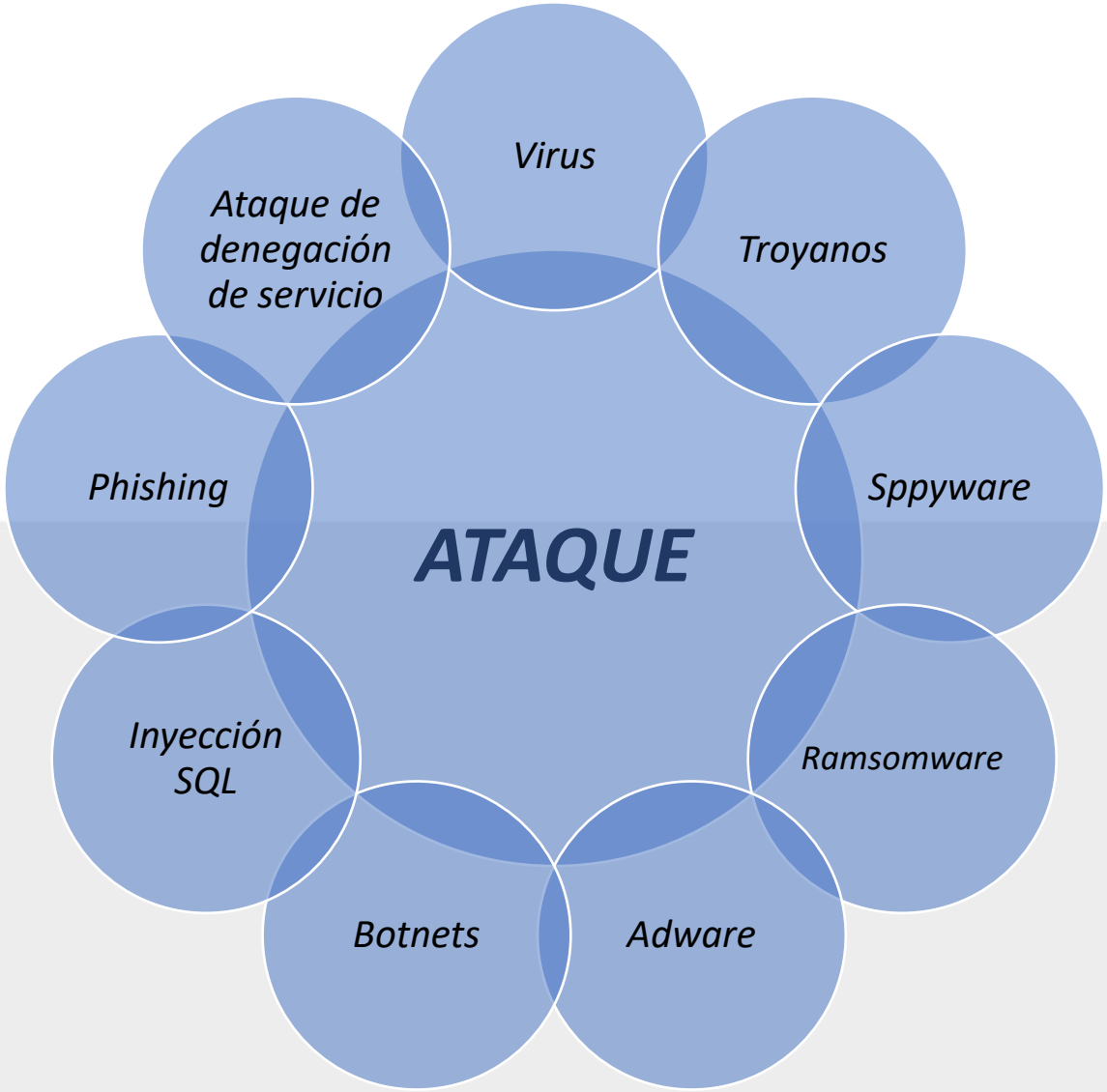
SISTEMAS DE INFORMACIÓN

AMENAZAS Y RIESGOS

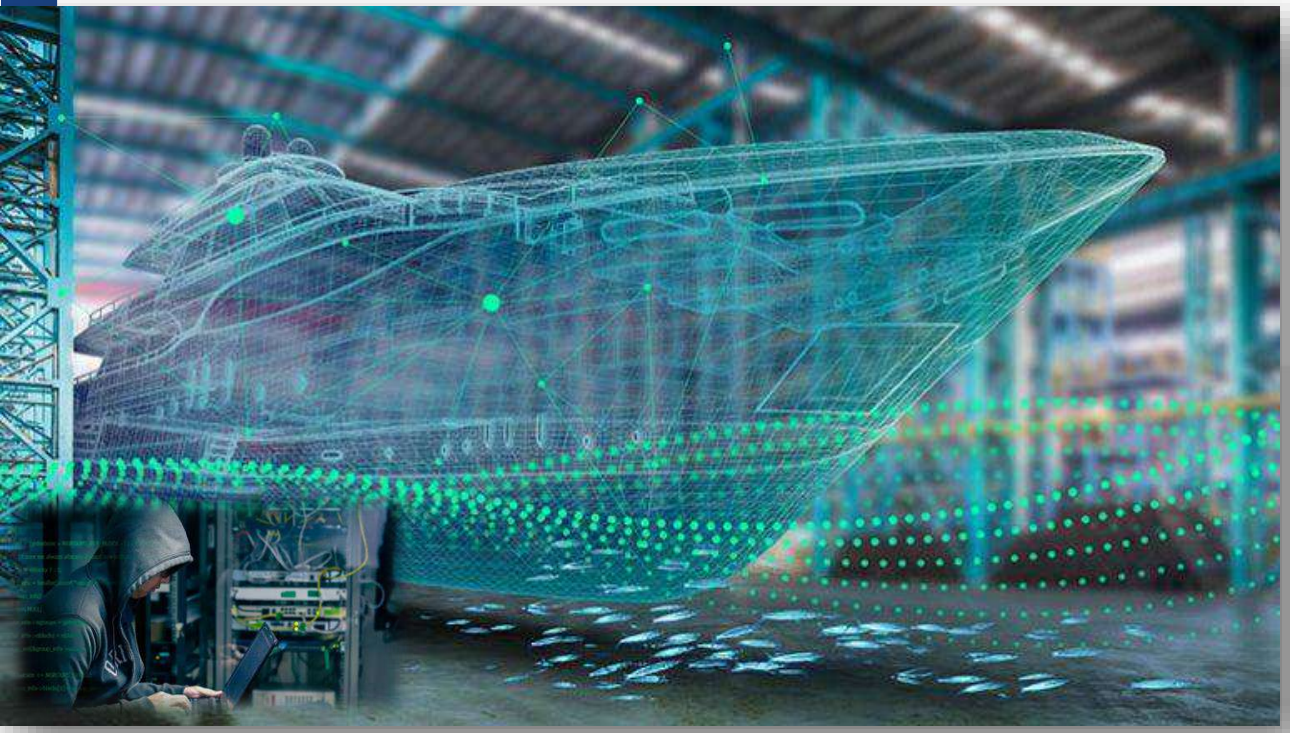


AMENAZAS Y RIESGOS

AMENAZAS Y RIESGOS

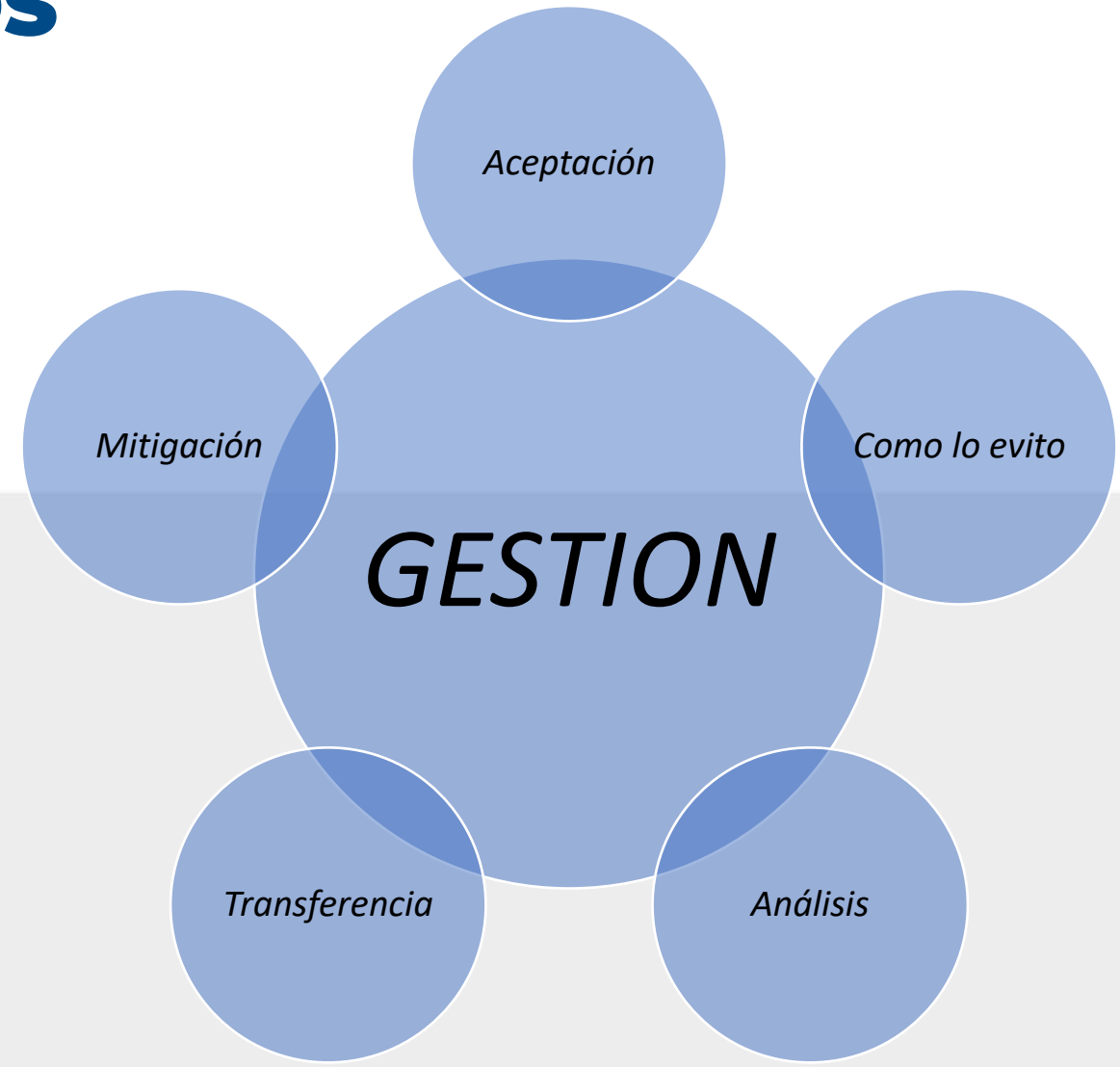


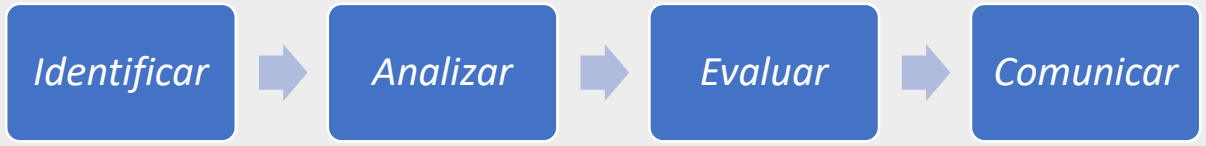
AMENAZAS Y RIESGOS



GESTIÓN DE LOS RIESGOS

La gestión de los riesgos cibernéticos cubre identificar, analizar, evaluar y comunicar estos riesgos pasando por su aceptación, cómo evitarlos, analizando la transferencia y mitigación de esos riesgos hasta niveles aceptables, considerando los costos y las ventajas para los involucrados.





GESTIÓN DE LOS RIESGOS


Los ataques de ransomware ocurren cada 10 segundos
Grupo de InfoSeguridad
El crimen organizado es responsable del 80% de todas las violaciones de seguridad y datos.
Verizon

OEA – Organización de los Estado Americanos

Reúne a los 35 Estados independientes de las Américas y constituye el principal foro gubernamental político, jurídico y social del Hemisferio

Programa de Ciberseguridad		
I	II	III
Desarrollo de políticas:	Creación de capacidades:	Investigación y divulgación:
Desarrollar estrategias nacionales de ciberseguridad que involucren a todas las partes interesadas relevantes. Adaptación a la situación legislativa, cultural, económica y estructural de cada Estado Miembro.	Ayuda a establecer equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT). Asistencia técnica personalizada y oportunidades de capacitación. La red CSIRT Américas, la cual rinda inteligencia sobre amenazas y tendencias cibernéticas.	Desarrolla documentos técnicos, herramientas e informes para orientar formulación de políticas, los CSIRT, los operadores de infraestructura, las organizaciones privadas y la sociedad civil

OTAN - Organización del Tratado del Atlántico Norte

Es una alianza militar intergubernamental que constituye un sistema de defensa colectiva, en el cual los Estados integrantes acordaron defender a cualquiera de sus miembros que sea atacado por una potencia externa.

Política de la OTAN sobre ciberdefensa			
Desarrollo de la capacidad de ciberdefensa de la OTAN	Aumento de la capacidad de ciberdefensa de la OTAN	Cooperando con los socios	Cooperando con la industria
La Capacidad de Respuesta a Incidentes Informáticos de la OTAN (NCIRC) Protege las propias redes de la OTAN al proporcionar apoyo de ciberdefensa centralizado Disponibilidad total.	Mejora el estado de su defensa cibernética a través de educación, entrenamiento y ejercicios. Lleva a cabo ejercicios regulares, como el Ejercicio de Coalición Cibernética anual.	Colabora con países socios y otras organizaciones internacionales para mejorar la seguridad compartida identificando los enfoques comunes. La Unión Europea (UE), las Naciones Unidas (ONU) y la Organización para la Seguridad y la Cooperación en Europa (OSCE).	Esfuerzos conjuntos El sector privado es un actor clave en el ciberespacio. El intercambio de información, los ejercicios, el entrenamiento y la educación

OMI - Organización Marítima Internacional

Organización de las Naciones Unidades, ubicada en el Reino Unido y que se responsabiliza en la protección y seguridad de la navegación además de prevenir la contaminación en el mar.

- Publicó las Directrices sobre la Gestión del Riesgo Cibernético Marítimo en 2017 para fortalecer la seguridad cibernética en consideración de la digitalización de los buques.
- Emitió la Circular MSC-FAL.1/Circ.3 Directrices sobre la gestión efectiva de los riesgos cibernéticos marítimos.
- Resolución MSC.428 de Gestión de los riesgos cibernéticos marítimos en los sistemas de gestión de la seguridad.

OCIMF – Foro Marítimo Internacional Compañías Petroleras

Otra organización que reacciona ante estos cambios y actualiza rápidamente sus guías a las nuevas circunstancias es la OCIMF asociación voluntaria de compañías relacionadas con el transporte marítimo de crudo, petróleo y gas.

TMSA (Tanker Management and Self Assessment) provee a dichas compañías de medios para mejorar y medir sus SMS, incluyendo en él aspectos y requisitos de ciberseguridad aplicables a estos sectores, entre los que se encuentran:

- Procedimientos sobre la gestión de parches y software.
- Procesos y guías para la identificación y mitigación de ciberamenazas.
- Procedimientos para la gestión de contraseñas.
- Desarrollo de un plan de concienciación y formación en ciberseguridad para todo el personal involucrado.

IMCA - International Maritime Contractors Association

Contratistas y cadenas de producción asociadas a la industria de construcción marítima, su principal objetivo es de ayudar a las organizaciones a priorizar la defensa contra los ataques actuales más comunes y dañinos a las infraestructuras TI.

Recomendaciones en ciberamenazas, incluidas en su guía Security Measures and Emergency Response Guidance - IMCA SEL 037/M 226, consta de 20 controles y sub-controles. Se incluyen:

- Gestión activa del inventario de dispositivos y del software autorizado y no autorizado.
- Medidas de aseguramiento de dispositivos finales y de red.
- Evaluación de las habilidades en ciberseguridad del equipo y programa de formación.
- Realización de pruebas de penetración para evaluar la fortaleza de las defensas de una organización.


VAN
CAP ANDREAS

RESUMEN

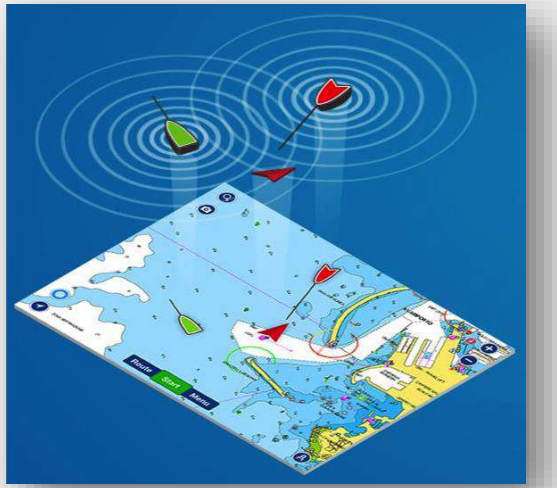
E.C.D.I.S.: Electronic Chart Display and Information System. Sistema de información geográfica utilizado para la navegación náutica.

Reemplazan a las cartas náuticas de papel a bordo de los buques, podría permitir el acceso de un atacante y la modificación de archivos y tablas a bordo o en tierra, lo que podría causar graves daños ambientales y financieros, incluso la pérdida de vidas humanas.

A.I.S.: Automatic Identification System, Sistema de identificación automático de naves, utilizado en el ámbito marítimo.

Permiten a los buques comunicarse con otras naves e intercambiar su posición y otros datos de interés

Con una radio V.H.F. de $100 dólares se ha podido modificar datos tales como: identidad, tipo, posición, rumbo y velocidad a las estaciones costeras.



RESUMEN

Los Sistemas de Posicionamiento Global (GPS), pueden ser atacados, causando graves problemas al transporte marítimo y poniendo en riesgo a miles de vidas humanas. La vulneración de este sistema fue demostrado con el ataque a la White Rose of Drax.

Sistema global de navegación por satélite (Global Navigation Satellite System, G.N.S.S.)

Los sistemas mundiales de navegación por satélite, GNSS11 se están convirtiendo en la quinta utilidad pública después del agua, la electricidad, petróleo/gas y telecomunicaciones.

Sin embargo, la falta de seguridad de éstos en el dominio civil, se estima preocupante, por lo que se encuentran desarrollando servicios con esquemas de autenticación de la data y contacto.

Armada Nacional de Colombia

Busca el aseguramiento de la información que es almacenada, procesada y transmitida en los diferentes activos informáticos y centros de datos.

Políticas de seguridad de la información, Directiva Permanente 2014-18.

Este manual abarca, entre otros, aspectos tales como:

Evaluación y tratamiento de los riesgos

Gestión de los activos.

Seguridad física y del entorno

Seguridad de las operaciones

Gestión de incidentes de seguridad de la información

CASO: Armada Nacional de Colombia

Consolidación de políticas

- Los operadores marítimos, desde el punto de vista industrial y comercial están obligados desde enero de 2021 al cumplimiento de una serie de requisitos y obligaciones de seguridad.

- Atender los principios de seguridad integral, gestión de riesgos, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y segregación de tareas

CONCLUSIONES

La ciberseguridad es una carrera entre atacantes y defensores, donde la ventaja la tiene quien ataca, debido a que puede elegir la metodología de ataque y cuenta con el tiempo para realizar de todo el estudio para elegir la mejor manera de hacerlo.

* se debe apropiar todo el conocimiento que podamos sumar entre los eventos ocurridos y el análisis tecnológico de nuestra organización.

CONCLUSIONES

El exponencial uso integral de los datos para su análisis y toma de decisiones, los buques inteligentes, el “internet industrial de las cosas” IIoT, entre otros factores aumenta día a día la cantidad de información disponible.

* La ciberseguridad marítima hacer parte inherente del buque en todos sus niveles, donde se incluya desde los directivos en tierra hasta el personal del buque, liderado por su capitán y los encargados tecnológicos de ciberamenazas.

CONCLUSIONES

La continua evolución tecnológica hace que todas las medidas que se tienen para la mitigación de riesgos a boro de los buques sean evaluadas de manera constante.

* Acorde a las políticas e informes que de manera permanente se generan desde los diferentes actores implicados en la operación y mantenimiento de los sistemas.

EN RESUMEN...

NO ESPERE SER VULNERADO

TRABAJO CONJUNTO

TRIDENTE: POLÍTICAS + METODOLOGÍA + HERRAMIENTAS

LINEAS DE TRABAJO

- Identificar dentro de los marcos de trabajo, estándares, guías, normas, etc. las posibles brechas existentes para proponer una solución aterrizada de manera inicial a los buques que se construyen e integran en COTECMAR.

- Apoyar la construcción de un Marco de Trabajo que permita caracterizar, medir y tomar acciones para la mitigación de vulnerabilidades tomando como eje principal de las bases de conocimiento, el aporte de expertos, etc.

- A partir de los puntos descritos, proponer la realización de un caso de estudio para realizar una revisión de: 1. Las prácticas de ciberseguridad aplicadas actualmente y 2. Las generadas a partir de la propuesta.

¡GRACIAS!

FGUEVARA@COTECMAR.COM
FMARTINEZ@COTECMAR.COM