3er. Encuentro Iberoamericano de Blockchain y Ciberseguridad
"Blockchain y Ciberseguridad para la Defensa y uso Dual"

Mares Ciberseguros: La Estrategia POSEIDÓN para una Defensa Marítima Resiliente

CC. Ferney Martínez Ossa
Dr. Luis Enrique Sánchez Crespo
Dr. Antonio Santos-Olmo
Dr. David Garcia Rosado
Dr. Eduardo Fernández-Medina

Grupo de Seguridad y Auditoría (UCLM)
Grupo PRODIN - COTECMAR

“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

TRANSFORMACIÓN DIGITAL MARÍTIMA

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.

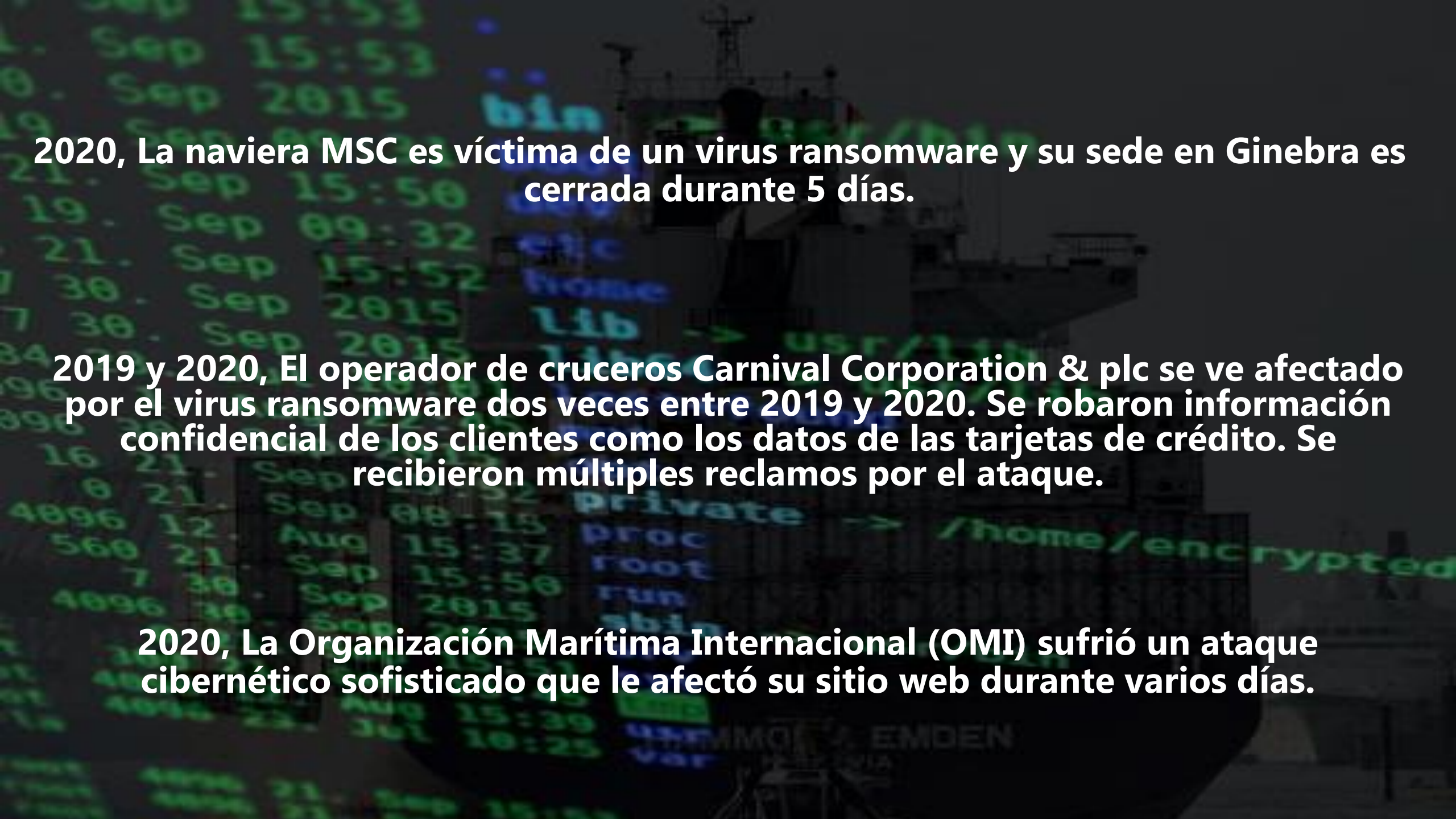
2016, En Corea del Sur, 280 barcos tienen que regresar a puerto después de experimentar problemas con sus sistemas de navegación. Se especula que fue un ataque cibernético desde Corea del Norte pero no existen pruebas.

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.

Ataque a Maersk

RESCATE
BITCOINS

300 mll
euros

Cifrado y
Bloqueo

Maquinas
Ordenadores
Sistemas
conectados a la
red

Reino Unido

2017

Petya

España

Rusia

Naviera
Maersk

80
puertos

Holanda

Francia

45.000 computadores

4.000 servidores

instalar 2.500
aplicaciones

Ucrania

Otros

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.

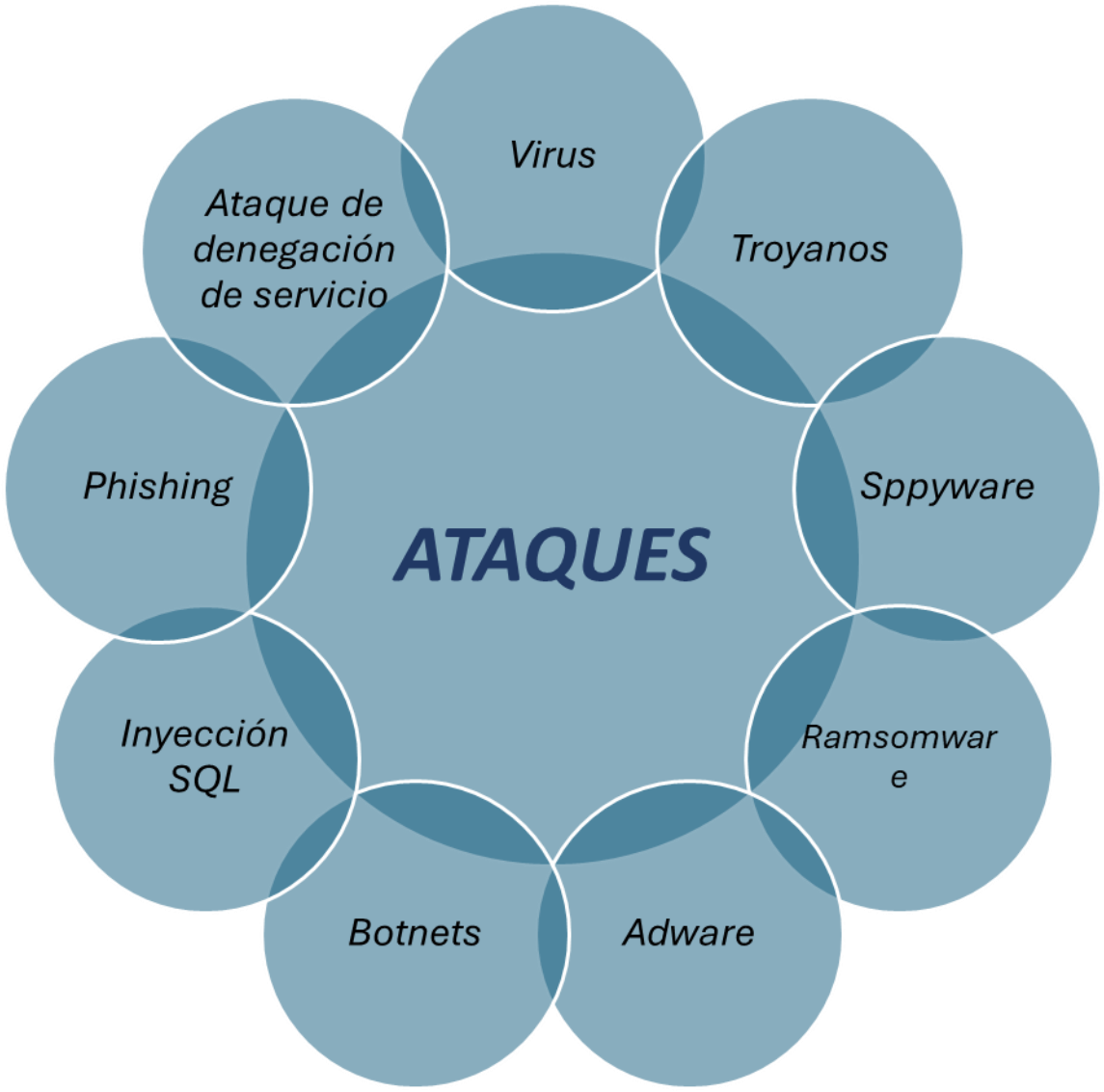
71% de todos los ataques cibernéticos están motivados económicamente

(Verizon)

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

(Grupo de InfoSeguridad)

AMENAZAS Y RIESGOS

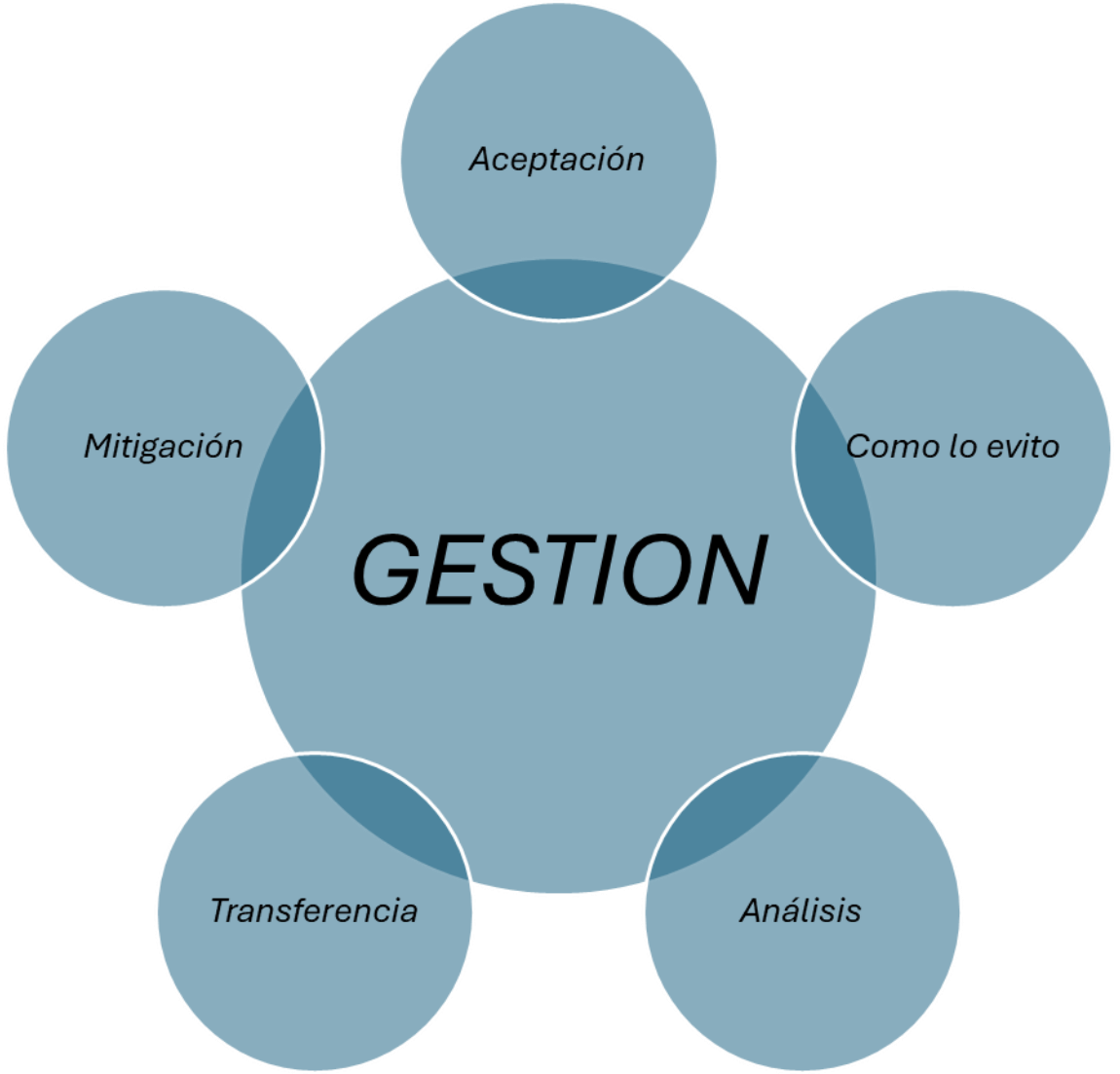


AMENAZAS Y RIESGOS

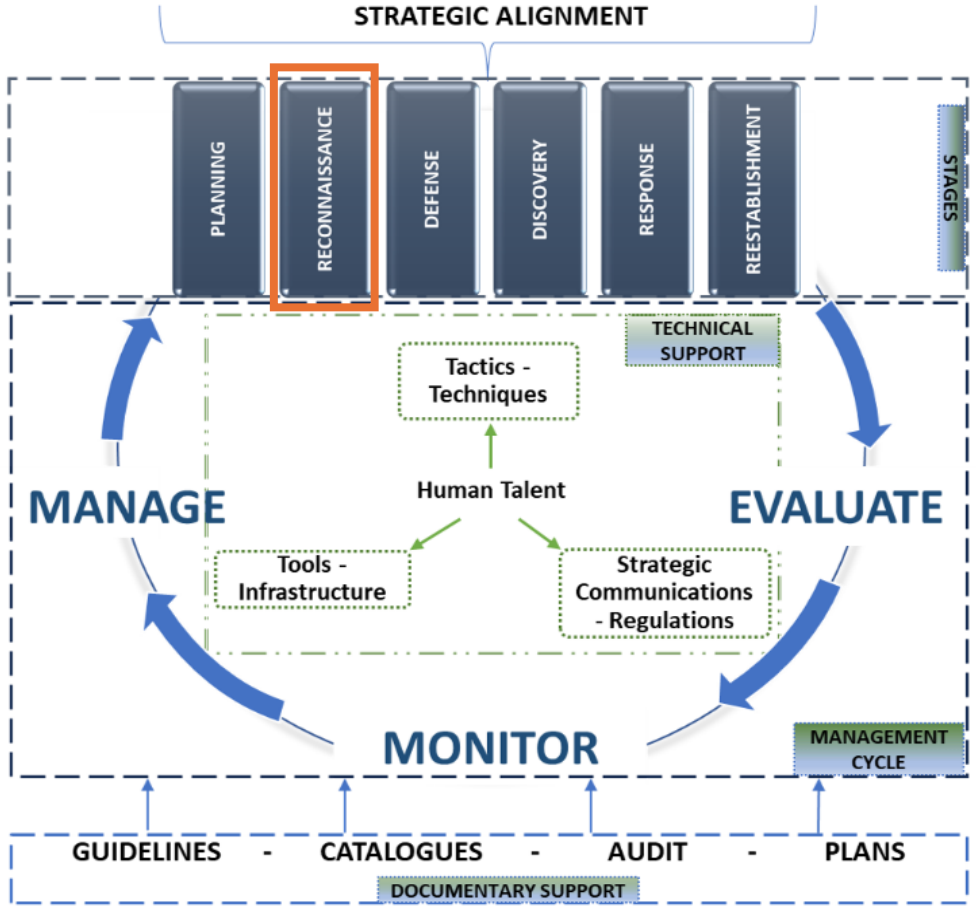

"No podemos cambiar el rumbo del mar, pero sí construir barcos más fuertes y tripulaciones más preparadas.”
Inspirada en Franklin D. Roosevelt

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: POSEIDON



Se propone el marco **POSEIDON**:

- Alineación estratégica
- Seguridad preventiva
- Resiliencia operativa
- **Gestión del talento humano** y **cultura de ciberseguridad**

POSEIDON no reemplaza, complementa lo existente

GESTIÓN DE LOS RIESGOS

¿Por qué planificar?

- Reduce tiempo de respuesta, errores humanos y dependencia externa.
- Mejora la coordinación, asignación de recursos y resiliencia.
- Responder tarde cuesta vidas
- Permite prever, priorizar y preparar
- Proactivo > Reactivo

Elementos Fundamentales

- Simulación, métricas, retroalimentación
- Involucra tripulación, sistemas y terceros
- Se entrena, se mide, se mejora

Es la única fase que **orquesta lo técnico, lo humano y lo doctrinal** desde el inicio.

GESTIÓN DE LOS RIESGOS

PLANIFICACIÓN

Contempla desde el inicio la evaluación de riesgos del entorno maritimo

Define la asignación de recursos criticos para responder a incidentes

- Considera factores específicos del sector naval, como el tipo de operación
- Integra el perfil del personal en la planificación de medidas de seguridad
- Se apoya en las lecciones aprendidas para optímizar la gestión de ciberseguridad
- Integra el perfil del personal en la planificación de medidas de seguridad
- Se apoya en las lecciones aprendidas para optimizar la gestión de ciberseguridad

Prevención
Centraliza información de múltiples fuentes.
Impacta en formación del personal.

Perfil del Personal
Establece criterios de formación.
Mejora la preparación de la tripulación y personal portuario.

Lecciones Aprendidas
Transforma experiencias pasadas en mejoras operativas.
Fortalece la cultura de seguridad y la capacidad de respuesta.

Prev. Operacional
Implementa medidas de seguridad en operaciones diarias.
Actúa en tiempo real ante amenazas emergentes.

Medidas con Terceros
Garantiza que proveedores cumplan estándares.
Protege la integridad de la cadena logística externa.

Gobernanza de Seguridad
Supervisa el cumplimiento de normativas internacionales.
Asegura coherencia en medidas de protección I/E

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

POSEIDON:

BUQUE DUAL
Características:

- Embarcación multifuncional
- Desempeña diversas tareas marítimas: transporte de carga, pasajeros, operaciones de búsqueda y rescate, y actividades de investigación científica, además de contar en algunos casos con capacidades militares.
- Versátil
- Opción flexible y eficiente para diversas aplicaciones marítimas

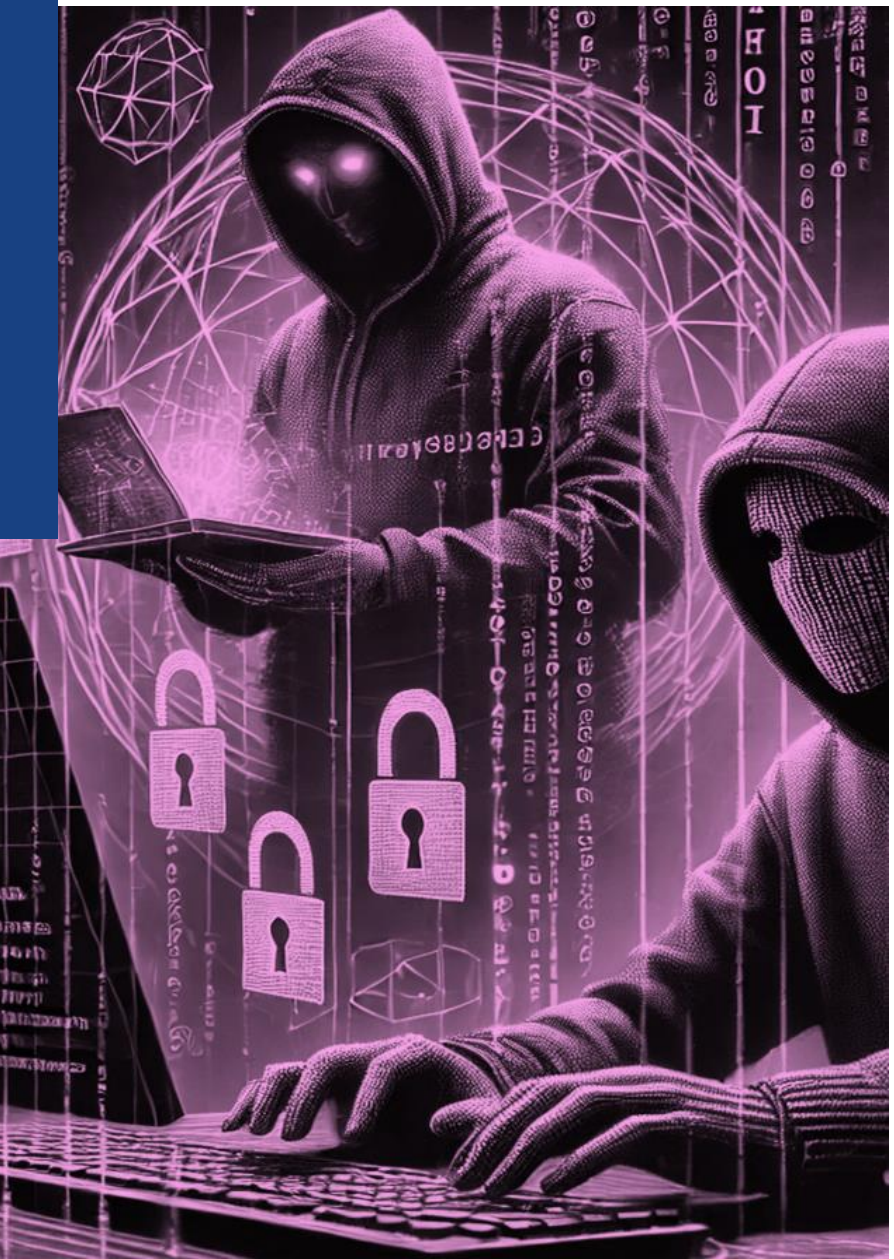
BALC SALUD

BDA

PAF-LIVIANA

LBF

POSEIDON:



IDENTIFICACIÓN DE AMENAZAS DEL BUQUE DUAL		
Familia de Amenazas	**Tipo de Amenazas**	**Impacto y estrategias de mitigación**
Desastres naturales, tecnológicos	Fallas tecnológicas y ambientales.	Sistemas de respaldo y redundancia para garantizar la continuidad operativa.
Interrupciones	Fallos en servidores, ataques a propulsores.	Plan de contingencia con servidores alternativos y protocolos de respuesta rápida.
Daño no intencional	Errores humanos, fuga de información.	Capacitaciones en ciberseguridad y control de accesos con autenticación multifactor.
Agresiones físicas	Piratería, hacktivismo.	Integración de seguridad física y digital para detectar ataques combinados.
Fallos en sistemas críticos	Fallos en GPS y mesa de cartas.	Sistemas de respaldo y redundancia en equipos de navegación.

SISTEMAS A BORDO ACORDE A NECESIDADES OPERACIONALES:
Equipos de navegación, Sistemas de propulsión, Sistemas de comunicaciones, Tecnología de seguridad y defensa, como sistemas de vigilancia, detección de intrusiones y sistemas de defensa, Equipos/redes administrativas, Sistemas de monitoreo, Equipos especializados: investigación científica, búsqueda y rescate, de manipulación de carga.

POSEIDON: PLANIFICACIÓN

Subcomponente	Acciones Implementadas	Resultados Obtenidos	Amenazas Abordadas
Prevención	- Vigilancia de vulnerabilidades **desde el diseño.** - Identificación de accesos no autorizados. - Refuerzo de autenticación. - **Jornadas de concienciación**.	- Fortalecimiento del sistema preventivo. - Reducción de exposición a vectores de ataque.	- Fallos en sistemas críticos - Agresiones físicas - Fallas tecnológicas y ambientales
Perfil del Personal	- Evaluación de conocimientos y conducta. - Capacitaciones periódicas con enfoque lúdico. - Protocolo para uso de dispositivos personales.	- Mejor manejo de incidentes. - Reducción de errores humanos. - Conciencia situacional mejorada.	- Daño no intencional - Agresiones físicas
Lecciones Aprendidas	- Registro y análisis de errores iniciales. - Rediseño de reglas de segmentación y comunicación entre sistemas.	- Mejora de arquitectura de red. - Evita repetición de fallos críticos.	- Fallos en sistemas críticos - Daño no intencional

POSEIDON: PLANIFICACIÓN

Subcomponente	Acciones Implementadas	Resultados Obtenidos	Amenazas Abordadas
Prevención Operacional	- Detección de tráfico anómalo (IDS). - Pruebas de penetración periódicas. - Actualización constante de software y reglas de seguridad.	- Detención temprana de amenazas. - Fortalecimiento de la postura defensiva.	- Interrupciones - Fallos en servidores - Fallas tecnológicas
Medidas con Terceros	- Auditoría a proveedores de TIC. - Control de cumplimiento de normativas y certificaciones. - Nuevas políticas de integración.	- Reducción de vulnerabilidades de la cadena de suministro. - Mayor control sobre elementos externos.	- Agresiones físicas - Daño no intencional - Fallas tecnológicas
Gobernanza de Seguridad	- Formalización de marco de gobernanza. - Coordinación internacional (OMI). - Integración de protocolos normativos.	- Alineación con normativas globales. - Mejora de la capacidad organizacional de respuesta.	- Todas las amenazas (rol transversal) - Coordinación ante desastres y eventos híbridos


VAN
CAP ANDREAS

RESUMEN

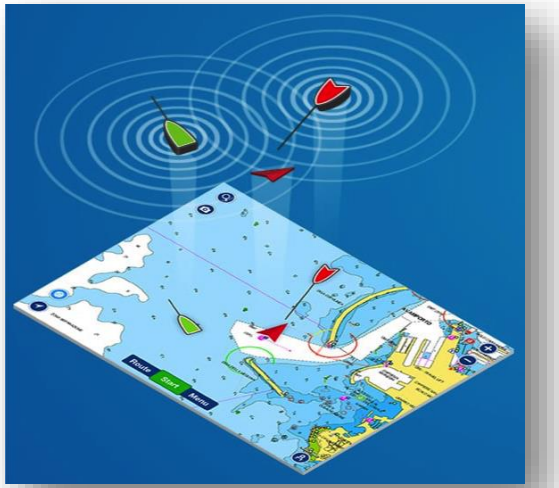
E.C.D.I.S.: Electronic Chart Display and Information System. Sistema de información geográfica utilizado para la navegación náutica.

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.

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.

Ciclos de mejora continua: Iteración de POSEIDON en diferentes escenarios operativos.

EN RESUMEN...

- **NO ESPERE SER VULNERADO**
- **TRABAJO CONJUNTO Y CULTURA DE LA CIBERSEGURIDAD**
- TRIDENTE: **POLÍTICAS + METODOLOGÍA + HERRAMIENTAS**

MODELO…

CASO REAL DE UN MODELO DE COLABORACIÓN

UNIVERSIDAD - EMPRESA - ESTADO

1. Innovación y Desarrollo Tecnológico
2. Formación de Capital Humano
3. Transferencia de Conocimiento
4. Impulso Económico y Competitividad
5. Optimización de Recursos

FF.MM.

Fórmula de Éxito:

$$\left(\text{ToT} + \text{Apropiación de Conocimiento} + \text{Trabajo Colaborativo} \right) = \begin{cases} \text{Innovación} \\ \text{nuevas capacidades} \\ \text{Sostenibilidad} \end{cases}$$

¡GRACIAS!

Grupo de Seguridad y Auditoría - GSyA
Universidad Castilla-La Mancha
España

Grupo de investigación Programa de Diseño e Ingeniería (PRODIN)
Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial – COTECMAR
Colombia

ferney.martinez@alu.uclm.es, luise.sanchez@uclm.es,
antonio.santosolmo@uclm.es, david.grosado@uclm.es, eduardo.fdezmedina@uclm.es