
# Universidad de Buenos Aires

## Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería

## Maestría en Seguridad Informática

## Tesis de Maestría

**Tema: Ciberseguridad en el sector transporte, focalizado en los subsectores ferroviario, de aviación civil y marítimo.**

**Título: Análisis de ciberseguridad para el transporte ferroviario, de aviación civil y marítimo de Argentina.**

**Autor**: Ing. Marcos Hernán Martinez.

**Directora de Tesis**: Mg. Patricia Prandini.

**Año de Presentación**: 2022.

**Cohorte del Maestrando**: 2019.

**Declaración Jurada de origen de los contenidos**

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Martinez Marcos Hernan
DNI 31.070.807
FIRMADO

## Resumen

En los últimos años los sistemas de transporte están siendo blanco de numerosos incidentes de seguridad informática debido al incremento de la digitalización, la interconexión entre sistemas, las vulnerabilidades propias de los dispositivos utilizados por los operadores del sector y el hecho de ser altamente atractivo para los ciberdelincuentes. Esto es así ya que cualquier problema de seguridad que afecte estos sistemas tiene el potencial de impactar en otros sectores críticos, en la economía, el medio ambiente e incluso, ocasionar la pérdida de vidas humanas.

Existen muchos desafíos que debe enfrentar el sector, sobre todo en las modalidades analizadas en este trabajo. Entre ellos se encuentran la falta de estándares específicos nacionales e internacionales, una capacitación deficiente en materia de ciberseguridad de quienes operan este tipo de instalaciones y la escasez de conocimientos en gestión de ciberseguridad.

En este Trabajo Final de Maestría, se analizan las principales iniciativas para la gestión de ciberseguridad en el transporte implementadas por Europa, Estados Unidos y Argentina, para los subsectores de aviación civil, ferroviario y marítimo.

Asimismo, se describen en cada subsector o modalidad de transporte las principales tecnologías, ataques y recomendaciones brindadas por entidades especializadas en la materia como ENISA (Agencia de Unión Europea para Ciberseguridad), OMI (Organización Marítima Internacional) y OEA (Organización de Estados Americanos), entre otros.

Finalmente, se incluye una serie de recomendaciones al sector del transporte argentino para fortalecer la ciberresiliencia, elaboradas en base a lo analizado, iniciativas internacionales e información obtenida de expertos en el tema.



**Palabras Clave: Ciberseguridad, transporte, aviación civil, ferrocarril, marítimo, OMI, IATA, FAA, OACI, Comisión Europea, ENISA, OEA, TSA, CISA, Ministerio de Transporte, Trenes Argentinos, GICSAFe, PSA, PNA.**

## Índice de contenidos

# Índice de ilustraciones

## Prólogo

En principio quisiera agradecer a Dios, mis padres, Yami y personas muy importantes para mí por estar siempre presentes en todo lo que hago.

Mi directora de Tesis, Patricia Prandini cuyo apoyo y guía fue imprescindible para poder finalizar esta tesis.

A todos los profesores de la maestría, los cuales además de ser expertos en el tema, mantienen la humildad y predisposición para explicar los contenidos de manera técnica y coloquial.

A la cohorte del año 2019 por ser muy buenos compañeros en los dos años del posgrado; compartiendo conocimientos e incluso momentos divertidos, sobre todo los sábados por la mañana.

Simplemente gracias a todos.

## Nómina de abreviaturas

WIFI: Wireless Fidelity, Fidelidad Inalámbrica.

LAN: Local Área Network, Red de Área Local.

UE: European Union, Unión Europea

ERTMS**:** European Rail Traffic Management System, Sistema Europeo de Gestión del Tráfico Ferroviario.

PTC: Positive Train Control, Control de Tren Positivo.

CONICET: Consejo Nacional de Investigaciones Científicas y Técnicas.

GICSAFe: Grupo de Investigación en Calidad y Seguridad de las Aplicaciones Ferroviarias.

ONU: United Nations, Organizaciones de las Naciones Unidas.

UIC: International Union of Railways, Unión Internacional de Ferrocarriles.

ISO: International Organization for Standarization, Organización Internacional de Normalización.

OACI: International Civil Aviation, Organización de Aviación Civil Internacional.

OMI: International Maritime Organization, Organización Marítima Internacional.

IMO: International Maritime Organization, Organización Marítima Internacional.

OEA: Organización de los Estados Americanos.

GPS: Global Positioning System, Sistema de Posicionamiento Global.

GPRS: General Packet Radio Service, Servicio General de Paquetes vía Radio.

GSM-R: Global System for Mobile Communications-Railways, Sistema Global de Comunicaciones Móviles para Ferrocarriles.

SCADA: Supervisory Control and Data Acquisition, Supervisión, Control y Adquisición de Datos.

RFID: Radio Frequency Identification, Identificación por Radiofrecuencia

MTU: Master Terminal Unit, Unidad Terminal Maestra.

PLC: Programmable Logic Controller, Controlador Lógico Programable.

IioT: Industrial internet of Things, Internet Industrial de las Cosas.

RGPD: General Regulation of Data Protection, Reglamento General de Protección de Datos.

NIS: Network and Information Security, Sistemas de Información y Redes.

APT: Advanced Persistent Threat, Amenaza Persistente Avanzada.

WinCC: Windows Control Center, Centro de Control Windows.

DoS: Denial of Service, Denegación de Servicio.

DDoS: Distributed Denial of Service, Denegación de Servicio Distribuido.

ECCSA: European Centre for Cybersecurity in Aviation, Centro Europeo para la Ciberseguridad en la Aviación

ENISA: European Network and Information Security Agency, Agencia Europea de Seguridad de las Redes y de la Información.

ERA: European Union Agency For Railways, Agencia Europea Para Ferrocarriles.

OES: Operators of Essential Services, Operador de Servicios Esenciales.

EMSA: European Maritime Safety Agency, Agencia Europea de Seguridad Marítima.

EASA: European Aviation Safety Agency, Agencia Europea de Seguridad Aérea.

IDS: Intrusion Detection System, Sistema de Detección de Intrusión IDS.

SOC: Security Operations Center, Centro de Operaciones de Seguridad.

CTV: Connected TV, Television Conectada.

CCTV: Closed-Circuit Television, Circuito de Televisión Cerrado.

VOIP: Voice over Internet Protocol, Voz sobre Protocolo de Internet.

SGSI: Information Security Management System, Sistema de Gestión de Seguridad de la Información.

PIMS: Personal Information Management Systems, Sistema de Gestión de la Información de Privacidad.

ISM: International Safety Management Code, Código internacional de gestión de la seguridad.

NIST: National Institute of Standards and Technology, Instituto Nacional de Normas y Tecnología.

CSIRT: Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas.

CERT-EU: The Computer Emergency Response Team for the EU Institutions, Equipo de Respuesta ante Emergencias Informáticas para instituciones de UE.

CERT: Computer Emergency Response Team, Equipo de Respuesta ante Emergencias Informáticas.

EE. UU.: United States, Estados Unidos.

DOT: United States Department of Transportation, Departamento de Transporte

de Estados Unidos.

TSA: Transportation Security Administration, Administración de Seguridad del Transporte.

DHS: United States Department of Homeland Security, Departamento de Seguridad Nacional de los Estados Unidos.

NSTS: National Strategy for Transportation Security, la Estrategia Nacional para la Seguridad del Transporte.

TSSCWG: Transportation Systems Sector Cyber Working Group, Grupo de trabajo de ciberseguridad del sector de sistemas de transporte.

CISA: Cybersecurity and Infrastructure Security Agency, La Agencia de Seguridad de Infraestructura y Ciberseguridad.

USCG: United States Coast Guard, Guardia Costera de los Estados Unidos.

ADS: Automated Driving System, Sistema de Conducción Automatizada.

PBIP: Protección de los Buques y de las Instalaciones Portuarias.

SOLAS: Safety of Life at Sea, Seguridad de la Vida en el Mar.

NVIC: Navigation and Vessel Inspection Circular, Circular de Inspección de Navegación y Embarcaciones.

IGS: International Security Management Code, Código Internacional de Gestión de la Seguridad.

NGS: National Safety Management Standard, Norma Nacional de Gestión de la Seguridad.

JST: Junta de Seguridad de Transporte.

PNA: Prefectura Naval Argentina.

PSA: Policía de Seguridad Aeroportuaria.

FAA: Federal Aviation Administration, Administración Federal de Aviación.

IATA: International Air Transport Association, Asociación Internacional de Transporte Aéreo.

MQTT: Message Queue Server Telemetry Transport, Transporte de telemetría de cola de mensajes.

UE: European Union, Unión Europea.

FBI: Federal Bureau of Investigation, Buró Federal de Investigaciones.

BIMCO: Baltic and International Maritime Council, Consejo Marítimo Báltico e Internacional.

## Introducción

El presente trabajo de maestría tiene por objetivo establecer el escenario actual en materia de ciberseguridad en el transporte. Este sector es particularmente relevante ya que forma parte de la infraestructura crítica de una nación. Particularmente, los subsectores marítimos, de aviación civil y ferroviario transportan un gran volumen de personas y mercaderías, en algunos casos alrededor de todo el mundo; involucrando distintos países.

Desde hace algunos años los subsectores o medios mencionados están siendo víctima de ciberataques, sobre todo por resultar atractivos a los ciberdelincuentes, por el incremento de la digitalización en el transporte y por la evolución de los atacantes en sus técnicas y organización. Entre los actores involucrados hay también estados que buscan desestabilizar a otros países con fines políticos y/o económicos.

Además, muchas tecnologías que se utilizan en estos subsectores no fueron pensadas desde la perspectiva de la seguridad informática y sin embargo, la realidad actual indica que se conectan a Internet. Esto las expone a una serie de vulnerabilidades que se acentúan ante la falta de mantenimiento y la carencia de estándares y controles acordes que entre otros motivos, incrementan sus posibilidades de ser víctimas de ciberataques.

La falta de concientización y la desinformación en la materia produce que muchos atacantes opten por poner su foco en las personas en vez de las tecnologías, provocando que sean utilizados involuntariamente como medio para acceder o causar un daño en los sistemas utilizados en el sector.

Lo anteriormente expuesto podría, además, impactar gravemente en otras áreas críticas, como la economía, el medio ambiente e incluso la salud de la población, debido al alto grado de dependencia que tienen con el sistema de transporte.

Si bien escasean los estándares internacionales y específicos en cada modalidad o subsector, las organizaciones y los países están cooperando para compartir información, generar normas, recomendaciones, directivas y especificaciones técnicas que ayuden a fortalecer la ciberresiliencia. En este proceder se pone de manifiesto el hecho de que comprenden la gravedad de la temática y se encuentran expuestos a las mismas vulnerabilidades,

amenazas y ataques.

El presente trabajo se dividirá en 6 capítulos recopilando en un solo documento los problemas, las principales iniciativas y una serie de recomendaciones en materia de ciberseguridad en las modalidades de transporte ferroviario, de aviación civil y marítimo. Respecto a las iniciativas, se hará foco en Europa, Estados Unidos y Argentina, y para el caso de las recomendaciones, se focalizarán en nuestro país a partir de su realidad y lo que ocurre en otros países.

El primer capítulo describirá las principales iniciativas/acciones para la gestión de la ciberseguridad en el transporte (a nivel general) implementadas por los tres ámbitos geográficos mencionados. Por ejemplo, si consideran al sector como crítico, cómo se subdivide y qué medidas se están tomando.

Desde el capítulo 2 hasta el 4 inclusive se desarrollará cada modalidad o subsector en particular de los mencionados precedentemente, que abarcará las principales tecnologías utilizadas, las vulnerabilidades y amenazas más usuales, los ciberataques registrados, los escenarios de ataque y las recomendaciones o buenas prácticas brindadas por organizaciones, instituciones y expertos en la materia.

En el capítulo 5 se brindarán recomendaciones generales al sector del transporte argentino en base a lo analizado y a información obtenida de expertos reconocidos en el tema.

Por último, se brindarán las conclusiones del trabajo final de maestría en base a la labor realizada.

Cabe resaltar que no se contempla en el desarrollo del trabajo el análisis del funcionamiento de los sistemas involucrados en cada subsector o modalidad, por ejemplo, los sistemas de gestión de tráfico, control, ERTMS (Sistema Europeo de Control de Trenes) o PTC (Control Positivo de Trenes).

Los dos últimos se aplican a Europa y Estados Unidos respectivamente y no en nuestro país, por lo que se consideró que no era de utilidad para los objetivos del estudio.

Asimismo, no se profundizan aspectos de privacidad, jurídicos en general (leyes, normas, directivas, etc.) y sobre la organización interna de las instituciones responsables del sistema.

# 1 Gestión de ciberseguridad en el transporte en la Unión Europea, Estados Unidos y Argentina

Este capítulo tiene el objetivo brindar un panorama de los avances en cuanto a la gestión de la ciberseguridad en el transporte en la UE (Unión Europea), EEUU y Argentina.

En este sentido, se mencionarán las actividades más importantes que permitan identificar las acciones, estrategias, políticas y departamentos/agencias intervinientes, así como otros actores relevantes involucrados. Por ejemplo, si consideran al transporte como crítico y, cómo subdividen el sector.

Cabe destacar que como ya se adelantó previamente, en los 3 capítulos subsiguientes, se realizará una descripción para cada modalidad analizada, es decir el ferrocarril, la aviación civil y el transporte marítimo.

## 1.1 Unión Europea

A fines del 2020, la UE presentó una nueva Estrategia de Ciberseguridad para la región [1], la cual tiene como objetivo fomentar la resiliencia frente a las ciberamenazas en los servicios esenciales (electricidad, salud, **transporte**, etc.) y en los dispositivos conectados, con el fin de construir una Europa digital, interconectada y más resiliente.

En este documento, la UE se compromete a apoyar los objetivos fijados en la propia estrategia, con una inversión sin precedentes para el período 2020 a 2027.

El 16 de diciembre del 2020 la UE generó una nueva versión de la Directiva NIS (Network and Information Systems)[1], denominada NIS2. Esta versión amplía el alcance de la anterior, añadiendo nuevos sectores. También impone un enfoque de gestión de riesgos a través de una lista mínima de elementos básicos de seguridad que deben aplicarse, medidas más estrictas de supervisión para las autoridades nacionales y requisitos de ejecución más

[1] Esta directiva surgió en 2016 debido al creciente número de ataques e incidentes y es el primer instrumento legislativo de ciberseguridad aprobado por la UE.

exigentes.

La directiva establece, además, las medidas necesarias para garantizar un nivel uniforme y elevado de seguridad en las redes y sistemas de información dentro de la UE [2]. Para ello, asegura la creación y cooperación de organismos gubernamentales encargados de supervisar la ciberseguridad en los estados miembros, requiriendo que colaboren con sus homólogos de otros países, compartiendo información [3].

Más específicamente para el sector bajo análisis, ENISA[2] junto a la UE, EASA (Agencia Europea de Seguridad Aérea), EMSA (Agencia Europea de Seguridad Marítima) y ERA (Agencia de Unión Europea para Ferrocarriles) organizaron en 2019 la primera conferencia sobre ciberseguridad en el transporte. En esta conferencia participaron 170 organizaciones públicas y privadas de toda Europa en representación de todos los medios de transporte del sector [4].

En su ámbito, se debatió sobre un marco legal de la UE para la ciberseguridad y la importancia de la cooperación entre todos los involucrados, impulsada por las agencias anteriormente citadas para cada modalidad del transporte. También se alentó a que se incluya en la agenda la ciberseguridad, un mayor diálogo con otros países y una mayor profundidad en la cooperación con organismos como OACI (Organización de Aviación Civil Internacional) y la OMI.

Además, se creó un foro especializado denominado TRANSSEC, formado por expertos en seguridad y resiliencia del transporte. Este foro tiene como objetivo reunir a expertos para intercambiar puntos de vista e ideas sobre las amenazas, desafíos y soluciones de ciberseguridad en los subsectores aéreo, ferroviario y acuático / marítimo [5].

En diciembre del año pasado, se llevó a cabo en Alemania el “Congreso de Seguridad del Transporte Europa 2021” [6] , el cual estuvo centrado en la industria en la aviación, el ferrocarril, la automoción y el transporte marítimo. Los temas que se presentaron fueron entre otros, la ciberseguridad, la seguridad física y las características de las regulaciones.

[2] Esta agencia, en cooperación con la comunidad en general, está dedicada a establecer un nivel alto y estándar de ciberseguridad para todos los países miembros de la UE . También es la encargada de la implementación de la Directiva NIS [1] .

La Comisión Europea, a raíz de la primera conferencia sobre ciberseguridad en el transporte, publicó el mismo día que la Directiva mencionada anteriormente (16 de diciembre del 2020) un conjunto de herramientas de ciberseguridad en el transporte, bajo la denominación *"Transport Cybersecurity Toolkit"* (en español, "Herramientas de ciberseguridad para el transporte"). Estas herramientas están alineadas a la estrategia y directiva anteriormente mencionadas y en ellas se enumeran buenas prácticas (recomendadas para todo el personal) con el fin de mejorar la ciberseguridad y la ciberresiliencia en las empresas del sector; independientemente de su tamaño y ámbito de actividad. Concretamente, las herramientas buscan mitigar cuatro amenazas que pueden afectar a las organizaciones de transporte: la difusión de malware, la denegación de servicio, el acceso no autorizado y el robo. Se agrega también la manipulación de software.

Así mismo, contiene información relevante para los profesionales de la seguridad y la ciberseguridad en las organizaciones de transporte y proporciona una guía sobre cómo identificar, proteger, detectar y responder a las amenazas de ciberseguridad en cada modalidad de transporte, sea esté aéreo, marítimo o terrestre.

Con el fin de tener mayor difusión, en el año 2021 la Comisión tradujo este documento a 22 idiomas como francés, portugués e italiano entre otros, además del inglés. También alienta a las empresas de transporte a difundirlo internamente [7] [8].

## 1.2 Estados Unidos

En su estrategia nacional de ciberseguridad se estableció el sector del transporte como un área crítica [9], dividido en siete subsectores:

- **Aviación:** incluye aviones, sistemas de control de tráfico aéreo, aeropuertos, helipuertos y pistas de aterrizaje.
- **Autopista y autotransportista:** abarca carreteras, puentes, túneles y vehículos como camiones (incluidos los que transportan materiales peligrosos), comerciales (micros escolares, etc.); sistemas de: licencias, conductores, gestión del tráfico y de ciberseguridad utilizados para la administración operativa.
- **Transporte marítimo**: incluye costas, puertos, vías fluviales y conexiones terrestres intermodales que permiten que otras modalidades de transporte trasladen personas y mercancías (desde, hacia y sobre el agua). En la estrategia nacional se plantea específicamente mejorar la ciberseguridad en este subsector.
- **Transporte masivo y tren de pasajeros:** incluye estaciones, sistemas operativos e infraestructura de apoyo para los servicios de pasajeros mediante autobuses de tránsito, monorraíl, tren o metro, abarcando el transporte público y las operaciones de trenes de pasajeros.
- **Sistemas de tuberías (oleoductos)**: atraviesan el país transportando casi todo el gas natural y alrededor del 65 por ciento de los líquidos peligrosos (ej. productos químicos). También se incluyen los activos sobre el suelo, como estaciones de compresión y de bombeo.
- **Ferrocarril de mercancías:** reúne todo el traslado de bienes y elementos por vías férreas y consta de siete transportistas principales y cientos de ferrocarriles más pequeños.
- **Correo Postal:** incluye grandes transportistas, servicios de mensajería regionales y locales y de correo, así como empresas de administración, flete y entrega.

Con el fin de asegurar la infraestructura crítica, se lleva a cabo una serie de acciones, entre las que pueden citarse incentivar las inversiones en ciberseguridad, trabajando con entidades (del sector público y privado),

priorizar la investigación con tecnologías emergentes, favoreciendo la resiliencia ante interrupciones a gran escala o de larga duración y mejorar el transporte marítimo respecto a su ciberseguridad.

El DOT (Departamento de Transporte) elaboró en 2011 una política departamental de ciberseguridad, la cual sirve como directiva fundamental sobre la que se basan guías, políticas, procedimientos, estándares y procesos complementarios que implementan requisitos obligatorios de ciberseguridad exigidos al organismo por otras entidades. Entre estas últimas se encuentran el NIST (Instituto Nacional de Normas y Tecnología) y el DHS (Departamento de Seguridad Nacional). La política antes citada está sujeta a adiciones, eliminaciones y / o modificaciones en su contenido en función de los requisitos cambiantes, las nuevas tecnologías y las amenazas que surjan, según se considere necesario [10].

El DOT tiene también una política de divulgación de vulnerabilidades, cuyo objetivo es brindar a los profesionales de seguridad pautas claras sobre cómo y qué debilidades informar. Describe sistemas y tipos de investigación (técnicas o métodos) utilizados, cómo enviar informes y cuánto tiempo esperar antes de revelar públicamente las vulnerabilidades.

Esta política se aplica a los siguientes sistemas y/o servicios ofrecidos desde los siguientes sitios web:

- www.transportation.gov.
- transportation.gov.
- safetydata.fra.dot.gov.

No obstante, si el especialista en seguridad considera que el sistema o servicio es de interés, recomiendan ponerse en contacto con el DOT [11] antes de realizar alguna acción.

En 2020 el DHS, en nombre de TSA (Administración de Seguridad del Transporte)[3] y DOT, presentó la NSTS (Estrategia Nacional para la Seguridad del Transporte) [12] con un enfoque basado en riesgos, con el objetivo de proteger los sistemas de transporte de la nación de ataques o interrupciones

[3] Esta administración asegura los cuatro modos generales de transporte terrestre: masivo, ferrocarril de carga, autotransportista y oleoductos. También brinda apoyo en la seguridad marítima a la Guarda Costera [58].

por parte de terroristas u otras amenazas. La mencionada estrategia cubre un lapso que llega hasta el 2025.

Adicionalmente, el DHS junto al DOT emitieron en 2015 el "Plan Específico del Sector de Sistemas de Transporte" y en ese mismo año, publicaron una "Guía de implementación del marco de ciberseguridad del sector de los sistemas de transporte" [13], junto a un documento complementario [14]. Estos documentos buscan orientar a los propietarios y operadores del sector respecto a cómo aplicar los principios del marco de ciberseguridad del NIST para asistir en minimizar los riesgos de ciberseguridad.

Si bien la TSA tiene autoridad para regular la ciberseguridad en el sector del transporte, desde 2010 ha adoptado enfoques colaborativos y voluntarios con la industria. Como resultado, se estableció el TSSCWG (Grupo de trabajo de ciberseguridad del sector de sistemas de transporte) para promover la ciberseguridad en todas las modalidades que caracterizan al sector.

Una de las primeras acciones del TSSCWG fue crear la estrategia de ciberseguridad a mediados de 2012, la cual hace hincapié en la colaboración y promoción de conciencia sobre esta temática [15].

La TSA, publicó en noviembre de 2018 un plan denominado" Hoja de ruta de ciberseguridad", que se alinea con la Estrategia de ciberseguridad del DHS[4], publicada a principios del 2018.

La hoja de ruta de ciberseguridad es una pieza clave de la estrategia de TSA[5] para mejorar la seguridad y salvaguardar el sistema de transporte, ya que además, se alinea con las estrategias y planes tanto departamentales como nacionales.

Esto le permite a la TSA el desarrollo de planes coherentes en los niveles estratégicos y tácticos para la protección del sector.

En el primer nivel, cabe hacer notar que el presidente Biden considera

[4] La estrategia tiene un alcance de cinco años y su objetivo es guiar al departamento con el fin de lograr que el ecosistema de ciberseguridad sea más seguro y resistente [73].

[5] La estrategia de la TSA 2018-2026 identifica tres prioridades: mejorar la seguridad, salvaguardar el sistema de transporte y comprometerse con la sociedad.

a la ciberseguridad como una de sus principales prioridades. Ante ello, en marzo del 2020, el secretario de DHS describió una hoja de ruta para abordar la temática a través de iniciativas en forma de “sprints” (o lapsos de tiempo, según la terminología utilizada por las metodologías ágiles) de 60 días cada uno:

- **Sprint de "ransomware" (abril y mayo de 2021)**: el DHS creó un grupo de trabajo interno con representantes de CISA (Agencia de Seguridad de Infraestructura y Ciberseguridad), el Servicio Secreto, la Guardia Costera (USCG), asuntos públicos y expertos del Congreso entre otros.

  CISA es el asesor de riesgos de la nación físicos y cibernéticos que trabaja con socios para defenderse de las amenazas y colabora para construir una infraestructura más segura y resistente.
- **Sprint "Cybersecurity Workforce" (mayo y junio de 2021):** se enfoca en construir una fuerza laboral de ciberseguridad más robusta y diversa del personal del DHS. Cubre una amplia gama de actividades basadas en el compromiso, diversidad, equidad e inclusión.
- **Sprint de “Sistemas de Control Industrial” (julio y agosto de 2021):** Está diseñado para movilizar acciones con el fin de mejorar la resiliencia de los sistemas de control industrial, en parte debido al intento de ciberataque a una planta potabilizadora de agua (a principios de 2021) y al ataque de ransomware a **Colonial Pipeline**[6].
- **Sprint "Ciberseguridad y transporte" (septiembre y octubre de 2021):** el objetivo es aumentar la resiliencia de ciberseguridad de los sistemas de transporte del país: aviación, ferrocarril, tuberías y el marítimo. La TSA, la USCG y CISA son parte del DHS. El propósito es aprovechar las mejores prácticas y profundizar la colaboración con el Departamento de Transporte y todos los interesados en la industria.
- **Sprint de "seguridad electoral" (noviembre y diciembre de 2021):** el propósito es asegurar la infraestructura necesaria para mantener la

[6] Colonial Pipeline es la compañía de oleoducto más importante del país, el 07 de mayo del 2021 fue víctima de un ransomware as a service denominado Darkside. provocando el corte del suministro (desde Texas hasta Nueva York) de nafta y diesel entre otros. También, se confirmó que robaron más de 100 GB con información de la compañía [66].

integridad de las elecciones.

- **Sprint de "Ciberseguridad internacional" (enero y febrero de 2022):** está dedicado a las actividades de ciberseguridad internacional del Departamento.

Finalmente, el 13 de septiembre de 2021 se realizó una conferencia en Miami, EEUU, que reunió a líderes empresariales y de seguridad de todos los sectores del transporte de pasajeros y mercancías para debatir temáticas como IoT (Internet de las cosas) y ciberseguridad, entre otros [16].

### 1.3 Argentina

La Estrategia Nacional de Ciberseguridad aprobada y publicada en el año 2019, menciona en su introducción que el sector analizado en este trabajo es crítico. Efectivamente, lo incluye cuando explica el concepto de servicios esenciales como aquellos que resultan" *… esenciales para la vida de las personas y para la economía, como la energía, el agua,* ***el transporte****…*". También hace referencia a que poseen una fuerte dependencia de las redes informáticas y que *"…su protección es extremadamente compleja, entre otras razones, porque implica la coordinación de esfuerzos de múltiples actores públicos y privados…*" [17]

Por otra parte, la Resolución N° 1523/2019 que define el concepto de Infraestructuras Críticas de Información y establece 11 sectores en las que se agrupan, reconoce al Transporte como uno de dichos sectores.

El autor consultó al Ministerio de Transporte respecto a cómo se sectoriza el transporte, es decir si existe alguna resolución o documento que especifique como se lo subdivide.

En respuesta, recibida por email el día 24 de agosto del 2021 se informó que: *"…El transporte se divide en diversas modalidades, entre las cuales se encuentra el transporte por automotor, ferroviario (de superficie y subterráneo), aerocomercial y fluvial, marítimo y de la marina mercante.*

*A la vez, tanto el transporte automotor, como el ferroviario, el aerocomercial y el fluvial, marítimo y de la marina mercante puede ser de pasajeros o de cargas…".* [18].

Dentro del Ministerio de Transporte se encuentra la JST (Junta de Seguridad en el Transporte**)** que se encarga de investigar sucesos (accidentes o incidentes) y emitir recomendaciones, promoviendo la cultura de seguridad en el transporte. No obstante, su enfoque es meramente a la seguridad ligada a accidentes operativos no intencionales. Es decir, no tiene en cuenta la protección contra amenazas o incidentes intencionales ni cibernéticos**.**

Respecto a la ciberseguridad, en Argentina existen iniciativas y acciones en las modalidades aéreo comercial, marítimo y ferroviario, las que serán desarrolladas en los capítulos siguientes.

# 2. Ferrocarril

En este capítulo se mencionarán las principales tecnologías utilizadas en el ferrocarril, así como algunos ataques ocurridos en el sector, especialmente ligados a la utilización de sistemas SCADA (Supervisión, Control y Adquisición de Datos)[7]. Efectivamente, este sector ha incrementado en forma notable la utilización de la tecnología, circunstancia que si bien ha mejorado el servicio, también ha incrementado enormemente la exposición a ciberataques.

Asimismo, se describirán los actores principales y dos escenarios posibles de riesgo y se agregará una serie de recomendaciones brindadas por organizaciones como la Comisión Europea para fortalecer la ciberresiliencia.

Por último, se revisarán las iniciativas y acciones que se están llevando a cabo en la Unión Europea, Estados Unidos y Argentina en este subsector y algunas organizaciones intervinientes, como la UIC (Unión Internacional de Ferrocarriles)[8].

La UIC realizó varios eventos y publicaciones para abordar temas de ciberseguridad en el sector ferroviario como, por ejemplo, una serie de Directrices para la ciberseguridad en los ferrocarriles [26].

## 2.1 Tecnologías utilizadas

El sector ferroviario en la UE está migrando sus servicios a la tecnología digital, incorporándola en procesos tales como la señalización, la venta de pasajes y la supervisión del suministro eléctrico de la red vial.

Los principales sistemas que se utilizan son [19] ventas, distribución y relaciones comerciales (compra de boletos o reserva de asiento), señalización (barreras, semáforos, etc.), comando y control (para el movimiento y frenado de trenes), telecomunicaciones (sistemas de radio, red, etc.), confort y

[7] Aplicación de software, diseñada con el motivo de controlar y gestionar procesos a distancia. Se basa en la adquisición de datos de los procesos remotos.

[8] La Union Internationale des Chemins de Fer es un organismo internacional fundado en 1922 que tiene como objetivo la normalización de las instalaciones y del material ferroviario, así como de los aspectos técnicos y organizativos del ferrocarril.

servicios al pasajero (anuncios, iluminación, elevadores, etc.), servicios auxiliares (energía, luces de emergencia, etc.), seguridad y mantenimiento (control de acceso, video vigilancia, sistemas de reporte, etc.).

Los sistemas utilizan las mismas redes, protocolos y activos digitales que las demás áreas, como por ejemplo, sensores, cámaras de video y PCs. A esto se suman los dispositivos que están intercomunicados a través del Internet industrial de las cosas (IioT, Industrial Internet of Things). Además, usan GPS (Sistema de Posicionamiento Global), GPRS (servicio general de paquetes vía radio), GSM-R (Sistema Global de Comunicaciones Móviles para Ferrocarriles), según sea el caso. Por ejemplo, en Europa emplean el último al pertenecer al ERTMS y en Estados Unidos, GPS al implementar PTC.

Por último, también utilizan SCADA para controlar sus sistemas críticos, desde el monitoreo del suministro eléctrico de los motores hasta la gestión del equipamiento de las estaciones como ascensores, escaleras mecánicas y ventilación.

## 2.2 Actores

En el sector ferroviario, existen principalmente tres perfiles de actores/atacantes con diversas motivaciones:

**Ciberterroristas:** este tipo de actores poseen una motivación ideológica. Sus objetivos son destruir vidas humanas e infraestructuras con el fin de instaurar el terror. Por ello es imprescindible controlar sus acciones.

**Hacktivistas**: motivados ideológicamente, sus objetivos no son letales e incluyen por ejemplo, alteración de sitios web por defacement, robo de información y filtración de datos. Utilizan los ataques de denegación de servicio, conocidos bajo la sigla “DoS” (Denial of Service) e infiltraciones en servidores web, entre otros.

**Cibercriminales**: persiguen objetivos económicos. El transporte les atrae por dos motivos. En primer lugar, porque se trata de un sector con un alto perfil público y en segundo lugar, debido a su importancia estratégica. Estos factores lo hacen vulnerable, por ejemplo, al ransomware[9].

[9] Es un tipo de malware que luego de comprometer un equipo secuestra la información y exige el pago de un rescate con la promesa de recuperar los datos y evitar daños

Según el informe de Thales [20] existen 12 grupos de atacantes activos (en distintas regiones/países) que operan contra el sector ferroviario. De éstos, 4 son considerados los más peligrosos. Concretamente, 3 están patrocinados por países: ATK4, ATK14 y ATK35 y el restante es un cibercriminal/hacktivista (ATK140). Ver ilustración siguiente:

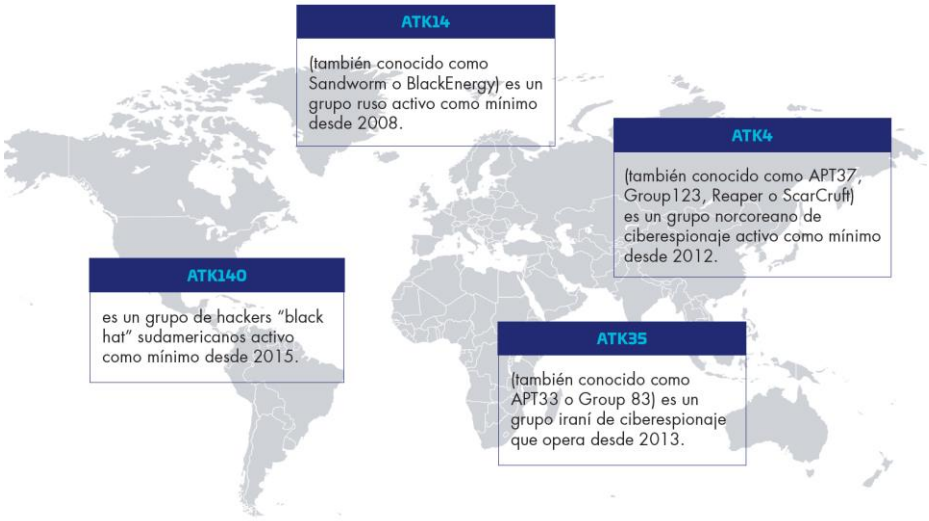


Ilustración 1: Principales grupos de atacantes alrededor del mundo.

Fuente: [21].

## 2.3 Amenazas y ataques

El aumento notable de la utilización de la tecnología ya mencionada incrementa enormemente la exposición a ciberataques. Si bien no hay registros a la fecha de eventos cibernéticos graves en sistemas críticos del sector ferroviario, se han producido problemas crecientes en áreas como la venta de pasajes, la comunicación a los pasajeros, la señalización y la videovigilancia.

Los ciberataques no solo comprometen la seguridad, sino también causan perjuicios a la reputación de los operadores y posibles implicaciones legales en el marco del RGPD[10] (Reglamento General de Protección de Datos) al vulnerarse los datos personales o sensibles de empleados y/o

colaterales.

[10] Es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos.

pasajeros.

Uno de los principales desafíos para el sector ferroviario es que sus vulnerabilidades no pueden minimizarse o eliminarse fácilmente. Esto se debe a que los activos están muy dispersos, son heterogéneos y suelen tener una utilización que excede la vida útil recomendada por el fabricante. Esto dificulta el despliegue rápido de parches y el mantenimiento.

Además de protegerse contra ataques externos, no deben descartarse tampoco los ataques internos.

Por otro lado, varios sistemas industriales SCADA ya han sido objeto de hackeo, con graves consecuencias sobre la operación que en algunos casos, implicó riesgos contra la vida. Algunas de las razones para que esto haya ocurrido es que estos sistemas fueron diseñados en la década del 60 y operaban en ambientes aislados con tecnología propietaria. Por lo tanto, no fueron pensados para ser seguros a nivel informático.

No obstante, con el advenimiento de Internet comenzaron a compartir información con sistemas corporativos, lo cual provocó nuevos riesgos debido a que muchos emplean software de base y programas muy antiguos que carecen de las últimas actualizaciones de seguridad y en la mayoría de los casos, son difíciles de actualizar. Además, estas redes necesitan controles adicionales y compensatorios para su protección, de modo de minimizar los riesgos a los que se exponen.

También el informe muestra en una matriz las tácticas y técnicas más utilizadas para atacar el sector.

Dicha matriz utiliza MITRE ATT&CK[11] y describe las 12 tácticas que un atacante puede utilizar**:** acceso inicial, ejecución, persistencia, escalación de privilegios, evasión de defensa, acceso a credenciales, descubrimiento, movimiento lateral, colección, comando y control, exfiltración e impacto.

Cada una de esas tácticas tiene entre 9 y 68 técnicas identificadas por MITRE para lograr esos pasos u objetivos. Por ejemplo, para obtener el acceso inicial se podría utilizar la técnica “Spearphishing Link” (estafa de

[11] Es una base de conocimientos abierta que informa sobre las tácticas y técnicas hostiles utilizadas mundialmente; se basa a través de observaciones del mundo real [56].

correo electrónico) y para persistencia, registrar claves en el Registro de Windows. Generalmente se emplean varias tácticas para concretar un ataque.

A continuación, se describen algunos ejemplos de ataques a infraestructuras ferroviarias, citados en el informe [22]:

**Ucrania:** en el año 2015, se llevó a cabo un ataque de DoS a gran escala para desestabilizar al gobierno apuntando a centrales eléctricas, infraestructura minera y ferroviaria. El objetivo consistía en paralizar la infraestructura pública y crítica, deshabilitando los Sistemas de Control Industrial (ICS).

**EEUU:** el 28 de noviembre de 2016, el metro de San Francisco fue víctima de un ransomware denominado HDDCryptor el cual afectó a servidores de correo, impresoras, bases de datos, máquinas de tickets en las estaciones y los monitores que muestran los horarios. Cabe destacar que los trenes no resultaron afectados.

Según la prensa local, los ciudadanos viajaron gratis ese día y el servicio se reestableció cuando se pagó el rescate de unos 100 Bitcoins, aproximadamente unos 73.000 dólares [23] [24].

**Alemania:** En mayo de 2017, la principal empresa ferroviaria de Alemania, Deutsche Bahn, fue víctima del ransomware WannaCry. Algunos dispositivos fueron afectados; provocando que los pasajeros no visualicen la información del sitio. A pesar del perjuicio ocasionado, no se interrumpió el funcionamiento del servicio.

**Suecia:** En octubre de 2017 ocurrieron 2 ataques de tipo DDoS (Distributed Denial of Service). El primero se llevó a cabo el día 11, afectando a la Administración de Transporte (Trafikverket). Este se realizó a través de sus dos proveedores de Internet y perjudicó al sistema que supervisaba la ubicación de los trenes. También eliminó el sistema de correo electrónico de la Agencia Federal, su sitio web y los mapas de tráfico por carretera. Además, los clientes no pudieron realizar reservas o recibir actualizaciones sobre los retrasos. Por otro lado, los operadores tuvieron que gestionar manualmente el tráfico de trenes y otros servicios afectados.

Al siguiente día, un segundo ataque DDoS afectó el sitio web de la Agencia de Transporte, un organismo gubernamental independiente, el cual

es responsable de regular e inspeccionar los sistemas de transporte. También perjudicó al operador de transporte público de Suecia Occidental denominado Vasttrafik, bloqueando su aplicación de reserva de boletos y su servicio de planificación de viajes en línea.

**Dinamarca**: en mayo de 2018, se produjo un ataque DDoS que afectó los sistemas de emisión de pasajes de la compañía de trenes de pasajeros más importante de Dinamarca: Danske Statsbaner (DSB). Según esta empresa, alrededor de 15 mil clientes no podían comprar boletos desde las máquinas expendedoras.

**Londres:** en agosto de 2019, alrededor de 1200 cuentas de tarjetas de Oyster, el sistema de pago para el transporte, fueron accedidas sin autorización por los ciberdelincuentes. Los nombres de usuario y las contraseñas fueron extraídas en alguna filtración en otro sitio, aprovechando la mala práctica de reutilizar credenciales en diferentes sitios web.

Como medida de precaución, se cerraron temporalmente las cuentas y tomaron contacto con los usuarios afectados. Según un portavoz de TFL (Transporte de Londres), los datos de pago no han sido expuestos [25].

**Reino Unido:** en marzo de 2020, se filtraron datos de alrededor de 10 mil personas que utilizaron una conexión gratuita de Wifi en una de las estaciones de tren. Las direcciones de correo electrónico y los detalles del viaje estuvieron expuestas en línea. El incidente ocurrió porque una base de datos de la aplicación 'Indian Rail' (provista por la empresa Apple) fue expuesta. Contenía 2.357.684 direcciones de correos electrónicos, fechas de nacimiento, detalles de viajes, nombres de usuario y contraseñas en texto plano.

**Suiza:** en mayo de 2020, el fabricante suizo de vehículos ferroviarios Stadler sufrió un ataque de ransomware, que afectó a todas sus sucursales. Esto permitió el robo de datos confidenciales de la compañía y se filtraron en la web documentos internos; después de que la empresa se negara a ceder a las demandas de rescate.

**España**: en julio de 2020, la entidad pública empresarial española denominada ADIF (Administrador de Infraestructuras Ferroviarias) fue atacada por un ransomware. A pesar de que no afectó a la infraestructura

crítica, se expusieron gigabytes de datos comerciales.

## 2.4 Escenarios de ataque

A continuación, se describen dos escenarios posibles de ataque. El primero se denomina “Triton” y puede afectar a los sistemas SCADA del sector energético. El segundo refiere a cómo infectar objetos industriales como, por ejemplo, cámaras CCTV (Circuito Cerrado de Televisión) con el objetivo de tomar el control de un sistema.

Triton es un malware muy sofisticado y peligroso, elaborado para manipular sistemas de control industrial utilizados en infraestructuras críticas. Se descubrió a finales de 2017, luego de provocar un apagón accidental de una planta petroquímica de Arabia Saudita.

Se cree que este ataque fue perpetrado por el grupo ATK91, el cual estaría vinculado al gobierno ruso.

Un ataque de este tipo en la infraestructura ferroviaria podría utilizarse para neutralizar/espiar las comunicaciones entre la MTU (Unidad Terminal Maestra) y el PLC (Controlador Lógico Programable) mediante un ataque de man in the middle (hombre en el medio). También es factible comprometer el PLC del sistema de control industrial o SCADA, tomando previamente el mando de la unidad maestra con el fin de enviar comandos legítimos pero dañinos.

A pesar de que no existen indicios de este tipo de ataques, se estima que hay como mínimo 30 grupos que utilizan APT (Amenazas Persistentes Avanzadas) [12] técnicamente capaces de realizarlo.

El segundo escenario involucra a dispositivos periféricos y busca comprometer con un malware algún dispositivo accesible como, por ejemplo,

[12] Este tipo de ataque consta de una amplia gama de técnicas de hackeo continuas y avanzadas para acceder a un sistema y permanecer allí durante un tiempo prolongado con consecuencias potencialmente destructivas. Es el de mayor peligro para el sector debido a que los ciberatacantes disponen de amplios recursos y a menudo cuentan con el patrocinio de países. Pueden incluir: el espionaje, robo o la interrupción del servicio.

una terminal dispensadora de pasajes o una cámara CCTV disponible en una estación o unidad de control ferroviario.

Para ejemplificar el segundo escenario, imaginemos que en el ataque se utiliza el malware Mirai[13], el cual una vez que infectó un equipo, escanea la red para conectarse a otros dispositivos vulnerables con el fin de controlarlos. Para ello utiliza una tabla de contraseñas por defecto.

Los dispositivos de bajo costo como cámaras y routers, ofrecen escasa seguridad nativa y utilizan protocolos y software muy conocidos por los desarrolladores y atacantes. Esto puede aprovecharse a través del alquiler de botnets o de la contratación de ciberdelincuentes especializados.

Cabe mencionar que las redes ferroviarias contienen miles de sensores accesibles y que suelen cubrir enormes áreas geográficas, lo cual dificulta su gestión en materia de seguridad física y lógica.

Imaginemos que una cámara instalada para supervisar una estación de ferrocarril fue expuesta accidentalmente a Internet. De este modo, a través del dispositivo se tiene acceso a los sistemas de IT y de OT (Tecnologías de la Operación) de la empresa, ya que este periférico podría encontrarse afectado por cualquiera de las vulnerabilidades que se publican cada año en Internet[14].

Una vez que el atacante ha penetrado en la red de su víctima, puede:

- Cortar la entrada de vídeo e incluso reproducir una falsa grabación.
- Espiar las comunicaciones, obtener información sobre el funcionamiento del sistema o interceptar datos de los clientes y/o empleados.

Como se explicó, las consecuencias pueden ser importantes y abarcar retrasos generalizados en los viajes, pérdidas económicas originadas en las demandas de rescate, robo/exposición de datos y daños a la

[13] Es considerado el botnet más potente del mundo, tiene como objetivo los dispositivos de Internet de las cosas (IoT, Internet of Things). Ej: cámaras, routers, etc.

[14] En 2019 se identificaron más de una docena de vulnerabilidades para este tipo de productos. Se estima que existen 180 mil dispositivos infectados.

reputación, por citar algunos.

## 2.5 Recomendaciones

En el informe de Thales [21] y de la Comisión Europea [7] se describen las principales buenas prácticas para gestionar a las ciberamenazas:

- **Gobernanza**: definir políticas y procesos con el fin de mejorar la ciberseguridad de los servicios y sistemas (incluyendo IT y OT). Asignar un rol senior para que administre la seguridad cibernética y física de la instalación.
- **Análisis de los riesgos de ciberseguridad**: identificar y evaluar posibles impactos que tendrían los ataques en sus activos. Para ello, se debe conocer en profundidad el hardware y software desarrollado para diferentes servicios en IT y OT para luego identificar e implementar medidas de tratamiento de riesgo y planes para mitigarlos.
- **Investigación de las amenazas y vulnerabilidades**: informarse acerca de las nuevas vulnerabilidades junto a su criticidad. Ser proactivo, adaptarse a los controles de seguridad y suscribirse a un servicio de inteligencia de amenazas para la ciberseguridad en el ámbito ferroviario.
- **Protección de la identidad y el acceso**: comprender, documentar y administrar los accesos a las redes y sistemas de información (IT y OT) que soportan las operaciones de funciones esenciales en el ferrocarril. Es importante que se aplique el principio del menor privilegio y se identifique y separe las cuentas administrativas de las operativas; controlando ambas. Por último, tener presente y proteger los accesos lógicos y físicos.
- **Gestión de parches y actualizaciones de seguridad**: definir una política para realizar actualizaciones que se adapten a las restricciones operativas, de seguridad y a los riesgos anteriormente identificados. Mantener al día el hardware y software de las estaciones de trabajo.

- **Gestión de la configuración de los activos**: aplicar las mejores prácticas en cuanto a la configuración de sistemas operativos y aplicaciones. Implementar controles estrictos en todas las entradas, incluidos los medios extraíbles.
- **Políticas de seguridad y procesos:** definir, implementar, comunicar y mejorar las políticas (contraseña, almacenamiento, etc.) y procesos (implementación de parches de seguridad y administración de hardware y sistemas de software), los cuales definen un enfoque global para asegurar los sistemas y datos que soportan operaciones esenciales en el transporte por ferrocarril.
- **Sistema de seguridad y datos**: proteger los datos (almacenados y transmitidos electrónicamente), redes críticas y sistemas (IT y OT) de ciberataques, tomando en cuenta el enfoque de administración de riesgos. Estas medidas de seguridad deberían incluir encriptación y protocolos para la comunicación de modo de proteger datos en tránsito de amenazas de ciberseguridad resultantes de ataques de man-in-the-middle (hombre en el medio).
- **Backup**: realizar pruebas periódicas de recuperación del sistema y de los datos, con el objetivo de estar preparados ante un ataque exitoso.
- **Control y supervisión de la cadena de suministros**: analizar las prácticas de seguridad de sus proveedores y su capacidad de respuesta para solucionar problemas de seguridad. Controlar periódicamente las operaciones de mantenimiento.
- **Diseño seguro del sistema:** aplicar principios de seguridad al diseño de los sistemas, por ejemplo: confianza cero y principio de menor privilegio.
- **Monitoreo de seguridad:** vigilar el estado de las redes y sistemas de información de IT y OT que soportan las operaciones de funciones esenciales del ferrocarril. Es necesario para detectar amenazas potenciales de seguridad e implementar

medidas efectivas de seguridad, como por ejemplo, logs de seguridad, detección de virus, etc.

- **Descubrimiento de eventos de seguridad**: detectar actividades sospechosas que puedan afectar la seguridad de redes y sistemas (incluyendo IT y OT) de aquellas funciones consideradas esenciales para el transporte ferroviario. Utilizar SOC (Centro de Operaciones de Seguridad), IPS (Sistema de Prevención de Intrusión), IDS (Sistema de Detección de Intrusión), etc.
- **Gestión de los registros de eventos y alarmas:** almacenar y centralizar ambos logs y dejarlos accesibles para que el SOC pueda detectar ciberataques.
- **Planificación de Recuperación y Respuesta:** definir, implementar y realizar testeos de procedimientos de gestión de incidentes, los cuales apuntan a mejorar la continuidad del negocio de servicios y sistemas y evitar daños materiales y a la reputación y sanciones de organismos reguladores. Para ello, deben:
  - Coordinar y colaborar con CSIRT/CERT[15] [16] (Equipos de Respuesta a Incidentes de Seguridad) nacionales y aquellos de naturaleza pública o comercial durante la ocurrencia de posibles incidentes de ciberseguridad.
  - Definir procedimientos para compartir información de incidentes de ciberseguridad con interesados relevantes, incluyendo la notificación de incidentes. Además, es recomendable compartir información con otras organizaciones, incluyendo proveedores en la cadena de suministro ferroviario.
  - Realizar ejercicios periódicos de ciberataques para evaluar las medidas de seguridad, los procedimientos y la resiliencia

[15] Es una entidad organizativa que tiene la responsabilidad de coordinar y respaldar la respuesta a un evento o incidente de seguridad informática.

[16] CERT es un término de marca registrada y se enfoca en mejorar la respuesta a incidentes como disciplina más que solo en su propia organización.

de las organizaciones ante ciberincidentes. Deben tener en cuenta las amenazas emergentes, vulnerabilidades conocidas y datos operativos en los sistemas de pago, las redes y los dispositivos de comunicaciones (por radio, Wifi, etc.), equipamiento a bordo, centros de control operacional, seguridad, comando de control, señalamiento, etc. Por último, asegurarse que las evaluaciones de riesgo cubran las actividades diarias del personal (uso de redes sociales, celulares, etc.).

- Tener acceso a almacenamientos de backup en caso de comprometerse la integridad y disponibilidad de almacenamiento de datos.
- Desarrollar manuales de seguridad con procedimientos detallados para administrar ciberincidentes y devolver rápidamente los servicios y sistemas a su funcionamiento normal.
- Definir procedimientos para hacer frente a fuga de datos, incluyendo aquellos que impliquen dar cumplimiento a GDPR y otras normas relevantes.

## 2.6 Unión Europea

En noviembre del año 2020, ENISA emitió un informe sobre la ciberseguridad en el ferrocarril [19] con el objetivo de evaluar el cumplimiento y las dificultades que presentan los estados miembros al implementar la directiva NIS.

Según dicho informe, las tendencias que se registran son:

- La implementación general de las medidas de seguridad en materia de gobernanza es heterogénea entre los distintos Estados miembros.
- Los OES (Operadores de Servicios Esenciales) maduros llevan aplicando las medidas de gobernanza desde hace mucho tiempo mientras que los restantes, recién comienzan a

implementarlas.

- Las medidas básicas de ciberseguridad tales como la comunicación con las autoridades competentes y los equipos de respuesta a incidentes de seguridad informática parecen estar implementadas. Sin embargo, las que requieren experiencia técnica avanzada muestran un nivel más bajo de implementación, ya que requieren una considerable experiencia y madurez en ciberseguridad (por ejemplo, correlación de registros y análisis).

Además, menciona las principales dificultades y problemas que enfrenta el sector para cumplir con la Directiva NIS:

- Las partes interesadas del ferrocarril dependen de proveedores con estándares técnicos y capacidades de ciberseguridad dispares, especialmente para tecnología operativa.
- Los sistemas OT para los ferrocarriles están obsoletos y suelen estar distribuidos por la red ferroviaria (estaciones, vías, etc.) lo cual dificulta alinearlos con los requisitos actuales de ciberseguridad, así como gestionarlos adecuadamente.
- Se observa una baja concientización digital y de ciberseguridad en el sector. En general, el nivel de concientización del personal sobre la necesidad de adoptar medidas de ciberseguridad sigue siendo baja.
- En cuanto a la transformación digital del sistema ferroviario, la mayoría de los OES ferroviarios están actualmente incorporando dispositivos conectados a Internet (IoT). Estos dispositivos se incorporan a los sistemas, sin haber sido adecuadamente configurados, lo que generalmente está ligado a la aparición de nuevas vulnerabilidades.
- Existe un marcado riesgo en materia de ciberseguridad en la cadena de suministro, debido a que los OES dependen en gran medida de sus proveedores y/o terceros para actualizaciones del sistema, de la administración de parches y de la incorporación de nuevos componentes, entre otros.

Actualmente, ENISA junto a ERA[17] están trabajando de forma conjunta debido a que la UE destaca los beneficios del ferrocarril como medio de transporte, siendo sostenible, inteligente y seguro. Por lo tanto, la ciberseguridad es un requisito clave ya que permite que los servicios se desplieguen y se aprovechen las bondades de un paradigma digital conectado.

El 16 y 17 de marzo del 2021, ambas agencias (por segundo año consecutivo) realizaron un Webinar donde debatieron sobre los últimos avances y desafíos en ciberseguridad que enfrenta el sector. Algunos temas tratados fueron:

- Desarrollo de políticas.
- Importancia del desarrollo de normas y certificaciones para el sector ferroviario.
- Formas de compartir información y cooperar para tener un sector ferroviario más ciberseguro en la UE.

Otra iniciativa es el proyecto SAFETY4RAILS, que comenzó el 1° de octubre 2020 y está planificado a 2 años. Esta iniciativa busca proporcionar métodos y sistemas para aumentar la seguridad y la recuperación del transporte ferroviario interurbano.

Su objetivo es aumentar la resiliencia, a través de la IA (Inteligencia Artificial) y herramientas automatizas de la infraestructura ferroviaria frente a amenazas, tanto de ciberseguridad como naturales. Para ello, ofrece un conjunto de herramientas que abordan la gestión del riesgo y de las crisis, la respuesta de las partes interesadas a incidentes y la recuperación del sistema [27] [28].

En julio del 2021 se publicó oficialmente la primera especificación técnica de ciberseguridad destinada al ferrocarril CLC/TS 50701[18]. La primera

[17] La Agencia de Ferrocarriles de la UE se estableció en 2004 para diseñar el marco técnico y legal que permita la creación de un Área Ferroviaria Única Europea (SERA) como lo exige la ley de la UE [67].

[18] CENELEC es una asociación que elabora estándares voluntarios en el campo electrotécnico y que agrupa a los Comités Electrotécnicos Nacionales de 34 países europeos. Entre ellos: Italia, España, Estonia, Reino Unido, etc. [76] [77].

sigla se corresponde con CENELEC (Comité Europeo de Normalización Electrotécnica) y la segunda a Technical Specification**.**

El objetivo de la especificación es garantizar que las características RAMS: Fiabilidad (*Reliability*), Disponibilidad (*Availability*), Mantenibilidad (*Maintianability*) y Seguridad (*Safety*) de los sistemas/ subsistemas/equipos ferroviarios no se puedan reducir, perder o comprometer en el caso de ciberataques intencionales.

Este documento se aplica al dominio de las comunicaciones, la señalización y el procesamiento, el material rodante (unidades) y las instalaciones fijas. Proporciona a los interesados del sector como operadores ferroviarios y proveedores de productos, orientación y especificaciones sobre cómo se gestionará la ciberseguridad en el contexto del ciclo de vida de EN 50126-1 RAMS.

Adicionalmente, esta norma ofrece una guía para que en todas las etapas del ciclo se apliquen los cinco atributos mencionados precedentemente. La prioridad y alcance del atributo correspondiente a la seguridad es que funcione sin fallos catastróficos, sin considerar ataques intencionales. De allí la utilidad de la CLC/TS 50701.

El autor consultó por correo a CENELEC si existía alguna fecha límite de implementación, si era obligatoria, quien la autorizó/aprobó y si es solo para Europa. Lo que sigue es la traducción al español de la respuesta, recibida por mail el 29/07/2021.

***"…****no hay obligación de seguirla ya que es de aplicación voluntaria. Por supuesto, puede llegar a ser obligatorio si se utiliza en obligaciones contractuales o si una regulación nacional o internacional determina que se haga obligatorio (no es el caso actualmente a nivel europeo).*

*El TS ha sido aprobado por los 34 organismos nacionales de normalización miembros del CEN-CENELEC.*

*El TS se ha desarrollado inicialmente para la industria europea, pero*

*puede utilizarse como documento de referencia en otras partes del mundo, pero, por supuesto, no puedo garantizarle que en otras partes del mundo no haya desarrollado también un documento equivalente…".*

Europa busca implementar un sistema ferroviario (ERTMS), en el que la señalización y las comunicaciones entre vía y equipos de a bordo sean compatibles en todo el continente y permita la interoperabilidad de las circulaciones ferroviarias entre los diversos estados de la Unión. Esto actualmente no es posible debido a las diferencias existentes en el ancho de las vías y en los sistemas tecnológicos, entre otros.

Este sistema consta básicamente de dos tipos de tecnologías. Uno de ellos es el ETCS (European Train Control System) relacionado a la señalización (en infraestructura y en trenes), aportando datos sobre la velocidad máxima en cada punto o distancia hasta la próxima baliza, así como el cálculo y la supervisión de la velocidad de circulación del tren en cada momento.

El otro es el GSM-R (Sistema Global de Comunicaciones Móviles para Ferrocarriles) que regula aspectos relativos a las comunicaciones entre el tren y los operadores del CTC (Centro de Control de Tráfico) [29].

## 2.7 Estados Unidos

El DHS a partir del 31 de diciembre del 2021 exigirá a las entidades ferroviarias de mayor riesgo que informen de incidentes cibernéticos al gobierno, identifiquen a los encargados de ciberseguridad y elaboren un plan de contingencia y recuperación en caso de que sean víctimas de ciberataques [30].

La TSA estableció mandatos de ciberseguridad a los sectores de transporte ferroviario a través de una directiva de seguridad, publicada a fines de 2021.

El DOT y la Administración Federal del Ferrocarril, en junio del 2020, redactaron un informe denominado *"Cyber Security Risk Management for Connected Railroads"* (en español, "Gestión de riesgos de ciberseguridad para ferrocarriles conectados") en el que se desarrolla una metodología que permite identificar posibles amenazas, vulnerabilidades y consecuencias de

ciber ataques para cada caso. Incluso recomienda estrategias para mitigar riesgos.

Estados Unidos utiliza PTC, que consiste en un sistema de control para incrementar la seguridad de los trenes en todo el país y prevenir colisiones entre trenes y descarrilamientos provocados por exceso de velocidad y cambios de vía.

Se trata de una tecnología basada en GPS que transmite material audiovisual que comunica las zonas conflictivas en el recorrido del tren. Entre ellas, avisa sobre señales cercanas y límites de velocidad [31].

### 2.8 Argentina

Para recopilar información sobre el ferrocarril se accedió a las páginas del Transporte Argentino, se visualizaron videos sobre un curso brindado por GICSAFe y se consultó por correo electrónico al Ministerio de Transporte.

El último, respondió a través del memo "**ME-2021-76241282-APN-GSYP#SOFSE**" producido por la Gerencia de Sistemas y Procesos de Gerencia de Sistemas y Procesos de SOFSE [32], de fecha 24 de agosto del 2021, lo siguiente:

*"…(...) "… En lo que respecta a ciberseguridad y Trenes Argentinos, esta organización promueve una conducta responsable en materia de ciberseguridad mediante la implementación de varias iniciativas que se encuentran alineadas a las leyes/normas vigentes para organismos públicos; …" "…(...)…te detallo algunas de ellas:*

***Decisión Administrativa N° 532/2021:*** *relacionada con la implementación de acciones relativas a la ciberseguridad y a la protección de las infraestructuras críticas de información, así como también a la generación de capacidades de prevención, detección, respuesta y recupero ante incidentes de seguridad informática del Sector Público Nacional y de los servicios de información y comunicaciones definidos en el artículo primero de la Ley Nº 27.078.*

***Infraestructura critica*** *Decreto N° 802 de la JEFATURA DE GABINETE DE MINISTROS, DE LA SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN (Contempla todas esas actividades esenciales que*

*dependen de las Infraestructuras Críticas: centrales eléctricas o nucleares, sistema de aguas, transporte ferroviario, sistema bancario, tecnología de satélite, sistemas de telecomunicaciones o de la Administración).*

*En Junio de este año se publicó un nuevo portal web del Equipo de Respuesta ante Emergencias Informáticas nacional (CERT, por su sigla en inglés), que se encarga de la gestión técnico-administrativa de los incidentes de seguridad informática en el Sector Público Nacional, el cual es un espacio de publicaciones, donde se puede encontrar un conjunto de textos, guías, buenas prácticas y recomendaciones orientados a la prevención y gestión de incidentes informáticos y, además, presenta un sector de reporte de accidente, que contiene el formulario de reporte público de un accidente o posible ciberataque. Este portal es de uso para todos los organismos del estado*

***Política de Seguridad de la Información*** *(Resolución 104/2012 del Ministerio del Interior y Transporte) Decisión Administrativa 669/2004: Establece que los organismos del Sector Público Nacional deberán dictar o adecuar sus políticas de seguridad. La cual, entre varios aspectos, contempla la conformación de Comités de Seguridad en la Información, definición de funciones de los mismos y responsabilidades en relación con la seguridad.*

***Requisitos mínimos de seguridad de la información*** *para organismos del Sector Público (Declaración Administrativa 641/2021, publicada en el Boletín Oficial el 25 de junio).*

*El intenso uso de las Tecnologías de la Información y las Comunicaciones conlleva un notable aumento de los riesgos y amenazas a los activos de información y a los sistemas esenciales utilizados para brindar de manera eficiente y constante los servicios que se prestan desde Trenes Argentinos y es por ello que estamos trabajando en el cumplimiento de las normativas antes mencionados, en pos del desarrollo de una cultura de ciberseguridad. (...)…".*

De lo mencionado precedentemente, cabe destacar que el Decreto N° 802 es del 2018 y actualmente no está vigente. También la Decisión Administrativa 669/2004 fue derogada por la Decisión Administrativa N°

641/2021.

El autor accedió a material del ferrocarril argentino brindado por el grupo CONICET-GICSAFe, los cuales confirmaron que el sistema de frenado, señalización y seguridad se maneja a través de relés, motivo por lo cual, al ser puramente mecánico y no digital, se tienen en cuenta aspectos relacionadas a la seguridad física y el error humano (safety), pero se excluyen actos mal intencionados o de ciberseguridad(security).

Además, manifiestan que la inversión para incorporar tecnologías que se utilizan en EEUU (PTC) o en la UE (ERTMS) sería muy costosa y difícil de implementar en Argentina.

Este grupo está conformado por investigadores, docentes, profesionales y estudiantes de distintas instituciones, entre las que se encuentran CONICET (Consejo Nacional de Investigaciones Científicas y Técnicas), UTN-FRH (Universidad Tecnológica Nacional - Facultad Regional Haedo) y UBA (Universidad de Buenos Aires) [33].

Existen una serie de proyectos en desarrollo a cargo de un grupo del CONICET-GICSAFe que involucra entre otros, el monitoreo de barreras [34]. Estos proyectos, según lo manifestado por un integrante de dicho grupo, podrían requerir componentes para los que amerite el tratamiento en cuanto a su ciberseguridad.

## 3. Aviación civil

En esta sección se revisarán las principales tecnologías utilizadas en la aviación civil, los actores que podrían estar interesados en comprometerlas, los ataques y los escenarios posibles en aeropuertos. Esto último es debido a que hay que tener en cuenta el contexto que rodea al avión y porque además no hay evidencia de incidentes que hubieran afectado directamente a las aeronaves. Al respecto, muchos expertos consideran que es imposible efectuar un ataque directo a un medio de esta naturaleza. No obstante, en la UE ya ha manifestado que EASA reforzará la seguridad ante potenciales amenazas.

También, se mencionarán las recomendaciones brindadas por organizaciones como la Comisión Europea para fortalecer la ciberresiliencia.

Por último, y como ya se realizó para otras modalidades del transporte, se explicarán las iniciativas y acciones realizadas por la UE, EEUU y Argentina en este sector.

Las organizaciones internacionales principales son OACI (Organización de Aviación Civil Internacional)[19] e IATA (Asociación de Transporte Aéreo Internacional)[20].

OACI en octubre de 2019 estableció su estrategia de ciberseguridad [35], la cual se base en siete pilares: Cooperación internacional, Gobernanza, Leyes y reglamentos eficaces, Política de ciberseguridad, Intercambio de información, Gestión de incidentes y planificación ante emergencias y Creación de capacidad, instrucción y cultura de ciberseguridad.

La visión de esta organización es que la aviación civil debe ser resiliente a los ciberataques, segura y fiable en todo el mundo; mientras continúa innovando y creciendo. Para ello se requiere:

- El reconocimiento del Convenio de Chicago por parte de los Estados, con los objetivos de asegurar la continuidad de la operatoria y la ciberseguridad.

[19] Es una agencia de la Organización de las Naciones Unidas (ONU) creada en 1944 por el Convenio de Chicago., está financiada y dirigida por 193 gobiernos [70].

[20] La misión de IATA es representar, liderar y servir a la industria de las aerolíneas, tiene programas de ciberseguridad y colabora con OACI [81].

- La coordinación de los aspectos de ciberseguridad de la aviación entre las autoridades estatales, con el fin de gestionar eficientemente los riesgos cibernéticos a escala mundial.

El compromiso de todas las partes interesadas de la aviación en profundizar la resiliencia y protegerse contra los ciberataques que pudiesen afectar al sector.

IATA en febrero del 2021 publicó una guía sobre seguridad cibernética de la aviación, detallando recomendaciones sobre cómo adoptar una postura mínima de ciberseguridad. También ofrece cursos remunerados de 3 días.

Por último, está desarrollando una estrategia de seguridad cibernética de la aviación en toda la industria, publica recomendaciones y colabora con OACI. Cabe destacar que IATA brindó su apoyo a la creación de la estrategia de seguridad cibernética de dicha entidad.

## 3.1 Tecnologías utilizadas

La industria de la aviación depende ampliamente de la tecnología para realizar operaciones como el control del tráfico aéreo y la gestión de los aeropuertos. Para ello, emplea un arsenal de nuevas tecnologías, entre las que se encuentran herramientas de IA, robótica e IoT, dispositivos inalámbricos y sistemas de posicionamiento como GPS y SCADA para administrar componentes de OT, entre otros.

Los sistemas SCADA se utilizan en el aeropuerto para monitorear y controlar varias infraestructuras físicas que van desde el aire acondicionado al suministro de energía, incluida la iluminación del aeródromo para los servicios de plataforma (puentes aéreos).

La fuerte utilización de estas tecnologías y la dependencia que se crea expone a la industria a enormes riesgos que podrían provocar daños importantes en términos económicos, técnicos e inclusive humanos.

## 3.2 Actores

Los actores maliciosos que podrían atacar a los aeropuertos, según un informe de ENISA [36] ,son:

- **Personal interno**: se trata del personal del aeropuerto con intenciones maliciosas que tienen acceso a áreas y sistemas restringidos y/o a dispositivos interconectados.
- **Pasajeros e invitados del aeropuerto**: estos atacantes están físicamente presentes.
- **Atacantes remotos**: no están físicamente dentro del aeropuerto e incluyen ataques automatizados como malware. También ataques dirigidos, como amenazas persistentes avanzadas (APT).

## 3.3 Amenazas y ataques

Como se mencionó previamente y a pesar de que el FBI (Federal Bureau of Investigation) y empresas como AIRBUS o Boeing afirman que es difícil vulnerar la seguridad de la aeronave y que, al día de la fecha, no se registraron ataques exitosos; no se puede afirmar que esto sea imposible. Efectivamente, en el año 2015 un experto en seguridad informática dijo que pudo cambiar la posición del avión mientras utilizaba un sistema de entretenimiento de la aeronave [37].

De todos modos, la mayoría de los expertos afirma que los riesgos actuales se encuentran en el entorno más que en el propio avión y que éstos se materializarían a través del compromiso de componentes de OT, los cuales son ampliamente utilizados en los aeropuertos. Este tipo de tecnologías se está integrando cada vez más en sistemas de manejo de equipaje, escáneres de seguridad, controles de pasaportes, escáneres biométricos, CCTV, bombas de combustible, aire acondicionado, control de dispositivos de entrada, etc. [38].

Entre los ataques registrados en aeropuertos [36]:

- **Aerolínea Delta:** en EEUU, en el año 2016 debido a un corte de energía, tuvo que suspender vuelos; perjudicando a miles de

pasajeros de todo el mundo. Esta situación afectó a las pantallas de aviso de los pasajeros, al sitio web de la compañía, al sistema de facturación del aeropuerto y a todas las aplicaciones móviles.

- **Aeropuerto de Nueva York:** en febrero 2017, una falla de seguridad expuso a los servidores críticos del aeropuerto de Nueva York. La unidad de almacenamiento conectada a Internet contenía varias imágenes de copia de seguridad de los servidores utilizados por el Aeropuerto Internacional Stewart, las cuales no estaban protegidas con contraseña, lo que permitía a cualquier persona acceder a su contenido, funcionando básicamente como un servidor web público. Los datos filtrados incluían, entre otros, 107 GB de correspondencia de correo electrónico personal desde el aeropuerto de Nueva York, varias cartas de la TSA, archivos confidenciales de recursos humanos, memorandos entre oficinas, datos de nómina y lo que parece ser una gran base de datos de seguimiento financiero.

  También fue expuesto un archivo con una lista de nombres de usuario y contraseñas para varios dispositivos y sistemas, lo que permitía el acceso sin restricciones a la red interna del aeropuerto, según dos investigadores de seguridad. Esto podría haber permitido que un pirata informático manipule las tarjetas de embarque y otra información de los pasajeros.

  A pesar de ello, según lo informado por los investigadores, no hubo indicios de una infracción directa y es muy posible que el archivo de respaldo no contuviera los datos de los pasajeros [39] [40].

- **Aerolínea EasyJet**: en Suiza, en el año 2020, fue hackeada. Los ciberdelincuentes pudieron obtener los datos de alrededor de nueve millones de usuarios. Este sería uno de los ataques más graves de la historia de la aviación debido a la cantidad de usuarios afectados y el alcance de la información obtenida. Además, a 2208 clientes le robaron los datos de la tarjeta de crédito [41].

En respuesta al ataque, la aerolínea informó que se percató en enero del año 2020 y que la vulnerabilidad asociada a su base de datos fue neutralizada. Indicaron también que se comunicaron con los clientes para que estuvieran al tanto y adoptaran las medidas del caso.

- **Aeropuerto San Francisco:** En EEUU, durante el año 2020, las autoridades del aeropuerto revelaron que accedieron ilegítimamente a dos de sus sitios web para robar nombres de usuario y contraseñas de sus empleados y contratistas.

  Los atacantes insertaron un malware en los sitios web para robar las credenciales de inicio de sesión de algunos usuarios que accedían desde fuera de la red del aeropuerto a través de Internet Explorer en un dispositivo personal basado en Windows o un dispositivo que no estaba bajo mantenimiento de la empresa. El objetivo era robar las credenciales de inicio de sesión de los usuarios. Se cree que los atacantes podrían usarlas para obtener acceso a la red del aeropuerto.

  En respuesta al ataque, los sitios web comprometidos y el código malicioso se eliminaron. Los funcionarios también pidieron a los usuarios que restablecieran sus contraseñas de correo electrónico y de red [42].

## 3.4 Escenarios de ataque

A continuación, se describen dos escenarios con alta probabilidad de ocurrencia en los aeropuertos. El primero es un ataque al sistema de manejo de equipaje y el segundo está relacionado con la manipulación de los sistemas de pasajes de autoservicio.

Los sistemas SCADA utilizados en el manejo de equipaje permiten la centralización del control y la visualización de la gestión de las maletas.

Un ataque exitoso a estos sistemas se desarrollaría a partir de un malware que podría cargarse durante el proceso de actualización, con la colaboración de empleados mal intencionados (amenaza interna) permitiendo enviar comandos maliciosos para detener o interrumpir las operaciones

normales del manejo de equipaje. Esto causaría una interrupción significativa en el desembarco y/o en los procedimientos de carga.

El ataque podría comprometer la seguridad de los pasajeros a través de actos terroristas (carga de explosivos en el equipaje) para dañar el avión u ocultar otros productos ilegales como, por ejemplo, drogas.

En los últimos años, los sistemas SCADA han sufrido varios ciberataques. La creciente interconexión e interdependencia entre estos sistemas y otros activos del aeropuerto junto con la falta de seguridad han abierto vulnerabilidades que pueden explotarse fácilmente.

El escenario mencionado anteriormente es similar a lo que ocurrió en el puerto de Amberes, descrito en la sección Marítima de este trabajo.

Para explicar el segundo escenario, debe aclararse que los sistemas de check-in de autogestión son operados y compartidos por varias aerolíneas, están ubicados en espacios públicos y en caso de no contar con el adecuado mantenimiento podrían accederse fácilmente por usuarios malintencionados.

Esto podría darse ya que la mayoría de estos dispositivos ejecutan comúnmente versiones obsoletas de Windows o Linux, que se conectan para acceder al contenido de los servidores de la empresa y proporcionar funcionalidades de gestión remota.

Los ataques de manipulación podrían ser asistidos o realizados por una persona con información privilegiada, por ejemplo, un empleado del proveedor externo a cargo de operar el servicio.

La manipulación puede implicar alterar físicamente el hardware, como obtener acceso a la PC al forzar un candado o realizar un pequeño orificio en el costado de la máquina. También se podría alterar la interfaz entre el pasajero y el dispositivo mediante la instalación de un keylogger[21] o, por ejemplo, explotar una vulnerabilidad del software.

El éxito del ataque permitiría que el delincuente pueda escalar privilegios de acceso de root/administrador del dispositivo, lo cual posibilitaría cambiar el comportamiento total del equipamiento para realizar acciones ilegítimas de cara al cliente e interacciones con otros sistemas conectados. A

[21] Es un malware que se usa para capturar información confidencial, como contraseñas o información financiera que posteriormente se envía a terceros para su explotación con fines delictivos. [78].

manera de ejemplo, se podría acceder/imprimir a las tarjetas de embarque de pasajeros, invalidar y/o modificar los pasajes existentes (mediante la manipulación de registros) o robar datos del pasaporte o tarjeta de crédito, entre otros.

La interrupción de los servicios de facturación puede crear inconvenientes a los pasajeros (es decir, más tiempo para abordar) pero también podría provocar más riesgos relacionados con la seguridad. Por ejemplo, ayudar con el embarque de pasajeros no habilitados en el avión.

Según el informe de ENISA [36], este fue uno de los posibles escenarios de ataque más citados por los entrevistados.

## 3.5 Recomendaciones

La Comisión Europea en su informe Transport Cibersecurity Toolkit [7] describe buenas prácticas para hacer frente a las ciberamenazas en este sector. Son las mismas que se especificarán en el subsector marítimo (capítulo 4) pero teniendo en cuenta los riesgos relativos al sector bajo análisis en este apartado, tales como la gestión de identidades, accesos y roles, las evaluaciones de riesgo, las políticas, la resiliencia de redes y sistemas, el monitoreo de la seguridad, el descubrimiento de eventos y la respuesta y el plan de recuperación.

Además de lo mencionado, brinda ejemplos de Frameworks para administrar el riesgo, como la familia 27000, el desarrollado por el NIST y los recomendados por OACI e IATA entre otros. Asimismo, ofrece recomendaciones para todos los sectores sobre cómo protegerse ante ataques de DDoS, malware y accesos no autorizados.

Siguiendo la línea del documento de la Comisión Europea, el Foro Económico Mundial [43] con la colaboración Willis Towers Watson, experto en seguridad de la aviación de IATA en Canadá, recomienda fomentar la cultura de ciberseguridad, capacitando e incorporando más profesionales con conocimientos en esta rama. Para ello, busca que las organizaciones se cuestionen la manera en que podrían implementar eficientemente programas de concientización en el transporte, medir su desempeño y por último, determinar los incentivos y recompensas que se podrían brindar a todo el

personal, principalmente a los que no se desempeñan en áreas técnicas de IT y ciberseguridad, con el fin de que adopten buenas prácticas.

### 3.6 Unión Europea

EASA[22] publicó en septiembre del 2019, su Estrategia de Ciberseguridad de la Aviación cuyos objetivos deben ser cumplidos en un lapso de entre 5 a 10 años. Plantea la necesidad de un enfoque colaborativo y de desarrollar las acciones requeridas para su implementación [44].

Las partes interesadas involucradas están en proceso de definir una hoja de ruta común para implementar esta estrategia.

Para promover el intercambio voluntario de información y la colaboración de expertos, EASA está apoyando la creación de un Centro Europeo para la Ciberseguridad en la Aviación (ECCSA) y proporcionando las capacidades operativas iniciales en colaboración con el Equipo de Respuesta a Emergencias Informáticas europeo (CERT-EU)[23].

ECCSA propone una asociación voluntaria y cooperativa dentro de la comunidad de la aviación, respaldada por EASA, para comprender mejor los riesgos emergentes de ciberseguridad del sector[24] [45].

Se presenta en cooperación estratégica con la Oficina Federal de Seguridad de la Información (BSI) de Alemania con el fin de comprender mejor las amenazas de ciberseguridad en la aviación e implementar mejores prácticas al gestionarlas. A tal efecto, el actual director ejecutivo de EASA (Patrick Ky) y el presidente de BSI (Arne Schönbohm) firmaron un Memorando de Cooperación en las oficinas de BSI en Bonn.

Según Schönbohm. “Los roles y responsabilidades de EASA y BSI son complementarios por lo cual estamos ampliando nuestra cooperación estratégica. Juntos, podremos extender un escudo de seguridad cibernética para aviones, fabricantes y aerolíneas, así como para aeropuertos y control

[22] Su misión es promover los más altos estándares de seguridad y protección ambiental en la aviación civil a nivel europeo [68].

[23] Está formado por expertos en seguridad informática de instituciones de la UE y coopera estrechamente con otros CERT en los estados miembros y empresas especializadas en seguridad informática [74].

[24] Desde julio de 2019 invita a las organizaciones, las cuales son evaluadas, a unirse al grupo de ciberseguridad para aumentar la cooperación y ciberresiliencia [69].

de tráfico aéreo” [46].

EASA actualmente está emitiendo dictámenes y recomendaciones en materia de ciberseguridad. En junio del 2021 publicó un dictamen sobre la gestión de riesgos de seguridad de la información, con el objetivo de salvaguardar todo el sistema de aviación civil contra los posibles efectos de seguridad causados por ciberataques.

En particular, propone la introducción de un sistema de gestión de la seguridad de la información (SGSI) para los organismos con competencias en la materia (incluida la propia EASA) y para las organizaciones en todos los ámbitos de la aviación. También exige que informen sobre incidentes y vulnerabilidades relacionados con la seguridad de la información.

El 1° de julio de 2020, EASA modificó algunas reglas relacionadas con las especificaciones para la certificación de productos con el objetivo de aumentar la ciberseguridad en las aeronaves (aviones y helicópteros). Con esto, busca reforzar la seguridad a bordo al mitigar los efectos potenciales de las amenazas provenientes de la interacción con las redes y sistemas electrónicos dentro de la aeronave.

Estas modificaciones o “enmiendas” fueron aprobadas en la denominada “Decisión ED 2020/006 / R”, a través de la cual se espera que se reduzca la vulnerabilidad de los sistemas de las aeronaves. Por ejemplo, se realizaron modificaciones en la Especificación de Certificación CS-25 para aviones grandes, que ahora tienen en cuenta la protección de los equipos y sistemas de interacciones electrónicas no autorizadas en la sección perteneciente al equipamiento [47] [48].

Como se mencionó anteriormente, la agencia encargada de ciberseguridad en los estados miembros de la UE es ENISA y ha desarrollado varios informes sobre ciberseguridad en esta área. También en el año 2018, en un evento denominado Cyber Europe, realizó un ejercicio que duró 2 días, el cual simulaba un ataque a los sistemas del equipamiento de facturación automática, aplicaciones de viaje, etc. Este ciberejercicio permitió identificar desafíos, comprender mejor la diseminación de incidentes a través de los distintos países y efectuar recomendaciones útiles a los participantes. En el evento estuvo presente EASA [49] [50].

## 3.7 Estados Unidos

TSA publicó a fin del año 2021 medidas para el sector aéreo a través de la nueva directiva de seguridad, que aplica también al transporte ferroviario. Exige a los operadores de aeropuertos críticos de EEUU, de aviones de pasajeros y de carga que designen coordinadores de ciberseguridad e informen los incidentes cibernéticos a CISA (Agencia de Seguridad de Infraestructura y Ciberseguridad) dentro de las 24 hs. de detectada su ocurrencia Esta directiva entró en vigor el 31 de diciembre del 2021 [51].

Además de las medidas inmediatas, la TSA está trabajando en un proceso de elaboración de normas a largo plazo para reforzar la ciberseguridad y la resiliencia en el sector del transporte. [30].

También se encuentra la FAA (Administración Federal de Aviación) **,** entidad gubernamental responsable de la regulación de todos los aspectos de la aviación civil. En materia de ciberseguridad, este organismo junto al Grupo de Ciberseguridad de la Organización de Tráfico Aéreo y otros interesados, realizaron un simposio de concientización sobre ciberseguridad en 2020 con el fin de debatir sobre los desafíos de seguridad actuales y afianzar la colaboración con interesados de la industria.

La FAA mediante el programa Cyber Threat Intelligence, analiza todas las fuentes de riesgos y vulnerabilidades de ciberseguridad para garantizar la seguridad y la eficiencia del vuelo. También desarrolla herramientas, requisitos, estándares de ingeniería y soluciones empresariales de ciberseguridad.

## 3.8 Argentina

La PSA (Policía de Seguridad Aeroportuaria) es la autoridad de aplicación del convenio de Chicago establecido por OACI en nuestro país y tiene como misión la *"…salvaguarda de la aviación civil nacional e internacional y la fiscalización y la adopción de medidas a fin de dar respuesta inmediata a situaciones de crisis que pudiera acontecer en el ámbito*

*aeroportuario y en las aeronaves…*" [53].

En el artículo 1° de la Disposición N° 727/2019 de la PSA**,** se aprueba el reglamento RSA N° 22 **"**Ciberamenazas a la seguridad de la aviación civil**"** [52] con carácter reservado. A pesar de no ser de acceso público, lo cual impide ser evaluado en este trabajo final de maestría, la existencia de este reglamento deja en evidencia la existencia de medidas y/o políticas para gestionar la ciberseguridad en este modo de transporte.

Asimismo, en noviembre del 2021 la OEA realizó un webinar para facilitar el diálogo sobre las mejores prácticas, identificación de necesidades y acciones requeridas para respaldar la infraestructura crítica dentro del aeropuerto en materia de ciberseguridad.

Este webinar se basó exclusivamente en la descripción de la experiencia en Europa y durante su realización, se describieron algunos ataques, sobre todo los realizados a través del ransomware, se resaltó la falta de concientización en este ámbito y se detallaron las vulnerabilidades/ problemas más habituales, las cuales fueron ya mencionados previamente en este trabajo.

Asimismo, se describieron buenas prácticas y acciones realizadas en Europa, como la cooperación y la implementación de capacitaciones, procedimientos, gestión del riesgo y reuniones periódicas, entre otras.

Los especialistas de la OEA manifestaron su acuerdo con las acciones implementadas en Europa e hicieron hincapié en la necesidad de reunirse nuevamente para seguir abordando esta temática.

# 4. Marítimo

Siguiendo la línea de capítulos anteriores, se mencionarán en esta sección las principales tecnologías utilizadas en el sector, se describirán los actores (delincuentes) más relevantes, los ataques y los escenarios posibles en el buque y en los puertos. Al igual que en cada en las demás modalidades analizadas, se describirán la infraestructura utilizada (estaciones, puertos, etc.).

Luego se describirán las recomendaciones brindadas por organizaciones locales e internacionales como la Comisión Europea, OMI (Organización Marítima Internacional) y OEA, para fortalecer la ciberresiliencia.

Por último, se plantearán las iniciativas y acciones realizadas por la Unión Europea, Estados Unidos y Argentina en este subsector.

## 4.1 Tecnología

Existen muchos sistemas en un buque y en los puertos como, por ejemplo, el Puente de Mando (navegación, control y comunicaciones), los de manipulación y gestión de carga, el control de acceso, las redes públicas y el servicio a los pasajeros, entre otros.

Estos sistemas utilizan principalmente tecnologías como SCADA para OT, WIFI y LAN para pasajeros y empleados, RFID en los dispositivos de identificación por radiofrecuencia habilitados para WIFI que reciben los datos de la carga conforme se va escaneando en el puerto, VOIP para comunicaciones, CTV para seguridad portuaria y control de accesos y GPS para el posicionamiento, entre otros.

## 4.2 Actores

Pueden detectarse distintos tipos de atacantes y motivaciones:

| Group | Motivation |
|---|---|
| **Accidental actors** | ■ No malicious motive but still end up causing unintended harm through bad luck, lack of knowledge or lack of care, eg by inserting infected USB in onboard IT or OT systems. |
| **Activists (including disgruntled employees)** | ■ revenge<br>■ disruption of operations<br>■ media attention<br>■ reputational damage |
| **Criminals** | ■ financial gain<br>■ commercial espionage<br>■ industrial espionage |
| **Opportunists** | ■ the challenge<br>■ reputational gain<br>■ financial gain |
| **States**<br>**State sponsored organisations**<br>**Terrorists** | ■ political/idealogical gain eg (un)controlled disruption to economies and critical national infrastructure<br>■ espionage<br>■ financial gain<br>■ commercial espionage<br>■ industrial espionage<br>■ commercial gain |

Ilustración 2: grupos de actores y su motivación de ataque.

Fuente: [53].

Como se visualiza en la imagen anterior los actores accidentales, a pesar de no poseer motivación dañina alguna, pueden constituirse en una amenaza para la seguridad de una tripulación, el medio ambiente y la nave. Por ejemplo, puede contarse con un elemento infectado como una memoria USB que sin estar en capacidad de dimensionar el potencial daño, al ser insertado en un dispositivo del buque, se constituya en un grave compromiso de ciberseguridad.

Por otro lado, existen numerosos actores o atacantes (criminales, activistas, estados, organizaciones, terroristas o empleados descontentos, entre otros) que poseen una o varias motivaciones concretas como puede ser venganza, espionaje, ganar dinero, etc.

## 4.3 Amenazas y Ataques

El número de ciberataques en busques se incrementó en un 400% desde febrero hasta junio del 2020. Este período coincide con el confinamiento del COVID-19 donde el uso de las comunicaciones por Internet,

el teletrabajo, las incidencias nefastas del malware, particularmente el ransomware, y los correos electrónicos de phishing se dispararon notablemente [54].

La amenaza para los barcos está creciendo a medida que se incrementa más su vinculación a sistemas en tierra para la navegación. Un ataque dirigido por un grupo importante o promovido por un Estado contra el transporte marítimo podría infligir daños importantes e interrumpir el comercio mundial, por ejemplo, al bloquear una ruta crítica de transporte.

Este tipo de eventos son atractivos para los atacantes porque tiene una cantidad elevada de transacciones que involucran importantes sumas de dinero.

Existen vulnerabilidades comunes, siendo las principales sistemas operativos y antivirus obsoletos, falla en la gestión y el uso de cuentas con privilegios de administrador, contraseñas por defecto, escaso uso del principio de privilegios mínimos, redes informáticas a bordo que carecen de medidas de protección perimetral e instancias de segmentación de redes, equipos o sistemas críticos para la seguridad siempre conectados con las instalaciones en tierra, así como controles de acceso inadecuados para terceros, incluidos contratistas y proveedores de servicios.

En los últimos años se han producido numerosos ataques de ciberseguridad exitosos contra organizaciones marítimas y quienes llevan adelante este tipo de actividad. A continuación, se mencionan algunos casos reales y/o potenciales [55] [56]:

**White Rose of Drax:** en el año 2013 un equipo de investigación de la Universidad de Texas-Austin demostró cómo un potencial atacante podría tomar control remoto de un buque, a través de la manipulación de su GPS.

El ataque consistió en transmitir señales falsas de GPS al yate White Rose of Drax con el fin de tomar el control del sistema de navegación, provocando que informe que había una desviación del rumbo establecido. Por ello, el equipo de navegación del puente realizó las acciones necesarias para orientar el destino, sin saber que lo estaban haciendo hacia una dirección equivocada y definida por personas no autorizadas. Si bien fue una prueba académica en un ambiente controlado, cabe plantearse qué hubiera sucedido

si lo hubiesen llevado a cabo delincuentes.

**Ataque a Maersk**: en el año 2017, la empresa Maersk, el mayor operador de buques portacontenedores del mundo y uno de los cinco mayores operadores de terminales portuarias, sufrió el ataque de un Ransomware denominado NotPetya, impidiendo o limitando el acceso de los usuarios a sus sistemas de control y administración, a su propio sistema informático. Esto afectó las operaciones de 17 terminales portuarias operadas por Maersk, entre ellas Nueva Jersey (Estados Unidos), Itajai (Brasil), los Ángeles (Estados Unidos) y Buenos Aires (Argentina). Este ataque tuvo efectos en toda la base de clientes de Maersk, y provocó retrasos en la carga para muchos clientes y causando entre 250 y 300 millones de dólares en pérdidas.

Los gobiernos de muchos países afectados y organizaciones intergubernamentales sospechan que un actor estatal era responsable de NotPetya y que lo sucedido correspondió a un daño colateral producto del ataque de hackers a Ucrania. Lo cierto es que fue el mayor incidente marítimo conocido.

**Otros ataques de ransomware:** en el año 2018, el Puerto de San Diego (EEUU) fue víctima de ransomware que también afectó a más de 200 entidades públicas y hospitalarias.

Ese mismo año, el Puerto de Barcelona (España) sufrió un ataque del mismo tipo que afectó algunos de sus servidores y sistemas. También la naviera Cosco sufrió un evento similar que afectó sus sistemas de comunicación en Estados Unidos, Canadá y Sudamérica**.**

En el año 2020, la empresa logística Toll Group reportó un ataque de este tipo que afectó muchos de sus sistemas informáticos.

**Puerto de Amberes**: Entre 2011 y 2013, los comunicados de prensa indican que un grupo de delincuencia organizada con sede en los Países Bajos reclutó a piratas informáticos para vulnerar los sistemas de información del Puerto de Amberes que controlaban el movimiento y la ubicación de los contenedores. Los atacantes penetraron los límites físicos de seguridad mediante intimidación física de los empleados de las instalaciones de la terminal. Una vez que lograron ingresar físicamente a las oficinas

administrativas, conectaron keyloggers a los dispositivos de red para obtener visibilidad de los sistemas con datos críticos. Lo hicieron para ocultar cocaína y heroína en cargamentos legítimos, como contenedores de madera y plátanos enviados desde países de América del Sur. Con la ayuda de los piratas informáticos, los delincuentes accedieron a los códigos de liberación de los contenedores seleccionados y obtuvieron conocimiento anticipado de cuándo y dónde enviar un camión para interceptar un contenedor antes de que llegara el propietario legítimo.

Estos ataques ilustran cómo las organizaciones marítimas, incluidos los buques, los operadores de terminales y los puertos, no operan de forma aislada, sino dentro de una misma comunidad en la que intercambian y almacenan regularmente datos de una gran variedad de grupos, como las compañías navieras, los agentes de los transportistas, los operadores de terminales, los agentes de carga, los operadores ferroviarios, el control e inspección de fronteras, el monitoreo del estado de los puertos y las autoridades aduaneras.

## 4.4 Escenarios de ataque

Se describirán dos escenarios de ataque. En el primero de ellos, se explica cómo se podría generar un accidente en los puertos, comprometiendo los sistemas OT. El segundo detalla cómo un ransomware podría perjudicar a las actividades portuarias [57].

Para comprender el primer escenario, resulta importante señalar que un puerto tiene varias redes OT, una cantidad importante de sistemas y dispositivos finales, tales como grúas para embarcaciones, carga y descarga en terminales portuarias, software en almacenes refrigerados para mantener los alimentos sensibles a una temperatura específica, sensores y sistemas utilizados para transportar, almacenar y monitorear mercancías peligrosas, etc.

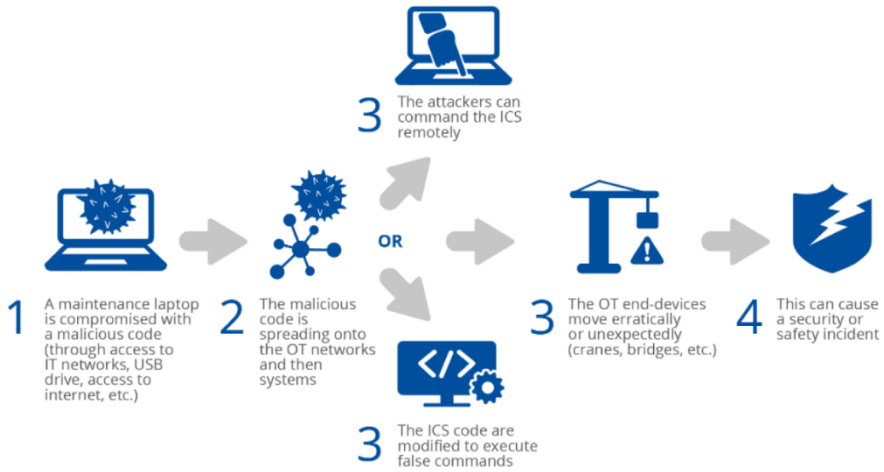


Ilustración 3: Descripción del escenario del ataque.

Fuente: [57].

El ataque se podría efectuar mediante una laptop infectada por un malware, utilizada para realizar mantenimiento a los sistemas de control OT. Esto ocasionaría, en caso de que no existan contramedidas adecuadas, que el código malicioso se propague a las redes y sistemas OT. Si los ICS utilizan IoT o servidores remotos, los atacantes podrían implementar mecanismos para controlarlo de forma remota. Caso contrario, se podría modificar el código ICS para ejecutar comandos predefinidos por los ciberdelincuentes. De cualquier forma, ocasionaría que los dispositivos finales de OT como grúas o puentes realicen acciones tales como movimientos inesperados, lo que podría dar lugar a incidentes tales como daños a la mercancía, destrucción de la infraestructura portuaria, lesiones a operarios o inclusive, accidentes graves o la muerte de empleados y pasajeros, entre otros.

El segundo escenario puede concretarse mediante un ataque que dirigido. Los ciberdelincuentes pueden desarrollar un ransomware explotando diferentes vulnerabilidades para difundirlo en las redes portuarias y cifrar uno o varios sistemas, archivos y/o dispositivos, ocasionando su destrucción o posible pérdida de datos críticos. Como consecuencia posible, se podrían registrar daños en la reputación, pérdidas financieras y de datos, demoras o cierre de las operaciones portuarias por tiempo indefinido.

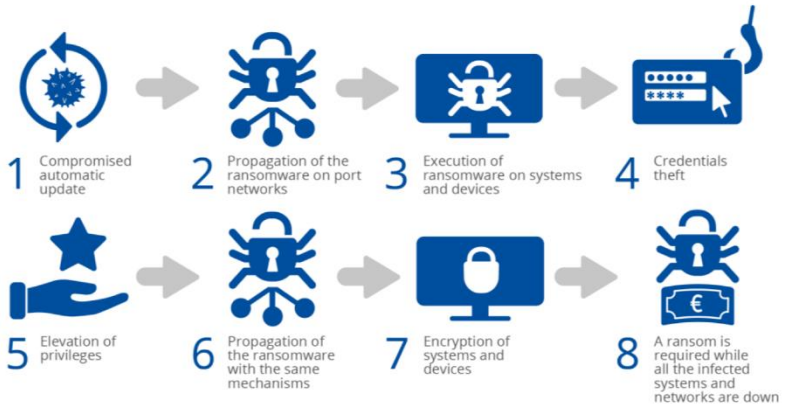


Ilustración 4: Pasos del funcionamiento del ransomware.

Fuente: [57].

Como se visualiza en la ilustración, es posible comprometer el funcionamiento de un puerto, a través de una actualización infectada por un ransomware en un servidor o por ingeniería social, mediante un ataque de phishing.

Una vez infectado el dispositivo, el ransomware se propaga a la red del puerto, aprovechando, por ejemplo, vulnerabilidades sin detectar o desatendidas o si no existe una adecuada segmentación de red.

Luego se podría ejecutar en los sistemas y dispositivos, sustrayendo sin autorización entre otros elementos valiosos, las credenciales almacenadas. Esto cual permitiría la elevación de privilegios con el fin de tomar total control de los activos vulnerados y propagarse a otra parte de la red del puerto a través del mismo mecanismo.

Además, los sistemas y dispositivos infectados podrían encriptarse, impidiendo su utilización, salvo que se abone un rescate, con la esperanza de que se puedan desencriptar y volver a estar operativos. Sin embargo, esto no siempre ocurre, como lo han demostrado casos de ataques similares en otras industrias.

## 4.5 Recomendaciones

En este apartado se describirán las principales recomendaciones/ buenas prácticas emitidas por instituciones y organizaciones relevantes como la Comisión Europea y OEA, así como provenientes de artículos académicos de referencia para el sector marítimo.

La Comisión Europea [7] recomienda adoptar un enfoque de gestión de riesgos. Para ello, se deben:

1. **Identificar las amenazas de ciberseguridad:** las organizaciones en el subsector necesitan entender las amenazas, incluidas las emergentes, para definir políticas y procesos de gobierno en sus enfoques de mejora de la ciberseguridad en servicios y sistemas (incluyendo IT y OT). Entre ellos se encuentran:
   - Nombrar un puesto de alto nivel con responsabilidades generales de gestión para la ciberseguridad de IT y OT. Este rol también debe considerar la seguridad física.
   - Definir claramente roles, responsabilidades, competencias y autorizaciones relacionadas con la ciberseguridad. Esto incluye niveles de autoridad y líneas de comunicación entre el personal de tierra y a bordo, quienes deben comprender y dar cumplimiento a las medidas adoptadas por la organización.
   - Garantizar la gobernanza de la ciberseguridad en toda la cadena de servicios de suministro de seguridad, incluidas las interfaces físicas y digitales, desde los fabricantes e integradores de tecnología hasta los proveedores de seguridad.
   - Definir el mecanismo de gobernanza (por ejemplo, las políticas) para cumplir con las obligaciones derivadas de los reglamentos y directivas pertinentes. Por ejemplo: el Código ISM (Código Internacional de Gestión de la Seguridad) para la operación segura de los buques y la prevención de la contaminación.

2. **Administrar el riesgo a partir de las amenazas de ciberseguridad identificadas**: las organizaciones necesitan

realizar las acciones necesarias con el fin de identificar, analizar, evaluar, evitar, transferir o mitigar el riesgo, para llevarlo a un nivel aceptable para la organización. Esto requiere un enfoque corporativo que involucre:

- Una visión clara de los diversos sistemas implementados, incluyendo el hardware y el software y cómo se conectan e integran.
- Identificar y evaluar las operaciones críticas a bordo del buque que son vulnerables a ataques de ciberseguridad. Una vez evaluadas, realizar estimaciones de riesgos en este contexto (incluir los posibles impactos operativos y la probabilidad de que ocurran) y establecer el vínculo con instituciones relevantes como la Organización Marítima Internacional (OMI), que puede proporcionar información sobre las amenazas dirigidas al transporte marítimo.
- Garantizar que las evaluaciones de riesgos incluyan las actividades habituales del personal. Ejemplo: uso de redes sociales y dispositivos personales.
- Identificar e implementar medidas de tratamiento y planes de mitigación de los riesgos de ciberseguridad. Por ejemplo: implementar un Sistema de Gestión de Seguridad de la Información (SGSI) y un Sistema de Gestión de la Privacidad de la información (PIMS) de modo integral. Estos sistemas deben incluir salvaguardas de protección de datos y privacidad.

3. **Protegerse contra las amenazas de ciberseguridad:** las organizaciones dedicadas al transporte marítimo deben implementar medidas de seguridad adecuadas para proteger sus redes y sistemas de información. Las medidas incluyen:
    - **Políticas de seguridad y definición de procesos**: definir, implementar y comunicar aquellos que involucren a los sistemas y datos que apoyan las operaciones esenciales en

el transporte marítimo. Por ejemplo: políticas de contraseña, procedimientos para parches, gestión de vulnerabilidades de sistemas de hardware/software (incluidos IT y OT), gestión de incidentes y protección de sistemas y redes.

- **Gestión de identidades y acceso**: administrar los accesos a las redes y sistemas de información (incluyendo IT y OT), que deben ser verificados, autenticados y autorizados. También se deben tener en cuenta las diferentes funciones y responsabilidades tanto de las cuentas normales como de las privilegiadas.
- **Datos y Sistema de Seguridad**: proteger los datos (almacenados y transmitidos electrónicamente), las redes críticas y los sistemas de información (incluyendo IT y OT) de ciberataques. Estas medidas deben permitir encriptar y asegurar los protocolos de comunicación para proteger de ataques, como por ejemplo del tipo “man-in-the-middle”. Además, es necesario administrar la seguridad física para proteger el acceso a sistemas como, por ejemplo, ser almacenados en áreas con acceso restringido para el caso de los datos y sistemas de navegación y comunicaciones por radio.
- **Resiliencia de Redes y Sistemas**: deben resistir, recuperase y mitigar el impacto de ciberataques. Esto se logra, por ejemplo, a través de redundancia de sistemas y redes, segregación de redes (en particular, de las de IT y OT) y medidas de seguridad multicapa, entre otras.

4. **Detectar Amenazas de Ciberseguridad:** Las organizaciones deben asegurarse de que las medidas y los controles sigan siendo efectivos. Para ello, es necesario:
    - **Monitorear seguridad**: supervisar el estado de seguridad de las redes y sistemas de información, por ejemplo, analizando logs de seguridad, servicios y

sistemas, tráfico de red, procesamiento de datos, etc.

- **Descubrimiento de eventos de seguridad:** detectar actividades maliciosas potenciales y afectadas. Estas medidas pueden requerir adoptar tecnologías específicas como Sistemas de Detección de Intrusiones (IDS) y el uso de un SOC (Centro de Operaciones de Seguridad).

5. **Respuesta y plan de recuperación**: con el fin de garantizar la continuidad del negocio ante incidentes de ciberseguridad, las organizaciones deben generar un plan que tenga en cuenta cuestiones tales como:
    - Establecer programas para simulacros y ejercicios (técnicos, de comunicación y coordinación entre los interesados, etc.) para responder a ciberataques y situaciones de emergencia.
    - Desarrollar procedimientos para respaldar la información en caso de comprometerse la integridad y disponibilidad de los datos.
    - Contar con manuales de seguridad con procedimientos detallados para administrar incidentes de ciberseguridad y restablecer servicios y sistemas a las condiciones de operación normales.
    - Definir procedimientos para compartir información de incidentes de ciberseguridad con los interesados relevantes.
    - Compartir información con otras organizaciones, incluyendo proveedores en la cadena de abastecimiento de servicios en el transporte marítimo.
    - Coordinar y colaborar con CSIRTs nacionales e internacionales durante la ocurrencia de incidentes de ciberseguridad.
    - Definir procedimientos para hacer frente a la fuga de datos; cumplimiento de GDPR y toda otra regulación y directiva relevante que sea aplicable.
    - Adquirir un seguro cibernético para compensar parcialmente

el daño que pudieran ocasionar los incidentes cibernéticos graves.

La OEA en un informe reciente sobre ciberseguridad marítima en el hemisferio occidental [56] ha destacado la importancia de la capacitación sobre la base de que varios estudios han determinado que los errores humanos son la razón principal del éxito de los ataques cibernéticos. Los empleados suelen ignorar las medidas de seguridad y muchas organizaciones reconocen que son su mayor debilidad en términos cibernéticos.

Por estas razones, el blanco de los ataques suele ser los humanos y no las tecnologías en sí. Por ello, se recomiendan capacitaciones para que el personal sea consciente y entienda de los riesgos de ciberseguridad y se encuentre alerta.

Para mayor detalle, la concientización debe ser de dos tipos: general y a medida.

La primera abarca a todo el personal (incluye a terceros que tengan acceso a sistemas IT y OT). Se recomienda que se utilice una variedad de canales (sitio web, correo, carteles, etc.) y que sea recurrente debido a la variedad y rapidez con que se implementan nuevos ataques. Algunos temas recomendados son el uso del correo electrónico e internet, ingeniería social, utilización de dispositivos móviles personales y detección de actividades sospechosas.

La segunda está dirigida al personal técnico y deben adaptarse a las características y el entorno informático de la organización. Las capacitaciones deben abarcar redes y sistemas críticos involucrados en operaciones críticas como la manipulación de cargas y el manejo de datos sensibles de los clientes. También es importante que estén entrenados en materia de detección de amenazas y vulnerabilidades.

En cuanto al correo electrónico, se recomienda formular una política de uso y resguardo de los e-mails.

## 4.6 Unión Europea

Este subsector en materia de ciberseguridad, junto a la colaboración internacional y de partes interesadas, se atiende principalmente a través de los estudios que realiza ENISA y EMSA[25].

EMSA brindó en el 2018 un curso de sensibilización de ciberseguridad en el subsector, cuyo desarrollo y material puede consultarse en la página oficial de la agencia. Esta breve capacitación fue realizada en base a videos de corta duración sobre temas tales como desafíos para el modo de transporte y el marco legal marítimo internacional y de la UE. También incluye conceptos básicos de ciberseguridad para el sector marítimo [58].

ENISA impulsa la ciberseguridad en el sector marítimo europeo proporcionando recomendaciones, apoyando el desarrollo de regulaciones, facilitando el intercambio de información y organizando eventos de sensibilización. Además, organizó dos talleres de seguridad marítima con EMSA.

La Directiva NIS clasifica como operadores de servicios esenciales a las organizaciones que administran los puertos, incluidas sus instalaciones, equipos, etc. Por lo tanto, están sujetos a la realización de evaluaciones de riesgo, considerando la seguridad, integridad y resiliencia de las redes y los sistemas de información**.**

La OMI[26] emitió en junio de 2020 una circular que incluyó la mención de la necesidad de hacer frente a los riesgos de ciberseguridad en los puertos.

A fines del 2020, ENISA publicó directrices de ciberseguridad para ayudar a los operadores portuarios europeos a gestionar los riesgos ciberseguridad a través de un conjunto de buenas prácticas, tales como [59]:

- Identificar e inventariar los activos, reconocer dependencias y la implementación de la automatización.
- Adoptar un enfoque integral para identificar y evaluar los riesgos de

[25] Agencia reguladora que apoya a la Comisión Europea y los estados miembros en el campo de la seguridad marítima, la protección y prevención de la contaminación de los barcos [75].

[26] Es el organismo de la ONU responsable de la seguridad, proteger la navegación y prevenir la contaminación del mar ocasionada por los buques [72].

ciberseguridad. Algunos aspectos a considerar son los indicadores de riesgo y el involucramiento de todas las partes interesadas relevantes, entre otros.

- Realizar una autoevaluación de la madurez de la ciberseguridad para identificar las prioridades de mejora y la asignación de recursos y presupuesto.
- Desarrollar un programa integral de ciberseguridad que implique un compromiso por parte de la alta dirección.
- Implementar programas de concientización sobre ciberseguridad en toda la organización y realizar capacitaciones técnicas para el personal de seguridad.

Cabe destacar que la circular de la OMI está basada en el Framework de ciberseguridad de infraestructuras críticas del NIST.

Este Marco consta de cinco áreas funcionales para gestionar riesgos [60] [56], que son:

1. **Identificar:** definir funciones y responsabilidades del personal en la gestión de riesgos de ciberseguridad. También reconocer los sistemas, activos y datos críticos que en caso de indisponibilidad pondrían en riesgo las operaciones del buque.
2. **Proteger:** implementar procedimientos y medidas para controlar los riesgos, con el fin de protegerse ante cualquier evento de ciberseguridad y contribuir a garantizar la continuidad de las operaciones del sector.
3. **Detectar:** implementar las actividades necesarias para descubrir oportunamente un evento de ciberseguridad y comunicar a las partes interesadas en caso de ser necesario.
4. **Responder:** desarrollar actividades y planes para ofrecer resiliencia ante un evento detectado.
5. **Recuperar:** aplicar medidas para respaldar y restaurar los sistemas necesarios para las operaciones marítimas afectadas y coordinar con las partes interesadas externas, en caso de ser necesario.

Actualmente ENISA está desarrollando una herramienta en línea para para que los operadores portuarios puedan gestionar los riesgos cibernéticos. También continúa su trabajo con los organismos y estados miembros de la UE como EMSA, con el fin de fortalecer la ciberseguridad en el sector.

En cuanto a los buques**,** en 2017 la OMI aprobó una resolución MSC.428(98) [61] y publicó orientaciones específicas sobre ciberseguridad. Esta resolución exige a los propietarios y gestores de buques que incorporen la gestión de riesgos de ciberseguridad a sus sistemas de gestión de seguridad de la información para cada buque, dando un plazo para incluirlo. También alienta a las autoridades nacionales a verificar el cumplimiento de este requisito.

Ese mismo año, la OMI complementó esta resolución con sus Directrices sobre la gestión de los riesgos cibernéticos marítimos, que proporcionan recomendaciones de alto nivel reconociendo que las tecnologías son esenciales para el funcionamiento y la gestión de los sistemas críticos para la seguridad del transporte marítimo y la protección del medio ambiente marino. Sin embargo, deja en claro que las organizaciones marítimas son vulnerables a los riesgos cibernéticos, por lo que se deben analizar desde el punto de vista de su seguridad, las maneras en que se accede a sus sistemas, las formas en que se interconectan entre sí y cómo se conectan en red.

## 4.7 Estados Unidos

El organismo que acompaña a TSA en la gestión de ciberseguridad es la USCG.

Las autoridades portuarias tienen la obligación de abordar la ciberseguridad. Por ejemplo, el Código PBIP (Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias) forma parte del Convenio para la Seguridad de la Vida Humana en el Mar, conocido por las siglas “SOLAS”, el cual establece disposiciones mínimas de seguridad para buques, puertos y organismos gubernamentales intervinientes.

En 2020, EEUU publicó la Circular de Navegación e Inspección de

Buques (NVIC) 01-20 con directrices para abordar los riesgos de ciberseguridad en las instalaciones reguladas por la Ley de Seguridad del Transporte Marítimo, la cual implementó el Código PBIP.

En esta circular, la USCG establece que los propietarios y operadores de instalaciones portuarias están obligados a abordar las vulnerabilidades y garantizar la ciberresiliencia. Esta directriz está basada en el marco NIST.

A partir del 1° de octubre de 2021, los propietarios y operadores de instalaciones portuarias deberán presentar enmiendas de ciberseguridad a las evaluaciones y planes que requiere la Ley de Seguridad del Transporte Marítimo de Estados Unidos durante las auditorías. La circular proporciona una orientación sobre la manera en que los propietarios y operadores de instalaciones portuarias pueden cumplir esos requisitos.

En diciembre de 2020, este país publicó un Plan Nacional de Ciberseguridad Marítima que requerirá que la USCG desarrolle un Framework para las evaluaciones de ciberseguridad en los puertos.

### 4.8 Argentina

La PNA (Prefectura Naval Argentina) es la autoridad marítima que cumple, entre otras funciones, la de policía de seguridad de la navegación, judicial y de prevención del orden público.

En materia de ciberseguridad, este organismo perteneciente a las Fuerzas de Seguridad de nuestro país, establece medidas preventivas orientadas a la protección de la infraestructura informática, las cuales contemplan las disposiciones pertinentes del Código PBIP[27] (Código internacional de protección de los buques y las instalaciones portuarias), del Código IGS (Gestión de Seguridad Internacional)[28], las directrices

[27] Es un Código Internacional para la Protección de los buques y de las Instalaciones Portuarias adoptado por la OMI. Establecen medidas y procedimientos para prevenir acciones que afecten la integridad de las personas y actos de terrorismo en puertos y buques [82].

[28] Los objetivos son: evaluación de todos los riesgos identificados en los buques, personal y medio ambiente; mejorar la gestión de seguridad del personal en tierra y a bordo de los buques, etc. [83].

mencionadas anteriormente en la resolución de la OMI MSC.428(98) y recomendaciones de la industria.

La PNA se encuentra abocada a la tarea de puesta en ejecución del Código PBIP. Para ello cuenta con un plantel de auditores que realizan evaluaciones de riesgo y capacitan al personal sobre el quehacer portuario. Representantes de este organismo han participado en distintos eventos internacionales como los realizados en Colombia y Estados Unidos, sobre temas relacionados con la seguridad de los puertos y los buques. Además, presta asistencia a aquellos países que lo requieran, en lo que respecta a la formación del personal que realiza tareas relativas a la protección marítima y portuaria.

Por último, en cuanto a la aplicación del código PBIP, la PNA participa en el Programa Internacional de Visitas Recíprocas en Materia de Seguridad Portuaria, llevado adelante por la USCG, cuyo objetivo es compartir experiencias, sugerencias y mejores prácticas.

Con la entrada en vigor de la Ordenanza N° 05-18 “Normas de Gestión de la Seguridad operacional del buque y la prevención de la contaminación (NGS)”, la PNA estableció, conforme a la resolución de la OMI MSC.428(98), que todo sistema de administración de la seguridad aprobado debería tener en cuenta los riesgos de ciberseguridad para prestar conformidad con el Código IGS (Gestión de Seguridad Internacional). Según la Disposición de la PNA 1242/2018: “…a más tardar en la primera verificación anual del Documento de Cumplimiento de la Compañía después del 1° de enero de 2021…” [62]. Con esto, el buque debe cumplir con lo requerido en dicha Disposición para poder circular.

La evaluación de riesgos de ciberseguridad deberá incluir, entre otros, los sistemas del puente, manipulación y gestión de carga, control de acceso y los sistemas administrativos y de comunicación, así como también las redes públicas para pasajeros.

El Departamento de Cibercrimen, que depende de la PNA, realiza investigaciones sobre las afectaciones de los sistemas de IT y OT vinculadas a la infraestructura informática crítica del transporte marítimo y al crimen organizado, con intervención de la Justicia.

Asimismo, se alienta la cooperación permanente entre los interesados como operadores de buques, proveedores de servicios, puertos, etc. con el fin de**:**

- Conservar la evidencia y la documentación correspondiente que permita la persecución penal.
- Compartir información relacionada con incidentes con el MINSEG-CSIRT [29](Equipo de Respuesta de Incidentes de Seguridad Informática del Ministerio de Seguridad) y otras organizaciones relacionadas con el transporte marítimo, con el objetivo de difundir y mitigar el impacto de nuevas amenazas, vulnerabilidades o ataques.
- Implementar políticas y buenas prácticas en materia de ciberseguridad, como por ejemplo no utilizar contraseñas débiles, cifrar información confidencial, etc.

[29] Es el equipo de respuesta a incidentes de seguridad informática, formado por personal de las cuatro fuerzas de seguridad federales: Gendarmería Nacional, Policía Federal, PSA y Prefectura Naval. Su comunidad objetivo está integrada por el Ministerio de Seguridad y sus instituciones dependientes [71].

## 5. Recomendaciones al Sistema de Transporte Argentino

En este capítulo se incluirán algunas recomendaciones para el sistema de transporte argentino, teniendo en cuenta los temas e iniciativas analizadas anteriormente. Al respecto, resulta necesario hacer hincapié en que el autor se basó mayormente en documentación pública y en las respuestas a las consultas realizadas. Con relación a estas últimas, cabe reiterar que solo algunas entidades contactadas respondieron los requerimientos que se hicieron oportunamente. Por lo tanto, algunas ideas propuestas en este acápite podrían estar implementadas ya o resultar no aplicables en el contexto actual.

- **Creación de una estrategia o política de ciberseguridad para el sector**: Resulta necesario que un organismo de jerarquía superior, con competencias como regulador del Transporte en nuestro país a nivel nacional, elabore una estrategia o política pública en materia de ciberseguridad, que debe estar alineada a la Estrategia Nacional de Ciberseguridad. Este documento deberá estar sujeto a actualizaciones en función del estado del arte en materia tecnológica, a los nuevos riesgos que vayan surgiendo y a los avances de otros Estados u organizaciones internacionales. A partir de esta estrategia, se deben organizar y orientar los planes y acciones a corto, mediano y largo plazo, como lo están haciendo otras naciones.
- **Incorporación de la ciberseguridad en el transporte en la agenda del gobierno**: en el capítulo 1 se describió como el presidente de EEUU viene realizando sprints referidos a la ciberseguridad. Entre ellos, uno fue dedicado al sistema de transporte, con el objetivo de aumentar la resiliencia de los sistemas de transporte del país, reuniendo a los principales organismos, autoridades e interesados en la industria. Iniciativas de este estilo deberían conducirse en este país, involucrando a las más altas autoridades.
- **Realización de reuniones nacionales**: En nuestro país no se realizan reuniones o conferencias referidas a la ciberseguridad

en las distintas modalidades del transporte. Sería conveniente que se organizaran encuentros de este tipo, principalmente para la aviación civil y el transporte marítimo, que son los más avanzados. Estos eventos son útiles para intercambiar metodologías e información, conocer los últimos avances y fomentar la colaboración entre los interesados con el fin de hacer frente a las vulnerabilidades relativas a la tecnología y llevar adelante iniciativas de concientización, entre otras. En los EEUU existe un Grupo de Trabajo dedicado a la ciberseguridad del sector para tiene por objetivo promover avances el tema en todas las modalidades. Resultaría valioso implementar la creación de mesas de trabajo semejantes en nuestro país

- **Generación de un Foro de Expertos**: crear un foro integrado por un grupo de expertos nacionales o internacionales para recibir asesoramiento en seguridad y resiliencia del transporte. Un ejemplo de una instancia de este tipo es el ya mencionado TRANSSEC en la UE, en el que se intercambien puntos de vista e ideas sobre amenazas, desafíos, estándares y soluciones de ciberseguridad para el sector.
- **Incorporación de una política de divulgación de vulnerabilidades para todas las modalidades del transporte:** Esto permitiría una permanente actualización y un fortalecimiento del sector, ya que se habilitaría un canal que permita la adopción de medidas preventivas.
- **Realización de capacitaciones con simulaciones y ciberejercicios**: a fin de mejorar el reclutamiento y entrenamiento del personal, se podrían realizar simulaciones de ataques a sistemas y equipamientos, orientadas a todo el personal del transporte, similares a las realizadas en la UE (Cyber Europe).
- **Investigación continua:** debería crearse un área dedicada a la investigación en materia de ciberseguridad en el transporte, que realice publicaciones periódicas, recomendaciones, etc.,

teniendo en cuenta el contexto nacional.

En cuanto al ferrocarril, Argentina no dispone a la fecha de tecnologías que sean vulnerables a ciberataques en sus unidades o sistema de señalamiento porque como se explicó, su seguridad se basa en relés. Según miembros de GICSAFe, no cuentan con sistemas SCADA ni ninguna tecnología como las utilizadas en la Unión Europea (ERTMS) o los EEUU (PTC).

No obstante, el sistema ferroviario utiliza GPS, cámaras e interfases web y procesa y almacena un volumen importante de datos personales. Si bien existen iniciativas e implementaciones en el Sector Público de acuerdo a las repuestas recibidas de Trenes Argentinos, debería contarse con un organismo que evalúe/audite su implementación**.** Al respecto, no se obtuvo evidencia de su existencia.

Estas iniciativas e implementaciones que buscan generar una cultura de ciberseguridad y defensa ante amenazas cibernéticas, tendrían que ampliar su alcance para contemplar los proyectos que está desarrollando el grupo GICSAFe, debido a que el monitoreo automático de barreras incorpora, entre ellos, IoT (protocolo MQTT). Sería fundamental que esto se gestione adecuadamente, ya que la tecnología mencionada no fue necesariamente diseñada teniendo en cuenta aspectos de ciberseguridad.

Al respecto, se recomienda tener en cuenta como mínimo, las diez vulnerabilidades de OWASP [63][30] sobre IoT e implementar medidas para abordar dichos riesgos. También, se deberían analizar las vulnerabilidades, recomendaciones y buenas prácticas de cada tecnología utilizada en los proyectos abordados**.**

Asimismo, es recomendable evaluar si la reciente especificación técnica de ciberseguridad CLC/TS 50701 brinda lineamientos e impulsa actividades que puedan aprovecharse en los proyectos de GICSAFe. Sobre todo, debido a que incorpora la ciberseguridad en todo el ciclo de vida de la norma EN 50126-1 RAMS. Esta última norma se aplica al dominio de

[30] Es una fundación sin fines de lucro que trabaja para mejorar la seguridad del software utilizando herramientas, una amplia comunidad y capacitaciones [79].

señalización. Según la página de GICSAFe, se trata de la primera organización argentina en aplicar la norma EN 50126 al desarrollo de sistemas ferroviarios [64].

Siguiendo la línea de los proyectos GICSAFe, el autor propone que se someta cada proyecto a la revisión de expertos en la ciberseguridad para que evalúen en profundidad los aspectos de ciberseguridad**.**

En cuanto a la aviación civil, sería recomendable que nuestro país solicite a un organismo internacional competente que incorpore entre sus exigencias, algún tipo de certificación de aeronaves en materia de ciberseguridad, como lo está haciendo EASA.

En cuanto al subsector marítimo, la PNA u otro organismo pertinente, debería implementar a través de un plan nacional, el desarrollo e implementación de un Framework para realizar las evaluaciones de ciberseguridad en los puertos, como ya lo llevó a cabo los EEUU.

También, deberían tenerse en cuenta las recomendaciones de ENISA y de otras organizaciones como BIMCO (Consejo Marítimo Báltico e Internacional)[31], la cual recientemente emitió junto a otros interesados de la industria, su cuarta versión de la guía para abordar la ciberseguridad en los buques [53].

[31] Es una de las asociaciones navieras internacionales más grandes. Afirma que su membresía representa aproximadamente el 60 por ciento del tonelaje del transporte marítimo mercante del mundo y que tiene miembros en más de 120 países.

# 6 Conclusiones

En el presente Trabajo final de Maestría se presentaron las principales iniciativas que llevan adelante la UE, los EEUU y la Argentina en materia de protección de las infraestructuras críticas de información del sector transporte, en sus modalidades ferroviaria, marítima y de aviación civil. Como se explicó, esta tarea es conducida en el mundo a través de distintas agencias gubernamentales con competencias en la materia y de diversas entidades públicas y privadas que participan en las actividades el sector.

Estas iniciativas coinciden en catalogar al transporte como un área crítica que por lo tanto, debe ser considerada en las estrategias nacionales de ciberseguridad. Algunos países que se encuentran más avanzados en este aspecto, también han desarrollado estrategias, políticas y planes específicos para el sector bajo análisis.

En el caso de nuestro país, si bien ha sido reconocido como un sector crítico en la normativa vigente, no existen a la fecha lineamientos específicos de ciberseguridad para el transporte a nivel general, que permitan orientar los esfuerzos en la materia abordada en este trabajo. Se registran solo algunos avances parciales en áreas específicas, como las relacionadas a la aviación civil o el sector marítimo. Esto muestra un atraso a nivel internacional, y expone a los sistemas locales a potenciales consecuencias de alto impacto social, medioambiental y económico, en caso de producirse un ciberataque o una falla masiva. Esta afirmación se acentúa en las modalidades de la aviación civil y del transporte marítimo, que han mostrado una mayor incorporación tecnológica para el logro de sus objetivos centrales.

El sector ferroviario por su parte, si bien como se explicó aún descansa en sistemas basados en un paradigma previo al avance de la tecnología digital, deberá modernizarse tarde o temprano y en ese proceso, deberá necesariamente contemplarse la incorporación de requerimientos de ciberseguridad.

Por otra parte, en el presente trabajo se describió cómo tanto los EEUU como la UE han reiterado en varias oportunidades la importancia de impulsar una fuerte articulación y colaboración entre los distintos subsectores del transporte y con organizaciones internacionales como OACI y OMI, para

compartir experiencias, recomendaciones y para la creación de estándares y especificaciones, así como la realización de encuentros periódicos, foros y mesas de trabajo con grupos de expertos. Sin embargo y como se explicó, no se han relevado experiencias de cooperación similares en nuestro país, lo que también muestra un grado importante de atraso.

Ya una realidad en el continente europeo, la iniciativa de materializar un sistema de transporte digital y verde para el cuidado del medio ambiente han comenzado a gestarse. Para ello, se prevén grandes inversiones y un conjunto de acciones basadas en el hecho de que la cercanía entre países podría ocasionar que si un estado miembro sufriera un ciberataque o una falla masiva, otros países del bloque podrían verse afectados. En el caso de nuestro país y la región en la que se encuentra, no parecen existir iniciativas ni instancias de análisis al respecto.

El presente trabajo buscó también demostrar que todas las modalidades o subsectores del transporte se encuentran expuestos a problemas similares en cuanto a las tecnologías que han incorporado, sobre todo al no contemplar rigurosamente la ciberseguridad en cada una de ellas. Esto es particularmente relevante en los sistemas SCADA y frente al incremento de la digitalización.

En el mismo sentido, se destaca que los estados más avanzados impulsan la concientización, colaboración, discusión de estándares, directivas y comunicación de incidentes con organizaciones nacionales e internacionales como OMI, OEA, OACI, IATA y ENISA para compartir información y soluciones para fortalecer la ciberresiliencia.

En este contexto, la falta de concientización en la temática, es un aspecto relevante a tener en cuenta ya que inevitablemente su ausencia ocasionará que los delincuentes busquen comprometer a las personas más que a la tecnología; provocando ataques que impactan en lo económico y ponen en peligro, incluso la vida de empleados, pasajeros y otros actores. Con esto se deja en evidencia la importancia de atender el factor humano en los procesos de incorporación tecnológica, cualquiera sea su naturaleza o fin, ya que las personas pueden constituirse como medio o blanco de las distintas modalidades de ciberataques.

Finalmente, a nivel internacional, la ausencia de estándares específicos en el sector obligan a los Estados a complementar sus políticas y estrategias con Frameworks generales de seguridad informática y gestión de riesgos de ciberseguridad en infraestructura crítica, que no siempre contemplan las particularidades del sector.

Particularmente para la modalidad del transporte ferroviario y como se explicó con anterioridad, este año se publicó oficialmente la especificación técnica CLC/TS 50701, como guía para gestionar riesgos de ciberseguridad en el ciclo de vida de los sistemas, aplicable no solo en Europa sino en otras partes del mundo. Por ello se recomendó evaluar su viabilidad en los proyectos de GICSAFe de Argentina. Si bien las iniciativas de este Grupo podrían considerarse un buen comienzo, la adhesión es de naturaleza optativa y por ello, habría que analizar en el futuro si las organizaciones involucradas realmente lo implementan debidamente. Cabe destacar que agencias tales como ENISA, ERA y las referentes de cada país, realizan un seguimiento de su nivel de aplicabilidad y las dificultades para llevarla a cabo, y sobre esta base, asesoran a las autoridades. Este modelo debería ser analizado a nivel local y eventualmente incorporado.

Por el lado de aviación civil, varias organizaciones internacionales como OACI, IATA y otras por ejemplo EASA, ENISA y OEA brindan recomendaciones sobre cómo gestionar riesgos de ciberseguridad, a pesar de que, como se explicó, aún no se han reportado casos reales que afecten aeronaves. Asimismo, EASA está trabajando en la certificación de productos con el fin de aumentar la ciberseguridad en los aviones.

Para esta modalidad, Argentina parece haber realizado avances con el Reglamento RSA N° 22 **"**Ciberamenazas a la Seguridad de la Aviación Civil**"**, si bien al haberse publicado con carácter reservado, no se ha podido acceder a sus contenidos.

Por parte del subsector marítimo, la OMI impuso ciertas restricciones a los buques que navegan por el mundo, que deben ser cumplidas para estar habilitados a circular y acceder a los puertos. Estas disposiciones son implementadas por la Argentina. Sin embargo, algunos expertos afirman que hace falta un estándar internacional específico en el subsector.

Nuestro país tiene una de las vías de salida hacia el mundo más grande del planeta y es el principal canal utilizado para exportar productos locales. Además, se encuentran bajo análisis varias inversiones relacionadas con la mejora de puertos y zonas de cruce. Por lo tanto, es necesario que se sigan incorporando y mejorando las medidas de ciberseguridad para garantizar el correcto funcionamiento y la expansión del subsector.

Proyectando hacia el futuro, el surgimiento de buques autónomos basados en IA, actualmente aún en período de prueba, incorporan tecnología como IoT, sensores y Big Data. Un ejemplo es el buque noruego, eléctrico y libre de emisiones Yara Birkeland. La empresa espera que en los próximos meses se pueda realizar un viaje desde la ciudad de Herøya a Brevik [65]. Tarde o temprano, este tipo de tecnologías llegará también a nuestro país.

Los expertos de países avanzados como Corea del Sur, estiman comercializar sus productos en 2025 naves autónomas sin intervención humana, lo que podría traer aparejados problemas de ciberseguridad, éticos y jurídicos. La OMI aún no estableció medidas de ciberseguridad en torno a este tipo de naves, lo que hace necesario que se considere su incorporación en el subsector y el impacto que podría traer aparejado.

En resumen, todos los subsectores o modalidades del transporte moderno alrededor del mundo se encuentran expuestas a vulnerabilidades en materia de ciberseguridad. Por ello, resulta evidente que se requerirán capacitaciones y recomendaciones a alto nivel, así como estándares internacionales y medidas de cumplimiento obligatorias específicas para cada caso. Estas medidas requerirán una constante revisión y adaptación debido al impacto social, ambiental y humano de los incidentes, al incremento de la digitalización y a la evolución del panorama de riesgos a los cuales, Argentina se encontrará inevitablemente expuesta.

Por lo tanto, es necesario que nuestro país analice la viabilidad de implementar las recomendaciones internacionales, varias de las cuales se han resumido en este trabajo, realice investigaciones continuas y profundas en cada subsector para fortalecer la ciberresiliencia y eventualmente, despliegue las acciones e iniciativas que se utilizan en el mundo. Como se explicó, la tendencia internacional demuestra que los países más avanzados

y las organizaciones internacionales son conscientes de los problemas y están trabajando en regulaciones, estándares y herramientas a los que Argentina podría sumarse.

# 7. Bibliografía


1] Comisión Europea, «Comisión Europea- Estrategia de ciberseguridad,» [En línea]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy. [Último acceso: 07 11 2021].

2] PARLAMENTO EUROPEO, CONSEJO EUROPEO, «Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión,» 07 19 2016. [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016L1148. [Último acceso: 06 06 2021].

3] Comision Europea, «Comision Europea-Politicas de ciberseguridad,» [En línea]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies. [Último acceso: 07 11 2021].

4] ENISA, «Ciberseguridad del transporte: subir el listón trabajando juntos,» [En línea]. Available: https://ec.europa.eu/transport/sites/default/files/2019-01-23-1st-transport-cyber-security-conference-conclusions.pdf. [Último acceso: 18 06 2021].

5] Enisa, «ENISA- Grupo de Expertos TRANSSEC,» [En línea]. Available: https://resilience.enisa.europa.eu/transport-security. [Último acceso: 26 01 2022].

6] Infosec, «Infosec- Congreso de Seguridad del Transporte Europa 2021,» [En línea]. Available: https://infosec-conferences.com/events-in-2021/transport-security-congress-europe/. [Último acceso: 07 11 2021].

7] Comision Europea, «Comision Europea-Ciberseguridad/Movilidad y Transporte- Transport cibersecurity toolkit,» 2020 12 20. [En línea]. Available:

https://ec.europa.eu/transport/themes/security/cybersecurity_en. [Último acceso: 06 10 2021].

[8] Comisión Europea, «La seguridad cibernética,» 16 12 2020. [En línea]. Available: https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en. [Último acceso: 26 01 2022].

[9] T. W. House, «Estrategia Nacional de Ciberseguridad,» 2018. [En línea]. Available: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. [Último acceso: 07 11 2021].

[10] DOT, «Departmental Cybersecurity Policy,» 21 06 2011. [En línea]. Available: https://www.transportation.gov/sites/dot.gov/files/docs/DOT%20Order%201351.37,%20Departmental%20Cybersecurity%20Policy.pdf. [Último acceso: 29 06 2021].

[11] DOT, «Política de divulgación de vulnerabilidades - Departamento de transporte de EE. UU.,» 27 05 2021. [En línea]. Available: https://www.transportation.gov/vulnerability-disclosure-policy. [Último acceso: 30 06 2021].

[12] DHS, «2020 Biennial National Strategy for Transportation Security (NSTS),» [En línea]. Available: https://www.dhs.gov/publication/2020-biennial-national-strategy-transportation-security. [Último acceso: 04 07 2021].

[13] U.S Departament of Homeland Security, «Transportation Systems Sector Cybersecurity Framework,» 26 06 2015. [En línea]. Available: https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf. [Último acceso: 20 04 2021].

[14] U.S Departament of Homeland Security, «/tss-cybersecurity-framework-workbook,» 08 05 2016. [En línea]. Available: https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-workbook-2016-508.xlsx. [Último acceso: 20 04 2021].

CISA, «TSA’s Approach to Voluntary Industry Adoption of the

15] NIST Cybersecurity Framework,» [En línea]. Available: https://www.cisa.gov/sites/default/files/publications/ExecutiveOrder_13636Sec10%28b%29Reportv5.pdf. [Último acceso: 01 07 2021].

16] Transport Security Congress, «Asista al Congreso de Seguridad del Transporte,» [En línea]. Available: https://transportsecurityworld.com/unitedstates/en/page/home. [Último acceso: 01 07 2021].

17] Comité de Ciberseguridad, «ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE LA REPÚBLICA ARGENTINA,» [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.argentina.gob.ar%2Fsites%2Fdefault%2Ffiles%2Finfoleg%2Fres829-01.pdf%23%3A~%3Atext%3DSu%2520finalidad%2520es%2520brindar%2520un%2Cdesarrollo%2520de%2520un%2520marco%2.

18] M. S. D. N. D. N. d. R. N. d. T. M. d. T. Chirdo, *Providencia: PV-2021-78093288-APN-DNRNTR%MTR,* Buenos Aires, 2021.

19] ENISA, «Ciberseguridad ferroviaria,» 11 2020. [En línea]. Available: https://www.enisa.europa.eu/publications/railway-cybersecurity. [Último acceso: 06 06 2021].

20] Thales, «Thales- Ciberamenazas en el sector ferroviario,» 2020. [En línea]. Available: https://thalesgroup-myfeed.com/LP=957?elqCampaignId=506&utm_source=hootsuite&utm_medium=social&utm_term=&utm_content=&utm_campaign. [Último acceso: 15 08 2021].

21] Thales, «Cybersecurity in Transportation,» Thales, Francia, 2020.

22] M. T. R. N. E. Dimitra Liveri, «Railway Cibersecurity,» 2020.

23] J. P. Arredondo, «Icorp-Sucumbe metro de San Francisco ante ciberataque ¡Y se vuelve gratuito!,» 28 11 2016. [En línea]. Available: http://www.icorp.com.mx/blog/ataque-metro-san-francisco/. [Último

acceso: 29 01 2022].

24] S. J. Julio, «Derechodelared 2021-El metro de San Francisco cae víctima de un ataque de ransomware,» 29 11 2016. [En línea]. Available: https://derechodelared.com/san-francisco-metro-hackeado/. [Último acceso: 29 01 2022].

25] Incibe-cert, «Incibe-cert-Ciberataque al sistema de pagos Oyster del transporte londinense,» 07 08 2019. [En línea]. Available: https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/ciberataque-al-sistema-pagos-oyster-del-transporte. [Último acceso: 29 01 2022].

26] UIC, «UIC ACTIVITY REPORT 2018,» 2018. [En línea]. Available: https://uic.org/IMG/pdf/uic_activity_report_2018.pdf. [Último acceso: 28 06 2021].

27] UIC, «Segundo SAFETY4RAILS Taller de proyectos con expertos del consejo asesor externo celebrado el 15 de marzo.,» 23 03 2021. [En línea]. Available: https://uic.org/com/enews/article/second-safety4rails-project-workshop-with-external-advisory-board-experts-held?var_recherche=SAFETY4RAILS. [Último acceso: 28 06 2021].

28] UIC, «SAFETY4RAILS proyecto celebró su tercer taller con los expertos externos del Consejo Asesor el 29 de abril de 2021,» 03 05 2021. [En línea]. Available: https://uic.org/com/enews/article/safety4rails-project-held-its-third-workshop-with-the-external-experts-of-the?var_recherche=SAFETY4RAILS. [Último acceso: 28 06 2021].

29] Adif, «Adif- ERTMS, Sistema Europeo de Gestión de Tráfico,» [En línea]. Available: http://www.adif.es/es_ES/ocio_y_cultura/fichas_informativas/ficha_informativa_00026.shtml. [Último acceso: 20 10 2021].

30] G. Sands, «CNN- La Administración de Seguridad en el Transporte establecerá mandatos de ciberseguridad a los sectores de transporte ferroviario y aéreo de EE.UU.,» 07 10 2021. [En línea]. Available: https://cnnespanol.cnn.com/2021/10/07/administracion-

seguridad-transporte-tsa-ciberseguridad-ferroviario-aviacion-trax/. [Último acceso: 09 10 2021].

31] S. Mudarra, «Trenvista-El Positive Train Control (PTC), sistema de seguridad mediante GPS,» [En línea]. Available: https://www.trenvista.net/formacion/escuela-trenvista/positive-train-control-ptc-seguridad-gps/. [Último acceso: 20 10 2021].

32] S. U. d. C. I. y. T. O. F. S. d. E. Marcela Alejandra Gigena, *Nota Número: NO-2021-76792119-APN-UCIYT#SOFSE,* Buenos Aires, 2021.

33] CONICET- GICSAFe, «CONICET-GICSAFe-¿ Quienes somos?,» [En línea]. Available: https://sites.google.com/view/conicet-gicsafe/inicio/cinco-preguntas-b%C3%A1sicas/qui%C3%A9nes-somos. [Último acceso: 07 10 2021].

34] CONICET-GICSAFe , «CONICET-GICSAFe-Monitoreo de barreras,» [En línea]. Available: https://sites.google.com/view/conicet-gicsafe/inicio/trabajos-realizados. [Último acceso: 08 10 2021].

35] OACI, «OACI,» 10 2019. [En línea]. Available: https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.SP.pdf. [Último acceso: 21 06 2021].

36] ENISA, *Securing Smart Airports,* 2016.

37] G. Michaca, «ConsumoTic,» 09 08 2018. [En línea]. Available: https://www.consumotic.mx/tecnologia/ciberseguridad-desafio-en-industria-de-la-aviacion/. [Último acceso: 26 03 2021].

38] M. Bird, «SNC Lavalin,» [En línea]. Available: https://www.snclavalin.com/en/beyond-engineering/how-can-airports-better-protect-themselves-against-cyber-attacks. [Último acceso: 03 26 2021].

39] L. Fran, «ItechPost-El aeropuerto de Nueva York filtra más de 750 GB de datos internos confidenciales,» 25 02 2017. [En línea]. Available: https://www.itechpost.com/articles/88034/20170225/new-york-airport-leaks-over-750-gb-sensitive-internal-data.htm. [Último acceso: 30 01

2022].

40] Z. Whittaker, «ZDNET- Falla de seguridad expuso los servidores críticos del aeropuerto de Nueva York durante un año,» 24 02 2017. [En línea]. Available: https://www.zdnet.com/article/unsecured-servers-at-new-york-airport-left-exposed-for-a-year/. [Último acceso: 30 01 2022].

41] A. Raya, «El español,» 19 05 2020. [En línea]. Available: https://www.elespanol.com/omicrono/software/20200519/easyjet-hackeada-millones-usuarios-robados-incluyendo-tarjetas/491201562_0.html. [Último acceso: 03 26 2021].

42] CISOMAG, «sitios web del aeropuerto de San Francisco hackeados; Credenciales de inicio de sesión de empleados comprometidas,» 14 04 2020. [En línea]. Available: https://cisomag.eccouncil.org/san-francisco-airport-websites-hacked-employee-login-credentials-compromised/. [Último acceso: 30 01 2022].

43] World Economic Forum, «Advancing Cyber Resilience in Aviation: An Industry Analysis,» 2020.

44] EASA, «Strategy for Cybersecurity in Aviation,» 10 09 2019. [En línea]. Available: https://www.easa.europa.eu/sites/default/files/dfu/Cybersecurity%20Strategy%20-%20First%20Issue%20-%2010%20September%202019.pdf. [Último acceso: 22 06 2021].

45] ECCSA, «Centro Europeo de Ciberseguridad en la Aviación (ECCSA),» [En línea]. Available: https://www.easa.europa.eu/eccsa/sectorial-news?category[2549]=2549&page=1. [Último acceso: 19 06 2021].

46] EASA, «EASA entra en cooperación estratégica con BSI de Alemania en seguridad cibernética,» 24 09 2020. [En línea]. Available: https://www.easa.europa.eu/newsroom-and-events/https://www.easa.europa.eu/newsroom-and-events/news/easa-enters-strategic-cooperation-germanys-bsi-cyber-security/easa-enters-strategic-cooperation-germanys-bsi-cyber-securi. [Último acceso: 27 06 2021].

EASA, «EASA da un paso importante para aumentar la
47] ciberseguridad de las aeronaves,» 13 07 2020. [En línea]. Available: https://www.easa.europa.eu/newsroom-and-events/news/easa-takes-important-step-increase-cybersecurity-aircraft. [Último acceso: 28 06 2021].

EASA, «CS-25 AMENDMENT 25 — CHANGE INFORMATION,»
48] [En línea]. Available: https://www.easa.europa.eu/sites/default/files/dfu/change_information_-_cs-25_amendment_25.pdf. [Último acceso: 28 06 2021].

ENISA, «La UE mejora su capacidad para hacer frente a las
49] cibercrisis: informe posterior a la acción de Cyber Europe 2018,» 20 12 2018. [En línea]. Available: https://www.enisa.europa.eu/news/enisa-news/eu-improves-its-capacity-to-tackle-cyber-crises-cyber-europe-2018-after-action-report. [Último acceso: 14 06 2021].

AESA, «AESA participó en el ejercicio internacional de
50] ciberseguridad “Cyber Europe 2018”,» 09 06 2018. [En línea]. Available: https://www.seguridadaerea.gob.es/es/noticias/aesa-particip%C3%B3-en-el-ejercicio-internacional-de-ciberseguridad-%E2%80%9Ccyber-europe-2018%E2%80%9D.

JDSUPRA, «TSA exige preparativos cibernéticos inmediatos
51] para propietarios y operadores ferroviarios luego de la imposición de requisitos similares en aeropuertos y aerolíneas,» 07 01 2022. [En línea]. Available: https://www.jdsupra.com/legalnews/tsa-mandates-immediate-cyber-5819407/. [Último acceso: 30 01 2022].

Argentina Presidencia Boletín Oficial de la República Argentina,
52] «Legislación y Avisos Oficiales,» 26 08 2019. [En línea]. Available: https://www.boletinoficial.gob.ar/detalleAviso/primera/214083/20190826. [Último acceso: 08 07 2021].

BIMCO,, Intercargo y otros, «THE GUIDELINES ON CYBER
53] SECURITY ONBOARD SHIPS,» 02 2021. [En línea]. Available: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf. [Último acceso: 09 07 2021].

J. Ovcina, «Cúpula naval: 400% de aumento en intentos de
54] piratería desde febrero de 2020,» 05 06 2020. [En línea]. Available: https://www.offshore-energy.biz/naval-dome-400-increase-in-attempted-hacks-since-february-2020/. [Último acceso: 07 09 2021].

J. C. Crawford, «Revista de Marina Nº 970, pp. 15-23,
55] CIBERATAQUE AL TRANSPORTE MARÍTIMO. ¿UNA AMENZA REAL O CIENCIA FICCIÓN?,» 06 2019. [En línea]. Available: http://portalcip.org/wp-content/uploads/2017/09/Cubic-Maritime-Cyber-Security_SPANISH_V1.pdf. [Último acceso: 07 09 2021].

OEA,Comité Interamericano contra el Terrorismo(CICTE), «La
56] seguridad cibernética marítima en el hemisferio occidental,» 2021. [En línea]. Available: https://www.oas.org/es/sms/cicte/docs/La-seguridad-cibernetica-maritima-en-el-Hemisferio-Occidental-introduccion-y-directrices.pdf. [Último acceso: 07 09 2021].

ENISA, «PORT CYBERSECURITY-Good practices for
57] cybersecurity in the maritime sector,» 2019.

EMSA, «Sensibilización en Ciberseguridad Marítima- EMSA,»
58] [En línea]. Available: http://www.emsa.europa.eu/we-do/safety/maritime-security/item/3477-cybersec.html. [Último acceso: 17 09 2021].

ENISA, «Ciberseguridad en el sector marítimo: ENISA publica
59] nuevas directrices para abordar el riesgo cibernético- ENISA,» 17 12 2020. [En línea]. Available: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-maritime-sector-enisa-releases-new-guidelines-for-navigating-cyber-risk. [Último acceso: 19 09 2021].

G. Garcia, «Ciberseguridad Marítima- SOV Consultores,» [En
60] línea]. Available: https://sovconsultores.com.ve/ciberseguridad-maritima/. [Último acceso: 19 09 2021].

OMI, «RESOLUCIÓN MSC.428(98),» 16 06 2017. [En línea].
61] Available: https://wwwcdn.imo.org/localresources/es/OurWork/Security/Documents/Pages%20from%20MSC%2098-23-Add.1%20-%20Anexo%2010.pdf.

[Último acceso: 14 02 2022].

62] Argentina Unida, «PREFECTURA NAVAL ARGENTINA,» 23 08 2018. [En línea]. Available: https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-1242-2018-313739/texto. [Último acceso: 07 11 2021].

63] Shubham Chougule, «OWASP- IoT Device Penetration Testing,» [En línea]. Available: https://owasp.org/www-chapter-toronto/assets/slides/2019-12-11-OWASP-IoT-Top-10---Introduction-and-Root-Causes.pdf. [Último acceso: 23 10 2021].

64] CONICET-GICSAFe, «CONICET-GICSAFe- ¿Como lo hacemos?,» [En línea]. Available: https://sites.google.com/view/conicet-gicsafe/inicio/cinco-preguntas-b%C3%A1sicas/c%C3%B3mo-lo-hacemos. [Último acceso: 07 10 2021].

65] Infobae, «Empresa noruega estrenará el primer carguero eléctrico 100 % libre de tripulación,» 26 08 2021. [En línea]. Available: https://www.infobae.com/tecno/2021/08/26/empresa-noruega-estrenara-el-primer-carguero-electrico-100-libre-de-tripulacion/. [Último acceso: 16 09 2021].

66] J. M. Harán, «Ataque de ransomware a compañía de oleoducto afecta el suministro de combustible en Estados Unidos- welivesecurity by eset,» 11 05 2021. [En línea]. Available: https://www.welivesecurity.com/la-es/2021/05/11/ataque-ransomware-compania-oleoducto-colonia-pipeline-afecta-suministro-combustible-estados-unidos/. [Último acceso: 01 07 2021].

67] ERA, «Sobre la Agencia,» [En línea]. Available: https://www.era.europa.eu/can-we-help-you/faq/289_en. [Último acceso: 08 06 2021].

68] EASA, «Sobre EASA,» [En línea]. Available: https://www.easa.europa.eu/the-agency/faqs/agency#category-about-easa. [Último acceso: 29 06 2021].

69] EASA, «Organizaciones elegibles invitadas a unirse al grupo de ciberseguridad ECCSA,» 24 07 2019. [En línea]. Available:

https://www.easa.europa.eu/newsroom-and-events/news/eligible-organisations-invited-join-cybersecurity-group-eccsa. [Último acceso: 27 06 2021].

[70] OACI, «OACI,» [En línea]. Available: https://www.icao.int/about-icao/Council/Pages/vision-and-mission.aspx. [Último acceso: 21 06 2021].

[71] Ministerio de Seguridad Presidencia de la Nación, «MINSEG-CSIRT,» [En línea]. Available: https://csirt.minseg.gob.ar/. [Último acceso: 12 07 2021].

[72] OMI, «Introducción a la OMI,» [En línea]. Available: https://www.imo.org/es/About/Paginas/Default.aspx. [Último acceso: 29 06 2021].

[73] DHS, «Estrategia de ciberseguridad del DHS,» [En línea]. Available: https://www.dhs.gov/publication/dhs-cybersecurity-strategy. [Último acceso: 04 07 2021].

[74] CERT-EU, «CERT-EU,» [En línea]. Available: https://cert.europa.eu/cert/plainedition/en/cert_about.html. [Último acceso: 27 06 2021].

[75] EMSA, «Acerca de,» [En línea]. Available: http://www.emsa.europa.eu/about/agency-structure/80-about.html. [Último acceso: 29 06 2021].

[76] CENELEC, «CENELEC- Sobre CENELEC,» [En línea]. Available: https://www.cencenelec.eu/about-cenelec/. [Último acceso: 08 10 2021].

[77] Wikipedia, «Wikipedia- Comité Europeo de Normalización Electrotécnica,» 18 07 2020. [En línea]. Available: https://es.wikipedia.org/wiki/Comit%C3%A9_Europeo_de_Normalizaci%C3%B3n_Electrot%C3%A9cnica. [Último acceso: 08 10 2021].

[78] kaspersky, «kaspersky-¿Qué es un keylogger?,» [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/keylogger. [Último acceso: 22 10 2021].

OWASP, «OWASP- ¿Quién es la Fundación OWASP?,» [En

79] línea]. Available: https://owasp.org/. [Último acceso: 23 10 2021].

OEA, «OEA- Programa de Ciberseguridad,» [En línea]. Available:
80] http://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp. [Último acceso: 06 11 2021].

IATA, «IATA-Seguridad cibernética de la aviación,» [En línea].
81] Available: https://www.iata.org/en/programs/security/cyber-security/. [Último acceso: 06 11 2021].

Argentina Unida, «Codigo PBIP,» [En línea]. Available:
82] https://www.argentina.gob.ar/prefecturanaval/proteccionmaritima/codigo-pbip. [Último acceso: 07 11 2021].

Argentina Unida, «Gestion Seguridad de buques,» [En línea].
83] Available:
https://www.argentina.gob.ar/prefecturanaval/seguridadnavegacion/buques. [Último acceso: 07 11 2021].