NOTA TÉCNICA N.° IDB-TN-03323

Ciberseguridad en el sector transporte en América Latina y el Caribe: estado y hoja de ruta

Autores
Paula Cruz Moreno
Adriana Calle Jordá
Santiago Paz González
Alejandra Caldo
Fernando Cuenca
Maite Álvarez Peñavieja
Juan Garate Añibarro

Editores BID
Fanny Bertossi
José Callero
Maria Pfeifer

Banco Interamericano de Desarrollo
Marzo de 2026

BID

Ciberseguridad en el sector transporte en América Latina y el Caribe: estado y hoja de ruta

Autores
Paula Cruz Moreno
Adriana Calle Jordá
Santiago Paz González
Alejandra Caldo
Fernando Cuenca
Maite Álvarez Peñavieja
Juan Garate Añibarro

Editores BID
Fanny Bertossi
José Callero
Maria Pfeifer

Banco Interamericano de Desarrollo
Marzo de 2026

Ciberseguridad en el sector transporte en América Latina y el Caribe: estado y hoja de ruta

http://www.iadb.org

Colaboradores externos:
Corrección: Gabriela Murdoch y María José Peralta
Diagramación: Mauro Collante

Fotografías:
Pág. 16: Adobe Stock (Jack)
Pág. 26: Adobe Stock (Comofoto)
Pág. 53: Pexels (Chait Goli)
Pág. 70: Adobe Stock (Kalafoto)
Pág. 91: Pexels (Pixabay)

Agradecimientos

Este estudio contó con el apoyo de múltiples colegas de la División de Transporte del BID en toda la región, a quienes expresamos nuestro agradecimiento.

Asimismo, agradecemos por sus valiosos aportes a todos los participantes de las entrevistas de recopilación de información en la región: el Ministerio de Transporte y la Agencia Nacional de Infraestructura de la República de Colombia; la Secretaría de Innovación de la República de El Salvador; la Autoridad del Canal de Panamá; la Unidad Operativa de Control de Tránsito del Ministerio de Transporte y Telecomunicaciones de la República Chile; el Ministerio de Transportes y Comunicaciones y la Secretaría de Transformación Digital de la República del Perú; la Secretaría de Infraestructura Comunicaciones y Transporte de México; Aerocivil Colombia; la compañía Transmilenio S.A., la Asociación Latinoamericana y del Caribe de Transporte Aéreo y DEME Group Brasil.

Contenido

Prólogo 8

Resumen ejecutivo 11

Abreviaturas y acrónimos 15

1. ¿Por qué necesitamos hablar de ciberseguridad en el transporte? 16

1.1 Conceptos y glosario 17

1.1.1. ¿Qué es la ciberseguridad y por qué la necesitamos? 17

1.1.2. Glosario y conceptos básicos 18

1.2 El sector del transporte como infraestructura crítica de un país 21

2. Análisis global de la ciberseguridad para el sector del transporte 26

2.1. Activos, servicios y amenazas en el transporte y sus subsectores 27

2.1.1. Transporte aéreo 29

2.1.2. Transporte marítimo 33

2.1.3. Transporte ferroviario 37

2.1.4. Transporte terrestre carretero: urbano e interurbano 40

2.2. Aspectos normativos y regulatorios a nivel global 47

2.2.1. Unión Europea 47

2.2.2. Estados Unidos 48

2.2.3. Otros países 50

2.2.4. Estándares de ciberseguridad aplicables 51

3. Análisis de la situación de la región de América Latina y el Caribe (ALC) 53

3.1. América Latina: la región con mayor crecimiento de incidentes reportados 54

3.2. Panorama de cooperación regional 55

3.3. Panorama legal 57

3.4. Panorama organizacional 59
3.5. Panorama técnico 60
3.6. Panorama de capacitación 62
3.7. Panoramas subsectoriales 62
3.7.1. Sector aéreo 63
3.7.2. Sector marítimo 65
3.7.3. Transporte terrestre carretero y transporte público 67
3.8. Presupuestar la ciberseguridad: una inversión a futuro 69
3.9. Conclusión sobre el estado de la ciberseguridad del sector del transporte en la región 69

4. Recomendaciones y hoja de ruta 70
4.1. Recomendaciones para formuladores de políticas 71
4.1.1. Sobre el gobierno de la ciberseguridad nacional 71
4.1.2. Entidades y agentes relacionados con el sector 72
4.2. Hoja de ruta 74
4.2.1. Marco regulatorio 78
4.2.2. Protección ante ciberamenazas 82
4.2.3. Respuesta y recuperación de incidentes 85
4.2.4. Instrumentos de mejora 87
4.3. Herramienta de autoevaluación 90

5. Anexos 91
5.1. Anexo I. Regulaciones internacionales 92
5.1.1. Estados Unidos 92
5.1.2. Unión Europea 92
5.1.3. Internacional 94
5.2. Anexo II. Estándares y marcos de ciberseguridad aplicables 95
5.2.1. Aviación 95
5.2.2. Marítimo 97
5.2.3. Ferroviario 98
5.2.4. Intelligent Transport Systems 98
5.2.5. Vehículos terrestres 100
5.2.6. Sistemas industriales 101
5.2.7. Productos IT 102
5.2.8. Infraestructuras críticas 102
5.2.9. Organizaciones 102

5.3. Anexo III. Modelo de entrevista con entidades públicas 104
5.3.1. Contexto de la entidad 104
5.3.2. Medidas legales / jurídicas 104
5.3.3. Medidas técnicas de respuesta 105
5.3.4. Medidas organizativas 106
5.3.5. Medidas de concienciación y capacitación 107
5.3.6. Medidas de cooperación 109

Referencias bibliográficas. 110

Prólogo

Los sistemas de transporte constituyen infraestructuras críticas para el desarrollo económico y social de los países de América Latina y el Caribe. Su correcto funcionamiento es esencial para garantizar la movilidad cotidiana de las personas, el acceso a servicios básicos, la integración territorial, la competitividad de las economías y el flujo eficiente de bienes a lo largo de las cadenas logísticas. Cuando estos sistemas se ven afectados, las consecuencias trascienden el ámbito del transporte y se extienden rápidamente a otros sectores de la economía y de la sociedad. La imposibilidad de que las personas lleguen a sus hogares o lugares de trabajo, así como las dificultades para que las empresas entreguen mercancías o reciban insumos esenciales, pueden generar impactos significativos en la productividad, el empleo, el bienestar social y la confianza en las instituciones.

En este contexto, el sector del transporte enfrenta una combinación de amenazas de diversa naturaleza. Además de los riesgos asociados a errores humanos, fallas operativas o fenómenos naturales exacerbados como consecuencia del cambio climático, los sistemas de transporte están expuestos cada vez más a amenazas de origen cibernético. Por su naturaleza compleja e interconectada, las fallas sistémicas en el transporte son inevitables; sin embargo, cuando estas fallas se originan o amplifican en el ciberespacio, sus efectos pueden propagarse con rapidez y magnitud, afectando simultáneamente múltiples servicios y actores.

La transformación digital del sector del transporte es hoy una tendencia irreversible. La incorporación de tecnologías digitales en la planificación, operación y gestión de infraestructuras y servicios ha permitido avances sustantivos en eficiencia, sostenibilidad y calidad del servicio. No obstante, esta misma digitalización ha ampliado la superficie de exposición a riesgos cibernéticos. Los sistemas de transporte dependen cada vez más de plataformas digitales, redes de comunicación, sistemas de control industrial y proveedores tecnológicos externos, lo que introduce nuevas vulnerabilidades y dependencias críticas. En este sentido, gestionar la seguridad cibernética de los sistemas de transporte no es solo una buena práctica técnica, sino un componente esencial de la resiliencia del sector y de su capacidad para entregar resultados confiables a la ciudadanía y a los mercados.

La experiencia reciente, tanto a nivel regional como global, demuestra que los riesgos cibernéticos ya no son hipotéticos. En América Latina y el Caribe, ataques de *ransomware* han afectado de manera directa e indirecta a Gobiernos y entidades públicas, paralizando temporalmente la prestación de servicios esenciales. En abril de 2022, un ataque directo al Gobierno de Costa Rica[1] impactó múltiples instituciones públicas. De forma similar, en septiembre de 2023, el Gobierno de Colombia[2] se vio afectado indirectamente por un ataque a un proveedor de servicios de telecomunicaciones. En ambos casos, los incidentes tuvieron un impacto notable en sistemas de aduanas, interrumpiendo trámites y el flujo de mercancías. Si bien ambos lograron restablecer sus sistemas y desde entonces han avanzado en el fortalecimiento de su ciberseguridad a nivel institucional, normativo y técnico, estos episodios evidencian la vulnerabilidad del sector frente a amenazas cada vez más sofisticadas.

1 Amerise, A. 2022, May 20. “Estamos en guerra”: 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia. *BBC News Mundo*. https://www.bbc.com/mundo/noticias-america-latina-61516874

2 Presidencia de Colombia, C. 2023. Boletín n.º 2 PMU-Ciberseguridad. En COLCERT. https://colcert.gov.co/800/w3-article-278842.html

A nivel global, incidentes originados en el sector privado también han puesto de manifiesto los riesgos sistémicos asociados a la dependencia tecnológica. En julio de 2024, ocurrió un caso conocido como *Crowdstrike*[3] donde una falla en un proveedor internacional de servicios tecnológicos provocó que más de 8 500 000 computadoras con sistema operativo Windows quedaran fuera de servicio, lo que afectó la operación normal de múltiples servicios críticos. El transporte aéreo fue uno de los sectores más impactados: organizaciones que dependen de sistemas en la nube para la programación de vuelos, la asignación de tripulaciones, el registro de pasajeros o la gestión de equipaje perdieron acceso a sus plataformas. Como resultado, se cancelaron más de 4000 vuelos y se registraron alrededor de 35 000 retrasos a nivel mundial, con pérdidas económicas inmediatas y afectaciones significativas para millones de personas. La recuperación fue lenta y compleja, al requerir intervenciones presenciales en los equipos afectados, lo que puso en evidencia la fragilidad de ciertos esquemas de operación altamente digitalizados.

Los ejemplos ilustran que el impacto de los incidentes cibernéticos en el transporte va mucho más allá del plano digital. Las interrupciones en los sistemas de pago electrónico pueden paralizar el transporte público urbano, impidiendo que las personas lleguen a sus trabajos y afectando directamente sus medios de subsistencia. Las disrupciones en puertos o aeropuertos pueden generar cuellos de botella logísticos con efectos en cascada sobre la economía. En los casos más extremos, los ciberincidentes pueden comprometer la seguridad física y la vida humana. La complejidad inherente de los sistemas de transporte, caracterizados por la interacción de múltiples actores públicos y privados, plantea desafíos particulares en materia de ciberseguridad. Cada subsector —aéreo, marítimo, carretero o de transporte público— presenta características operativas específicas y distintos niveles de exposición a los riesgos cibernéticos.

En este escenario, fortalecer la resiliencia cibernética del sector del transporte se convierte en una prioridad estratégica para los países de América Latina y el Caribe. La ciberseguridad debe ser abordada de manera integral, considerando no solo la protección de los sistemas, sino también la capacidad de respuesta, recuperación y mejora continua frente a incidentes en un entorno de amenazas en constante evolución. Este desafío requiere marcos normativos adecuados, capacidades institucionales sólidas, recursos financieros y humanos suficientes, y una coordinación efectiva entre niveles de Gobierno, sectores y actores.

Esta publicación busca ser una herramienta práctica y oportuna para apoyar a los Gobiernos de la región en este proceso. Ofrece un análisis de las tendencias globales en gobernanza y regulación de la ciberseguridad en el sector del transporte, junto con un diagnóstico del estado actual de la región basado en investigaciones y entrevistas realizadas con actores clave. A partir de este análisis, se presentan recomendaciones fundamentadas para la formulación de políticas públicas y una hoja de ruta integral que abarca el desarrollo de marcos regulatorios, la protección frente a ciberamenazas, la respuesta y recuperación ante incidentes y la implementación de instrumentos de mejora continua.

Como Banco Interamericano de Desarrollo reafirmamos nuestro compromiso de acompañar a los países de América Latina y el Caribe en su desarrollo al promover infraestructuras de transporte sostenibles, resilientes e inclusivas. A través de nuestra estrategia institucional BIDImpact+, impulsamos la transformación digital del sector público y el fortalecimiento de las capacidades institucionales, mediante la integración de la ciberseguridad como un elemento central para garantizar

3 Euronews Travel. 2024. CrowdStrike chaos: Why did the global IT outage ground so many planes last week? Euronews Group. https://www.euronews.com/travel/2024/07/23/crowdstrike-chaos-why-did-the-global-it-outage-ground-so-many-planes-last-week#:~:text=There%20were%20more%20than%204%2C000,for%20Dutch%20carrier%20KLM%20explains.

la seguridad digital y física de los sistemas de transporte, mejorar la calidad de los servicios y crear un entorno confiable para el sector privado.

La ciberseguridad en el transporte no es un tema técnico aislado, sino una dimensión clave en el desarrollo. Su abordaje exige liderazgo político, cooperación entre sectores y una visión de largo plazo. Es urgente avanzar en decisiones coordinadas que fortalezcan los marcos institucionales y regulatorios, desarrollen capacidades y fomenten una cultura de ciberseguridad en todos los niveles. Este informe invita a Gobiernos y partes interesadas a actuar con decisión para proteger los avances logrados y construir un futuro más seguro, resiliente y conectado para los ciudadanos de nuestra región.

Ana María Pinto A.

Ana María Pinto A.
Jefa de División Transporte

Paula Acosta

Paula Acosta
Jefa de División Innovación
en Servicios al Ciudadano

Resumen ejecutivo

La ciberseguridad es una preocupación en el sector del transporte, ya que una falla puede interrumpir de forma marcada los flujos de transporte con impactos en las cadenas logísticas y el desplazamiento nacional e internacional de pasajeros. A medida que el sector del transporte adopta tecnologías digitales para mejorar su eficiencia y sostenibilidad, también se vuelven estos sistemas más vulnerables a los ciberataques. Por su esencia compleja e interconectada, las fallas sistémicas en el transporte son inevitables. Prevenir y mitigar las consecuencias de estas fallas cuando surgen desde el ciberespacio es esencial.

Si consideramos el Índice de Gobierno Digital[4] de las Naciones Unidas (*E-GOV Development Index*), la región ha tenido un crecimiento aproximado del 25 % en su desarrollo digital en los últimos diez años y, actualmente, se encuentra en tercer lugar luego de Norteamérica y Europa. No obstante, si consideramos índices de ciberseguridad como el *Global Cybersecurity Index*[5], encontramos que América Latina y el Caribe (ALC) tiene la peor media de madurez comparada con otras regiones.

La digitalización en el sector del transporte en América Latina y el Caribe ha traído beneficios innegables, como mejores servicios para la ciudadanía o más información para mejorar la planificación de políticas e inversiones. Pero también presenta retos. En este sentido, las operaciones, servicios e infraestructuras de transporte, tanto físicas como digitales, dependen de sistemas que pueden fallar. Además, sus operadores o usuarios están poco familiarizados con todos sus componentes y las interdependencias que necesitan para protegerse de las ciberamenazas.

La buena infraestructura tiende a ser invisible para sus usuarios hasta que falla[6]; esto es relevante tanto para las propias infraestructuras de transporte como para todos los sistemas e infraestructuras digitales que soportan los servicios y operaciones hoy en día.

Este informe revela cómo la ciberseguridad no es solo un tema que considerar como una buena práctica más, sino un aspecto esencial y transversal que debe ser tomado en cuenta tanto por el sector privado como por el sector público en todo el proceso de gestión, planeación y elaboración de políticas públicas de transporte.

Se analizan los subsectores del transporte aéreo, marítimo, ferroviario, terrestre de carga y pasajeros. En cada uno se analizan los activos claves y vulnerabilidades específicas. Se identifican, también, las distintas amenazas que los pueden afectar mediante un repaso del estado del arte y de algunos ejemplos de ciberataques recientes en las infraestructuras de transporte.

4 United Nations. 2024. E-Government Development Index. https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index

5 International Telecommunication Union (ITU). 2024. Global Cybersecurity Index. https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

6 Star, SL. 1999. La etnografía de la infraestructura. American Behavioral Scientist. https://doi.org/10.1177/00027649921955326

El informe ofrece un análisis de las tendencias globales en regulación y gobernanza de la ciberseguridad en el sector del transporte, que incluyen:

- **Enfoque en la gestión de riesgos.** Los Gobiernos y las organizaciones están adoptando marcos de gestión de riesgos para identificar, evaluar y mitigar los riesgos de ciberseguridad en el sector del transporte.

- **Enfoque en la colaboración público-privada.** Se resalta la necesidad creciente de una mayor colaboración entre los Gobiernos y el sector privado para abordar los desafíos de la ciberseguridad en el transporte.

- **Creación de espacios de intercambio y canales de información sobre incidentes.** Los Gobiernos y las organizaciones deben compartir mayor y mejor información sobre las amenazas y vulnerabilidades de ciberseguridad para mejorar la conciencia y capacidades de respuesta a incidentes.

- **Mayor inversión en ciberseguridad.** Los Gobiernos y las organizaciones necesitan invertir más recursos en ciberseguridad para proteger los sistemas de transporte de las amenazas cibernéticas. Sin embargo, las inversiones actuales no están todavía a la altura de las crecientes amenazas.

- **Creación y refuerzo de marcos para proteger las infraestructuras críticas del sector del transporte.** Debido a su papel esencial en la seguridad física y el bienestar de los ciudadanos, la protección de infraestructuras críticas debe incluir la gestión de riesgos cibernéticos, ya que los ataques a los sistemas de transporte acarrean graves consecuencias, desde pérdidas económicas hasta riesgos para la seguridad y la vida humana.

- **Enfoque hacia la creación de resiliencia cibernética.** El enfoque en la protección es importante, pero no se puede negar la realidad ni la creciente complejidad del panorama de riesgos cibernéticos. Las entidades del sector del transporte también deben centrar sus recursos en crear sistemas que permitan pronta recuperación y resiliencia hacia los riesgos cibernéticos.

De acuerdo con los hallazgos de este informe, se encuentra que el estado de la ciberseguridad en el sector del transporte en América Latina y el Caribe se caracteriza por una serie de desafíos y áreas de mejora. Algunos de los puntos clave incluyen:

- **Rápida digitalización pospandemia:** La creciente digitalización en América Latina y el Caribe está superando la capacidad de la región para fortalecer su ciberseguridad. En 2024, América Latina y el Caribe fue la región de más rápido crecimiento en incidentes cibernéticos divulgados, con una tasa promedio de crecimiento anual del 25 % en la última década.[7]

- **Toma de conciencia**: Persiste una falta de conciencia sobre los riesgos de ciberseguridad en el sector del transporte entre los responsables de la toma de decisiones y el público en general.

7 Vergara Cobos, E. 2024. *Cybersecurity Economics for Emerging Markets.* https://doi.org/10.1596/978-1-4648-2120-2

- **Brecha en la legislación:** Muchos países de la región carecen de leyes y regulaciones específicas sobre ciberseguridad en el sector del transporte, lo que dificulta la aplicación de medidas de protección y la sanción de delitos cibernéticos.

- **Falta de inversión:** La inversión en ciberseguridad en el sector del transporte es insuficiente en muchos países de la región, lo que limita la capacidad de las organizaciones para implementar medidas de protección adecuadas.

- **Escasez en recursos humanos capacitados en ciberseguridad:** Existe una escasez de profesionales formados en ciberseguridad en la región, lo que dificulta la contratación y retención de personal calificado para proteger los sistemas de transporte.

A pesar de estos desafíos, el informe también destaca que algunos países de la región están tomando medidas para mejorar su ciberseguridad en el sector del transporte con innovaciones legislativas, liderazgos a partir de nuevos espacios de colaboración, construcción de conocimiento e integración de la ciberseguridad en temas como sistemas de transporte público. Sin embargo, se necesita el refuerzo de los espacios de cooperación a nivel regional para abordar los desafíos de manera efectiva y garantizar la seguridad de los sistemas de transporte en América Latina y el Caribe. El reto de la ciberseguridad es global y sistémico; las respuestas deberían ser proporcionalmente colaborativas e interconectadas.

Este informe insta a los líderes a tomar medidas decisivas para fortalecer la ciberseguridad en el sector del transporte. Para lograr una mayor resiliencia cibernética, propone una hoja de ruta integral basada en los siguientes elementos:

- **Marco regulatorio:** Se recomienda desarrollar e implementar leyes, normas y estándares específicos para la ciberseguridad en el transporte, lo cual requiere crear un entorno legal que fomente la adopción de buenas prácticas y la protección de la infraestructura crítica.

- **Protección ante ciberamenazas:** Se deben implementar medidas técnicas y organizacionales para prevenir, detectar y responder a los ciberataques, como la adopción de sistemas de seguridad avanzados, la capacitación del personal y la realización de simulacros periódicos.

- **Respuesta y recuperación de incidentes:** Es fundamental contar con planes y procedimientos claros para responder y recuperarse de incidentes de ciberseguridad de manera efectiva. Esto implica establecer equipos de respuesta a incidentes, definir protocolos de comunicación y realizar copias de seguridad periódicas de los datos críticos.

- **Instrumentos de mejora:** Se deben utilizar herramientas y mecanismos para evaluar y mejorar continuamente la ciberseguridad en el sector del transporte. Esto incluye la realización de auditorías de seguridad, la participación en foros de intercambio de información y la adopción de nuevas tecnologías de seguridad.

La hoja de ruta propuesta busca crear un ecosistema de ciberseguridad sólido en el sector del transporte, donde la prevención, la detección y la respuesta a los ciberataques sean una prioridad constante.

Es urgente tomar decisiones coordinadas para fortalecer los marcos regulatorios, desarrollar políticas públicas y fortalecer el ecosistema de ciberseguridad con el fin de responder a las amenazas actuales. Se insta a los Gobiernos y a todas las partes interesadas a actuar con decisión y rapidez para establecer un marco institucional robusto, diseñar planes de acción que refuercen la preparación y respuesta ante incidentes y fomentar una cultura de ciberseguridad en todos los niveles.

Esperamos que este informe sirva como una guía oportuna y valiosa para los Gobiernos, empresas y actores del sector del transporte en América Latina y el Caribe, que los impulse a tomar medidas proactivas y coordinadas para construir un sector de transporte más resiliente y seguro ante las amenazas cibernéticas.

Abreviaturas y acrónimos

ALC América Latina y el Caribe
ARC-IT Arquitectura de Referencia para el Transporte Inteligente y Cooperativo (del inglés *Architecture Reference for Cooperative & Intelligent Transportation*)
APT Amenaza Persistente Avanzada (del inglés *Advanced Persistent Threat*)
ATC Control Automático de Trenes
ATS Supervisión Automática de Trenes
CERT Equipo de Respuesta a Emergencias Informáticas (del inglés *Computer Emergency Response Team*)
CICTE Comité Interamericano Contra el Terrorismo
CCS Sistemas de Comunidad de Carga (del inglés *Cargo Community System*)
CIS Centro de Seguridad de Internet (del inglés *Center for Internet Security*)
CISA Agencia de Seguridad Cibernética y de la Infraestructura (del inglés *Cybersecurity and Infrastructure Security Agency*)
CSIRT Equipo de Respuesta a Incidentes de Seguridad Informática (del inglés *Computer Security Incident Response Team*)
CSMS Sistema de Gestión de Ciberseguridad (del inglés *Cyber Security Management System*)
DCS Sistema de Control Distribuido (del inglés *Distributed Control System*)
DDoS Denegación de servicio (del inglés *Denial of Service*)
ECU Unidades de Control Electrónico (del inglés *Electric Control Unit*)
ENISA Agencia de la Unión Europea para la Ciberseguridad
ERP Planificación de Recursos Empresariales (del inglés *Enterprise Resource Planning*)
HMI Interfaz Hombre-Máquina (del inglés *Human-Machine Interface*)
IICC Infraestructuras Críticas
ICS Sistemas de Control Industrial (del inglés *Industrial Control Systems*)
IDS Sistema de Detección de Intrusiones (del inglés *Intrusion Detection System*)
IPT Transporte Público Inteligente (del inglés *Intelligent Public Transport*)
IT Tecnologías de la Información (del inglés *Information Technology*)
ITS Sistemas Inteligentes de Transporte (del inglés *Intelligent Transport System*)
LACNIC Registro de Direcciones de Internet para América Latina y Caribe (del inglés *Latin American and Caribbean Internet Addresses Registry*)
MitM Hombre en Medio (del inglés *Man in the Middle*)
NIST Instituto Nacional de Estándares y Tecnología de Estados Unidos (del inglés *National Institute of Standards and Technology*)
OEA Organización de los Estados Americanos
OMI Organización Marítima Internacional
OT Tecnologías de Operación (del inglés *Operation Technology*)
PCS Sistema de Comunidad Portuaria (del inglés *Port Community System*)
PLC Controlador Lógico Programable (el inglés *Programmable Logic Controller*)
RTU Unidad Terminal Remota (del inglés *Remote Terminal Unit*)
SAE Sociedad de Ingenieros Automotrices (del inglés *Society of Automotive Engineers*)
SCADA Control de supervisión y Adquisición de Datos (del inglés *Supervisory Control and Data Acquisition*)
SOC Centro de Operaciones de Seguridad (del inglés *Security Operation Center*)
TIC Tecnologías de la Información y la Comunicación
UE Unión Europea
VTS Servicio de Tráfico de Buques (del inglés *Vessel Traffic Service*)
VTMIS Sistemas de Información para la Gestión del Tráfico de Buques (del inglés *Vessel Traffic Management Information Systems*)

1

¿Por qué necesitamos hablar de ciberseguridad en el transporte?

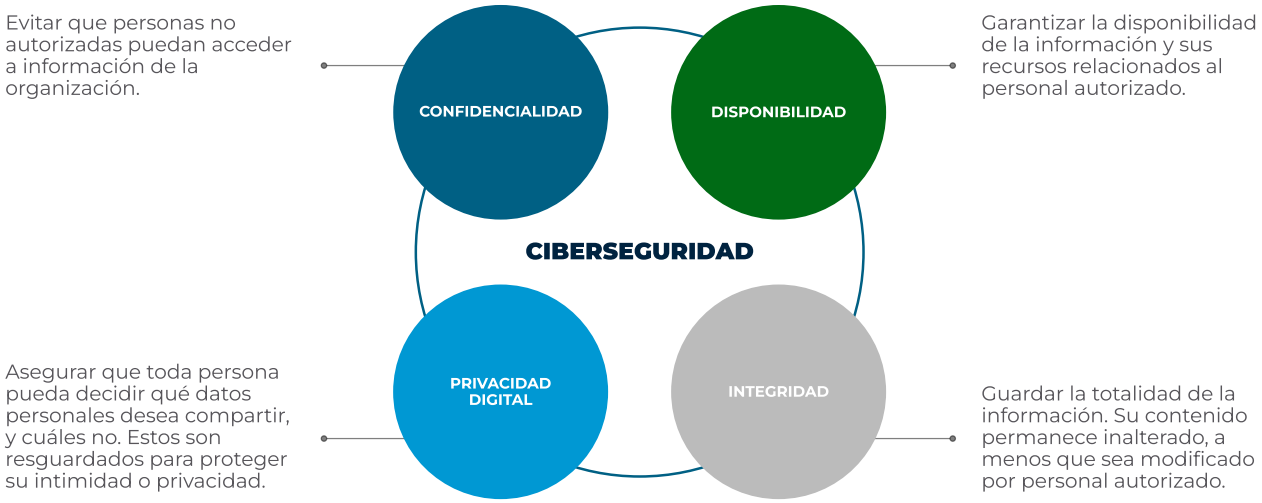
La adopción de tecnologías digitales en el sector del transporte ha generado beneficios significativos, pero también ha introducido desafíos en seguridad cibernética. Este primer capítulo aborda los conceptos básicos de la ciberseguridad y la necesidad de implementarla en el sector del transporte desde la perspectiva de la infraestructura crítica, que lo considera como un sector vital para la seguridad física y el bienestar de los ciudadanos.

1.1. Conceptos y glosario

1.1.1. ¿Qué es la ciberseguridad y por qué la necesitamos?

La ciberseguridad es el conjunto de acciones que tienen por objeto asegurar el uso del *ciberespacio propio* de una organización y protegerlo frente a terceros que no cuenten con la correspondiente autorización. Este *ciberespacio propio* es el espacio digital o virtual en el que una organización existe y lleva a cabo sus actividades; es decir, el lugar donde se encuentra el conjunto de sus activos cibernéticos y físicos, tanto de tecnologías de la información como operacionales. Asegurarlo implica no solo proteger dichos activos, sino entender cómo estos interactúan con tecnologías de comunicación y redes (internet, NFC, *bluetooth*, etc.). A continuación, se exponen los objetivos principales de la ciberseguridad:

Figura 1. Objetivos principales de la ciberseguridad



Fuente: Elaboración propia.

Gestionar la ciberseguridad en el transporte implica a una serie de actores, desde los Estados que establecen leyes y normativas para proteger sistemas y entornos, hasta los proveedores de los distintos tipos de activos físicos o digitales, como *software* o *hardware*, pasando por los usuarios de los sistemas de transporte. Estos actores deben entender los riesgos o vulnerabilidades que presentan, a fin de eliminar o minimizar la posibilidad de ocurrencia de un ataque, que podría perjudicar las operaciones de una entidad de transporte, generar pérdidas económicas o afectar al personal o a los usuarios divulgando información confidencial. Los ataques cibernéticos a los sistemas de transporte pueden tener consecuencias inmediatas, interrumpiendo la prestación de servicios de transporte público o perturbando la capacidad de realizar trámites al paralizar el flujo de bienes y personas; además, pueden disminuir la confianza de los usuarios o ciudadanos en las entidades de transporte, lo que evidencia que no suponen solo un riesgo técnico, sino también social. Más aún, la desconfianza puede provocar que los usuarios dejen de utilizar los sistemas y plataformas del transporte público (aplicaciones, registro de cuentas, tarjetas de transporte personalizadas, etc.), lo cual repercutirá en una mayor dificultad tanto en la planeación de la operación como en la gestión de los viajes por parte de los

usuarios. Asimismo, el desuso de estas herramientas, sumado a la desconfianza en los sistemas, puede derivar en un incremento del costo generalizado del viaje. Esto fomentaría un cambio modal que desincentiva el transporte público, el uso de bicicletas compartidas y otros, impulsando en su lugar el uso de vehículos particulares, que impactará negativamente en la congestión, emisiones y siniestralidad vial. Las consecuencias de contar con sistemas poco ciberseguros —o la percepción de riesgo de parte de los usuarios en el tráfico vehicular— también pueden extenderse a otro tipo de herramientas digitales, como las aplicaciones de navegación. Esto agravaría la congestión y empeoraría la situación tanto para el usuario individual como para la sociedad en general, que se ve penalizada por el tráfico (Gómez-Lobo *et al.*, 2022).

En el caso del transporte de mercancías, al reducirse el uso de herramientas digitales que optimizan los flujos de transporte en los canales de distribución, se pueden incrementar las ineficiencias del sector, lo que aumentará los costos para las organizaciones y, por ende, para el consumidor. De forma similar, las pérdidas de eficiencia pueden resultar en mayores emisiones del transporte con consecuencias para el clima y la salud de las personas.

1.1.2. Glosario y conceptos básicos

Amenaza: Violación potencial de la seguridad. Puede materializarse al explotar una vulnerabilidad para causar una infracción de la seguridad.

Agentes de riesgo: Personas u organizaciones que pueden exponer y explotar, de forma deliberada o involuntaria, puntos vulnerables que puedan causar incidentes y afectar a los servicios de transporte, en especial su seguridad, protección, negocios, finanzas y reputación.

Análisis forense: El análisis forense en ciberseguridad, también conocido como *análisis forense digital*, es un proceso que se lleva a cabo tras un incidente de seguridad informática, como un ciberataque, un robo de datos o una intrusión. El objetivo principal es recopilar y analizar la evidencia digital encontrada en los sistemas afectados para determinar qué sucedió, cómo ocurrió y quién es el responsable.

Atacante: Persona o grupo que dirige ataques de manera deliberada contra organizaciones para vulnerar la seguridad de sus sistemas. Los tipos de atacantes varían, al igual que varían sus motivaciones; pueden tanto ser actores individuales como organizaciones delictivas.

Campos cibernéticos (*cyber ranges*): Entornos virtuales simulados que se utilizan para el entrenamiento en ciberseguridad y para la investigación y desarrollo de tecnologías relacionadas. Estos entornos permiten a los profesionales de la seguridad informática practicar la defensa contra ciberataques y mejorar sus habilidades en un entorno controlado y seguro.

Ciberataque: También conocido como *ataque*, es una violación deliberada de la política de seguridad de un sistema. A continuación, se describen los distintos tipos de ataque:

- **Ciberguerra:** Operaciones cibernéticas con el fin de destruir o degradar las infraestructuras de un país.
- **Cibercrimen:** Actividad criminal con el fin de obtener beneficios económicos.

- **Ciberterrorismo:** Convergencia del ciberespacio y del terrorismo que causa pérdida de vidas o graves daños económicos.

- **Ciberactivismo:** Ciberataques que tratan de influir en la opinión pública o en la reputación de las organizaciones, o bien hacer proselitismo a favor de causas específicas.

- **Cibermalicia:** Ataques arbitrarios de aficionados que causan molestias y daños menores.

***Hacking* ético:** El *hacking* ético (en inglés, *ethical hacking*) es una práctica de seguridad informática en la que un profesional capacitado simula ataques maliciosos contra sistemas informáticos, aplicaciones o redes para identificar fallos de seguridad y vulnerabilidades. Estos profesionales, conocidos como *hackers de sombrero blanco*, son contratados para ayudar con sus habilidades a las organizaciones a protegerse de ciberamenazas y reforzar sus medidas de seguridad.

Hardware: Todos los conjuntos de los componentes físicos de un sistema informático, con sus componentes eléctricos, electrónicos y electromecánicos.

Infraestructura crítica: Procesos, sistemas, instalaciones, tecnologías, infraestructuras físicas, redes, activos y servicios esenciales para la salud, la seguridad o el bienestar económico de una nación y el funcionamiento eficaz de su gobierno.

Ingeniería social: En ciberseguridad, es una técnica de manipulación que se aprovecha de las tendencias y comportamientos humanos para obtener información confidencial o acceso a sistemas o comprometer la seguridad de manera general. Es conocida como el *hacking humano* porque, en lugar de atacar directamente los sistemas informáticos, se enfoca en engañar a las personas para que cometan errores de seguridad. Los ataques de ingeniería social pueden incluir:

- Suplantación de identidad de marcas o personas de confianza.

- Correos electrónicos o mensajes que parecen legítimos y piden información sensible.

- Llamadas telefónicas con pretextos convincentes para obtener datos personales.

- Amenazas o promesas que llevan a las víctimas a realizar acciones no seguras.

Investigación, desarrollo e innovación (I+D+i): Es un concepto reciente en el contexto de los estudios de ciencia, tecnología y sociedad. Engloba tres actividades distintas, pero interrelacionadas, que impulsan el progreso científico y tecnológico. El concepto de I+D+i evoluciona del término I+D al incorporar la dimensión de la innovación como un elemento clave para el progreso. Su campo de aplicación es amplio y diverso: desde la investigación científica básica hasta el desarrollo de nuevas tecnologías y la creación de productos y servicios innovadores.

Malware: También conocido como *software malicioso,* se refiere a cualquier programa o código diseñado para dañar, infiltrarse o acceder a un sistema informático de forma intencionada sin el consentimiento del usuario. Las motivaciones detrás del desarrollo y

difusión del *malware* tienden a ser dolosas. Sin embargo, existen sutilezas con algunos *malware* que tienen fines publicitarios o, en algunos casos, de vandalismo sin consecuencias graves para los sistemas.

Phishing: Técnica de ingeniería social utilizada por ciberdelincuentes para obtener información confidencial de forma fraudulenta. Los atacantes engañan a las víctimas para que compartan con ellos datos sensibles, como contraseñas, números de tarjetas de crédito y credenciales de inicio de sesión. Esto se logra a través de correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web falsificados que parecen legítimos. Los ataques de *phishing* suelen crear una sensación de urgencia o miedo para presionar a la víctima a actuar rápidamente, lo que puede llevar a revelar información personal o descargar *malware*.

Prueba de penetración o *pentesting:* Evaluación de seguridad que consiste en simular ataques cibernéticos contra sistemas informáticos, redes o aplicaciones para identificar y explotar vulnerabilidades. Estas pruebas son realizadas por profesionales de la ciberseguridad conocidos como *hackers éticos,* que utilizan técnicas y herramientas similares a las de los atacantes maliciosos, pero con el objetivo de mejorar la seguridad y proteger los sistemas.

Las pruebas de penetración son de varios tipos, como:

- Prueba de penetración de la red: Evalúa la seguridad de la infraestructura de red.
- Prueba de penetración física: Examina la seguridad física de las instalaciones.
- Prueba de penetración de aplicaciones web: Se centra en las vulnerabilidades de las aplicaciones web.
- Prueba de penetración de redes inalámbricas: Busca fallos en la seguridad de las redes wifi.

Ransomware: Ataque realizado a través de programas maliciosos con el propósito de bloquear o cifrar los datos o dispositivos de una organización y exigir el pago de un rescate para restaurar el acceso. Los atacantes suelen pedir el pago en criptomonedas, como bitcóin, ya que proporcionan un cierto grado de anonimato, y suelen afectar sistemas de información vitales para el buen funcionamiento de operaciones o negocios. El *ransomware* puede afectar a individuos, empresas y organizaciones gubernamentales, y puede propagarse a través de correos electrónicos de *phishing,* descargas maliciosas o explotando vulnerabilidades de seguridad. Los ataques de *ransomware* han evolucionado con el tiempo. Algunos incluyen tácticas como la doble extorsión, por la cual los atacantes no solo cifran los datos, sino que amenazan con publicarlos en línea si no se paga el rescate. También pueden implicar ataques adicionales a clientes o socios comerciales de la víctima utilizando los datos robados.

Sistemas de información: En informática, es un conjunto integrado de agentes o componentes que interactúan para procesar, recopilar, almacenar, recuperar o distribuir información con un propósito o misión específica. Estos componentes incluyen elementos como la infraestructura física (computadoras y dispositivos), los programas y las aplicaciones que gestionan los datos, los datos en sí, los actores o usuarios y los procesos que estructuran el flujo de información.

Sistemas de transporte: Conjunto de elementos que conecta la necesidad de desplazamiento de las personas o mercancías (demanda) con los servicios de transporte disponibles (oferta) en un área determinada. Un sistema de transporte puede incluir carreteras, vías férreas, aeropuertos, puertos marítimos y fluviales, así como también redes de transporte público como autobuses y metros.

Sistemas Inteligentes de Transporte (ITS): Integración de componentes tecnológicos que permiten automatizar procesos que antes se realizaban manualmente o bajo instrucción del usuario humano. Se les denomina *inteligentes*, ya que digitalizan o automatizan tareas como la percepción del entorno, el análisis de datos o la toma de decisiones en estos vehículos o infraestructuras de transporte. Estos sistemas se basan en la convergencia de tecnologías de la información y la comunicación, sensores, sistemas de posicionamiento global y plataformas de *software* para recopilar, procesar y analizar datos en tiempo real. Incluyen vehículos inteligentes, carreteras inteligentes, sistemas de gestión de tráfico y aplicaciones o servicios para usuarios del transporte.

Software: Conjunto de programas o aplicativos que permiten que un ordenador o computadora realice determinadas operaciones.

Subsectores del transporte: Se definen en función del medio a través del cual se realiza el transporte de pasajeros o mercancías. Incluyen el transporte aéreo civil, el transporte marítimo y fluvial, el transporte por carretera y la movilidad urbana. Su gestión implica tanto la construcción, planificación y operación de las infraestructuras que los habilitan como la regulación y organización de las relaciones entre los múltiples actores que prestan servicios o usan estas infraestructuras.

Vulnerabilidad: Debilidad o fallo en un sistema de información que pone en riesgo la seguridad, pudiendo permitir que un atacante comprometa la integridad, disponibilidad o confidencialidad del sistema, por lo que es necesario encontrarla y eliminarla lo antes posible.

1.2. El sector del transporte como infraestructura crítica de un país

Se consideran infraestructuras críticas aquellas que son necesarias para mantener actividades esenciales que abarcan aspectos sociales y económicos. Una interrupción en un servicio o infraestructura crítica conlleva un impacto significativo en cualquiera de estos aspectos.

Desde el punto de vista social, es necesario mantener aquellos elementos esenciales que afectan la calidad de vida de los ciudadanos, preservando la base del bienestar físico (incluyendo aspectos como la salud o la seguridad física), material, social y emocional que les permita mantener sus ingresos, pertenencias, relaciones personales, etc.

Desde la perspectiva económica, su carácter crítico supone que debe ser posible mantener tanto la prestación de servicios como los ingresos, pero también las operaciones comerciales de las propias organizaciones y de otros segmentos económicos que puedan verse afectados, así como su imagen.

Sectores que se sustentan sobre infraestructuras físicas —energía, agua y saneamiento, transporte y telecomunicaciones— junto con otros vitales —salud, finanzas o

alimentos— son los que suelen ser considerados por los Estados como infraestructuras críticas (Fisher y Gamper, 2017). Se puede realizar un diagnóstico de la criticidad de cada uno de ellos teniendo en cuenta los riesgos a los que se enfrentan (incluidos los cibernéticos), sus vulnerabilidades e interdependencias.

La forma en la que se gestionan y operan las infraestructuras críticas puede variar de un país a otro e involucra agentes públicos y privados, lo que aumenta la complejidad al establecer la gobernanza de su seguridad y resiliencia, dada la distribución de funciones y responsabilidades.

Cuando se producen interrupciones en los servicios de transporte, tanto de pasajeros como de mercancías, la sociedad y la economía se ven afectadas. Estas situaciones no solo comprometen derechos como la movilidad, la seguridad y la privacidad de los ciudadanos, sino que también desencadenan efectos en cadena: desde retrasos en la entrega de mercancías hasta la paralización de la producción o las actividades de las empresas.

Además, existen diferencias en la forma en que los sectores críticos pueden verse afectados por los ataques cibernéticos. No es igual una intrusión en un sistema crítico como el financiero o administrativo que un ataque a sistemas industriales con consecuencias físicas u operacionales directas. En este punto, es necesario distinguir los ataques de tipo IT (Tecnologías de la Información) de los que afectan a las OT (Tecnologías de Operación).

Las *tecnologías de la información* se relacionan con infraestructuras en las que los sistemas involucrados son normalmente *hardware* y *software* que procesan datos. En el sector del transporte son sistemas que normalmente están asociados a su propia gestión o a la del negocio; es decir, a sistemas de gestión de personal, sistemas de pago, relación con el usuario, contabilidad y finanzas, compras, inventarios, etc.

Las *tecnologías de operación*, en cambio, están relacionadas con todos los sistemas que gestionan los propios procesos físicos a través de la monitorización y control de dispositivos. En este nivel se encuentran no solo las computadoras que controlan, por ejemplo, una línea de fabricación, sino también sistemas más sofisticados que gestionan y monitorean operaciones industriales. En el caso del transporte, incluye los procesos que gestionan los movimientos de las grúas en una terminal portuaria, los sistemas de optimización de rutas de vehículos, los sistemas de manejo y control de equipajes, la apertura de controles de acceso a terminales de carga, los sistemas de Control de Supervisión y Adquisición de Datos (SCADA), etc.

La tipología de los ataques a las OT y, sobre todo, su impacto son muy diferentes a los efectuados a las IT, ya que pueden producirse desviaciones en el comportamiento de elementos físicos que pondrían en riesgo la integridad física de las personas o del entorno y el medioambiente.

Los entornos en los que operan las IT y las OT son notablemente diferentes. Las IT funcionan dentro de un entorno informático general y se ocupan de sistemas operativos estándares para tareas centradas en los datos. Las OT, por el contrario, están adaptadas a entornos industriales y tienden a emplear sistemas especializados, a menudo patentados, para satisfacer requisitos operativos específicos. Actualmente, se está produciendo una transformación que lleva a la integración progresiva de estos dos entornos anteriormente

aislados, lo que conduce a lo que se conoce como convergencia IT/OT. Esta integración es un fenómeno multifacético que implica la conexión física o la interconexión de interfaces, programas o procesos digitales dentro de un entorno.

La convergencia IT/OT está impulsada por la transformación digital y los avances en tecnologías como el Internet de las cosas (IoT) y el análisis de *big data*. La fusión de IT y OT permite un flujo continuo de datos entre el mundo digital y el físico, salvando la brecha entre los sistemas de gestión de datos y las operaciones industriales. La convergencia de sistemas IT y OT es especialmente importante para el sector del transporte debido a la creciente complejidad y dependencia de sistemas conectados para la operación y gestión de redes de transporte. Aquí se incluyen todas las tecnologías que impulsan la transformación digital del transporte, como la planificación de rutas, la gestión de flotas y el control del tráfico en tiempo real.

Sin embargo, esta convergencia también aumenta la superficie de ataque, exponiendo a los sistemas de transporte a ciberamenazas que pueden afectar de forma sistémica lo que antes podía estar más aislado, comprometer la seguridad de los pasajeros y causar pérdidas económicas significativas.

Según el informe *Panorama de Amenazas* de 2025, publicado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA), los ataques de ciberdelincuencia se dirigen e impactan cada vez más a las infraestructuras críticas (ENISA, 2025). Se observa que, durante el periodo de julio de 2024 a junio de 2025, entre los principales sectores de infraestructura crítica afectados estuvieron los de administración pública, transporte e infraestructura digital y servicios.

El *ransomware* o secuestro de datos es una de las principales amenazas, y el sector del transporte no está exento de sufrirlo. La principal motivación de este tipo de ataques cibernéticos son las ganancias económicas que los actores criminales obtienen al extorsionar a las empresas que quieren recuperar el acceso a sus datos. Este tipo de ataques puede impactar en empresas u organizaciones de todos los sectores del transporte. Por ejemplo, en el 2025 el aeropuerto de Kuala Lumpur fue afectado por un grupo de *ransomware* que afectó sus sistemas de información (Bischoff 2025). De forma similar, el sistema de transporte público de la ciudad de Vancouver en Canadá fue víctima de un ataque de *ransomware* que impidió por tres días que los usuarios pudiesen usar medios de pago digitales para la adquisición de billetes (CBC News, 2020).

Una breve historia del transporte como infraestructura crítica

Las infraestructuras físicas de transporte son consideradas como críticas debido a que, en caso de ser afectadas, pueden presentar riesgos graves para el buen funcionamiento de la sociedad. La determinación de la criticidad de una infraestructura es definida por cada país, según determine cuáles son esenciales para su seguridad, riqueza y salud. En el caso del transporte, la criticidad es determinada según permita la circulación de ciertas personas, bienes o servicios considerados esenciales.

La expresión *infraestructura crítica* proviene, en su versión moderna, de las políticas de Estados Unidos; la primera definición fue plasmada en la Orden Ejecutiva 13010 de 1996. Esta orden ejecutiva abordaba las inquietudes relativas a las infraestructuras y definía las infraestructuras críticas del país, identificaba ciertas amenazas y creaba la Comisión Presidencial para la Protección de las Infraestructuras Críticas. Dentro de esta primera directiva ya estaba incluido el sector del transporte y el Departamento de Transporte de la nación quedaba a cargo de este tema en la comisión. También se mencionaban los ataques de naturaleza electrónica. Poco a poco, se construyó esta política de infraestructura crítica, con una expansión de la definición tras los atentados terroristas de septiembre de 2001. Con el Acta de Protección de Infraestructuras Críticas de 2001, se extendió la definición de *infraestructura crítica* para incluir aquellos "sistemas y activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos, que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitador sobre la seguridad, la seguridad económica nacional, la salud pública nacional o la seguridad, o cualquier combinación de estos asuntos" (Newbill, 2019). Hoy en día, la protección de la infraestructura crítica de transporte se gestiona con su propio plan, que incluye riesgos cibernéticos, y es manejada de manera conjunta por el Departamento de Seguridad Nacional (Homeland Security) y el Departamento de Transporte de los Estados Unidos (CISA, s. f.).

Definiciones similares y la inclusión del sector del transporte fueron adoptadas progresivamente por otros países. Por ejemplo, en la Unión Europea (UE), el Consejo Europeo encargó en 2004 la elaboración de una estrategia integral de protección de las infraestructuras críticas, que culminó en 2006 con la creación del Programa Europeo de Protección de Infraestructuras Críticas; en este, ya se incluía el transporte como prioridad. En 2008, la Directiva 2008/114 estableció un procedimiento para identificar y designar las infraestructuras críticas europeas en los sectores del transporte y la energía que, en caso de perturbación o destrucción, tendrían importantes repercusiones transfronterizas (Parlamento Europeo y Consejo Europeo, 2008). En paralelo, por el Reglamento (CE) n.° 460/2004 del Parlamento Europeo y del Consejo, se creó la Agencia de la Unión Europea para la Ciberseguridad (ENISA), cuyo trabajo comenzó a abordar la protección de las infraestructuras críticas de transporte desde la perspectiva cibernética (ENISA, s. f.).

Varias empresas de logística y transporte han sufrido ataques cibernéticos en los últimos años, lo cual ha tenido un alto impacto económico y operacional, en general, en la región o la zona geográfica donde operan estas empresas. Un ejemplo destacado es el de Transnet Soc. Ltd. (INCIBE-CERT, 2021), empresa estatal sudafricana dedicada a actividades de logística y cadena de suministro de ferrocarriles, puertos y oleoductos. En julio de 2021 sufrió un ciberataque que le obligó a ejecutar ciertas actividades de forma manual y declarar el estado de *fuerza mayor*. Otro ejemplo más reciente es el puerto de Nagoya en Japón, también víctima de un ciberataque que lo obligó a suspender sus operaciones por múltiples horas (Glover, 2023).

Según datos de la Asociación Internacional de Puertos (IAPH), solo entre febrero y mayo de 2020 los ciberataques dirigidos a la industria marítima se multiplicaron por cuatro. Específicamente, aquellos destinados a *hackear* tecnología operativa OT aumentaron un 900 % entre 2017 y 2021 (PierNext, 2021).

Más allá de las motivaciones económicas, también existen razones políticas: los propios Estados o grupos afiliados a ellos pueden tener interés en desestabilizar ya sea su propio país u otros Gobiernos, atacando o inhabilitando algunas de sus infraestructuras críticas (puertos, aeropuertos, sistemas financieros, etc.).

Para hacer frente a esta situación e intentar mejorar el nivel de la seguridad cibernética de las infraestructuras críticas, muchos Estados están optando por desarrollar normativas o regulaciones de cumplimiento obligatorio para las empresas que ofrecen servicios esenciales.

2

Análisis global de la ciberseguridad para el sector del transporte

En este capítulo se analizan los activos, servicios y vulnerabilidades específicas de los sistemas de transporte contemporáneos que deben ser protegidos de riesgos cibernéticos. Este ejercicio permite entender, por subsector del transporte, qué activos lo conforman y cuáles son los principales componentes digitales que deben ser protegidos. También se explican las tendencias globales en la regulación y gobernanza de la ciberseguridad del sector para que el transporte sea seguro en el mundo digital.

2.1. Activos, servicios y amenazas en el transporte y sus subsectores

Los sistemas de transporte, en general, se encuentran sometidos a amenazas de diferente naturaleza. Además de estar expuestos a fenómenos naturales, errores humanos o fallos de terceras partes, pueden ser objetivo de acciones maliciosas de origen cibernético e intentos de comprometer activos o acciones que pongan en riesgo la integridad o disponibilidad de los propios servicios que prestan, o bien la integridad de los datos de sus usuarios.

Un aspecto general que se aplica a todos los subsectores del transporte es la complejidad de sus ecosistemas con múltiples organizaciones de diferente naturaleza que interactúan para proveer el servicio final de movilidad de personas o mercancías. Estos involucran organizaciones e instituciones de distintos tamaños, tanto del ámbito público como del privado, cuyos servicios tienen impacto a nivel del negocio, social o ambiental. Identificar los distintos activos y servicios de cada caso, distinguiendo cuáles son digitales, permite localizar dónde pueden existir vulnerabilidades a riesgos cibernéticos.

Cada subsector del transporte, por sus propias características, tiene diferentes tipos de activos y servicios; en ellos la interacción de lo cibernético con lo físico difiere y la naturaleza de las vulnerabilidades se diversifica. La digitalización en las operaciones del sector aéreo, por ejemplo, es mucho mayor que en la operación de carreteras y, por ende, los riesgos cibernéticos son diferentes. Para lo anterior, desde el año 2015, ENISA abordó, en una serie de diversos estudios, los activos y servicios de cada subsector del transporte, para identificar buenas prácticas y recomendaciones de ciberseguridad.

Se designan como *activos* todos aquellos activos físicos necesarios para operar la infraestructura de transporte: desde carreteras y puentes, pasando por vehículos y semáforos, hasta máquinas de billetaje en transporte público y equipos de infraestructura de IT que habilitan el funcionamiento de los sistemas de transporte. Por *servicios*, en este caso, se entienden aquellos servicios necesarios para la operación de los sistemas de transporte, como, por ejemplo, los de gestión de tráfico y de vehículos, o de cobro y billetaje.

Independientemente del medio de transporte utilizado, el impacto de un incidente de ciberseguridad puede suponer: pérdidas económicas de uno o varios agentes; facilitar el tráfico ilegal de mercancías o personas; el robo de datos sensibles, tanto personales como comerciales; el daño a elementos de la infraestructura (fija o móvil); posibles afecciones al medioambiente; y perjuicios personales, que pueden llevar incluso a la muerte de pasajeros, público en general o personal de las propias empresas.

Las motivaciones que pueden llevar a los atacantes a diseñar y ejecutar un ciberataque son diversas, ya que las amenazas pueden provenir de organizaciones criminales en las que predomine el ánimo de lucro, pero también de atacantes con ambiciones más estratégicas que persigan la paralización de una infraestructura crítica de un país o región y que dispongan de medios y recursos para ello.

Entre los potenciales atacantes figuran colaboradores de las diferentes organizaciones que forman parte del ecosistema, que tengan intenciones maliciosas y que, además, cuenten con acceso a sistemas y áreas de acceso restringido. También pueden ser personas (pasajeros y acompañantes) presentes en las terminales, vías y medios de transporte,

así como atacantes remotos, que son los que, en la mayoría de los casos, explotan los vectores de ataque disponibles.

Algunas de las amenazas cibernéticas más representativas para el sector del transporte son:

- **Ataques de ingeniería social:** empleados de las organizaciones sin la debida conciencia y capacitación sobre seguridad, o que no sigan los procedimientos, pueden representar un riesgo significativo. Esto puede derivar en un posterior uso indebido de privilegios, precedido del robo de credenciales a través de la ingeniería social, como el *phishing* dirigido contra el personal.

- **Violación de acceso (físico o lógico) y suplantación de identidad:** ocurre cuando hay un fallo en la autenticación y podemos encontrar fraudes de identidad, lo que permite que delincuentes ingresen a las instalaciones o accedan a los sistemas de información de la organización.

- **Explotación de vulnerabilidades:** aquellos elementos de cualquier sistema que no estén funcionando con las condiciones de seguridad adecuadas pueden ser un objetivo.

- **Ataques a la red o los dispositivos físicos:** estos se realizan para la escucha o modificación de las comunicaciones, que pueden ser intervenidas, tanto con el fin de recopilar datos confidenciales para espionaje del país o a nivel corporativo, como para manipularlas y alterar el comportamiento previsto de elementos físicos de la infraestructura.

- ***Software* malicioso en activos IT:** se presenta con la instalación de *malware* en dispositivos de los usuarios finales, incluidos los dispositivos de los pasajeros o el personal, los servidores u otros componentes inteligentes.

- **Fuerza bruta:** utilizada para obtener acceso no autorizado a los recursos de una organización (es decir, datos, sistemas, dispositivos, etc.) a través de muchos intentos de adivinar la clave o contraseña correcta, generalmente mediante un *software* desarrollado para tal fin. Pueden ser especialmente vulnerables a este tipo de ataques aquellas infraestructuras cuyos sistemas permitan la utilización de contraseñas simples o predeterminadas, aquellas que no tengan límite de intentos de acceso o aquellas que no implementen CAPTCHA[8].

- **Manipulación de dispositivos IT u OT:** sucede, por ejemplo, a través de modificaciones no autorizadas en *hardware* o *software* que permitan obtener el control total de los sistemas o generar un comportamiento que suponga un problema derivado de seguridad física.

- **Robo, secuestro y abuso de datos:** es la obtención de datos sensibles e información confidencial a través de diferentes medios, como datos personales de los pasajeros o del personal, de la carga transportada, de las operaciones, etc. En esta categoría, se encuentran los llamados ataques de *ransomware,* que explotan vulnerabilidades y secuestran, a través del cifrado de información, datos vitales para

8 Prueba de seguridad que verifica si un usuario es humano y no un robot. Es un acrónimo que significa "Prueba de Turing Pública Completamente Automatizada para Decir a las Computadoras y a los Humanos aparte".

la operación de sistemas. En algunos casos, incluso, se filtra información confidencial bajo amenaza de difusión; a cambio de recuperar el control y la información, se exige el pago de un rescate.

- ***Denial of Service* (DDoS) o denegación de servicio:** puede afectar determinados sistemas y las consecuencias pueden incluir la interrupción de la red, la ralentización del control de seguridad, retrasos de los pasajeros, cancelación de servicios de transporte, pérdida de confianza, daños a la reputación y daños financieros.

- **Ataques *Man-in-the-Middle* (MiTM):** tipo de ciberataque en el que el atacante intercepta y retransmite subrepticiamente mensajes entre dos partes que creen estar comunicándose directamente entre sí. Los objetivos de un ataque MitM pueden variar, pero generalmente incluyen el robo de información confidencial, el espionaje, la manipulación de datos, la interrupción de la comunicación o la suplantación de identidad. El atacante puede robar información valiosa como credenciales de inicio de sesión, datos bancarios o personales, espiar las comunicaciones entre las víctimas, modificar los datos que se transmiten, interrumpir la comunicación o hacerse pasar por una de las partes para engañar a la otra.

Hoy en día, la prevalencia de la inclusión de herramientas de Inteligencia Artificial, en particular la de tipo generativo, en la entrega de funcionalidad de los sistemas informáticos, introduce nuevas fuentes de amenazas que deben tenerse en cuenta (OWASP, 2025).

En la siguiente sección, se incluyen las principales categorías de activos y amenazas, y algunos ejemplos de escenarios de ataques de los subsectores del transporte marítimo, aéreo, de carreteras y de movilidad urbana.

2.1.1. Transporte aéreo

2.1.1.1. Activos

Las autoridades aeroportuarias, en general, operan los aeropuertos como “servicios públicos que brindan infraestructura a los proveedores de servicios y su cadena de suministro bajo una regulación financiera de ingresos neutrales” (ENISA, 2016). Esta actividad crea un ecosistema de entidades que cooperan para trabajar desde dos perspectivas principales. La primera es la perspectiva organizativa, que abarca las actividades limitadas al ámbito de control o propiedad de la autoridad o administración aeroportuaria. Aquí podemos mencionar el diseño y la configuración de la infraestructura aeroportuaria (incluida la IT) y los procesos y procedimientos operativos que sustentan la eficiencia de la propia organización. La segunda es la perspectiva de *servicio,* que contempla la cadena de suministro del aeropuerto y los servicios de apoyo, entre ellos los de IT y soporte (servicios de comunicación de información de vuelos, las plataformas detrás de los quioscos de *check-in* autónomo, los sistemas de comunicación, entre otros).

Entre las entidades más relevantes en este ecosistema encontramos a las autoridades gubernamentales, que participan como operadoras realizando tareas como el control del tránsito aéreo o de las actividades de aduana e inmigración, y también como entes reguladores. Junto con los Gobiernos locales, suelen ser responsables de la dirección estratégica de los aeropuertos.

Otros grupos de interés son: los operadores de aeropuertos, entidades independientes encargadas de realizar la operación y supervisión de uno o varios aeropuertos; las aerolíneas, compañías que prestan los servicios de transporte aéreo, ya sea de carga o pasajeros; los operadores de transporte de superficie, que facilitan el acceso al lugar por diferentes medios: trenes, taxis, buses, vehículos de alquiler, etc.; los proveedores de otros servicios —normalmente privados—, que operan tanto en el lado aire como en el lado tierra, encargados de la gestión del tránsito aéreo, el combustible, el manejo y control de equipaje, IT, comunicaciones, seguridad, alimentos y bebidas, comercio, alojamiento, entre otros.

Para un entendimiento desde las funciones realizadas en un aeropuerto, ENISA propone en *Securing Smart Airports* (ENISA, 2016) una clasificación de los activos (primarios y secundarios) más relevantes desde el punto de vista de la ciberseguridad en las siguientes categorías:

- **Administración aeroportuaria:** Ubicada en las propias terminales, incluye los sistemas de gestión empresarial, inventario de activos, recursos humanos, compras, políticas y finanzas y, sobre todo, riesgos.

- **Instalaciones y mantenimiento:** Abarca el mantenimiento de vehículos aeroportuarios, sistemas de control de edificios, gestión de la energía, ascensores, pasarelas y puentes aéreos, sistemas SCADA, plataformas, áreas auxiliares, viales, servicios públicos y sistemas de gestión ambiental.

- **Gestión de personal:** Incluye la gestión de expedientes y reclutamiento, y los sistemas de autenticación del personal (por ejemplo, el sistema de identificación biométrica).

- **Gestión de pasajeros:** Comprende los sistemas logísticos dentro del aeropuerto, dispositivos de quiosco (por ejemplo, para *e-ticketing*), sistemas electrónicos de visualización de información, registro y embarque de pasajeros, registros de nombres de pasajeros, sistema central de reservas y servicios de orientación.

- **Servicios auxiliares para clientes:** Incluye los cajeros automáticos, puntos de venta, servicios comerciales de gestión cruzada (*duty free,* etc.), vuelos privados, vuelos VIP y servicios de soporte para personas con discapacidad.

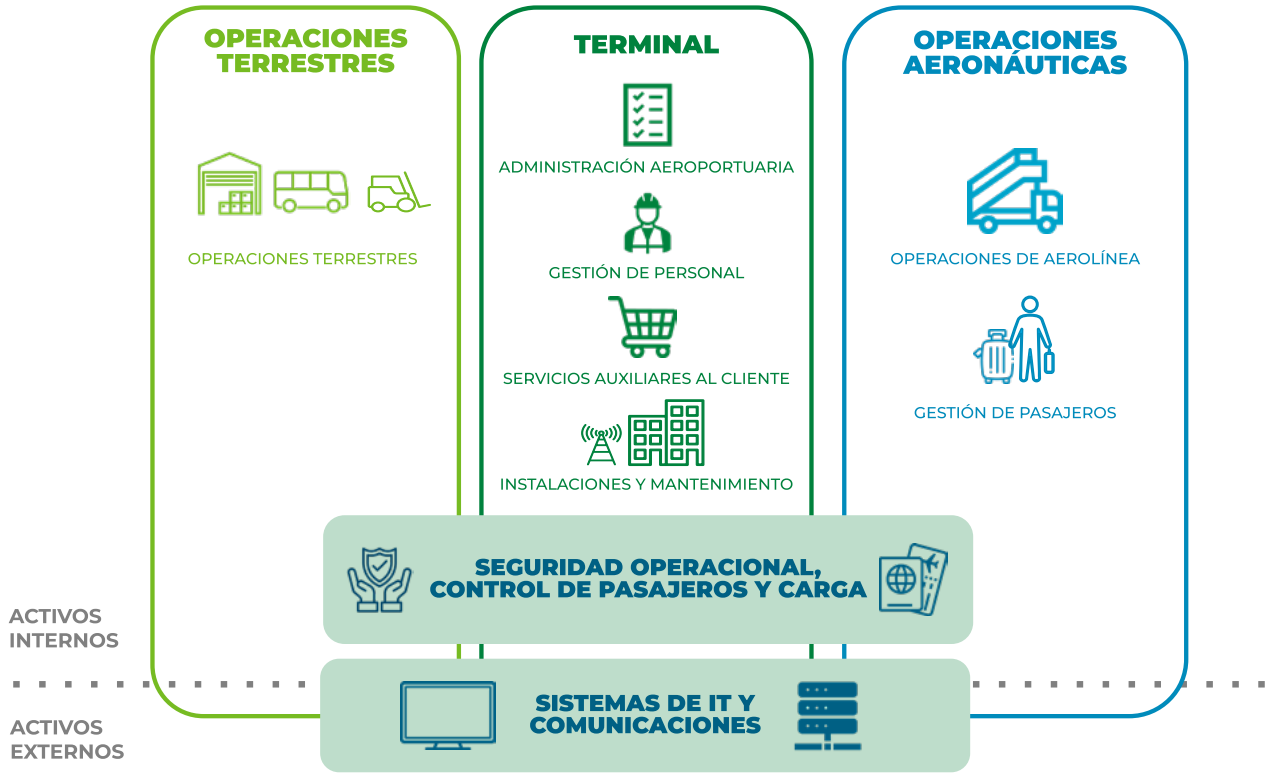
- **Operaciones de aerolíneas/zonas de operaciones:** Abarca la gestión del tráfico aéreo, sistemas de seguimiento de vuelos, sistemas de control de salidas, sistemas de información meteorológica, sistemas de gestión de infraestructuras y recursos aeroportuarios, como iluminación del aeródromo y sistemas de control y seguimiento de pistas (incluyendo equipos de medición de distancia), sistemas de procesamiento de carga, comunicación, navegación y vigilancia, sistemas de repostaje de aeronaves y bases de datos de operaciones aeroportuarias.

- **Operaciones terrestres:** Comprende el centro de control del sistema de operaciones terrestres del aeropuerto, identificación automática de vehículos, gestión de combustible, sistemas de detección de iluminación, sistemas de gestión de estacionamiento o peajes electrónicos y sistemas de transporte público y privado.

- **Seguridad operacional, control de pasajeros y carga:** Incluye los sistemas de control de acceso, sistemas de autenticación, sistemas de credencialización, sistema de control de carga, inspección de equipaje, sistemas de vigilancia inteligente, aduanas e inmigración, sistemas de detección de explosivos y sistemas de inspección de pasajeros.

- **Sistemas de IT y comunicaciones:** Engloba los sistemas de comunicaciones, tales como sistemas de gestión de espectro de radio, LAN, VPN, WAN, wifi de pasajeros, sistemas de comunicación pasajero-aerolínea y sistemas de comunicación aire-satélite, sistemas de localización (GIS, GPS/EGNOS/SBAS), bases de datos, equipos informáticos (*hardware* y *software*), red móvil y aplicaciones, datos en la nube y servicios de aplicaciones, Centro de Operaciones de Seguridad (SOC) —incluido el equipo de respuesta a incidentes informáticos—, supervisión de registros y notificación de eventos y sistemas de gestión de la seguridad de la red.

Figura 2. Grupos principales de activos en aeropuertos



Fuente: Adaptado de ENISA (2016). *Securing Smart Airports.*

Todos los activos mencionados resultan importantes para la correcta operación de un aeropuerto. No obstante, tras una revisión con expertos del sector que identificaron los cinco activos más importantes en materia de ciberseguridad, ENISA propone como prioritarios los siguientes:

1. Facturación y embarque de pasajeros.
2. Sistema de manipulación de equipaje.
3. Sistema de Gestión del Tráfico Aéreo (ATM por sus siglas en inglés) y ayudas a la navegación.
4. Sistema de procesamiento de pasajeros de uso común (CUPPS, por sus siglas en inglés).[9]
5. Sistemas de comunicaciones, LAN y VPN.

2.1.1.2. Amenazas

A partir de la selección antes mencionada, los expertos han definido los siguientes escenarios de ataque como los más relevantes en la actualidad:

- **Manipulación de los sistemas de registro automático en aeropuertos:**

  Este tipo de sistema está cada vez más presente en los aeropuertos. Son sistemas que se encuentran en la terminal y, por tanto, son físicamente accesibles, por lo que son susceptibles de ser manipulados físicamente, alterando algunos de sus componentes, accediendo al ordenador que integran o modificando la interfaz de usuario. Todo ello puede derivar en el acceso a datos personales de los pasajeros cuando están haciendo el registro, la emisión de tarjetas de embarque inválidas, o incluso el acceso a otros sistemas o repositorios de datos con los que se comuniquen las máquinas. Las consecuencias pueden ser, además de provocar inconvenientes a los pasajeros o retrasos, otros riesgos de seguridad derivados del embarque de pasajeros desconocidos en los vuelos o robo de datos sensibles.

- **Ataque de red a sistemas de equipaje:**

  Para realizar la gestión y manejo del equipaje, normalmente se hace uso de sistemas SCADA. Este es un tipo de sistema muy extendido para el control de actividades y flujos en los sistemas industriales y, dado su alto nivel de conectividad con los elementos y dispositivos que monitorizan el proceso, hace que se vean expuestos a muchos vectores de ataque. Vulnerabilidades como una mala configuración del sistema, la no actualización de parches de seguridad, la instalación de *malware*

9 CUPPS: gama de servicios, especificaciones y estándares promulgados para permitir que múltiples aerolíneas, proveedores de servicios u otros usuarios compartan el registro físico o en puerta de embarque, sea de forma simultánea o consecutiva. (https://www.iata.org/contentassets/1dccc9ed041b4f3bbdcf8ee8682e75c4/cupps-rfp-guidance-document-july_2018.pdf).

o el uso de *ransomware* contra operadores de servicios en tierra son algunas de las que se pueden mencionar. Estas vulnerabilidades pueden manifestarse en el compromiso del sistema de control de manejo y gestión de equipajes y derivar en interrupciones en el proceso de embarque o desembarque de las aeronaves, en la carga de ciertos elementos a través del ocultamiento de productos ilegales (por ejemplo, drogas, explosivos, etc.) o en el hurto organizado de carga. Por ejemplo, en el año 2022, el aeropuerto de Zúrich experimentó retrasos y disrupciones a causa de un ataque de *ransomware* a un operador de carga y servicios en tierra.[10]

- **Intercepción de comunicaciones entre aeronaves, aeropuertos y control de tráfico y aerolíneas:**

  Las aeronaves utilizan el Sistema de Vigilancia Dependiente Automática (ADS-B por sus siglas en inglés) para transmitir sus posiciones en función de los instrumentos de navegación a bordo y la tecnología GPS. Este sistema se utiliza para apoyar la vigilancia y garantizar que las aeronaves estén suficientemente separadas para evitar accidentes o colisiones, pero no está encriptado ni autenticado, lo que posibilita la falsificación o la interferencia en las comunicaciones, con la inyección de datos falsos o la inhabilitación del envío o la recepción de mensajes, lo que puede suponer un problema de seguridad en vuelos y aterrizajes, al disponer de información no fiable.

2.1.2. Transporte marítimo

2.1.2.1. Activos

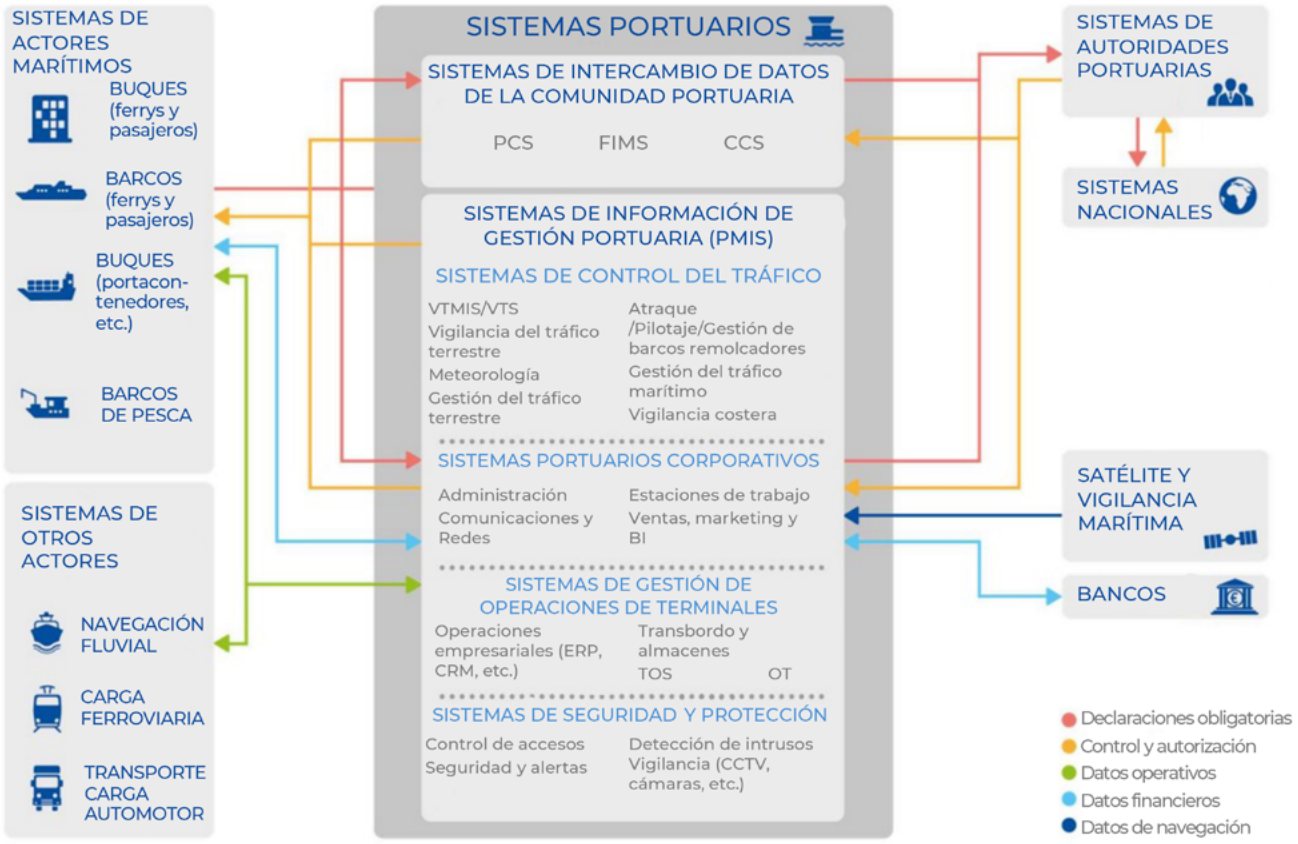
El ecosistema del transporte marítimo también es complejo e involucra un gran número de entidades. El puerto se sitúa en este ecosistema como el elemento central, pero cada puerto adecúa su infraestructura y servicio al contexto en el que se sitúa, pudiendo especializarse en aspectos de pesca, turismo, transporte de mercancías, materias primas, etc. Esta infraestructura global comprende la infraestructura marítima (dársenas, muelles, espigones, etc.), la infraestructura de distribución (carreteras internas, vías férreas o pasarelas, etc.) y, finalmente, los edificios y terminales gestionados y mantenidos por las autoridades portuarias. Normalmente, estas instalaciones son explotadas por operadores privados para realizar las diferentes actividades que se realizan en el puerto, gestionando y manteniendo la superestructura necesaria para ello (grúas, silos, etc.).

Según el informe de ENISA para el sector portuario, los servicios del puerto pueden agruparse en siete categorías: atraque; carga y descarga de buques; estancia y almacenamiento temporal; transferencia y distribución; apoyo a los anteriores; seguridad; y autoridades (aduanas, guardacostas, controles sanitarios, prevención de contaminación, etc.).

Esta complejidad y diversidad en cuanto a la especialización de cada puerto hace que los sistemas IT y OT que podemos encontrar en cada uno sean diferentes. ENISA propone un modelo de referencia de alto nivel en el que se presentan tanto los sistemas del propio puerto como los de las terceras partes (ENISA, 2019).

10 Ransomware attack on Swissport causes delay at Zurich Airport.

Figura 3. Modelo de referencia de alto nivel de los sistemas del puerto



Fuente: ENISA (2019). *Good practices for cybersecurity in the maritime sector.*

Todos estos servicios son soportados por diferentes activos que se presentan en las siguientes categorías:

- **Infraestructura fija:** Incluye edificios, sistemas de suministro de energía, conectividad de transportes (con el mar, pero también como plataforma intermodal en la que pueden existir conexiones con canales, vías férreas, carreteras, etc.), sistemas de tratamiento de residuos y sistemas de seguridad y protección (torre de control, instalaciones médicas, extinción de incendios, etc.).

- **Infraestructura móvil:** Compuesta por vehículos especiales terrestres, buques de servicio específicos en el agua, boyas inteligentes y barreras flotantes físicas (de protección de embarcaciones o contención de fugas).

- **Redes y sistemas OT:** Abarca sistemas de control industrial para la gestión de accesos, atraque de buques y operación de infraestructuras. Estos incluyen elementos e infraestructuras industriales como: Controlador Lógico Programable (PLC por sus siglas en inglés), Unidad Terminal Remota (RTU por sus siglas en inglés), MES, Sistema de Control Distribuido (DCS por sus siglas en inglés), SCADA, Interfaz Hombre-Máquina (HMI por sus siglas en inglés), SIS, etc. Todos ellos se complementan con las propias redes que utilizan protocolos industriales y componentes de comunicaciones tales como *switches*, puntos de acceso inalámbricos, etc.

- **Dispositivos finales OT:** Esta es una categoría amplia, ya que muchos de los servicios que se prestan requieren de un equipamiento o de dispositivos finales de operación. Podemos encontrar dispositivos necesarios para:

  – El atraque de buques o su carga y descarga, tanto de personas como de mercancías. Abarca los sistemas de manipulación (grúas, cintas, transportadores, rampas para pasajeros, etc.), sistemas de seguimiento y control (lectores RFID, básculas, contadores de líquidos, etc.), escáneres de vehículos y personas, entre otros.

  – Las áreas portuarias destinadas al almacenamiento temporal, que pueden estar especializadas para guardar mercancías con características especiales (peligrosas, refrigeradas, vehículos, etc.) y disponer de sistemas de transporte interno necesarios para mover la carga (camiones), además de los equipos de almacenamiento (como tanques o estanterías de palés).

  – La conectividad *hinterland*, con dispositivos necesarios para el control de la entrada y salida de mercancías o pasajeros, y transporte a otros modos. Por ejemplo, se tienen sistemas de control e inspección (escáneres o rayos X), equipos de control de acceso (lectura de matrículas, tarjetas o códigos de barras), etc.

  – Específicos del diseño de la instalación portuaria, como puede ser el vallado o equipamiento determinado de seguridad y protección.

- **Sistemas IT:** En el puerto existen diferentes sistemas de gestión de la información, entre los que se destacan los siguientes (en función de los servicios especializados que prestan):

  – Sistemas corporativos portuarios y financieros, Planificación de Recursos Empresariales (ERP por sus siglas en inglés), mercadeo, sistemas de gestión de recursos humanos, etc.

  – Sistemas de Comunidad Portuaria o *Port Community System* (PCS), normalmente administrado por la autoridad portuaria, al que acceden los actores del ecosistema portuario. Son plataformas de intercambio de información logística y, a veces, aduanera.

  – Sistemas de Comunidad de Carga o *Cargo Community System* (CCS), que permiten el intercambio de información entre actores de logística relacionada con la carga, su contenido, la localización de los contenedores, las horas de movimiento de la mercancía, etc. En este caso, el sistema es administrado generalmente por empresas privadas a cargo de las operaciones portuarias.

  – Sistemas de gestión de operación en terminales, Servicio de Tráfico de Buques (VTS por sus siglas en inglés) y Sistemas de Información para la Gestión del Tráfico de Buques (VTMIS por sus siglas en inglés).

  – Sistemas de gestión de atraques, utilizados por las autoridades para gestionar la seguridad en el amarre, con la asignación de puestos de atraque que conectan con datos meteorológicos o ambientales.

- **Dispositivos finales IT:** Computadoras, dispositivos móviles y componentes de comunicación y redes (servidores, sistemas de radio, redes y protocolos IT, *switches*, *routers*, etc.).

- **Información y datos:** incluye datos financieros y comerciales, datos de navegación, declaraciones obligatorias para los barcos (según regulación internacional), datos de control y autorización de movimiento de buques y carga o datos operacionales compartidos.

- **Sistemas de seguridad:** Entre estos activos destacan los Circuitos Cerrados de Televisión (CCTV), Sistema de Detección de Intrusiones (IDS por sus siglas en inglés) o detección de anomalías, los sistemas de monitorización del tráfico, de inspección de sistemas, de control de acceso, de identificación y autenticación (reconocimiento facial, sistemas biométricos, etc.).

Además de los sistemas, es necesario considerar la parte del personal y grupos de interés. Esto incluye desde los pasajeros y el público en general hasta los diferentes profesionales que trabajen para la autoridad portuaria o en las compañías que se ocupan de las terminales o la tripulación de los barcos. Este factor humano también debe ser considerado en los análisis de vulnerabilidades, ya que puede contribuir, o no, al riesgo cibernético.

2.1.2.2. Amenazas

La catalogación de activos y servicios en el ecosistema marítimo y la revisión de las posibles amenazas a las que se enfrentan han llevado a los expertos del sector a definir los siguientes principales escenarios de ataque:

- **Datos críticos comprometidos para robo de carga o tráfico ilegal**

  Este tipo de ataques es considerado como una Amenaza Persistente Avanzada (APT por sus siglas en inglés), es decir, un conjunto de acciones sigilosas perpetradas en el tiempo por organizaciones delictivas con objetivos determinados. Un ejemplo de este tipo de ataques ocurrió en una de las terminales del puerto de Amberes en Bélgica (Robertson y Riley, 2015) con el fin de facilitar el tráfico de substancias ilícitas. Normalmente, incluyen tácticas tanto de ingeniería social (*phishing* para el robo de credenciales e identificación de personal que usa los sistemas de gestión de la mercancía), como tácticas técnicas en las que los atacantes instalan componentes a través de los cuales pueden escanear las redes para obtener información o explotar vulnerabilidades de determinados sistemas como los Sistemas de Comunidad de Carga (CCS), donde se encuentra la información de los contenedores, como su carga, localización o fecha de recogida, lo que les permite obtener conocimiento anticipado de cuándo y dónde interceptar un contenedor y planificar así su operativo criminal.

- **Bloqueo de las operaciones en el puerto**

  Al cifrar diferentes sistemas y dispositivos (incluidos los respaldos) a través de *ransomware*, los atacantes pueden paralizar total o parcialmente las operaciones

portuarias. Este fue el caso en 2017, cuando las operaciones de Maersk en Rotterdam fueron afectadas por el *malware* NotPetya (Shoorbaje, 2017). Además de las pérdidas económicas que derivan de la necesidad de gestionar y operar manualmente durante un tiempo —lo que provoca retrasos en la carga de muchos clientes—, el impacto puede llevar a que ciertos sistemas de seguridad se vean afectados y comprometan la integridad física del personal portuario.

- **Manipulación o robo de datos de PCS**

  En estos sistemas, habitualmente encontramos una diversidad de agentes que interactúan y que están expuestos a la necesidad de abrirse a comunicaciones con terceros. La diversidad de los sistemas implicados en estos procesos hace que las vulnerabilidades puedan ser muy variadas, desde problemas en el diseño e implementación de aplicaciones web hasta la falta de mecanismos para la autenticación en la conexión a determinados servicios. Estos ataques, además de interrumpir o entorpecer las operaciones portuarias, pueden bloquear el acceso a elementos críticos, como la cadena de suministro de combustibles, tal como sucedió en un reciente ataque a puertos europeos (Associated Press, 2022).

- **Ataque a la red OT del puerto**

  Al igual que en otras instalaciones industriales, en el puerto encontramos diferentes Sistemas de Control Industrial (ICS) en cuyo diseño y operación no se han tenido debidamente en cuenta los aspectos de ciberseguridad. En algunas ocasiones, las vías de entrada provienen de la red IT. En otras, se conectan dispositivos USB a un elemento de la red OT para su actualización. El impacto al comprometer este tipo de activos OT puede llevar al control remoto o al malfuncionamiento de, por ejemplo, los sistemas de la infraestructura móvil, lo que puede ocasionar la parálisis de la operación en el puerto, accidentes, daños del personal y problemas de contaminación ambiental.

2.1.3. Transporte ferroviario

2.1.3.1. Activos

El transporte ferroviario, aunque menos presente que otros modos de transporte en la región de América Latina y el Caribe (ALC), también debe ser tomado en cuenta en un análisis de activos, tanto desde las líneas de carga que existen en algunos países como en los sistemas de transporte de pasajeros por rieles, entre los que se encuentran sistemas masivos de transporte público en ciudades como metros o tranvías.

Entre los operadores de servicios esenciales en el sector del transporte ferroviario, se identifican dos tipos de empresas: las gestoras de infraestructuras, encargadas de la gestión y el mantenimiento de la infraestructura ferroviaria, incluida la gestión del tráfico, el control-mando y señalización; y las ferroviarias, públicas o privadas, cuya actividad principal es la prestación de servicios para el transporte de mercancías o pasajeros por ferrocarril, con el requisito de que la empresa garantice la tracción.

ENISA propone en sus informes para el sector (ENISA, 2020b, 2021) una taxonomía para identificar y seleccionar los activos y servicios con cinco categorías, para cada una de las cuales se identifican los diferentes sistemas:

- Sistemas de preoperaciones
  - Elaboración de horarios en cada línea y preparación de las listas de recursos (activos y personal).
  - Venta y distribución de billetes y reservas, y otras relaciones con los clientes, como canales de atención al cliente, tarjetas de fidelización, mercadeo, etc.
  - Asignación de red: sistemas que permiten a las empresas ferroviarias reservar la infraestructura (corredores) para operar e informar de cualquier característica especial de los trenes o sus cargas.
  - Adquisición de activos: sistemas que permiten a las organizaciones contabilizar sus activos (infraestructura o trenes, por ejemplo), adquirir nuevos activos y gestionar la logística.
- Operaciones
  - Sistemas de señalización para dirigir el tráfico ferroviario, tales como sistemas de enclavamientos electrónicos, sistemas de pasos a nivel, etc.
  - Comando y control: utilizados para permitir el movimiento de trenes; por ejemplo, Control Automático de Trenes (ATC), Supervisión Automática de Trenes (ATS) o sistemas *Energy Traction*.
  - Sistemas auxiliares, como sistemas de energía, HVAC (Calefacción, Ventilación y Aire Acondicionado) y sistemas de iluminación para emergencias.
  - Comodidad y servicios para los pasajeros, tales como sistemas de información, climatización e iluminación, ascensores y escaleras mecánicas, etc.
  - Sistemas de telecomunicaciones, tales como sistemas de radio dedicados a la señalización, sistemas alámbricos para comunicaciones en red, comunicaciones de voz, etc.
- **Seguridad, protección y mantenimiento:** incluyen sistemas de control de acceso, videovigilancia, detección de incendios, acreditación de personal y mantenimiento de activos para las empresas gestoras y operadoras de servicios.
- **Sistemas corporativos** (correo electrónico, finanzas, recursos humanos, comunicaciones, etc.) y sistemas de desarrollo, que abarcan todo lo que se utiliza para desarrollar el emprendimiento. Incluyen los sistemas de licitación para que el gestor de la infraestructura o la empresa ferroviaria responda a las licitaciones para la explotación de trenes, la gestión de infraestructuras, la investigación y la ingeniería.

En cada una de estas categorías de sistemas se identifican con más detalle diferentes tipos de activos, que se pueden clasificar en: IT; OT; redes y comunicaciones; o sistemas provistos por proveedores. También se debe considerar como activo el equipo físico que se encuentra tanto en la infraestructura como en la vía (edificios, raíles, catenarias, etc.) y a bordo (trenes, vagones, iluminación y HVAC, etc.).

En una encuesta a más de 29 operadores de servicios esenciales de 21 países de la UE, se identificaron los sistemas de información críticos que respaldan dichos servicios (ENISA, 2020). En general, los sistemas más críticos señalados por todos los tipos de operadores son los sistemas de seguridad y protección y los sistemas de la categoría de operaciones, encargados de la señalización, comando-control y telecomunicaciones. Desde el punto de vista del gestor de la infraestructura ferroviaria, la amenaza más crítica es un ciberataque a estos sistemas de señalización o a un sistema de control automático de trenes, ya que podrían provocar un accidente de tren con sus posibles consecuencias para la seguridad humana y la operación del sistema (ENISA, 2021).

En el sector ferroviario, los sistemas OT suelen ser más vulnerables que los sistemas IT. Ello se debe, en parte, a que son sistemas que tienen un ciclo de vida largo, de varias décadas, y que, en muchos casos, fueron diseñados y construidos hace tiempo. Esto dificulta su actualización con los requisitos actuales de ciberseguridad y su integración. Además, estos sistemas suelen estar distribuidos por la red férrea, lo que dificulta un monitoreo integrado de la ciberseguridad.

2.1.3.1. Amenazas

Teniendo en cuenta lo expresado y cuáles son los activos más críticos, se definen los siguientes escenarios, basados en algunos incidentes conocidos del sector:

- **Comprometer un sistema de señalización o un sistema de control automático del tren.**

  En este caso se plantea la posibilidad de que el atacante diseñe y construya algún dispositivo o *software* mediante el cual inyecte información falsa al sistema de señalización, lo que puede llevar a una interrupción del servicio o incluso a un siniestro del tren. Es necesario un conocimiento técnico profundo, por lo que *a priori* no es un escenario probable. Un incidente de esta clase ocurrió en 2008 en la ciudad de Lodz, en Polonia, en el que un atacante logró *hackear* el sistema de tranvías, causando 12 heridos (Altaf *et al.*, 2019).

  – **Sabotaje de los sistemas de supervisión de tráfico**

    Este sabotaje se ejecuta a través de *malware* para sistemas de control industrial, que puede ser introducido vía *phishing* o por el uso de dispositivos USB o similares en sistemas OT. El *malware* permitiría manipular de forma remota la memoria del sistema para inyectar órdenes en las pilas de ejecución de los programas de los sistemas de supervisión de tráfico con el fin de interrumpir o modificar su flujo habitual de ejecución.

– Ataques de *ransomware*

  Los ataques de *ransomware* en sistemas ferroviarios pueden causar desde la disrupción de servicios hasta la paralización de sistemas enteros. Un incidente de esta clase ocurrió en mayo de 2017, cuando la infraestructura ferroviaria de Deutsche Bahn, de Alemania (Gompel, 2017), se infectó con el *ransomware* WannaCry, lo que provocó que aparecieran mensajes de rescate en las pantallas de información de la estación, con el fin de exigir un pago a cambio de recuperar la información y el control del sistema.

– Robo de datos personales de clientes

  Los datos robados de sistemas de gestión de reservas pueden ser posteriormente vendidos en la internet oscura, para ser usados en estafas u otras actividades maliciosas. Ejemplo de ello fueron los ataques sufridos por Rail Europe North America (RENA) (Banerd, 2018) y por la plataforma oficial de reservas en línea de China Railway (*Cyware Hacker* News, 2020). Esto puede derivar de una debilidad en la protección de determinados repositorios de información por parte de un proveedor, tal como ocurrió en 2020, cuando las direcciones de correo electrónico y los detalles de viaje de unas 10 000 personas que usaron wifi gratuito en las estaciones de tren del Reino Unido se expusieron al no estar protegidos por contraseña (Kleinman, 2020).

2.1.4. Transporte terrestre carretero: urbano e interurbano

2.1.4.1. Activos

Ante la creciente digitalización del transporte, dos tecnologías presentan, junto con sus beneficios, nuevas vulnerabilidades cibernéticas. La primera de ellas corresponde a los ITS[11] —como se denomina a la aplicación combinada de TIC en los sistemas de transporte— y se implementa en infraestructura, sensorización, señalización, esquemas de recaudo y vehículos, asegurando la conectividad para el intercambio de información y la interacción con los distintos tipos de usuarios de servicios o información digitales (Crotte *et al.*, 2017). La segunda corresponde a los vehículos autónomos, como se denomina a los vehículos con algún grado de autonomía e intervención de un conductor humano. La Sociedad de Ingenieros Automotrices (SAE) clasifica la automatización de los vehículos en seis niveles, de 0 a 5. En el nivel 0, el vehículo no es autónomo y todas las funciones de conducción requieren de la intervención de un conductor; en los niveles 4 y 5, el vehículo puede responder de forma autónoma a todas las situaciones de conducción (Calatayud *et al.*, 2020). Ambas tecnologías son usadas tanto en entornos urbanos, para el transporte público y particular, como en vías interurbanas y otras carreteras.

11 Por ITS se entienden los sistemas inteligentes de transporte definidos en el glosario, que también son aplicados en los sectores aéreo, marítimo y ferroviario. En esta sección, abarcan los modos de transporte terrestre de carga y pasajeros, así como las infraestructuras que los respaldan.

- Sistemas Inteligentes de Transporte

El Departamento de Transporte de Estados Unidos trabaja en un programa de investigación en ciberseguridad en ITS, en el cual se define una Arquitectura de Referencia para el Transporte Inteligente y Cooperativo (ARC-IT por sus siglas en inglés), que provee de un marco común a los diferentes agentes involucrados en la comunidad de los ITS. Los componentes se organizan en cuatro perspectivas diferentes.

Figura 4. Visión general de arquitectura ARC-IT

Fuente: Adaptado de *Architecture Reference for Cooperative and Intelligent Transportation*, United States Department of Transportation.

En la perspectiva del negocio, se considera la perspectiva organizacional que identifica los diferentes tipos de personas y organizaciones involucradas en el ecosistema y encargadas de planificar, desarrollar, mantener o incluso usar los ITS. La perspectiva funcional reconoce los procesos y flujos de datos que soportan los requisitos funcionales del sistema. La perspectiva física permite encontrar la definición de los objetos físicos, sistemas y dispositivos que proveen las diferentes funcionalidades. Finalmente, la perspectiva de las comunicaciones define los estándares y perfiles que especifican cómo se puede compartir información de forma segura entre los diferentes objetos físicos.

En la figura observamos lo que se denominan *service packages*, o paquetes de servicio, que abarcan las cuatro perspectivas de los servicios específicos ITS. Estos paquetes se agrupan según diferentes áreas:

- **Construcción y mantenimiento:** monitorización, mantenimiento y mejora de la infraestructura, es decir, de las vías y su equipamiento.

- **Gestión de tráfico:** gestión de la circulación de todo tipo de vehículos, así como de los peatones que utilizan la red de transporte. Contempla los sistemas de monitoreo de estado de las vías para la recolección o toma de decisiones en tiempo real.

- **Transporte público:** sistemas necesarios para gestionar, operar y mantener el transporte público, incluyendo gestión de flotas de vehículos, sistemas de información a usuarios y sistemas de pago electrónico multimodal.

  - **Gestión de estacionamiento:** vigilancia y gestión del espacio de estacionamiento y los sistemas de pago electrónico, incluyendo las zonas de aparcamiento públicas.

  - **Operaciones de vehículos comerciales:** gestión y optimización de flotas de vehículos comerciales, transportes intermodales y movimiento de carga.

  - **Seguridad pública:** gestión de emergencias o incidentes en la red de transporte por parte de agencias como la policía, los bomberos, etc., en coordinación con las agencias de transporte.

  - **Información a viajeros:** sistemas que proporcionan información estática y dinámica sobre la situación de la red de transporte a los usuarios.

  - **Gestión de datos:** sistemas que pueden ser utilizados por agencias de transporte u otro tipo de organizaciones para el análisis, la planificación y el control de los sistemas de transporte. Estos datos suelen ser captados por sensores conectados a infraestructuras.

  - **Transporte sostenible:** sistemas para minimizar el impacto medioambiental, como el monitoreo de emisiones, la gestión de estaciones de carga eléctrica o la gestión de zonas de bajas emisiones en la ciudad.

  - **Seguridad de vehículos:** sistemas que mejoran la seguridad, protección y eficiencia en vehículos automatizados, conectados, como sistemas de alertas V2V, consciencia situacional o infraestructura de control de crucero adaptativo, servicios de soporte de seguridad con información de incidencias meteorológicas, etc.

- Vehículo automatizado y conectado

  Este tipo de vehículos inteligentes incluye cada vez más sistemas de ayuda y automatización para la conducción, que se componen de multitud de subsistemas (cámaras, sensores acústicos, radar o LiDAR, etc.) y miles de líneas de códigos que implementan los diferentes niveles de automatización de la SAE. Es importante

tener una visión general de cómo está constituida la estructura de red dentro de un vehículo moderno. Los denominados *sistemas embarcados* se distribuyen por controladores de dominio, que normalmente están clasificados en propulsión, chasis, *infotainment*[12] y carrocería. A pesar de que cada uno de ellos puede utilizar un tipo de bus de comunicaciones concreto y estar físicamente aislado, las Unidades de Control Electrónico (ECU) de diferentes dominios pueden comunicarse a través de una *gateway* o elemento central. Esta característica supone que un posible ataque a través del dominio de *infotainment* podría llegar a tomar el control de la ECU del motor y, como consecuencia, generar un posible accidente, lo que pondría a sus ocupantes en grave peligro, o bien causar perjuicio de otras maneras, deteniendo los vehículos, bloqueando el tráfico o llevando a los usuarios a un destino distinto con fines delictivos.

En la siguiente figura se muestran los activos que componen los diferentes dominios de un vehículo inteligente.

Figura 5. Activos y funciones de los vehículos inteligentes

Fuente: ENISA (2017). *Cyber Security and Resilience of Smart Cars. Good practices and recommendations.*

12 Por *infotainment* se conoce al conjunto de servicios de información y entretenimiento del vehículo, tales como los sistemas de audio, radio, CD, MP3, *bluetooth*, navegadores, conexión a internet, etc.

2.1.4.2. Amenazas

Con infraestructuras y vehículos cada vez más automatizados, inteligentes e interconectados, se incrementa la superficie de ataque y existe una mayor probabilidad de que algún atacante explote una vulnerabilidad de todos los sistemas que componen estos ecosistemas digitales.

- **Transporte por carretera interurbana**

  La infraestructura ITS puede estar expuesta en carreteras y vías que no cuenten con supervisión, lo que hace que sea accesible físicamente y facilite ataques, por ejemplo, a través de puertos de comunicación expuestos (USB, PS2, etc.) que puedan infectar los sistemas con *software* malicioso. Las redes de comunicación entre vehículos e infraestructura son un componente importante de las carreteras inteligentes, las cuales utilizan una serie de elementos tecnológicos para recopilar y analizar datos en tiempo real, facilitando la comunicación bidireccional de vehículos e infraestructuras y permitiendo informar a los usuarios de manera ágil. Aunque estas redes tienen la capacidad de mejorar la seguridad vial y disminuir la congestión vehicular mediante el intercambio de información crítica, son susceptibles de ciberataques como información falsa, MitM y Denegación de Servicio Distribuido (DDoS). Estas amenazas buscan engañar a los vehículos y elementos que componen la red, impidiendo la identificación o modificación de los mensajes que se reciben o comprometiendo la disponibilidad de determinados sistemas, lo que puede impactar en la seguridad vial.

  También se observan ataques como los realizados a las señales de tráfico (Greenberg, 2020) o los sistemas de señalización o información al viajero, en los que se han producido modificaciones en los mensajes que se muestran en señales luminosas de la carretera (WAQAS, 2016).

  En el ecosistema de los actores del transporte por carretera, alrededor de los sistemas de gestión de carga, se pueden encontrar ataques con el objetivo de impedir las operaciones, como el que le sucedió a la empresa FedEx (Shoorbaje, 2017); o ataques a los sistemas de cobro de peaje electrónico, como el sufrido en Puerto Rico en 2022 (Associated Press, 2022).

- **Vulnerabilidades en vehículos**

  Con vehículos cada vez más inteligentes, las vulnerabilidades aumentan. Teniendo en cuenta que un vehículo puede llegar a tener decenas de ECU —hasta 100 en vehículos de gama alta modernos—, la superficie de ataque es bastante elevada, y, efectivamente, se ha visto que es posible acceder a casi cualquiera de los sistemas embarcados del vehículo, como ya fue demostrado en 2015 (Drozhzhin, 2015).

  El uso de tecnología inalámbrica en un contexto de vehículos inteligentes y conectados (Vehículo a Vehículo, Vehículo a Infraestructura, Vehículo a Todo [V2V, V2I o

V2X]) aumenta las vulnerabilidades a ataques de *spoofing*[13] o *sniffing*[14] en las redes de comunicaciones, e incluso puede ser un punto de entrada al bus de la red CAN[15] del vehículo, comprometiendo la integridad de los mensajes que se envían y las funciones que deben realizar los sistemas. Todo ello puede tener impacto en dos aspectos clave: la seguridad y la privacidad de los usuarios.

En resumen, algunos de los escenarios de ataque que podrían presentarse en contextos donde existen vehículos automatizados son los siguientes:

- Manipulación de comunicaciones en el bus CAN a través de acceso físico. Si se dispone de acceso físico al vehículo, por ejemplo, a través del puerto de diagnóstico ODB-II, el acceso a la red CAN es viable. Dado que este protocolo carece de protección de seguridad, es posible realizar ataques de tipo MitM y modificar los mensajes (ENISA, 2017).

- Ataques remotos para obtener acceso no autorizado a los sistemas o la red del vehículo. La posibilidad de este tipo de ataques fue demostrada en el 2015 en un experimento llevado a cabo por los investigadores de ciberseguridad Chris Valasek y Charlie Miller, que pudieron *hackear* remotamente un vehículo. Como resultado, se retiraron más de 1,4 millones de vehículos de circulación (ENISA, 2017).

- Instalación no autorizada de *software*, tanto por parte de usuarios legítimos como de otros que pueden hacer uso del equipamiento de diagnóstico de los vehículos. En este caso, el objetivo sería modificar el *firmware* de una ECU para, por ejemplo, *tunear* o personalizar el coche o eludir algunos comportamientos de fábrica.

- Uso no autorizado de sistemas y dispositivos. Uno de los más habituales es el hackeo de los sistemas de encendido por botón o sin contacto que disponen cada vez más vehículos.

- Fuga de información. La información de datos que gestionan las ECU y los sistemas del vehículo, como, por ejemplo, el contenido relevante sobre localización o pagos, puede ser robada, lo que compromete la privacidad de los usuarios del vehículo.

- Los ataques de *ransomware* también han afectado áreas del sector orientadas al turismo, como las empresas de alquiler de vehículos. En la primavera de 2022, la compañía alemana de alquiler de coches Sixt sufrió un ciberataque que afectó sus operaciones y se cerraron todos los servicios no esenciales. Se supuso que los grupos de *ransomware* se enfocaron en una organización como Sixt debido a la inminente temporada turística (Page, 2022).

13 *Spoofing:* suplantación de identidad.

14 *Sniffing:* robo o interceptación de datos mediante captura del tráfico de la red.

15 Bus CAN *(Controller Area Network)*: protocolo de comunicaciones desarrollado por Bosch para la transmisión de mensajes entre los microcontroladores y dispositivos que se incluyen en un vehículo.

También debe tenerse en cuenta el incremento de la superficie de ataque que surge del uso de herramientas de Inteligencia Artificial. Un ejemplo representativo son los ataques a sistemas de visión computacional que incorporan los vehículos autónomos (Robbins, Daggett y Houst, 2026).

- **Transporte público inteligente y amenazas a agencias de transporte público**

El Transporte Público Inteligente (IPT) es la parte específica del transporte urbano público y masivo dentro de los ITS. El tema se aborda en general desde una perspectiva urbana, en la cual existen condiciones de mercado e infraestructura de conectividad y física necesarias para permitir que el transporte público se vuelva inteligente. Desplegar sistemas IPT implica la integración exitosa de tecnologías ciberfísicas e infraestructura urbana. Esto implica la vinculación de infraestructuras (físicas) y procesos (digitales) que no siempre están bien integrados (ENISA, 2016a). Ya en 2016, ENISA identificó tanto los activos críticos como las posibles amenazas a los sistemas de transporte público inteligente, con una serie de recomendaciones clave (ENISA, 2016a).

Los activos del transporte público inteligente son multifacéticos y combinan varios componentes y funciones en una sola unidad. Por ejemplo, una estación de bus deja de ser solo una infraestructura física para resguardar pasajeros y pasa a ser también una interfaz de información al usuario, un captador de datos o un proveedor de wifi. En el ITP, los activos siempre cuentan con elementos físicos y digitales, y la barrera entre lo cibernético y lo físico se borra. La naturaleza del ITP también lleva a que los activos individuales no solo se interconecten constituyendo sistemas, sino que de esos sistemas deriven otros suprasistemas.

En lo que atañe a la seguridad, los activos ITP, al ser ciberfísicos, están expuestos a una serie de amenazas, tanto físicas como cibernéticas. En consecuencia, la ciberseguridad y la seguridad física resultan interdependientes, dado que los ataques pueden afectar el funcionamiento físico de los activos habilitados. Además, la integración del IPT en el contexto de una ciudad inteligente desdibuja los límites y responsabilidades entre un operador de transporte y el resto de la ciudad. Esta falta de claridad puede afectar significativamente la forma en que se llevan a cabo las evaluaciones de riesgos de los sistemas de transporte.

Otra de las principales amenazas en el sector del transporte público surge, no tanto de la perspectiva de las infraestructuras conectadas, sino desde las agencias de transporte público. Estas recaban la mayoría de los incidentes en el subsector, y son generalmente víctimas de *ransomware*, que bloquea sus operaciones, pero también de robo o fuga de datos de sus usuarios y empleados. En junio de 2023, por ejemplo, Transport for London, la empresa de transporte público de la ciudad de Londres, fue afectada por un ataque de *ransomware* que apuntaba a robar datos de sus empleados y usuarios (Vallance, 2023). En Vancouver, en 2021, un ataque de *ransomware* que apuntaba a extorsionar al sistema de transporte público por más de siete millones de dólares paralizó los sistemas de pago de la empresa y afectó los sistemas de seguimiento de rutas (Hurst, 2021).

2.2. Aspectos normativos y regulatorios a nivel global

Para contrarrestar amenazas crecientes en el sector del transporte, y de manera general, muchos países han creado marcos regulatorios y definido estándares para promover la ciberseguridad. Estas medidas buscan enmarcar las acciones de sus Gobiernos y promover buenas prácticas en el sector privado. Existen diversos ejemplos de buenas prácticas provenientes de la UE, Estados Unidos y otras regiones, que marcan la pauta y proveen un *corpus* robusto de referencias para regular y difundir la ciberseguridad en el sector del transporte. Estas regulaciones normalmente hacen referencia a aspectos como:

- Los derechos de privacidad de los individuos sobre sus datos: es habitual que se publiquen regulaciones que gestionen el derecho que tiene cualquier persona a decidir qué datos personales desea compartir y cuáles desea mantener resguardados para proteger su intimidad.

- La realización de ciertas actividades o funciones que deben ser ejecutadas por operadores de infraestructuras críticas: en muchos casos se impone o promueve la aplicación de estándares o marcos de gestión de la seguridad cibernética para gestionar el riesgo cibernético y realizar actividades para identificar, proteger, detectar, responder o recuperarse de incidentes de ciberseguridad.

- La necesidad de implementar o incluir certificaciones de ciberseguridad en determinados productos o servicios, sobre todo en aquellos que se consideran relevantes para la ejecución de funciones esenciales del operador.

El Anexo I contiene una tabla con el compendio de las regulaciones más relevantes.

2.2.1. Unión Europea

La UE cuenta con diferentes directivas y regulaciones que se aplican a los diversos modos de transporte, promoviendo un transporte más sostenible, eficiente, interoperable y seguro. Dispone de dos instrumentos regulatorios a través de los cuales gestiona los requisitos normativos en la UE y sus diferentes Estados miembros.

Por un lado, están las directivas, que son normas que vinculan a todo Estado miembro destinatario en cuanto al resultado que hay que alcanzar, dejando a las instancias nacionales la facultad de escoger la forma y los medios para ello. Es decir, cada Estado miembro tiene que cumplir los fines, pero los debe adaptar a su marco legal, teniendo la libertad de elaborar la legislación interna para su cumplimiento. Por otro lado, están los reglamentos, que tienen alcance general y son obligatorios en todos sus elementos y directamente aplicables en cada Estado miembro.

A nivel regulatorio, en temas de ciberseguridad, se aplican regulaciones como la GDPR (*General Data Protection Regulation*), destinada a proteger la privacidad de los datos personales, que en este caso pueden ser tanto del personal de las empresas del sector como de los clientes y usuarios finales de los servicios de transporte. Por otra parte, existen aspectos regulatorios que conciernen a estas entidades consideradas como infraestructura crítica o esencial, en los que juegan un papel importante la Directiva CER y la Directiva (UE) 2022/2555 (conocida como NIS2), que estipulan requisitos específicos para

la identificación de las infraestructuras críticas en los Estados miembros, la necesidad de comunicar incidentes y otros aspectos para establecer colaboración y cooperación entre diferentes organismos para mejorar su resiliencia. NIS2 tiene como objetivo fortalecer las capacidades de ciberseguridad de la UE, con propuestas para el intercambio de información y la cooperación en la gestión de cibercrisis a nivel nacional y de la UE. La directiva CER, por su parte, proporciona un marco de todos los riesgos para ayudar a los Estados miembros a garantizar que las entidades críticas puedan prevenir, resistir y recuperarse de incidentes disruptivos, cualquiera sea su origen. El foco se extiende más allá de las organizaciones que ofrecen servicios críticos, pues abarca toda la cadena de suministro.

2.2.2. Estados Unidos

En Estados Unidos, a nivel federal, numerosas agencias imponen estándares de ciberseguridad a través de una variedad de mecanismos regulatorios y de aplicación. Existen leyes federales, como la ley de intercambio de información sobre ciberseguridad, cuyo objetivo es mejorar la seguridad compartiendo información sobre amenazas; o la ley de mejora de la ciberseguridad de 2014 para fortalecer, entre otras cosas, la I+D en ciberseguridad, la fuerza laboral, la educación y la conciencia pública. Los Gobiernos estatales también han trabajado en el aspecto normativo de la protección de datos personales o en la ciberseguridad, sobre todo en algunos sectores, como el financiero o el de la salud. Estados como Nevada o Dakota del Norte han hecho esfuerzos por introducir leyes para proteger servicios financieros (Nevada Senate Bill 44, y North Dakota House Bill 1127 en 2025). Otros ejemplos como la ley de seguridad cibernética de Nueva York de 2019, o la ley de privacidad del consumidor de California de 2018 fueron pioneros en su momento.

En materia de infraestructuras críticas, en el año 2013 se publicó una orden ejecutiva (Exec. Order No. 13636, 2013) para mejorar su ciberseguridad, donde se encargó al Instituto Nacional de Estándares y Tecnologías (NIST) el desarrollo del hoy conocido como *Marco NIST o NIST Framework*. Este es un marco que, aunque nació para la protección de las infraestructuras críticas, tiene amplia aplicabilidad y es utilizado como referencia para la gestión de los riesgos cibernéticos por muchos tipos de organizaciones a nivel mundial.

Marco de Ciberseguridad del NIST

El Marco de Ciberseguridad del NIST incluye funciones, categorías, subcategorías y referencias. Las funciones ofrecen una visión general de mejores prácticas por categoría en materia de seguridad; no son secuenciales, sino que conforman los pilares de un cambio dentro de las organizaciones hacia una cultura y práctica de la ciberseguridad.

Las categorías y subcategorías proporcionan planes de acción más concretos para departamentos o procesos específicos dentro de una organización.

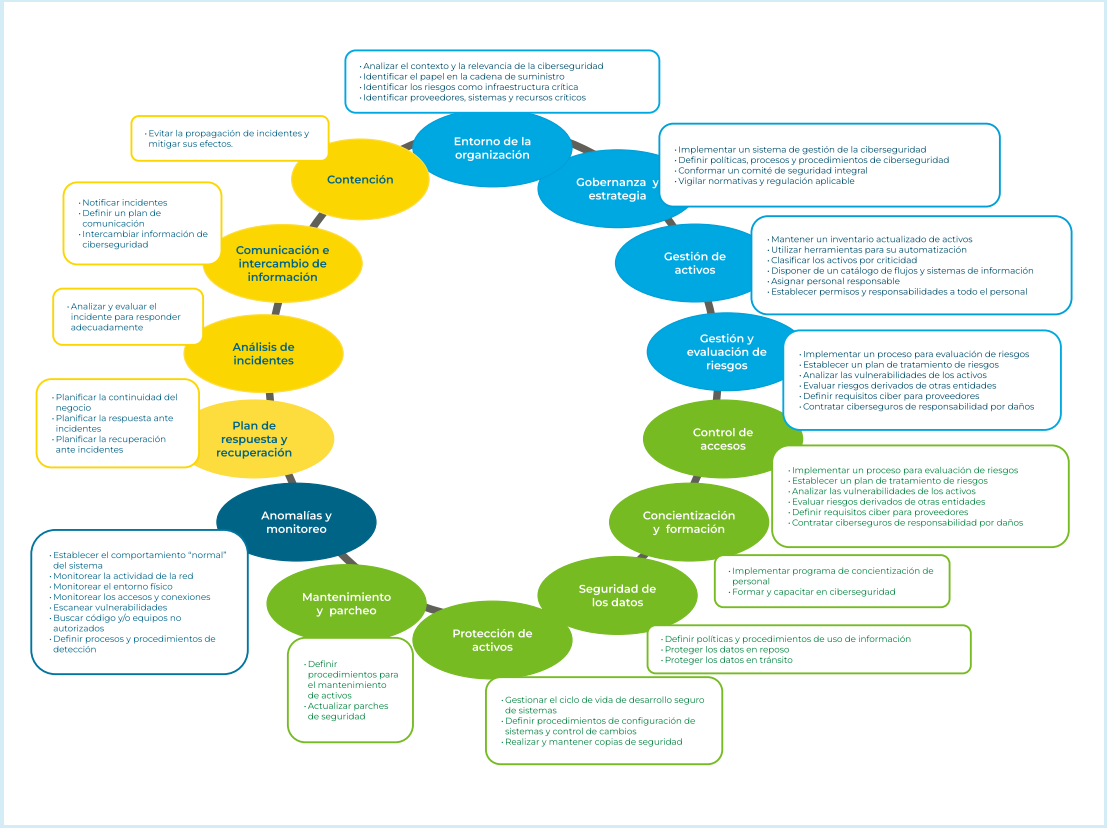
El marco clasifica todas las capacidades, proyectos, procesos y actividades diarias de ciberseguridad en cinco funciones básicas: identificar, proteger, detectar, responder, recuperar y gobernar.

Las siguientes figuras resumen las funciones y acciones del Marco de Ciberseguridad del NIST.

Figura 6. Funciones básicas para la ciberseguridad

Función	
Identificar	¿Qué procesos y activos necesitan ser protegidos?
Proteger	Proteger contra amenazas y vulnerabilidades
Detectar	Aplicar las precauciones necesarias para garantizar la protección de los activos y los mecanismos adecuados para identificar incidentes de ciberseguridad
Responder	Desarrollar mecanismos para contener el impacto de los incidentes de ciberseguridad
Recuperar	Implementar los procesos adecuados para restaurar las capacidades y servicios afectados por incidentes de ciberseguridad
Gobernar	Establecer, comunicar y supervisar la estrategia, las políticas y la gestión de riesgos de ciberseguridad.

Figura 7. Marco de Ciberseguridad del NIST



En 2021 se incluyeron las necesidades de la parte OT y se publicó un memorándum (NSM-22, 2021) para mejorar la ciberseguridad en los sistemas de control industrial en infraestructuras críticas. A través de la Agencia de Seguridad Cibernética y de la Infraestructura (CISA) y NIST se han publicado varios recursos y buenas prácticas.[16]

Específicamente en materia de transporte, el Gobierno ofrece el documento *Surface Transportation Cybersecurity Toolkit* (U.S. Department of Homeland Security, s. f.), de utilidad para el transporte de superficie. Incluye circulares informativas que proveen recomendaciones para el transporte de superficie y también para el reporte de incidentes en el sector ferroviario. La Administración Federal de Transporte (FTA) publicó en 2023 una herramienta de evaluación de la ciberseguridad para el tránsito que apunta a ayudar a las organizaciones de transporte público a desarrollar y reforzar sus programas de ciberseguridad para identificar y mitigar mejor los riesgos. A nivel federal, para promover la protección de infraestructuras críticas de transporte, el Departamento de Seguridad Nacional ofrece un programa de subvenciones para sistemas de transporte público elegibles, que incluye autobuses intraurbanos, transbordadores y todas las formas de ferrocarril de pasajeros (U.S. Department of Homeland Security, 2023).

2.2.3. Otros países

Además de los Estados de la UE y de Estados Unidos, otros países han abordado aspectos interesantes de ciberseguridad en su regulación.

China, por ejemplo, puso en vigor en 2017 su ley de ciberseguridad, de aplicación a operadores de red y empresas de sectores críticos. Entre otras cuestiones, incluye aspectos de obligatoriedad para que los operadores de red tengan sus datos dentro de China, que ciertos sistemas dispongan de certificación y la posibilidad de realizar controles por parte de las autoridades (People's Republic of China, 2018).

Singapur cuenta con su *Cybersecurity Act* de 2018 (Republic of Singapore, 2018) y, a través de la CSA (*Cyber Security Agency*), publica sus normas y códigos de buenas prácticas en materia de seguridad cibernética.

A nivel internacional, en el año 2001, el Comité de Ministros del Consejo de Europa lanzó el denominado *Convenio sobre la Ciberdelincuencia de Budapest*. En él, se explicita la necesidad de cooperación entre los Estados y el sector privado para luchar contra la ciberdelincuencia y la consiguiente necesidad de cooperación internacional en materia penal. Por eso, entre los capítulos que incluye, aparecen definidas las medidas que deberán adoptarse a nivel nacional para los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, o delitos relacionados con infracciones de propiedad intelectual y de derechos afines, pornografía infantil, etc. Desde 2001, multitud de países se han ido adhiriendo y firmando el convenio; entre ellos, se encuentran muchos de ALC, como México, Colombia, Argentina, Costa Rica, Uruguay, Chile, República Dominicana, Panamá y Perú.

16 Control Systems Goals and Objectives | CISA.

2.2.4 Estándares de ciberseguridad aplicables

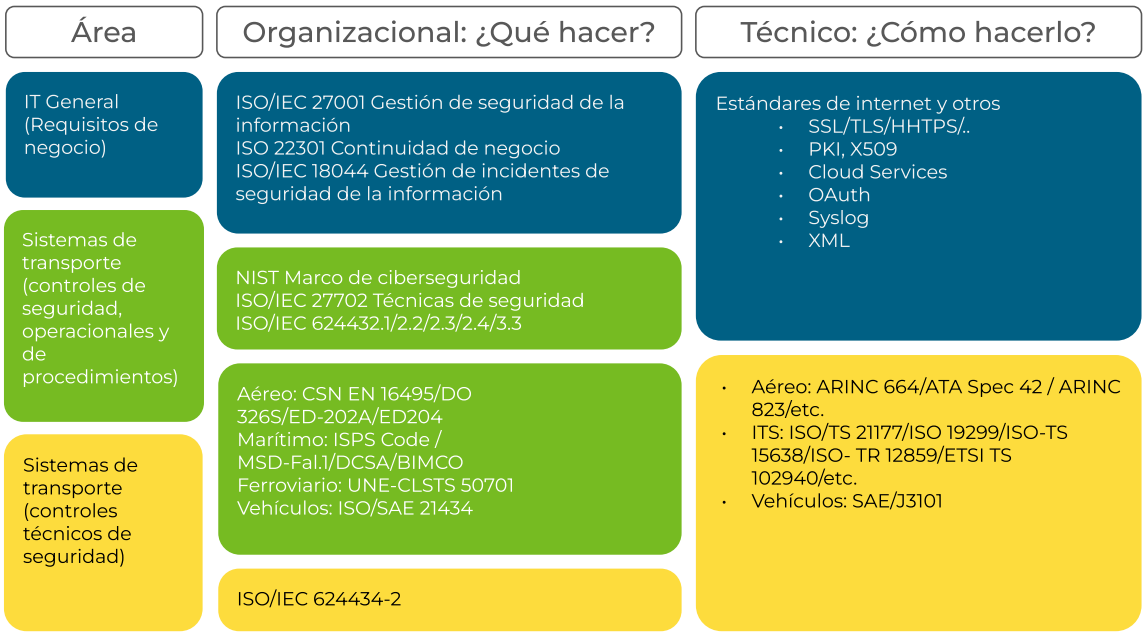
Otra de las herramientas de las que se pueden servir las organizaciones para mejorar su resiliencia son los estándares de ciberseguridad, que abarcan diferentes temas y destinatarios.

Existen estándares de ciberseguridad de tipo organizacional que se aplican, por ejemplo, a la definición e implementación de un sistema de gestión de la seguridad. Entre los más relevantes, figura la norma ISO 27001 para la definición de un plan de seguridad de la información. Para llevar este concepto al ámbito de las empresas industriales, la referencia es la normativa IEC 62443 Parte 2-1.

Para complementar este tipo de estándares, hay controles técnicos que deben ser satisfechos tanto por productos como por sistemas. Normalmente destinados a los fabricantes de equipamiento, en ellos figuran los requisitos para realizar funciones habituales de seguridad cibernética, como la identificación, autenticación y autorización o la aplicación de medidas de protección a través del uso de criptografía, entre otros.

La siguiente figura resume la estructura de los principales estándares aplicables organizados por áreas de aplicación (a quién o qué van destinados) y motivación (organizativa o técnica).

Figura 8. Estándares relevantes en el sector del transporte



Fuente: Elaboración propia con base en la literatura revisada para esta nota.

En el Anexo II, “Estándares y marcos de ciberseguridad aplicables”, se puede consultar la lista de los diferentes estándares de ciberseguridad para cada uno de los modos de transporte considerados: aéreo, marítimo y ferroviario, además de los vehículos terrestres.

Asimismo, y considerando que en el entorno de sistemas y activos del transporte hay tanto sistemas IT como OT, se incorporan algunos de los estándares más importantes para los sistemas industriales, como la normativa IEC 62443; y los productos IT, como los *Common Criteria*. A ellos se añaden estándares que facilitan la definición o gestión de políticas y procedimientos que pueden desplegarse en una organización para la implementación de sistemas de gestión de la seguridad. Entre los marcos más conocidos aplicables a las infraestructuras críticas destacan el Marco NIST y la familia o serie de normas ISO/IEC 2700x e ISO 22301 para la implementación de un sistema de gestión para la continuidad del negocio.

3

Análisis de la situación de la región de América Latina y el Caribe (ALC)

Este capítulo analiza la situación de la ciberseguridad en el transporte de ALC e integra las perspectivas de los sectores público y privado. Los resultados se basan en investigaciones propias y entrevistas cualitativas realizadas desde 2022 hasta la fecha a entidades regionales con el fin de evaluar el estado de la región en materia de políticas y estrategias de ciberseguridad.

3.1. América Latina: la región con mayor crecimiento de incidentes reportados

América Latina es la región del mundo con el mayor aumento de incidentes reportados de ciberdelincuencia en la última década. Según un estudio del Banco Mundial, los ciberincidentes han crecido anualmente 25 % entre 2014 y 2023 (Vergara Cobos, 2024). Gracias a un análisis de datos avanzado de millones de artículos de los últimos 10 años, este informe permitió armar una base de datos de 30 000 ciberincidentes. La cifra confirma el complejo panorama de la región, donde la información sobre ciberincidentes en la región tiende a ser escasa, ya sea por temas de seguridad nacional o por prácticas desactualizadas. La situación es particularmente preocupante, pues, según datos del Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones, también es una de las regiones con menos avances en compromisos con la ciberseguridad.

En general, tanto el sector del transporte público como el privado parecen estar siendo cada vez más objetivos de ciberataques. Sin embargo, la proporción parece ser menor que en otros sectores, estando por debajo del 15 % de los incidentes reportados (Vergara Cobos, 2024).

Más allá de las vulnerabilidades, la región ha tenido avances en la definición de leyes o políticas de infraestructura crítica y múltiples iniciativas regionales están viniendo a colmar las brechas existentes.

En este capítulo se busca ofrecer un panorama más claro del estado de la ciberseguridad en el sector del transporte en ALC, tanto desde la perspectiva del sector público como del privado. Las conclusiones y la información están basadas en la investigación de los autores entre 2022 y 2025 y en una serie de entrevistas realizadas en 2022, principalmente a administraciones y otras entidades públicas del sector del transporte de diferentes países de la región. Estas entrevistas cualitativas permitieron evaluar el estado de la región en materia de políticas y estrategias de ciberseguridad en el sector de transporte.

Para obtener la información, se diseñó un modelo de entrevista[17] que indagaba en las dimensiones legal, organizacional, técnica, de cooperación y de capacitación:

- **Legal:** para medir la existencia de instituciones y marcos legales que se ocupen de la ciberseguridad en infraestructuras críticas y específicamente en aquellas relacionadas con los segmentos del transporte y la logística tratados.

- **Organizacional:** para medir la existencia de instituciones de coordinación de políticas y estrategias para el desarrollo de la ciberseguridad, tanto a nivel nacional como dentro de las propias organizaciones. Se consideran en este punto aspectos como la tipología de las entidades involucradas en la definición de estrategias en materia de TIC, de ciberseguridad en general o específicas para las infraestructuras críticas o el sector del transporte, así como la existencia de los mecanismos que utilizan para coordinarse entre ellas.

17 Las entrevistas fueron realizadas a través de videoconferencias donde estuvieron presentes, además de los entrevistados, representantes del Banco Interamericano de Desarrollo (BID) y del centro tecnológico TECNALIA.

- **Técnica:** para medir la existencia de instituciones o marcos técnicos que se promuevan en relación con la ciberseguridad, además de la adopción e implementación de controles técnicos o para el establecimiento de prácticas de ciberseguridad en las organizaciones.

- **Cooperación:** para medir la existencia de asociaciones, marcos de cooperación y redes de intercambio de información, tanto intersectorial como de cooperación internacional.

- **Capacitación:** para identificar la existencia de programas de investigación y desarrollo, educación o formación y de profesionales certificados, empresas de servicios especializadas en ciberseguridad o agencias del sector público que fomenten el desarrollo de capacidades en el sector de la logística y el transporte.

En el Anexo III se incluye el modelo de cuestionario utilizado para la realización de las entrevistas. A partir de estas entrevistas también fue identificada una serie de buenas prácticas en materia de ciberseguridad que están llevando a cabo las entidades de la región.

3.2. Panorama de cooperación regional

En la región, los primeros esfuerzos coordinados para abordar el tema de la ciberseguridad comenzaron en 2004 tras la declaración de Montevideo, en la que el Comité Interamericano contra el Terrorismo (CICTE) se comprometió a combatir amenazas emergentes, tales como las de la seguridad cibernética. Enseguida, la Asamblea General de la Organización de los Estados Americanos (OEA) promovió la adopción de la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética con la resolución AG/RES. 2004 (XXXIV-O/04). Con esta resolución, se insta a los Estados miembros a implementar dicha estrategia y, entre otras cosas, a establecer un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés). También deben adoptar normas técnicas de seguridad cibernética y disponer de legislación específica para delitos cibernéticos, facilitando medidas para la coordinación de esfuerzos que sirvan para incrementar la ciberseguridad. En 2012 se afianzó esta vía a través de la declaración del fortalecimiento de la seguridad cibernética en las Américas, con el compromiso renovado de implementar la Estrategia Interamericana de Seguridad Cibernética, adoptada anteriormente.

Desde el propio CICTE se promueve el desarrollo de proyectos en este sentido, en particular el Programa de Ciberseguridad que viene brindando apoyo a los Estados de la región en materia de desarrollo de políticas, creación de capacidades, investigación y divulgación. En el CICTE también se enmarca la red CSIRTAmericas, que conecta a actores y contribuye al fortalecimiento de capacidades de diversos CSIRT en la región. En ella se encuentran involucrados 21 países y 36 CSIRT con más de 200 especialistas que trabajan para promover el intercambio de información sobre alertas de ciberseguridad, brindando asistencia técnica para fortalecer los servicios de los CSIRT y ofreciendo capacitaciones a especialistas en ciberseguridad.

En 2016, el BID lanzó en alianza con la OEA el primer informe regional sobre ciberseguridad, denominado “Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?”, que señalaba un panorama de múltiples atrasos en este tema. En 2020, el segundo informe, “Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe”, fruto de esta alianza, permitió apreciar que los Estados miembros mejoraron sus capacidades de ciberseguridad, pero que el nivel de madurez promedio de la región seguía siendo bajo. El informe utilizó el Modelo de Madurez de Capacidad en Ciberseguridad para Naciones de Oxford (CMM, por sus siglas en inglés). Indicó que la mayoría de los países han comenzado a formular iniciativas, incluidas medidas para la creación de capacidades en ciberseguridad, y que el tema está cobrando importancia en la agenda política y normativa de la región. Sin embargo, el nivel promedio de la región está todavía en su etapa inicial de acuerdo con el CMM. En la misma línea, el BID y la OEA desarrollaron el informe "Ciberseguridad 2025: desafíos de vulnerabilidad y madurez para cerrar brechas en América Latina y el Caribe", que compara avances entre países usando el CMM.

Otra iniciativa regional interesante en términos de ciberseguridad es LACNIC-CSIRT, que ayuda a garantizar la disponibilidad, integridad y confidencialidad de los recursos de internet en la región. Es impulsada por el Registro de Direcciones de Internet para América Latina y Caribe (LACNIC), organización no gubernamental internacional establecida en Uruguay en el año 2002, responsable del registro y asignación de recursos numéricos (IPv4, IPv6 y ASN) de ALC. Su trabajo garantiza el acceso a internet, que las direcciones sean administradas de manera eficiente y que la comunidad tenga voz en las políticas que rigen esta tecnología. En ciberseguridad, la iniciativa trabaja para fortalecer la capacidad de respuesta a incidentes de seguridad relacionados con los recursos de internet en ALC.

La Red de Gobierno Electrónico de América Latina y el Caribe (Red GEALC) es otra iniciativa regional que busca fortalecer la colaboración entre los países de ALC en gobierno digital. Su objetivo es promover el intercambio de experiencias, conocimientos y buenas prácticas para avanzar hacia la transformación digital de los Gobiernos y mejorar servicios a los ciudadanos. Dentro de esta red, en 2021 se incorporó la línea de trabajo en ciberseguridad con la creación de un grupo de trabajo conformado por responsables públicos de los Gobiernos de la región. Su formación ha permitido diálogos en una perspectiva multisectorial, teniendo miembros tanto de agencias especializadas y de ministerios de información y comunicación como de organizaciones multilaterales.

En lo que concierne específicamente al transporte, cabe destacar las actuaciones de asociaciones sectoriales, sobre todo en los sectores aéreo y marítimo, que están comenzando a priorizar el tema de la ciberseguridad en sus discusiones y eventos. Sin embargo, el tema de la ciberseguridad en la política de transporte sigue siendo relativamente poco abordado. Se considera muy importante iniciar colaboraciones con entidades nacionales e internacionales para compartir experiencias, incidentes ocurridos y otros aspectos sobre ciberseguridad, pero también para prestar apoyo técnico en la implementación de soluciones y estrategias o de responder ante incidentes reales. Una buena práctica que se identifica en la región es la firma de memorandos de cooperación técnica; por ejemplo, la Autoridad del Canal de Panamá ha firmado acuerdos con diferentes actores internacionales expertos en ciberseguridad marítima. Sin embargo, o no hay un gran volumen de acuerdos formales establecidos con terceras partes, o bien estos no se aplican de forma práctica.

Buenas prácticas: Cooperación entre entidades civiles y militares

En Colombia, Aerocivil es la autoridad aeronáutica. Se ocupa de la reglamentación, vigilancia y control de la aviación civil, además de la prestación de los servicios de navegación aérea y administración del espacio aéreo bajo la jurisdicción del Estado colombiano. Esta institución civil coopera y colabora con la Fuerza Aérea Colombiana a través, entre otros mecanismos, del SOC, que fue creado por la misma, y también ha cooperado realizando capacitaciones orientadas a la ciberseguridad de OT y de IT y sobre sistemas críticos en el sector aéreo.

3.3. Panorama legal

La normativa y regulación en materia de ciberseguridad en la región es muy diversa, con distintos niveles de avance de un país a otro. Ciertos países de la región ya cuentan con leyes y reglamentos relacionados con la ciberseguridad en diferentes niveles de gobernanza; otros están en proceso de actualización y ampliación de leyes existentes; y algunos se encuentran en proceso de definición y aprobación de marcos normativos en ciberseguridad. En general, se observa una preocupación a nivel político sobre los riesgos de la ciberseguridad en la mayoría de los países de la región. Gran parte de los países imponen la aplicación de la legislación de ciberseguridad en el sector público. Las entidades privadas no siempre están sujetas a ella, ya que se trata de legislaciones relativamente nuevas. Se prevé que se amplíe y afecte a aquellas entidades privadas cuya operación se considere como crítica.

La legislación con respecto a la definición e identificación de infraestructuras críticas en la región puede considerarse como poco madura. Si bien existen países que están más avanzados que otros y algunos ya cuentan con leyes a tal efecto, todavía es necesario un impulso en la elaboración de legislación para definir e identificar las infraestructuras críticas de los países, imponer el establecimiento de ciertos requisitos de ciberseguridad y determinar controles del cumplimiento de la legislación por parte de la autoridad pertinente.

Desde las propias entidades públicas y privadas del sector de aquellos países en los que ya existe una normativa de ciberseguridad general vigente, se considera interesante e importante que desde los propios ministerios de Transporte se den pautas y recomendaciones o se cree regulación específica sobre la aplicación de la ciberseguridad para el sector; esto último todavía no existe en la región.

Una buena práctica identificada es que, a veces, de manera complementaria, y otras por falta de un marco nacional legislativo para la ciberseguridad que tome en cuenta las especificidades del sector del transporte, la regulación para la ciberseguridad procede de fuentes heterogéneas. En ocasiones, las leyes de gobierno digital abordan el tema, como es el caso en Colombia y Perú. Otra fuente de regulación pueden ser también los decretos y normas internas administrativos de los propios Gobiernos. Esta política se enmarca en la Estrategia Nacional Digital de Colombia para 2023-2026.

En Colombia, la Política de Gobierno Digital (Decreto 767 de 2022) establece, entre otros aspectos, los lineamientos de seguridad que deben cumplir las entidades del Gobierno respecto del tratamiento de la información. Entidades sectoriales como el Ministerio de Transporte deben proveer anualmente sus planes de seguridad de la información, incluyendo proyectos, herramientas y acciones, al equipo del Ministerio de Tecnologías de la Información y la Comunicación, a cargo de estos temas.

En 2021, Argentina publicó la normativa DECAD-2021-641-APN-JGM "Requisitos mínimos de Seguridad de la Información para los Organismos del Sector Público Nacional", que establece las pautas de ciberseguridad (gestión de activos, personas, aspectos organizacionales) para todos los organismos del Gobierno. Un aspecto interesante de esta normativa es que establece una serie de puntos focales de comunicación entre los diferentes ministerios. En el caso de la Secretaría de Transporte, además de dicho punto focal, la implementación destaca por la designación de otros puntos focales (técnicos) en los organismos descentralizados dependientes de esta institución. Ellos asisten a reuniones con una periodicidad de entre 15 y 30 días en las que reciben capacitación especializada sobre ciberseguridad, con la responsabilidad de transmitir posteriormente la información de forma interna en cada una de sus entidades. Las normativas relacionadas vigentes en el país son la Resolución 44/2023 de la Secretaría de Innovación Pública (aprueba la Segunda Estrategia Nacional de Ciberseguridad), el Decreto 941/2025 (crea el Centro Nacional de Ciberseguridad) y la Disposición 1/2026 del Centro Nacional de Ciberseguridad (aprueba el reglamento técnico que establece los requisitos y características esenciales en la elaboración e implementación de políticas de planes de contingencias y centros de procesamiento de datos alternativos).

Buenas prácticas: Nueva Ley de Ciberseguridad de Chile

En abril de 2024, Chile aprobó la nueva Ley de Ciberseguridad de Chile, un avance significativo en la protección de infraestructuras críticas e información sensible frente a las ciberamenazas. Esta ley establece un marco regulatorio sólido y fortalece la capacidad del país para prevenir, detectar y responder a incidentes cibernéticos. Uno de sus pilares fundamentales es la creación de la Agencia Nacional de Ciberseguridad (ANCI), organismo autónomo encargado de regular y supervisar el cumplimiento de las normas de ciberseguridad, así como de coordinar las acciones de los diferentes actores involucrados.

Otro aporte de la ley es la creación del Consejo Multisectorial sobre Ciberseguridad, integrado por miembros tanto del Gobierno como del sector privado, el ámbito académico y la sociedad civil. El Consejo tiene la función de estudiar las amenazas existentes y potenciales en el ámbito de la ciberseguridad, lo que le permite anticipar y adaptarse a los cambios y desafíos que surgen en este campo dinámico. La iniciativa demuestra cómo la ciberseguridad es un fenómeno integral y transversal a la sociedad, que debe ser acompañada de una visión integral y colaborativa con la participación y transparencia de todos los sectores.

La ley también contribuye a solidificar el marco regulatorio y la importancia de asegurar la seguridad cibernética del sector transporte. Sin enfocarse solo en el transporte, define como servicios esenciales no solo a aquellos prestados directamente por el Estado como infraestructura crítica, sino que abarca los servicios prestados bajo concesiones de servicios

públicos y los proveídos por instituciones privadas. La ley menciona tanto el transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de sus infraestructuras respectivas, y otros sectores que habilitan la prestación de servicios como las telecomunicaciones, la infraestructura digital, los servicios digitales, los servicios de IT gestionados por terceros y los servicios financieros, banca y medios de pago.

3.4. Panorama organizacional

El hecho de que varios países de la región hayan sufrido ataques de *ransomware* en diferentes niveles ha promovido una mayor conciencia de las amenazas, tanto en instituciones públicas como en entidades privadas. Según datos de Palo Alto Networks, entre 2022 y 2023, los ataques de *ransomware* aumentaron un 38 % en la región, habiéndose producido 180 ataques relevantes en 20 países analizados. Entre ellos, destaca el número de ataques relevantes en Brasil, que alcanzó los 59 en 2022 (Forbes Staff, 2023).

Otras referencias indican que se producen 7160 (Kaspersky, 2023) ataques de *ransomware* diarios en las empresas de ALC, incluyendo ataques menores. Esto ha generado una mayor conciencia de la importancia de la seguridad cibernética, por lo que se ha visto una relativa urgencia de aplicar medidas de ciberseguridad.

Hay consenso entre las organizaciones entrevistadas en que es fundamental que exista apoyo directo por parte de la dirección de las organizaciones para que el tema de la ciberseguridad se trabaje en todos los niveles. Contar con una visión transversal dentro de las organizaciones, con equipos específicos y gerentes dedicados a los temas de ciberseguridad, puede hacer la diferencia.

La pandemia de covid-19 puso de manifiesto las carencias en ciberseguridad de muchas entidades públicas y privadas a la hora de promover y favorecer los trabajos remotos. Esto ha servido para impulsar la implementación de medidas de ciberseguridad que anteriormente no se realizaban.

- Una de las preocupaciones generales es la protección jurídica cuando ocurre un incidente de ciberseguridad, ya que no es algo que se suela tratar. Es necesario trabajar en la protección y evaluar las consecuencias jurídicas.

- Dos de las condiciones para seguir avanzando en materia de ciberseguridad en la región son:

  – Disponer de los mecanismos financieros, tanto a nivel gubernamental como privado, para desplegar los controles y estrategias de ciberseguridad necesarios.

  – Disponer de personal humano cualificado para poder afrontar implementaciones de ciberseguridad, que, teniendo en cuenta la complejidad de los sistemas del sector del transporte, es difícil de encontrar.

Buenas prácticas: Relacionarse con los proveedores, generar confianza y sensibilizar

Dependiendo del tipo de servicio para el que haya sido contratado un proveedor, la relación puede contribuir a mejorar la ciberseguridad o generar vulnerabilidades en una organización.

Por ejemplo, el Ministerio de Transporte de Colombia toma un rol proactivo de sensibilización en temas de ciberseguridad y tratamiento de la información con sus proveedores, haciéndoles respetar los lineamientos contractuales establecidos por el Estado colombiano y con capacitaciones.

Sin embargo, los proveedores, sobre todo aquellos a cargo de servicios tecnológicos con amplia experiencia mundial y trayectorias demostradas, pueden aportar conocimiento y competencias

Buenas prácticas: Centros de Operaciones de Seguridad (SOC) en entidades del sector transporte

Un SOC consiste en un equipo encargado de monitorear y supervisar la infraestructura de IT dentro de un organismo. Puede ser creado internamente o contratado externamente. Su objetivo es prevenir y detectar rápidamente incidentes de ciberseguridad para evitar que tengan consecuencias o que sus acciones afecten las operaciones de una organización. En el sector del transporte en ALC existen algunos ejemplos de esta buena práctica.

El Puerto de Valparaíso, por ejemplo, creó un SOC para el monitoreo de ciberamenazas que, entre sus múltiples funciones, monitorea posibles vulnerabilidades provenientes del teletrabajo de sus empleados.

La empresa Transmilenio S.A., a cargo del Sistema Integrado de Transporte Público de Bogotá, D.C., también cuenta con servicios de SOC para monitoreo de red. En esta misma ciudad, la Secretaría Distrital de Movilidad, autoridad de transporte de la ciudad, constituyó un SOC para la protección de su infraestructura tecnológica.

3.5. Panorama técnico

En varios países de ALC existen estructuras de CERT/CSIRT para el reporte de incidentes de seguridad, y en algunos casos incluso para proveer de ciertos servicios especializados a entidades que así lo requieran, como análisis de vulnerabilidades, pruebas de penetración, análisis forenses y capacitaciones especializadas. A la fecha, no se ha constatado la existencia de ningún CERT/CSIRT sectorial en transporte en la región.

Es necesario que cuando las instituciones adquieran ciertos servicios o sistemas incluyan o amplíen cláusulas más exigentes relacionadas con ciberseguridad; incluso que exijan el cumplimiento de ciertos estándares de esta materia en función de la criticidad del servicio prestado. Asimismo, es indispensable establecer posteriores controles o mecanismos para comprobar que se cumplan los requisitos impuestos.

Normalmente, el sector del transporte es consciente de los peligros y amenazas en la parte IT de los sistemas. En este sentido, muchas de las entidades disponen de mecanismos de protección tradicionales. Sin embargo, hay una menor conciencia de los peligros con respecto a la parte OT, ya sea porque los sistemas OT se presuponen aislados y seguros; o bien porque muchos de ellos son construidos o gestionados por proveedores que asumen que tienen y aplican amplios conocimientos de ciberseguridad.

Muchas de las soluciones que se utilizan para el control de operaciones en el transporte aéreo, marítimo, ferroviario y terrestre son sistemas complejos que han sido construidos por empresas especializadas con un profundo conocimiento sectorial y múltiples implantaciones en todo el mundo. Hasta cierto punto, esto aporta una garantía de seguridad implícita, bajo la premisa de que, al construirse para clientes multinacionales con niveles de ciberseguridad diferentes, dichas soluciones se conciben como seguras *per se*. Aun así, es necesario establecer mecanismos de supervisión de estas soluciones y de la manera en la que operan, ya que muchos de los riesgos provienen de su mal uso. En este sentido, se puede trabajar el tema de la ciberseguridad en los instrumentos de compra pública, incluyendo consideraciones o requerimientos en pliegos o documentos de licitación y contratación.

Buenas prácticas: *Hacking* ético y pruebas de penetración regulares

Una buena práctica esencial en la búsqueda de mejorar la ciberseguridad es monitorear e identificar vulnerabilidades en los sistemas IT y OT de las organizaciones de transporte de la región. Para ello, existen múltiples servicios y técnicas, como las pruebas de penetración y el uso de *hacking ético*.

Las pruebas de penetración son evaluaciones con un alcance específico contratadas por clientes a equipos independientes. Los distintos tipos de pruebas de penetración se centran en aspectos específicos de los sistemas de una organización, pudiendo incluir: pruebas de redes externas e internas, que buscan vulnerabilidades y problemas de seguridad en los servidores, *hosts*, dispositivos y servicios de red de una organización, como también evalúan el daño que podría causar un atacante al acceder a los sistemas internos; y pruebas de aplicaciones web, redes inalámbricas y vulnerabilidad del personal al *phishing*.

El *hacking* ético es una disciplina más integral con mayor variedad de técnicas, que incluye, entre otras, las pruebas de penetración, y cuenta con la responsabilidad de hacer recomendaciones después de identificar las posibles vulnerabilidades.

En la región, instituciones como la Autoridad del Canal de Panamá realizan capacitaciones específicas para sus empleados en ambos temas.

3.6. Panorama de capacitación

Las diferentes instituciones entrevistadas realizan en su mayoría campañas de sensibilización de ciberseguridad dirigidas a diferentes beneficiarios, desde la población en general hasta empleados de organizaciones privadas y empleados públicos. En Perú, por ejemplo, el Centro Nacional de Seguridad Digital (CNSD) ha capacitado a cerca de 70 000 personas a nivel nacional en temas de seguridad, incluyendo capacitaciones directas a funcionarios públicos y ciudadanos de diferentes sectores.

Otro ejemplo son las simulaciones de ataques que realiza la Autoridad del Canal de Panamá para comprobar si el personal del canal ha adquirido los conocimientos básicos que se esperan en materia de ciberseguridad (por ejemplo, conocimiento de lo que es el *phishing*). También se están realizando campañas sobre la salvaguarda de la identidad digital y cómo esta, aunque sea personal, puede afectar a la empresa.

En general, en la región se observa que todavía no existen formaciones especializadas y dirigidas específicamente al sector del transporte, pero la oferta con respecto al tema de infraestructura crítica viene creciendo. Las organizaciones de la región también manifiestan que hay una notable demanda de talento especializado en temas de ciberseguridad dentro y fuera del sector público, aunque este talento sigue siendo difícil de encontrar y mantener.

Buenas prácticas: Red CIBERLAC

La ciberseguridad demanda un enfoque multidisciplinario que involucra a la academia, la industria y los Gobiernos. La creación de conocimiento y la formación de profesionales se erigen como pilares fundamentales para enfrentar los desafíos de un mundo digital y conectado. Desde el punto de vista de la academia y el conocimiento, cabe destacar el trabajo de CIBERLAC, la Red de Excelencia en Ciberseguridad de Latinoamérica y el Caribe, constituida por universidades y centros de investigación sobre ciberseguridad en la región. El Banco Interamericano de Desarrollo (BID) actúa como institución impulsora y de articulación de la Red.

La Red Ciberlac facilita la colaboración y el intercambio de conocimientos, experiencias y recursos entre las instituciones que la integran, y promueve la creación de sinergias con el fin de potenciar sus capacidades educativas y de investigación. Su meta es contribuir a reducir el déficit de profesionales en ciberseguridad, tanto en la industria como en la academia. Además, busca potenciar el nivel de preparación en esta materia en los países de la región, mediante el fomento a la formación de capital humano, la investigación y la innovación.

3.7. Panoramas subsectoriales

El análisis de ciberseguridad en el sector del transporte exige un enfoque específico para cada subsector debido a la diversidad de tecnologías y sistemas empleados en el transporte aéreo, marítimo, ferroviario y terrestre. Cada subsector utiliza procedimientos operativos únicos y sistemas interconectados. Por ejemplo, la aviación depende de complejas

redes de navegación y control del tráfico aéreo, mientras que el sector marítimo cuenta con una intrincada red de barcos, puertos e instalaciones de carga. Esta diversidad tecnológica requiere evaluaciones de riesgos y medidas de seguridad adaptadas para abordar eficazmente las vulnerabilidades específicas inherentes a cada subsector.

Además, el panorama de amenazas y las posibles consecuencias de un ciberataque varían significativamente entre los subsectores. La aviación, por ejemplo, podría ser más susceptible a ataques dirigidos a los sistemas de control de vuelo, lo que supondría riesgos catastróficos para la seguridad. El transporte marítimo, por su parte, podría ser más vulnerable a las interrupciones del seguimiento de la carga y las operaciones portuarias, lo que provocaría importantes pérdidas económicas. Comprender estas amenazas distintas y sus posibles repercusiones es crucial para una gestión eficaz de los riesgos y la priorización de medidas de seguridad.

Finalmente, la interconexión de los subsectores del transporte, junto con los diversos requisitos reglamentarios y un panorama de amenazas en evolución, refuerza la necesidad de un análisis de riesgos específico para cada subsector. Un ciberataque en un subsector puede tener efectos en cadena en otros, interrumpiendo las cadenas de suministro y afectando a todo el ecosistema del transporte. El análisis de riesgos por subsector permite a las organizaciones cumplir con los requisitos reglamentarios específicos, adaptarse a las amenazas emergentes y, en última instancia, desarrollar estrategias de ciberseguridad particulares que mejoren la resiliencia de toda la red del transporte.

En la siguiente sección se presentan los diferentes panoramas subsectoriales para el subsector aéreo, marítimo y de transporte terrestre, carretero y público, fruto de la investigación y entrevistas realizadas por los autores. No se presenta un panorama del subsector ferroviario para la región, ya que en el momento del desarrollo de la investigación no se encontraron fuentes suficientemente representativas para llegar a conclusiones sobre el subsector tanto en las entrevistas como en la de revisión de literatura.

3.7.1. Sector aéreo

Altamente regulado a nivel internacional, el sector aéreo siempre se ha preocupado por la seguridad operacional relacionada con los aspectos de seguridad física. Sin embargo, tras los numerosos incidentes de seguridad cibernética en los últimos años, son necesarios más esfuerzos para reforzar la estrategia de ciberseguridad en aras de proteger las operaciones aéreas, incluyendo los sistemas y servicios de tierra.

Si bien existen estándares técnicos a nivel mundial para la construcción y operación de aeronaves, hay conciencia en la industria de las aerolíneas sobre la necesidad de contar con estándares más específicos en materia de ciberseguridad, que incluyan desde la reserva hasta el vuelo.

Se observa la necesidad de afrontar los retos de ciberseguridad de manera integral. Los ecosistemas aéreos son complejos, pues en ellos convergen diferentes actores que interactúan constantemente, ya sea por compartición de sistemas o por envío y recepción de información, de tal forma que la superficie de ataque se extiende a los diferentes actores del ecosistema.

El sector reconoce la necesidad de reforzar su estrategia de ciberseguridad tanto en la parte IT como en la parte OT. Si bien históricamente la prioridad era la ciberseguridad de IT, ya que anteriormente la parte de operación se encontraba aislada, la realidad actual es distinta. De hecho, tras análisis realizados por algunas entidades, se ha descubierto que existen puntos de conexión entre la infraestructura que soporta los servicios IT y los servicios OT. Es decir, no existe una segmentación entre ambas, lo que puede derivar en posibles brechas de seguridad que deben ser convenientemente analizadas.

En este marco, algunas entidades del sector realizan una vigilancia tecnológica de soluciones que se han implementado en otras regiones del mundo para replicarlas. Con ese fin, mantienen una constante comunicación con asociaciones sectoriales regionales e internacionales. Se considera necesaria la realización de auditorías periódicas o de análisis de ciberseguridad en los elementos y organizaciones que componen el ecosistema aéreo para identificar posibles brechas de seguridad y establecer estrategias de defensa integral ante amenazas de ciberseguridad. La cooperación y el diálogo entre el sector público de seguridad y los actores del sector privado aéreo se hacen todavía más importantes ya que los niveles de avance y de conciencia pueden ser muy heterogéneos.

En cuanto al nivel de digitalización, existen diferencias en las empresas que operan servicios de transporte aéreo. Las de mayor nivel, aun estando más expuestas a posibles ciberincidentes y siendo más sensibles a los aspectos de ciberseguridad, encuentran dificultades para la implementación y aplicación de medidas de seguridad, como cantidad limitada de recursos, especialización de personas, etc. Pero hay coincidencia en la necesidad de reforzar los mecanismos de protección, establecer vínculos de cooperación y dedicar mayores recursos financieros y humanos a los aspectos de ciberseguridad.

En cuanto a la formación en ciberseguridad, se identifican necesidades en dos ámbitos: por una parte, una capacitación orientada a concienciar al personal de las organizaciones que trabajan en el ecosistema aeroportuario de las posibles amenazas que pueden derivar, por ejemplo, del mal uso de los sistemas, el acceso no controlado por parte de terceras empresas, la mala gestión de las credenciales y la falta de rigor en la salvaguarda de información confidencial; y, por otra parte, una capacitación más formal y especializada que permita a cierto personal entender en profundidad las amenazas a las que se enfrentan y establecer medidas de protección, sea con personal interno o con ayuda de proveedores externos.

Dada la complejidad del ecosistema aéreo, con multitud de sistemas diferentes y distintas tecnologías involucradas, es escaso el talento humano especializado en ciberseguridad que tenga una visión integral y global, lo que implica la necesidad de desarrollar este talento para la región.

Buenas prácticas: Promover la ciberseguridad desde la cooperación en el sector aéreo

ALTA (Asociación Latinoamericana y del Caribe de Transporte Aéreo) es una organización privada sin fines de lucro, cuyo objetivo es coordinar los esfuerzos colaborativos de las empresas miembros para facilitar el desarrollo de un transporte aéreo más seguro, eficiente y amigable con el medioambiente.

Desde esta asociación se lideran múltiples iniciativas en materia de ciberseguridad que impactan a sus miembros del sector privado. Entre otras acciones, cuentan con un comité conjunto con la Asociación Internacional de Transporte Aéreo (IATA) relativo al fraude, que estudia y analiza los fraudes realizados en los sistemas de las aerolíneas, siendo los sistemas de fidelización y de pagos los más afectados.

También acaban de lanzar el comité de ciberseguridad y fraudes cibernéticos, cuya misión es analizar aquellas problemáticas de ciberseguridad que se producen en las aerolíneas.

3.7.2. Sector marítimo

La mayor frecuencia de ataques registrados en los últimos años, tanto en las instalaciones portuarias como en las compañías de transporte logístico, ha impulsado al sector marítimo a reforzar su estrategia de ciberseguridad para proteger las operaciones marítimas.

En materia de protección de infraestructuras críticas, ocurre que, o no hay una regulación, o la hay, pero no se audita su cumplimiento. Ante esta situación, ciertas organizaciones del sector marítimo de la región están adoptando buenas prácticas de ciberseguridad basadas en estándares internacionales, como son el Marco NIST y los controles de seguridad sugeridos por la norma ISO 27000 y el Centro de Seguridad de Internet (CIS), para alinear los procesos de la organización con las mejores prácticas de ciberseguridad existentes en el mundo.

Las empresas concesionarias son las responsables de salvaguardar la ciberseguridad. Sin embargo, muchos de los contratos de concesión de operación de infraestructura portuaria datan de hace unos cuantos años, cuando los aspectos de ciberseguridad no eran considerados tan importantes o no eran tan relevantes. A pesar de este problema, se ha constatado que algunas de ellas disponen de un área de ciberseguridad para atender a estas necesidades.

Existe mucha diferencia en el estado del tratamiento de la ciberseguridad de los actores que conforman el sector. Las grandes infraestructuras portuarias, en general, establecen e implementan mecanismos de ciberseguridad tanto en la parte IT como en la parte OT, acordes a su tamaño y relevancia, dedicándoles recursos financieros y tecnológicos. Al mismo tiempo, existen una multitud de pequeñas entidades que, sea por falta de recursos financieros o de recursos humanos especializados, no cuentan con la capacidad de implementar soluciones de ciberseguridad de una manera integral.

Si bien en las grandes infraestructuras portuarias se están implementando estrategias de ciberseguridad enfocadas tanto en la parte IT como en la OT, existiendo políticas y planes de ciberseguridad, en muchos casos todavía queda un largo camino de análisis e implementación de mecanismos de ciberdefensa que tengan en cuenta todo el ecosistema portuario y las relaciones entre los diferentes actores que lo conforman. Algunos de los actores del sector destacan que es necesario afrontar el problema desde un punto de vista integral.

Algunas entidades del sector llevan a cabo análisis de riesgos y consideran necesario y vital llegar a un mayor nivel de especificidad a la hora de definirlos e identificarlos, para evitar hacerlo en términos muy generales, ya que es necesario realizar los análisis de riesgo de acuerdo con la operativa real de cada entidad.

Desde la administración pública, se considera necesario incluir de manera sistemática aspectos de ciberseguridad en las licitaciones públicas marítimas, de forma tal que puedan ser añadidos contractualmente y luego supervisados y controlados para asegurar que sean debidamente aplicados.

Muchos de los sistemas que se utilizan en las operaciones críticas de gestión portuaria, sobre todo en infraestructuras grandes, han sido diseñados y desarrollados por compañías internacionales que, por lo general, implementan los mecanismos necesarios para garantizar su correcto funcionamiento desde el punto de vista de la ciberseguridad. Aun así, en estos casos es necesario realizar el control y seguimiento de los sistemas y el análisis de posibles incidentes de seguridad.

Muchas entidades del sector marítimo señalan la necesidad de difundir el mensaje de “darle a la ciberseguridad la importancia que merece”. Es decir, manifiestan que la ciberseguridad debe visualizarse como algo necesario y vivo que necesita ser revisado y actualizado desde la perspectiva de todos los actores.

Existen referentes importantes de implementación de sistemas de ciberseguridad en la región. Se observa la necesidad de realizar un esfuerzo para compartir sus experiencias y aplicar buenas prácticas de ciberseguridad con el fin de ayudar a establecer estrategias comunes en el sector, tanto a nivel nacional como regional.

Al igual que en muchos sectores, es necesario ofrecer formación en dos ámbitos: por una parte, una capacitación orientada a concienciar al personal de las diferentes organizaciones que trabajan en el ecosistema portuario de las posibles amenazas que pueden derivar, por ejemplo, del mal uso de los sistemas, el acceso no controlado por parte de terceros, la mala gestión de las credenciales y la falta de rigor en la salvaguarda de información confidencial; y, por otra parte, una capacitación más formal y especializada que permita a cierto personal entender en profundidad las amenazas a las que se enfrentan y establecer medidas de protección, sea con personal interno o con ayuda de proveedores externos.

Buenas prácticas: Promover la capacitación en colaboración con actores internacionales

En Brasil, a través de un acuerdo con la IMO (International Maritime Organization), el personal de diversas autoridades portuarias es formado en cursos especializados en universidades europeas sobre temas de ciberseguridad en el sector portuario. Asociaciones sectoriales, como la Asociación Americana de Autoridades Portuarias, también organizan seminarios y eventos que abordan el tema de la ciberseguridad en el sector.

3.7.3. Transporte terrestre carretero y transporte público

En esta sección incluimos las conclusiones del análisis tanto del estado de la ciberseguridad en el transporte público como en el transporte carretero. Como conclusiones sobre el estado del sector podemos destacar:

- En los ITS se constata una preocupación general por los aspectos de ciberseguridad, sobre todo en lo que atañe a los que se denominan *sistemas auxiliares de operación,* como pueden ser los sistemas de pago o de control de personas, lo que ha impulsado, en algunos casos, mecanismos de ciberseguridad para evitar ataques a dichos sistemas.

- Una buena práctica referida en este tema que podría servir para concienciar aún más a las autoridades y a las empresas privadas es cuantificar el costo de no tener ciertas prácticas de ciberseguridad y el ahorro que supone invertir en soluciones que minimicen ese costo.

- Al igual que en el resto de los segmentos de transporte, se suelen implementar controles de seguridad relacionados con la parte IT, existiendo una falta de incorporación de controles de seguridad aplicados a la parte OT.

- No existe la costumbre de exigir requisitos de ciberseguridad OT a los proveedores de sistemas y a los concesionarios, al menos por parte de la mayoría de las organizaciones responsables de escribir los términos de referencia, aunque sí se incluyen aspectos relacionados con ciberseguridad IT general. No obstante, se ha constatado que algunas suelen exigir a sus proveedores la aplicación de mecanismos de seguridad tanto a nivel IT como a nivel OT.

- En los grandes gestores de infraestructura de transporte terrestre se observa la implementación de buenas prácticas de ciberseguridad internacionales, sobre todo las establecidas por la norma ISO 27001 y controles de CIS.

- En muchos casos se adoptan planes de ciberseguridad que siguen los estándares mundiales, pero no siempre son adecuadamente aplicados ni actualizados.

- Algunas entidades realizan ejercicios de *hacking* ético para determinar cómo están los sistemas, pero muchas veces no tienen en cuenta la especificidad de los

sistemas OT o de la operación de la entidad, y a menudo los resultados de estos ejercicios se reducen a una serie de recomendaciones y estudios que no contemplan toda su infraestructura.

- Al igual que en los sectores aéreo y marítimo, es necesario ofrecer formación en dos ámbitos: por una parte, una capacitación orientada a concienciar al personal de las diferentes organizaciones que pertenecen al ecosistema de transporte terrestre y, por otra parte, una capacitación más formal y especializada que permita a cierto personal de las organizaciones entender en profundidad las amenazas a las que se enfrentan y establecer medidas de protección, sea con personal interno o con ayuda de proveedores externos. Es patente la falta de expertos en ciberseguridad en ITS.

- En algunos países existe la creencia, al menos en ciertos sectores públicos, de que se debe tener la información en las instalaciones, *on-premise,* en vez de en la nube. Lo anterior evidencia que hay resistencia a alojar información fuera de las instalaciones de las entidades por miedo a su robo o a su degradación, o por falta de confianza en los proveedores en la nube.

- Se está produciendo una modernización de muchos sistemas del sector de transporte terrestre (dispositivos o elementos con mayor conectividad, mayor número de dispositivos localizados en las ciudades con acceso a los sistemas de control), lo que hace necesario incluir aspectos de ciberseguridad que anteriormente no se consideraban por el tipo de sistemas que se utilizaban o, en algunos casos, todavía se usan.

- Se evidencia una carencia de herramientas tecnológicas que permitan alertar de forma temprana ante incidentes de seguridad. Algunas instituciones han desarrollado SOC y otras han empezado a monitorear los sistemas más críticos en busca de anomalías; en general, hay mucho margen de mejora, tanto en las instituciones públicas como en las privadas.

- Hay entidades que en sus desarrollos internos incorporan prácticas que tienen en cuenta los riesgos de seguridad y las pautas establecidas por el Proyecto Abierto de Seguridad de las Aplicaciones Web (OWASP por sus siglas en inglés). En algunos casos, se han creado protocolos de desarrollo que establecen procesos de verificación para revisar los controles de seguridad (autenticación, sesión, manejo de datos, redirección, consumo de servicios, etc.).

Buenas prácticas: Cláusulas licitatorias

Una buena práctica que las entidades de transporte público de la región están implementando es la inclusión de estándares y auditorías de ciberseguridad en sus cláusulas licitatorias. Esto permite seleccionar mejor posibles proveedores y garantizar la atención a los temas de ciberseguridad a lo largo del ciclo de vida de un proyecto. En Colombia, la empresa Transmilenio S.A., a cargo del Sistema Integrado de Transporte Público de Bogotá, las incluye en sus licitaciones de tecnología y, también, en cláusulas y contratos con concesionarios. En Chile, igualmente, la Unidad Operativa de Control de Tránsito, a cargo de los ITS en muchas ciudades del país, introduce temas de ciberseguridad en las especificaciones técnicas de sus procesos de licitación.

3.8. Presupuestar la ciberseguridad: una inversión a futuro

Otro aspecto relevante identificado por organizaciones del transporte en ALC en materia de ciberseguridad es la conciencia de las necesidades presupuestarias. Muchas de las entidades entrevistadas manifestaron que, en su entorno, la ciberseguridad se ve como un gasto y no como una inversión. Es necesario que esta mentalidad se transforme y que se entienda, desde los Gobiernos, que es necesario invertir en ciberseguridad, tanto en tecnología como en talento humano.

Se han hecho esfuerzos, como, por ejemplo, en Perú, donde el Centro Nacional de Seguridad Digital (CNSD) cubre algunas necesidades de ciertas entidades que no tienen presupuesto suficiente, proveyendo servicios como detección de vulnerabilidades o evaluaciones forenses cuando se han producido incidentes.

Una buena práctica, que podría ayudar a cambiar la mentalidad, es la de cuantificar el costo de no tener ciertas prácticas de ciberseguridad en caso de producirse una caída en un servicio crítico y estimar las pérdidas en casos de incidentes para así valorar la necesidad de invertir en soluciones que mitiguen estos costos.

3.9. Conclusión sobre el estado de la ciberseguridad del sector del transporte en la región

La región ha hecho progresos significativos en ciberseguridad en los últimos 20 años, desde 2004, con la implementación de la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética. Se han establecido los CSIRT y se han creado estrategias y adoptado normas técnicas y legislación específica para delitos cibernéticos. Sin embargo, el nivel de madurez promedio de la región sigue siendo bajo, aunque se están tomando medidas para mejorar las capacidades en ciberseguridad.

En el sector del transporte, la ciberseguridad está comenzando a ser una prioridad, con los subsectores aéreo y marítimo más avanzados que los subsectores de transporte carretero y público. Sin embargo, la diferencia en ciberseguridad está marcada por el tamaño de la entidad y su interconexión con actores internacionales.

En cuanto a las IT, casi todos los actores reconocen las amenazas que conciernen a la ciberseguridad y han comenzado a tomar medidas. Sin embargo, en las OT hay una menor conciencia de los peligros. El sector del transporte tiene todavía mucho camino que recorrer para garantizar la resiliencia de sus infraestructuras en una era en la cual las amenazas no harán sino crecer.

El rol de la cooperación internacional en la promoción de la agenda de ciberseguridad ha sido importante en política nacional y asociaciones sectoriales. Infortunadamente, estos esfuerzos no han llegado a todo el sector del transporte, y, sobre todo, alcanzan muy poco a la constelación de pequeñas y medianas empresas que constituyen la mayoría de los actores en el sector.

Otra conclusión es que hay una gran necesidad de invertir financieramente y crear talento especializado en temas de ciberseguridad, tanto en general como con enfoque en el sector del transporte.

4

Recomendaciones y hoja de ruta

A partir de la investigación y el análisis de las mejores prácticas internacionales y del contexto de la región, se expone en esta parte una serie de recomendaciones para los formuladores de políticas en el sector del transporte. También se presenta la Herramienta de Autoevaluación en Ciberseguridad para organizaciones del sector del transporte desarrollada por el BID para la región.

Se reconoce, nuevamente, la complejidad y multidimensionalidad del sector del transporte, que se refleja en la variada tipología y naturaleza de las organizaciones que lo componen.

4.1. Recomendaciones para formuladores de políticas

La forma en la que se gestionan y operan las infraestructuras del transporte puede ser diferente de un país a otro, involucrando a agentes tanto públicos como privados. Establecer cómo gobernar la seguridad y resiliencia en el sector del transporte es, por tanto, uno de los primeros retos, debido a las múltiples funciones y responsabilidades distribuidas.

Cabe hacer hincapié, igualmente, en la transversalidad y la inherente internacionalidad de las amenazas cibernéticas actuales. Se entiende que una buena política pública de ciberseguridad debe ser integral, sostenible en el tiempo y con una visión a largo plazo en las agendas de políticas públicas de la región, con amplios recursos financieros y humanos.

4.1.1. Sobre el gobierno de la ciberseguridad nacional

Normalmente, los Estados inician el camino hacia la ciberseguridad partiendo de la definición de un marco para la mejora de la seguridad cibernética general. De manera paralela, en muchas ocasiones las infraestructuras críticas se reconocen o se han reconocido históricamente como un ámbito al que se debe prestar especial atención en materia de seguridad. No obstante, puede ocurrir que estas iniciativas lleven muchos años en vigor y no incluyan explícitamente aspectos de seguridad cibernética. Si este es el caso, una primera acción suele ser alinear y complementar ambas aproximaciones; es decir, el marco general de ciberseguridad y el marco de seguridad de infraestructura crítica.

En este caso, suele definirse un marco legal para la protección de infraestructuras críticas, cuyo ámbito de aplicación son tanto las entidades públicas como privadas y, sobre todo, aquellas que provean de servicios especialmente críticos por su singularidad o que conlleven riesgos significativos en la región. No obstante, cada vez es más común observar que muchas de las brechas de ciberseguridad se encuentran en las empresas muy pequeñas a través de las cuales los cibercriminales alcanzan objetivos de mayor interés. Por eso, en Europa, por ejemplo, se ha promovido la publicación de la actualización de la directiva NIS2, que plantea la necesidad de involucrar a entidades de toda la cadena de suministro del sector.

Dos de los aspectos o acciones que se promueven en estos marcos son:

1. La generación de un inventario de las infraestructuras críticas del país, que se mantiene actualizado a lo largo del tiempo.

2. El establecimiento de ciertas obligaciones para las entidades que operan o gestionan parte de este inventario, tales como abordar una gestión de riesgos (incluyendo cibernéticos) y notificar incidentes significativos a la mayor brevedad.

Conocer las especificidades propias a las que se enfrenta el sector del transporte es de vital importancia, por lo que resulta imprescindible involucrar a entidades relevantes del propio sector, tanto del ámbito público como privado, para adaptar, difundir, promover e incluso monitorear y hacer cumplir las regulaciones y normas que se establezcan. Es necesario, por tanto, que se analice en profundidad la estructura de gobierno que se va a diseñar para llevar adelante todas las funciones y distribuir las responsabilidades que van a ser requeridas en los diferentes estamentos del sector.

No puede obviarse que el transporte tiene asociado un ecosistema complejo de entidades, tanto en tipología como en extensión geográfica, cuando se consideran, por ejemplo, flujos de transporte internacionales. Esto hace que existan muchas dependencias e interconexiones entre entidades, e incluso entre países o regiones, y deriva en la necesidad de establecer mecanismos que fomenten la comunicación y cooperación para hacer frente a ciberamenazas o ciberataques y sus efectos. Un incidente en una infraestructura como un aeropuerto puede afectar la operación y negocios de otros países, incluso facilitar la amplificación del ataque, ya que las empresas que se ven afectadas en una ubicación pueden extender el problema a otras regiones donde también estén operando sus servicios.

Desde los propios entes públicos, se puede fomentar el establecimiento de marcos de colaboración internacionales, la promoción de eventos o encuentros específicos para determinados agentes o segmentos del sector del transporte, etc., en los que se puedan poner en común buenas prácticas, compartir conocimiento e incluso desarrollar grupos de trabajo que sean capaces de identificar nuevas amenazas y diseñar soluciones de prevención de forma conjunta.

Este último aspecto, el de la capacitación y la concientización, es otro de los que no deben faltar en las actuaciones prioritarias que se realicen desde la administración pública. Entre sus responsabilidades está crear un ecosistema que facilite la capacitación de su personal y promover una cultura de ciberseguridad en los diferentes sectores económicos y la población en general, para lo que necesariamente se debe colaborar con entidades del sector y con el sector académico.

4.1.2. Entidades y agentes relacionados con el sector

El incremento de la ciberresiliencia del sector del transporte no es responsabilidad única de los Gobiernos. Otros agentes relevantes de los propios segmentos del transporte y de la ciberseguridad pueden, e incluso deben, participar y mejorar el nivel de seguridad cibernética del sector. Entre ellos se encuentran las asociaciones empresariales, sectoriales o clústeres de transporte. Son entidades que conocen en profundidad la problemática de las empresas que forman el sector y están en continuo contacto con ellas.

Algunas de las recomendaciones sobre actuaciones que pueden realizar son:

1. **Participar en los grupos de trabajo que se promuevan desde las administraciones y Gobiernos:** El conocimiento que tienen de la realidad del sector hace que estas asociaciones sean un canal de comunicación bidireccional eficiente entre empresas y Gobierno. Muchos segmentos empresariales del transporte están constituidos por mipymes, que no pueden destinar recursos para ciertas actividades, más allá de la operación de su negocio. Por ello, las asociaciones sectoriales son necesarias, en primer lugar, para la transmisión de las necesidades del sector al Gobierno, al facilitar que este promueva o diseñe respuestas adecuadas para las empresas del transporte. En segundo lugar, las asociaciones pueden facilitar la comunicación y llegada de los mensajes a las empresas, eligiendo los medios y tiempos para ello.

2. **Sensibilizar a las empresas del sector:** La cercanía de las asociaciones del sector a las empresas puede ayudar a transmitir con mayor eficacia los mensajes sobre

la importancia de la ciberseguridad en la gestión de los riesgos que se corren, con el fin de construir empresas resilientes que puedan enfrentarse a las amenazas cibernéticas. Es fundamental que las asociaciones del sector destinen recursos a generar sesiones de sensibilización y organizar foros de discusión e incluso de capacitación sobre riesgos cibernéticos y medidas de higiene cibernética mínimas que puedan ser adoptadas por diferentes tipos de empresas.

3. **Promover la generación de la definición de prácticas y procedimientos de ciberseguridad específicos para el sector:** Esta acción puede realizarse en coordinación con expertos en metodologías, estándares y tecnologías de ciberseguridad. Los expertos pueden ser buenos conocedores desde el punto de vista técnico, pero probablemente carezcan de la visión de los retos y dificultades propios del sector. La propia asociación puede conocer la viabilidad de aplicar ciertas cuestiones en determinados subsegmentos, por las dificultades que derivan de su tamaño, su capacidad técnica, sus recursos y limitaciones, etc. En algunos casos, además, es fundamental tener una visión del contexto en el que operan las empresas y las amenazas a las que se enfrentan. Facilitar metodologías de análisis de riesgos del propio sector puede ser un primer paso para que algunas de ellas aborden una evaluación y gestión de sus riesgos cibernéticos.

La participación del sector académico también es importante para mejorar la capacitación de los profesionales. En este sentido, existen actividades que se pueden realizar desde la academia, tales como:

1. **Diseño de capacitaciones en ciberseguridad para el transporte:** Se pueden diseñar módulos específicos destinados a actuales y futuros profesionales. En este aspecto, hay que considerar las diferentes ofertas formativas que se pueden necesitar, al menos, en los siguientes perfiles:

    - Los perfiles de ingeniería, economía o similares que participan en funciones de gestión y operación de las empresas del transporte, ya que deben incorporar aspectos de análisis o evaluación de los riesgos cibernéticos y las medidas que se pueden diseñar para su gestión.

    - Los perfiles técnicos que diseñan y desarrollan equipamiento y productos utilizados en los diferentes segmentos del transporte. Es fundamental que esos productos incluyan una aproximación de ciberseguridad desde el diseño.

    - Los perfiles destinados a trabajar en el sector de la ciberseguridad, con el fin de que conozcan ciertas especificidades que se aplican a los sectores críticos en general, en especial aquellos cuya operación tiene como base tecnologías del ámbito de la ciberseguridad industrial, como el transporte, la energía, etc.

2. **Captación de talento para la ciberseguridad en transporte:** En este punto se considera la necesidad de promover el interés en este tipo de estudios. Para ello, pueden proponerse ciertas actividades, tales como competiciones de estudiantes para la resolución de retos en ciberseguridad, propuestas por empresas del sector del transporte o el establecimiento de acuerdos para la estancia en prácticas en sus instalaciones.

3. **Participación en proyectos de I+D+i:** Desde las propias universidades se puede promover la participación en proyectos de I+D+i en coordinación con empresas del sector del transporte. De esta manera pueden abordarse problemas específicos del sector que requieran de una investigación tecnológica, pero también de una transferencia de conocimiento, así como mejorar aspectos organizativos a través de proyectos de innovación. Los propios proveedores de productos y servicios para empresas de transporte pueden ser participantes claves en este tipo de actividad, ya que deben avanzar con el fin de incrementar la ciberseguridad de sus desarrollos.

Es importante que el propio sector de ciberseguridad trate de ofrecer soluciones especializadas para el transporte, particularmente en la región, donde el mercado crece constantemente. En este sector hay proveedores de productos y servicios gestionados de ciberseguridad que pueden realizar las siguientes actividades:

1. Especialización de productos para OT en transporte: A nivel corporativo o IT, las empresas de transporte pueden beneficiarse de los productos de ciberseguridad de aplicación general. Sin embargo, en operación OT pueden existir muchas especificidades derivadas del equipamiento de tipo industrial utilizado y de los protocolos y estándares técnicos de aplicación que se requieren para el sector. Por ello, es necesario que los proveedores de soluciones de ciberseguridad, como sistemas de prevención y monitoreo de ciberseguridad, consideren esas necesidades y hagan un esfuerzo por cumplir los requisitos que se imponen.

2. SOC especializados: Además de proveedores de productos, los proveedores de servicios de seguridad gestionados, así como los propios CERT/CSIRT, deberían mejorar sus conocimientos del sector y adecuarse también a sus necesidades.

Una de las cuestiones que pueden ser impuestas, sea legalmente o por ciertas partes del sector, es la certificación de productos, organizaciones e incluso profesionales en ciberseguridad. En este sentido, es necesario contar con las entidades de certificación preparadas y acreditadas para emitir certificaciones de las normativas y estándares específicos.

4.2. Hoja de ruta

En este apartado, se ofrece una visión de las diferentes actuaciones propuestas para incorporar en una hoja de ruta que pueda llevarse a cabo desde los propios Estados o administraciones públicas. En muchas de estas actuaciones, no obstante, se pone de manifiesto la necesidad de compartir o involucrar a algunos agentes relevantes del sector ya mencionados.

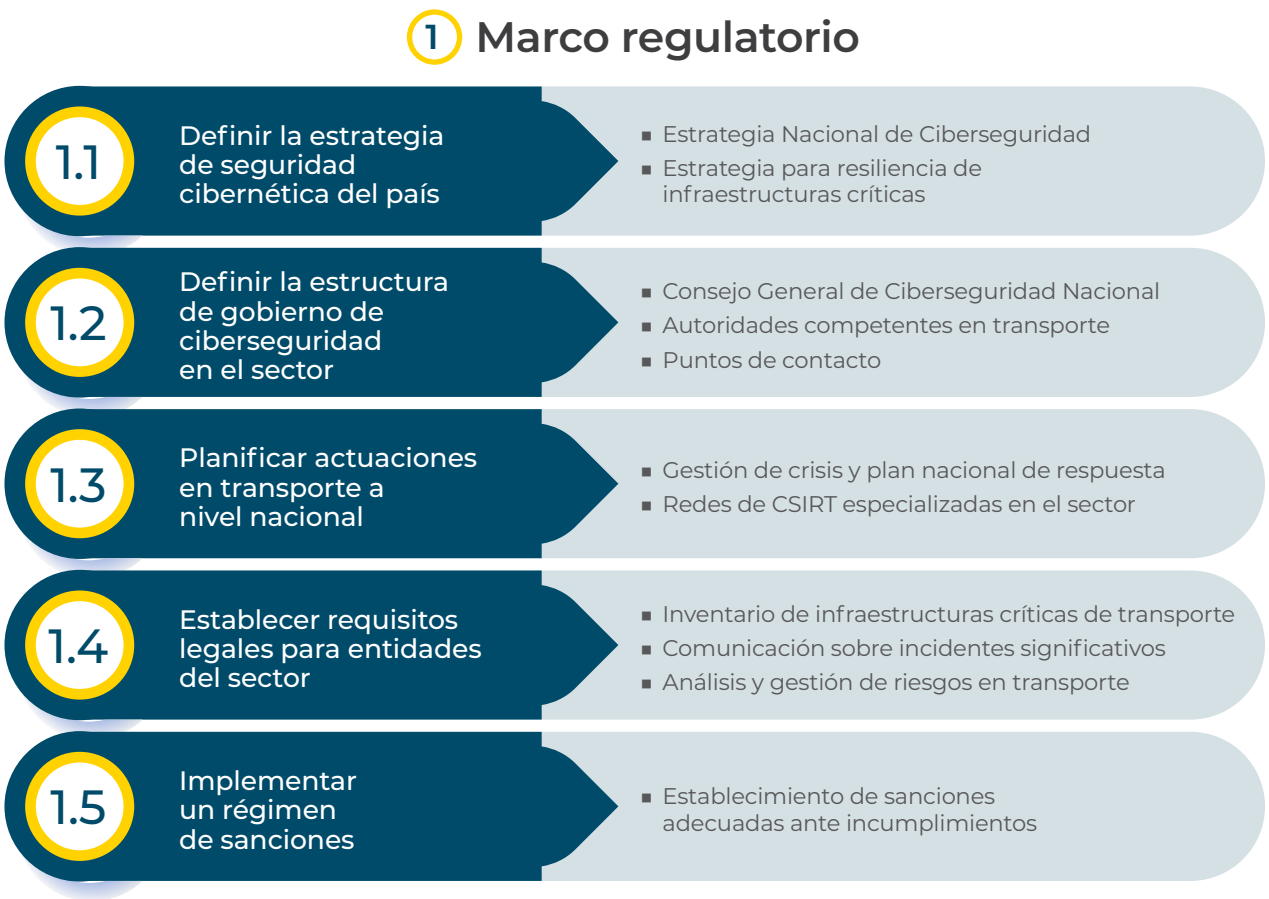
La hoja de ruta para las administraciones públicas se divide en actuaciones que responden a cuatro objetivos concretos:

Figura 9. Resumen de objetivos de la hoja de ruta de administraciones públicas

Fuente: Elaboración propia.

Las siguientes figuras resumen las actuaciones correspondientes a cada uno de los objetivos mencionados anteriormente:

Figura 10. Resumen de actuaciones del marco regulatorio



Fuente: Elaboración propia.

Figura 11. Resumen de actuaciones de protección ante ciberamenazas

Fuente: Elaboración propia.

Figura 12. Resumen de actuaciones de respuesta y recuperación de incidentes

Fuente: Elaboración propia.

Figura 13. Resumen de actuaciones de instrumentos de mejora

Fuente: Elaboración propia.

4.2.1. Marco regulatorio

Objetivo 1

Disponer de un marco regulatorio que facilite la implementación de medidas de protección de infraestructuras críticas del sector del transporte.

Actividad 1. Definir la estrategia de seguridad cibernética del país

- **Estrategia nacional de ciberseguridad**

Uno de los primeros pasos debe ser contar con una estrategia nacional de ciberseguridad que establezca los objetivos estratégicos, los recursos necesarios para alcanzarlos y las medidas apropiadas para conseguir y mantener el nivel de seguridad cibernética deseado. Aun existiendo una estrategia común para todo el país, es necesario revisar y evaluar la adecuación de esa estrategia al propio sector del transporte. Por lo tanto, se pueden evaluar aspectos tales como:

- Objetivos y prioridades de los sectores considerados, teniendo en cuenta la posibilidad de que se extienda no solo a las entidades fundamentales del sector del transporte, sino también a toda su cadena de suministro.

- Marco de gobernanza que aclare funciones y responsabilidades a nivel nacional y facilite la cooperación y coordinación entre autoridades competentes, tanto las del sector como aquellas con las que se tengan relaciones.

- Posible mecanismo para identificar entidades o activos críticos o esenciales del sector del transporte en los que una disfunción o interrupción del servicio pueda provocar problemas significativos en toda la nación.

- Medidas específicas para garantizar que las entidades del sector se encuentren preparadas para enfrentar posibles incidentes cibernéticos y para responder y recuperarse en caso de que se produzcan. Hay que tener en cuenta que muchas entidades del sector incluyen elementos tanto del nivel IT (corporativo) como del OT (de operación), por lo que se hace especialmente necesario tomar medidas propias de lo que se denomina *ciberseguridad industrial*.

- Mecanismos para cooperar e intercambiar información entre los diferentes agentes o entidades del sector, no solo en el ámbito regional o nacional, sino también transnacional.

- Planes y actuaciones para elevar el nivel de concientización y capacitación de las entidades y personas que forman parte del sector, y también de la ciudadanía en general.

- **Estrategia de resiliencia de entidades críticas**

  Además de una estrategia general de ciberseguridad, suele ser de interés definir una estrategia de resiliencia de entidades críticas, entre las que normalmente se consideran sectores como los de energía, finanzas, salud o transporte. En ocasiones estas estrategias ya existen, pues mantener y mejorar la resiliencia de estos sectores es fundamental no solo para el país, sino también en muchos casos para los países limítrofes. Por ejemplo, en las redes de energía y transporte, el nivel de codependencia entre dos Estados puede ser alto.

  La estrategia de resiliencia de infraestructuras críticas debe considerar todo tipo de riesgos —físicos, medioambientales, sociales, etc.—. Es fundamental que estas estrategias estén actualizadas y alineadas con la estrategia nacional de ciberseguridad y que, por tanto, incluyan también los riesgos cibernéticos y las medidas necesarias para hacerles frente.

Actividad 2. Definir la estructura de gobierno de la ciberseguridad en el sector

- **Consejo Nacional de Ciberseguridad**

  La complejidad de las autoridades y competencias en materia de seguridad y ciberseguridad a nivel nacional y las dependencias y relaciones que existen entre los diferentes sectores y organismos de la administración hacen que sea de interés definir un Consejo Nacional de Ciberseguridad en el que tomen parte representantes del sector del transporte, además de otros sectores, como el de las infraestructuras de comunicaciones o los responsables de la transformación digital del país.

- **Autoridades competentes**

  Es necesario designar autoridades competentes en materia de ciberseguridad en transporte, tanto a nivel público como privado. Estos organismos deben ser responsables de que las estrategias y disposiciones regulatorias establecidas se apliquen correctamente en el sector. Es decir, estas autoridades deben velar por la aplicación del marco regulatorio a escala nacional y podrán tener asignadas las funciones de supervisión de las entidades del sector, tanto públicas como privadas, que sean necesarias.

- **Puntos de contacto**

  Adicionalmente, es de interés establecer un punto de contacto único en el país que ejerza de enlace para garantizar la cooperación transnacional e intersectorial con otras autoridades competentes del país que pueda ser necesaria para coordinar actuaciones con otros sectores relacionados.

Actividad 3. Planificar actuaciones en transporte a nivel nacional

En el sector del transporte, la probabilidad de que se produzca un incidente más allá del ámbito local, que afecte a una región geográfica o social amplia, es bastante alta. Ofrecer

una respuesta ante una crisis a nivel nacional resulta, por tanto, fundamental, por lo que es de interés disponer de un marco nacional de gestión de crisis a gran escala y definir un plan nacional de respuesta a incidentes.

En este plan se consideran las funciones y responsabilidades de las diferentes autoridades competentes ante una crisis de ciberseguridad, detallando las medidas y actividades que deben realizar en materia de preparación y los procedimientos a seguir ante incidentes significativos en la infraestructura o entidades críticas del transporte. Su implementación a escala nacional busca facilitar la cooperación y la coordinación de actividades en todo el país. El objetivo final es articular una respuesta de forma que el sector pueda ofrecer y mantener niveles de servicio mínimos para otros sectores dependientes y para la ciudadanía en general.

- **Red de CSIRT**

  Designar o establecer uno o varios CSIRT de referencia para el sector y sus diferentes subsegmentos es de interés para mejorar la resiliencia del sector del transporte. Estos CSIRT deben ser los responsables de la gestión de incidentes conforme a un procedimiento claramente definido.

  Además, se deben proveer mecanismos para facilitar la cooperación entre los CSIRT del sector o con otros CSIRT nacionales o internacionales, de modo que se faciliten intercambios de información para estar preparados ante amenazas o dar respuestas coordinadas cuando proceda.

Actividad 4. Establecer requisitos legales para entidades del sector

- **Inventario de infraestructuras críticas**

  Es necesario disponer de un inventario actualizado de infraestructuras críticas de transporte para el país. Para ello, el Estado debe hacer una evaluación de riesgos a nivel nacional, que considere si la entidad presta servicios esenciales, si opera infraestructuras críticas en su territorio y si un incidente que la afecte puede llegar a tener un efecto significativo en la economía o el medioambiente del país.

  Además, debe desarrollar un mecanismo para la actualización del inventario y la revisión de los riesgos de forma periódica. La información referente a las entidades incluidas en dicho inventario debe ser comunicada tanto a las propias entidades como a las autoridades competentes en materia de seguridad.

- **Comunicación de incidentes significativos**

  Es importante asegurarse de que cualquier incidente que tenga un impacto significativo sea notificado lo más pronto posible, especialmente si se produce en alguna de las entidades identificadas como críticas en el sector.

  La notificación debe realizarse a las autoridades competentes y puntos de contacto establecidos con información suficiente para que se puedan evaluar las

consecuencias y medidas que adoptar. Se debe facilitar la participación de los CSIRT especializados en el sector para dar respuesta al incidente concreto.

Cuando proceda, se debe notificar también el incidente y sus efectos a los destinatarios del servicio ofrecido por la entidad de transporte afectada.

- **Gestión de riesgos en el sector**

El Estado debe asegurarse de que todas las entidades críticas del sector del transporte adopten medidas para la gestión de riesgos cibernéticos.

En el sector del transporte coexisten entidades públicas y privadas. Además, en numerosas ocasiones, algunos segmentos del sector del transporte están constituidos por empresas pequeñas con dificultades para abordar un proceso de transformación digital que también tome en cuenta aspectos de seguridad cibernética. Por lo tanto, podría ser necesario evaluar cuál sería la mejor estrategia para promover requisitos de ciberseguridad en los diferentes tipos de entidades del sector.

En los inicios, y con mayor prioridad, es necesario promover que las propias entidades públicas del sector realicen una gestión de los riesgos para la seguridad de los sistemas de redes e información que utilicen, tanto en sus operaciones como en la prestación de sus servicios. De esta manera, se podrán evaluar más adelante las medidas técnicas, operativas y organizativas adecuadas para abordarlas en cada caso.

Adicionalmente, se debe promover la aplicación de esta actividad también en aquellas entidades, tanto públicas como privadas, que hayan sido identificadas como críticas y formen parte del inventario de infraestructuras críticas del transporte en el país.

En el futuro, este tipo de actuaciones puede extenderse a otras entidades del sector e incluso a la propia cadena de suministro.

Para poder aplicar estas prácticas progresivamente y ampliar su uso a todos los segmentos del sector, puede ser beneficioso incluir, desde las entidades públicas —en las licitaciones o solicitudes de equipamiento o prestación de servicios de terceros— un análisis de riesgos cibernéticos o requisitos de ciberseguridad que los proveedores deban contemplar.

Actividad 5. Implementar un régimen de sanciones

- **Sanciones**

Es necesario establecer sanciones adecuadas para las entidades que incumplan con las obligaciones estipuladas en el ámbito de la seguridad cibernética. Una baja concienciación en materia de ciberseguridad por parte de una entidad puede llevar a que esta considere las medidas de mitigación como un gasto en lugar de una inversión. En consecuencia, podría optar por no implementar dichas medidas si la penalización resultante es inferior al monto que debe invertir. Por lo tanto, es fundamental establecer sanciones que prevengan estas situaciones y que penalicen

el incumplimiento de las medidas destinadas al mantenimiento de la resiliencia en el sistema de transporte del país.

4.2.2. Protección ante ciberamenazas

Objetivo 2

Mejorar la seguridad en el sector a través del desarrollo de medidas de protección ante amenazas cibernéticas.

Actividad 1. Identificar vulnerabilidades y estado de ciberseguridad del sector

- **Divulgación de vulnerabilidades en transporte**

  Uno de los aspectos fundamentales que considerar en materia de seguridad cibernética es tener un conocimiento actualizado de las vulnerabilidades que existen en las organizaciones y sistemas utilizados. En el ámbito nacional, se debe establecer que los CSIRT ofrezcan un servicio de divulgación de vulnerabilidades, especialmente de aquellos sistemas y equipamientos utilizados, tanto a nivel corporativo como operativo, en las organizaciones de los diferentes segmentos del transporte.

  Además, se debe proveer un mecanismo en el CSIRT para facilitar la comunicación de vulnerabilidades detectadas o notificadas a través de cualquier vía (personas físicas, proveedores de equipamiento, empresas de servicios de ciberseguridad, etc.).

  El CSIRT puede actuar como la entidad que facilite la comunicación a las posibles entidades afectadas, informando de la naturaleza y gravedad de la vulnerabilidad, los productos o equipos afectados, las circunstancias en las que puede explotarse y la disponibilidad de posibles parches de seguridad asociados.

- **Informe de situación de ciberseguridad en el sector**

  Además de las vulnerabilidades, es importante realizar un análisis periódico de la situación de la ciberseguridad en el sector, que incluya información sobre ciberamenazas que enfrentan las entidades del sector del transporte, así como ciberincidentes sufridos. Para ello, es relevante la participación de entidades públicas y privadas del sector, por lo que es fundamental que se habiliten mecanismos y canales para la compartición de información en esta materia.

  Adicionalmente, con el fin de establecer un mecanismo para la mejora continua del sector a nivel nacional, resulta útil incluir una evaluación de las capacidades de ciberseguridad, tanto de las entidades públicas como privadas del sector, especialmente de las incluidas en el inventario de infraestructuras críticas. De esta manera pueden definirse acciones para promover o facilitar la adopción de las prácticas requeridas en los diferentes tipos de entidades de la cadena de suministro del sector del transporte.

Desde el Estado se deben analizar cuáles son los organismos necesarios para ejecutar este tipo de actividades. Las funciones pueden distribuirse entre los CSIRT especializados y las autoridades competentes o, incluso, ser promovidas mediante la creación de comités u organismos específicos que involucren a diferentes agentes relevantes del sector.

Actividad 2. Gestionar riesgos y resiliencia de infraestructuras críticas

- **Evaluación de riesgos en entidades críticas del transporte**

  Resulta prioritario promover o, incluso, imponer la adopción de prácticas de gestión y evaluación de riesgos a las entidades identificadas en el inventario de entidades e infraestructuras críticas. En esta categoría, además de los riesgos naturales y de origen humano, se deben considerar aquellos de naturaleza cibernética.

  A la hora de evaluar el riesgo, es preciso valorar el grado de dependencia que tiene la entidad de otros servicios esenciales prestados por otros sectores y viceversa. Es decir, se necesita considerar el impacto que un incidente significativo puede tener en otros sectores económicos, lo mismo que su impacto social o medioambiental.

- **Medidas de resiliencia en el sector**

  La evaluación de riesgos requiere la identificación, definición e implementación de contramedidas que ayuden a gestionarlos y mitigarlos. Por tanto, se debe asegurar que las entidades críticas incluidas en el inventario del sector adopten medidas de carácter técnico u organizativo orientadas a paliar específicamente los riesgos cibernéticos.

  Más allá de que las entidades del transporte realicen estas actividades con personal propio, puede ser de utilidad establecer un comité o grupo de expertos —desde la administración o alguna de las autoridades competentes— que las apoyen y asesoren.

- **Evaluación de antecedentes personales en entidades críticas**

  Las amenazas internas pueden llegar a ser tan importantes o peligrosas como las amenazas externas. Por ello, permitir la comprobación de antecedentes personales —especialmente en personas con responsabilidades, funciones o cargos delicados en una entidad crítica— puede ser una buena práctica.

- **Fortalecimiento de la toma de decisiones**

  Uno de los objetivos que se persiguen es fortalecer la capacidad de toma de decisiones a nivel nacional por parte de las autoridades competentes en la protección de la infraestructura de transporte. Para ello, se puede impulsar el desarrollo de metodologías y herramientas que faciliten un monitoreo de métricas asociadas a los riesgos (cibernéticos) y medidas adoptadas por las entidades críticas del sector.

Actividad 3. Supervisar y controlar requisitos normativos y legales

- **Medidas de supervisión y control de entidades a cargo de infraestructuras críticas**

  Corroborar el cumplimiento de la estrategia y los requisitos normativos o legales impuestos al sector (en particular a las entidades a cargo de infraestructuras críticas) exige establecer mecanismos para que las autoridades competentes designadas tengan la facultad de realizar inspecciones y auditorías. Además, deben supervisar y exigir a las entidades críticas del sector información y pruebas sobre las medidas implementadas.

  En caso de detectar incumplimientos, las autoridades pueden llegar a emitir órdenes para subsanarlos o, incluso, exigir sanciones.

Actividad 4. Cooperar a escala nacional

- **Comité de resiliencia para entidades críticas del transporte**

  Para garantizar una correcta cooperación a escala nacional en materia de resiliencia en transporte, se puede impulsar la creación de un comité conformado por representantes de autoridades competentes y agentes relevantes del sector (públicos o privados). Su objetivo es intercambiar información sobre diferentes aspectos de seguridad para reforzar la capacidad de garantizar la resiliencia de las entidades críticas. Este grupo puede analizar mejores prácticas, contribuir a la definición de directrices y políticas de seguridad específicas para los diferentes segmentos del transporte, etc.

- **Mecanismos de intercambio de información**

  El intercambio voluntario de información sobre ciberseguridad entre entidades del sector puede facilitar la prevención, detección, respuesta y recuperación de incidentes.

  Es de suma importancia que la administración pública se encargue de facilitar la generación de herramientas que permitan compartir este tipo de información, en particular aquella relacionada con amenazas, vulnerabilidades, incidentes, indicadores de compromiso, tácticas de adversarios y recomendaciones sobre la configuración de equipamiento propio utilizado en el sector, entre otros aspectos. En este sentido, hay que prestar especial atención a dos cuestiones:

  – Las herramientas de este tipo deben respetar los derechos de privacidad y confidencialidad de la información que las entidades deseen establecer. Numerosos datos son clasificados como altamente sensibles. Para que las entidades estén dispuestas a compartir determinada información, es necesario establecer un mecanismo que impida su accesibilidad.

  – Difundir y distribuir este tipo de herramientas entre las asociaciones, comunidades y entidades clave —*early adopters* o *usuarios clave* del sector— puede ser una buena práctica para conseguir mayor impacto.

Actividad 5. Cooperar a escala internacional

- **Canales de colaboración internacional**

  Los ataques significativos que se producen a gran escala en una infraestructura de transporte pueden comprometer no solamente los servicios y operaciones del propio país en el que reside la infraestructura, sino los de otros países colindantes. Incluso pueden afectar a otras entidades internacionales que operen o hagan uso de la infraestructura de la región.

  Una función que algunas de las autoridades de ciberseguridad del sector del transporte pueden asumir es explorar vías para establecer acuerdos de colaboración internacionales con terceros países u organizaciones internacionales que cooperen tanto en la preparación ante amenazas como en la respuesta ante incidentes.

4.2.3. Respuesta y recuperación de incidentes

Objetivo 3

Mejorar la eficacia en la respuesta y recuperación ante incidentes de ciberseguridad en el sector del transporte.

Actividad 1. Especializar y capacitar técnicamente a los CSIRT

- **Competencias de los CSIRT sectoriales**

  Es fundamental que los CSIRT designados como responsables iniciales de la gestión de incidentes en el sector estén dotados de los recursos y capacidades necesarios para cumplir sus funciones. Esto supone la disponibilidad de herramientas, capacidades y conocimientos específicos de los riesgos y amenazas que puede sufrir el sector del transporte.

  Cobra importancia considerar que, a nivel operacional, muchas entidades y operadores de transporte utilizan equipamientos industriales, lo cual exige conocimientos específicos de ciberseguridad industrial.

  Los propios CSIRT, además, deben estar concebidos como infraestructuras seguras y resilientes. Por un lado, van a ser gestores de información muy sensible, lo que conllevará la necesidad de que garanticen su confidencialidad y fiabilidad. Por otro, van a ser entes muy relevantes en la coordinación de las operaciones de respuesta, por lo que se deben prever mecanismos para mantener y garantizar la disponibilidad y continuidad de los servicios que ofrecen.

Actividad 2. Notificar incidentes de ciberseguridad

- **Procesos de notificación eficientes**

Para ofrecer una respuesta rápida, es fundamental tener conocimiento de los incidentes de ciberseguridad lo antes posible. Es útil, por lo tanto, generar mecanismos que faciliten a las autoridades competentes la recepción de la información relevante de un incidente a través de sistemas que fomenten el reporte de incidentes en tiempo real y en un formato estandarizado.

Este tipo de herramienta debe facilitar, además, un análisis más inteligente de los datos; por ejemplo, al correlacionar eventos en diferentes entidades, podrían identificarse estrategias asociadas a campañas de ataque de mayor complejidad.

Actividad 3. Entrenar en respuesta y recuperación

- **Divulgación de planes de respuesta y recuperación**

Además de contar con un plan nacional de gestión de crisis, se pueden diseñar procedimientos tanto estandarizados como especializados para los diferentes tipos de organizaciones y segmentos del sector del transporte con el fin de facilitar la mejora de las capacidades de recuperación. Estos procedimientos pueden divulgarse a través de los CSIRT del sector en forma de *manuales* que las organizaciones pueden adaptar según sus particularidades.

Los procedimientos deben considerar posibles disfunciones o incidentes cibernéticos que sucedan en el nivel corporativo (IT) y en el nivel de operación (OT), ya que las entidades del sector del transporte pueden verse afectadas en ambos niveles y la recuperación puede conllevar diferentes estrategias en cada uno.

- **Entrenamiento y campos cibernéticos**

El entrenamiento de los procedimientos de respuesta y recuperación puede mejorar desplegando infraestructuras de campos cibernéticos especializados para el sector. Estas infraestructuras, opcionalmente, pueden ser gestionadas por la red de CSIRT especializados.

A través de los campos cibernéticos es posible realizar simulacros de incidentes y pruebas tanto de los procedimientos de respuesta y recuperación de las entidades del sector, como de los mecanismos establecidos en los planes nacionales de respuesta sectorial ante posibles crisis.

4.2.4. Instrumentos de mejora

Objetivo 4

Proporcionar un marco de instrumentos que faciliten la incorporación de mejoras para la ciberseguridad en el ecosistema del sector del transporte.

Actividad 1. Promover esquemas de certificación

- **Estándares para la gestión de la ciberseguridad**

  El mercado impone numerosas normas técnicas. No obstante, existen situaciones en las que, aunque no se requiera de manera explícita, la aplicación de normas y especificaciones técnicas internacionales puede resultar beneficiosa para mejorar la resiliencia de las organizaciones.

  Puede ser útil, por lo tanto, que desde la propia administración se impulse o fomente, sobre todo en organizaciones críticas, la utilización de ciertas normas, estándares o marcos de ciberseguridad sin imponer o favorecer el uso de tecnologías específicas. Cabe mencionar que existen estándares, tales como las normas ISO 27001, IEC/ISO 62443 y el Marco NIST, entre otros, que pueden facilitar a las organizaciones la implementación de un proceso de mejora continua en su sistema de gestión de la seguridad cibernética.

- **Normas y especificaciones técnicas para productos**

  Al igual que en el caso anterior, la utilización o aplicación de especificaciones técnicas que consideren aspectos de ciberseguridad en productos (o servicios/proveedores) puede ser de interés para incrementar el nivel de ciberseguridad en el sector. En estos casos se puede promover o, incluso, exigir a entidades esenciales que utilicen productos, servicios o procesos que incorporen tecnologías de información y comunicaciones, y que estén certificados bajo algún esquema nacional o internacional de ciberseguridad. Igualmente, se puede promover el uso de servicios de confianza cualificados.

- **Certificación de profesionales clave**

  Además de las organizaciones y productos, puede ser exigible que el personal clave de las entidades responsables de la seguridad cibernética cumpla con ciertos estándares de cualificación en materia de ciberseguridad. Impulsar desde la propia administración instrumentos que fomenten la certificación de este personal es una práctica recomendable, que además facilita el reconocimiento de la excelencia para muchos profesionales en este ámbito. En situaciones de esta índole, puede resultar beneficioso ofrecer mecanismos o incentivos (financiación de estudios, disponibilidad en horario laboral, permisos retribuidos, etc.) que faciliten la realización de estudios y prácticas y la obtención de las pruebas de certificación correspondientes.

Actividad 2. Capacitar y concientizar al personal

- **Capacitación de profesionales reglada**

  El propio sector de ciberseguridad manifiesta en ocasiones que las entidades de formación oficiales (escuelas de formación profesional, universidades, etc.) no disponen de una oferta educativa que genere un conjunto de profesionales con conocimientos suficientes.

  Desde la administración se puede entablar un diálogo con las entidades oficiales de formación para que se diseñen cursos, grados, masterados, etc., específicamente orientados a instruir en capacidades técnicas a los actuales profesionales del sector, y también para generar una cantera de nuevos profesionales. Estos planes de estudios deberían estar homologados.

  Además de promover la adquisición de competencias prácticas, se pueden establecer acuerdos con empresas para la realización de pasantías. En muchos casos puede ser necesario construir laboratorios con equipamiento especializado, especialmente en sectores como el de transporte, que demanda prácticas de ciberseguridad industrial orientadas a resolver la problemática del nivel de operación OT.

- **Campañas de concientización en el sector**

  El primer paso para disponer de un sector ciberseguro es que las propias empresas y personas que lo integran sean informadas sobre la importancia que tiene la seguridad cibernética en su organización, y por extensión en el país. El sector del transporte está compuesto en muchos de sus segmentos por una gran cantidad de mipymes y autónomos que, día a día, deben hacer frente a multitud de problemas y pueden llegar a obviar o ignorar los riesgos cibernéticos a los que se enfrentan. Esto, sumado a la falta de conocimientos técnicos en ciberseguridad y disponibilidad de profesionales expertos, crea un ambiente propicio para la entrada y propagación de ataques a través de la propia cadena de suministro.

  Es de suma importancia, por lo tanto, que se realicen campañas de concienciación diseñadas para todos los segmentos del sector, con el fin de sensibilizarlos acerca de la importancia de mantener hábitos de higiene de seguridad.

  Otra medida recomendada es habilitar canales de comunicación abiertos (por ejemplo, desde los propios CERT/CSIRT especializados) para brindar apoyo y asesoramiento, en especial a los segmentos más vulnerables (pequeñas empresas, autónomos, etc.) del sector.

- **Competiciones de conocimiento**

  Con el fin de incentivar la mejora en el talento, la administración puede fomentar concursos, certámenes o eventos orientados a estudiantes para mejorar sus capacidades técnicas. De esta manera, es posible generar en la comunidad de futuros expertos en ciberseguridad un interés por abordar retos específicos del sector y evaluarse ante situaciones que puedan encontrar en su posterior vida profesional.

También se pueden diseñar estructuras de evaluación del nivel de madurez en ciberseguridad, orientadas a las organizaciones y profesionales del sector del transporte, que reconozcan la adopción de medidas y faciliten un proceso de mejora continua en la gestión de riesgos cibernéticos.

Actividad 3. Adoptar herramientas para prevención y monitoreo

- **Herramientas de protección de información sensible**

  En el sector del transporte, los sistemas corporativos (IT) a menudo utilizan información sensible tanto de sus empleados como de sus clientes. Esto deriva de los propios servicios ofrecidos por el sector, donde se maneja información de datos personales, métodos de pago, información del material y contenido de las órdenes de transporte, etc. Promover herramientas que permitan establecer medidas de protección de este tipo de datos resulta fundamental para proteger a los usuarios del transporte y reducir incidentes relacionados con el robo de identidades, fraudes, etc.

- **Herramientas de ciberinteligencia en transporte**

  Las autoridades competentes pueden promover el desarrollo de soluciones que busquen de forma proactiva ciberamenazas específicas del sector del transporte (*cyber threat hunting*) y detecten, a partir de comportamientos anómalos, a actores maliciosos que estén operando en el contexto de las organizaciones.

  Pueden diseñarse herramientas basadas en información compartida por el sector que permitan tener una visión más estratégica de las amenazas. En un ámbito local, se pueden aplicar herramientas que realicen un monitoreo del tráfico de la red interna de una empresa y sus sistemas de archivos, registro o autenticación. Una mención especial merece el diseño de herramientas de monitoreo que consideren protocolos de comunicación específicos del nivel OT que puedan estar utilizándose en los diferentes segmentos de transporte.

Actividad 4. Promover instrumentos financieros para la mejora continua

- **Financiación para la I+D+i en productos y servicios**

  La innovación para la generación de productos y servicios más ciberseguros debería ser estimulada desde la administración, de forma que se incentive al propio sector de proveedores de soluciones de transporte (y toda su cadena de suministro) para mejorar en esta materia.

  En este sentido, pueden diseñarse instrumentos que faciliten avanzar en el proceso con aproximaciones tales como:

  – La financiación parcial de proyectos de I+D+i en el sector público y privado en empresas de la región.

- La aplicación de exenciones o deducciones fiscales a empresas que aborden proyectos en innovación para seguir un proceso de mejora continua en ciberseguridad.

- El establecimiento de acuerdos de colaboración con otras regiones o países para diseñar instrumentos que faciliten el traspaso de conocimientos en materia de ciberseguridad.

- La habilitación de oficinas técnicas que ayuden a promover la participación de empresas de la región en programas de investigación internacionales.

- **Cooperación público-privada**

  Para especializar todas las actuaciones, puede ser de interés fomentar el establecimiento de marcos de cooperación público-privada que fomenten que el sector privado y la administración pública diseñen conjuntamente instrumentos destinados a las entidades y organizaciones de toda la cadena de valor de los diferentes segmentos del sector del transporte.

4.3. Herramienta de autoevaluación

Como complemento de este estudio, las divisiones de transporte y el equipo de ciberseguridad de la División de Innovación para Servir al Ciudadano del BID crearon la Herramienta de Autoevaluación en Ciberseguridad para organizaciones de transporte en la región de ALC.

Totalmente gratuita y anónima, esta nueva herramienta permite a las organizaciones conocer su nivel de preparación en ciberseguridad y, de acuerdo con el resultado, emite recomendaciones basadas en el Marco de Ciberseguridad del NIST, específicamente en la versión actualizada (v2.0) del marco de referencia, para la mejora de la ciberseguridad en infraestructuras críticas.

Se recomienda que la herramienta y su cuestionario sean utilizados por personal a cargo de sistemas, tecnología o ciberseguridad en las organizaciones interesadas. Así, se pretende ayudar a promover la protección y la resiliencia de infraestructuras críticas y otros sectores importantes para la economía y la seguridad nacionales, aunque puede ser empleado por organizaciones de cualquier sector de la economía o la sociedad. No es específico para Estados Unidos, tal como lo evidencia el hecho de que organizaciones de otros países lo están usando.

La herramienta utiliza procesos de gestión de riesgos para permitir a las organizaciones priorizar decisiones relativas a la ciberseguridad; también les brinda la capacidad de seleccionar dinámicamente y dirigir la mejora en la gestión del riesgo de la seguridad cibernética para los entornos de IT y OT.

DESCUBRA LA HERRAMIENTA

Anexos

5.1. Anexo I. Regulaciones internacionales

5.1.1. Estados Unidos

IDENTIFICACIÓN	AÑO	TEMA	DESCRIPCIÓN	LINK
Executive Order (EO) 13636	2013	IICC	Executive Order - Improving Critical Infrastructure Cybersecurity, donde se encarga al NIST el desarrollo del marco de ciberseguridad para la protección de infraestructuras críticas, lo que hoy se conoce como el NIST Cybersecurity Framework.	https://www.federal-register.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity
Surface Transportation IC- 2021-01 (Information Circular): Enhancing Surface Transportation Cybersecurity	2021	IICC -Transporte de superficie	Circular informativa que provee recomendaciones para mejorar las prácticas de ciberseguridad en el sector del transporte; aplicable a operadores y propietarios de redes ferroviarias y buses de carretera.	https://www.tsa.gov/ sites/default/files/20 211201_surface-ic- 2021-01.pdf
Security Directive 1580-21-01: Enhancing Rail Cybersecurity	2021	IICC -Ferrocarril	Aplicable a transportistas ferroviarios de carga, en la que se insta a designar un coordinador de ciberseguridad, reportar incidentes de ciberseguridad a la CISA, desarrollar un plan de respuesta a incidentes y realizar análisis de vulnerabilidades.	https://www.tsa.gov/ sites/default/files/sd- 1580-21-01_signed.pdf 01_signed.pdf
Security Directive 1582- 21-01: Enhancing Public Transportation and Passenger Railroad cybersecurity	2021-2025	IICC -Ferrocarril	Aplicable a transportistas ferroviarios de pasajeros, en la que se insta a designar un coordinador de ciberseguridad, reportar incidentes de ciberseguridad a la CISA, desarrollar un plan de respuesta a incidentes y realizar análisis de vulnerabilidades. Desde su creación en 2021, ha recibido actualizaciones en el marco del proceso de formalización normativa de la TSA para la gestión de riesgos cibernéticos en el transporte de superficie): *Enhancing Public Transportation and Passenger/Freight Railroad Cybersecurity.*	https://www.tsa.gov/ sites/default/files/sd- 1582-21-01_signed.pdf 01_signed.pdf https://www.tsa.gov/sites/default/files/signed_security-directive-1582-21-01d-and-transmittal-memo-508c-1.pdf

5.1.2. Unión Europea

IDENTIFICACIÓN	AÑO	TEMA	DESCRIPCIÓN	LINK
EU Cyber Solidarity Act (Regulation 2025/38)	2025	Ciberseguridad	Establece nuevas capacidades en la UE para mejorar la resiliencia contra amenazas cibernéticas y mejorar los mecanismos de cooperación.	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R0038

IDENTIFICACIÓN	AÑO	TEMA	DESCRIPCIÓN	LINK
EU Cybersecurity Act: Reglamento (UE) 2019/ 881 del Parlamento Europeo y del Consejo, del 17 de abril de 2019	2019-2025	Ciberseguridad	Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la UE. Fue enmendada en 2025.	https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R0037
NIS2 Directive	2022	Ciberseguridad	Relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad, por la que se deroga la Directiva (UE) 2016/1148.	https://eur-lex.europa.eu/eli/dir/2022/2555
Directiva 2008/114/CE	2008	IICC	Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.	https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32008L0114
Ley 8/2011 y Real Decreto 704/2011 sobre Protección de Infraestructuras Críticas	2011	IICC	Ley para el establecimiento de estrategias y estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las administraciones públicas en materia de protección de infraestructuras críticas, previa identificación y designación de estas.	https://www.boe.es/eli/es/l/2011/04/28/8/con
Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, del 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas	2022	IICC	Tiene por objeto mejorar la prestación en el mercado interior de servicios esenciales para el mantenimiento de funciones sociales o actividades económicas vitales, aumentando la resiliencia de las entidades críticas que prestan tales servicios.	https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32022L2557
Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016 (GDPR). Reglamento general de protección de datos	2016	Privacidad- Datos personales	Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, por el que se deroga la Directiva 95/46/CE.	https://eur-lex.europa.eu/eli/reg/2 016/679/oj

IDENTIFICACIÓN	AÑO	TEMA	DESCRIPCIÓN	LINK
Reglamento de Ejecución (UE) 2015/1998 de la Comisión, del 5 de noviembre de 2015, seguridad aérea	2015	IICC - Transporte aéreo	Reglamento por el que se establecen medidas detalladas para la aplicación de las normas básicas comunes de seguridad aérea.	https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02015R1998-20230401&qid=1685014180519
Reglamento de Ejecución (UE) 2019/1583 de la Comisión, del 25 de septiembre de 2019	2019	IICC - Transporte aéreo	Modifica el Reglamento de Ejecución (UE) 2015/1998 por el que se establecen medidas detalladas para la aplicación de las normas básicas comunes de seguridad aérea, en lo que se refiere a las medidas de ciberseguridad..	https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32019R1583
Directiva 2010/40/UE del Parlamento Europeo y del Consejo, del 7 de julio de 2010	2010	ITS	Establece el marco para la implantación de los sistemas de transporte inteligentes en el sector del transporte por carretera y para las interfaces con otros modos de transporte. Hace referencia a los aspectos de privacidad de datos personales, así como a requisitos de disponibilidad y accesibilidad de datos para la provisión de servicios ITS.	https://eur- lex.europa.eu/legal- content/ES/ALL/?uri=celex%3A32010L004 0

5.1.3. Internacional

IDENTIFICACIÓN	AÑO	TEMA	DESCRIPCIÓN	LINK
UN Regulation N1 155- Cyber security and cyber security management system (CSMS)	2021-2023	IICC - Vehículo	Propuesta de un nuevo reglamento de la Organización de las Naciones Unidas (ONU) sobre disposiciones uniformes referentes a la aprobación de vehículos en lo que respecta a la ciberseguridad y el sistema de gestión de ciberseguridad. Últimas propuestas de actualización en 2023.	https://unece.org/sites/default/files/2021- 03/R155e.pdf https://docs.un.org/en/ECE/TRANS/WP.29/2023/45

IDENTIFICACIÓN	AÑO	TEMA	DESCRIPCIÓN	LINK
UN Regulation No. 156 - Software update and software update management system	2021-2025	IICC - Vehículo	Acuerdo relativo a la adopción de reglamentos técnicos armonizados de las Naciones Unidas aplicables a los vehículos de ruedas y los equipos y piezas que puedan montarse o utilizarse en estos, y sobre las condiciones de reconocimiento recíproco de las homologaciones concedidas conforme a dichos reglamentos de la Organización de las Naciones Unidas (ONU). Últimas propuestas de actualización en 2025.	https://unece.org/sites/default/files/2021- 03/R156e.pdf https://docs.un.org/en/ECE/TRANS/WP.29/2025/45

5.2. Anexo II. Estándares y marcos de ciberseguridad aplicables

5.2.1. Aviación

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
NAS 9933	Aerospace Cybersecurity Standard	AIA (Aerospace Industries Association)	Estándar voluntario publicado para facilitar el establecimiento de requisitos de ciberseguridad en la industria aeronáutica. Consiste en 20 familias publicadas por el CIS y dos adicionales desarrolladas con Exostar, empresa proveedora de nube segura para industrias altamente reguladas. El objetivo es proveer de una indicación para determinar el perfil de ciberseguridad de una compañía.
ARINC 664	Aircraft Data Network	ARINC (Aeronautical Radio, Incorporated)	Estándar sobre el bus de datos para sistemas aeronáuticos, ferroviarios y militares, que, junto con otros estándares, como ARIC 429 Data Bus y ARINC 629, tiene el fin de crear arquitecturas confiables que faciliten el aislamiento y segregación de sistemas, además de asegurar la integridad de los datos.
ATA Spec 42	Aviation Industry Standards for Digital Information Security	A4A (Airline for America, former ATA)	Describe los requisitos y especificaciones de Public Key Infraestructure (PIK) para la industria de aviación civil. Es un estándar de autentificación y encriptación de información sensible digital para la industria.

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
ARINC 811	Commercial Aircraft Information Security Concepts of Operation and Process Framework	ARINC (Aeronautical Radio, Incorporated)	Desarrolla un concepto de operación para un marco de seguridad común y un conjunto de mecanismos de seguridad comunes que, cuando se diseñan e implementan, no afectan la capacidad de volar y despachar aeronaves de manera segura y oportuna.
ARINC 823 Part 1	Datalink Security / ACARS Message Security (AMS)	ARINC (Aeronautical Radio, Incorporated)	Estándar de la industria que permite que los mensajes de enlace de datos se intercambien entre aeronaves y sistemas terrestres de manera segura y autenticada, utilizando un marco de seguridad uniforme.
ARINC 823 Part 2	Datalink Security / AMS Key Management	ARINC (Aeronautical Radio, Incorporated)	Establece la orientación y disposiciones para aerolíneas y proveedores de servicios de enlace de datos para la gestión del ciclo de vida de las claves criptográficas que son necesarias para el funcionamiento adecuado y seguro de ASM.
CSN EN 16495 - Air Traffic Management	Information security for organisations supporting civil aviation operations	CEN	Esta norma europea define las directrices y los principios generales para la implementación de un sistema de gestión de la seguridad de la información en las organizaciones que apoyan las operaciones de aviación civil.
ED-201	Aeronautical Information System Security (AISS) Framework	EUROCAE	Responsabilidad compartida para la Seguridad de los Sistemas de Información Aeronáutica (AISS) en la aviación civil que involucra a todas las partes interesadas relevantes.
DO 326S / ED-202A	Airworthiness Security Process	EUROCAE	Orientación para gestionar amenazas a la seguridad de la información para la seguridad de las aeronaves.
ED-203	Airworthiness Security Methods and Considerations	EUROCAE	Directrices, métodos y herramientas utilizados en la realización de un proceso de seguridad de la aeronavegabilidad.
ED-204	Instruction for Continued Airworthiness	EUROCAE	Actividades que deben realizarse en la operación y mantenimiento de la aeronave cuando se trata de seguridad cibernética.

5.2.2. Marítimo

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
ISM Code +MSC.428 (98)	International Safety Maritime Code	IMO (International Maritime Organization)	Norma internacional para la gestión y operación seguras de los buques y para la prevención de la contaminación. El Código IGS, respaldado por la Resolución de la Organización Marítima Internacional (OMI) OMI MSC.428(98), requiere que los propietarios y administradores de buques evalúen el riesgo cibernético e implementen las medidas pertinentes en todas las funciones de su sistema de gestión de la seguridad.
ISPS Code	International Ship and Port Facility Code	IMO (International Maritime Organization)	Habiendo entrado en vigor, en virtud del capítulo XI-2 del Convenio SOLAS, el 1 de julio de 2004, el también conocido como Código Internacional para la Protección de los Buques y las Instalaciones Portuarias (Código PBIP) ha constituido la base del régimen de seguridad obligatorio para el transporte marítimo internacional.
MSC-FAL.1/ Circ.3	Guidelines on maritime cyber risk management	IMO (International Maritime Organization)	Directrices que proporcionan recomendaciones de alto nivel sobre el riesgo cibernético marítimo.
DCSA cyber security implementation guide	DCSA Implementation Guide for Cyber Security on Vessels v1.0	DCSA (Digital Container Shipping Association)	Marco de gestión de ciberseguridad para embarcaciones, ya sea en el mar, amarradas o atracadas.
BIMCO Guidelines	The guidelines on cyber security onboard ships (version 4)	BIMCO (Baltic and International Maritime Council)	Conjunto de pautas de seguridad cibernética para barcos con el fin de ayudar a la industria naviera mundial a prevenir problemas importantes de seguridad, ambientales y comerciales que podrían resultar de un incidente cibernético a bordo de un barco.
CIRM Cyber Risk Code of Practice	CIRM Cyber Risk Code of Practice for Vendors of Marine Electronic Equipment and Services.	CIRM (Comité International Radio- Maritime)	Conjunto de principios rectores para que los utilicen todos los miembros de la cadena de valor de las partes interesadas con el fin de establecer una cadena de confianza demostrable para un entorno marítimo digital seguro.

5.2.3. Ferroviario

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
UNE-CLC/TS 50701:2021	Aplicaciones ferroviarias. Ciberseguridad	UNE / CEN CENELEC	Tiene como objetivo proporcionar requisitos y recomendaciones para manejar la ciberseguridad de manera unificada para el sector ferroviario. Esta especificación técnica es de aplicación desde el dominio de las comunicaciones, señalización y procesamiento, hasta los sistemas de peaje o instalaciones fijas.

5.2.4. Intelligent Transport Systems

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
ISO/TR 21186-3	Cooperative intelligent transport systems (C-ITS) Guidelines on the usage of standards. Part 3: Security	ISO	Sistemas inteligentes de transporte cooperativos (C-ITS). Directrices sobre el uso de normas. Seguridad.
ISO/TS 21177	Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices	ISO	Contiene especificaciones para un conjunto de servicios de seguridad de estaciones ITS necesarias para garantizar la autenticidad de la fuente y la integridad de la información intercambiada entre entidades de confianza.
ISO 19299	Electronic fee collection — Security framework	ISO	Define un marco de seguridad de la información para todas las entidades organizativas y técnicas de un esquema EFC y para las interfaces relacionadas, basado en la arquitectura del sistema definida en la norma ISO 17573-1. El marco de seguridad describe un conjunto de requisitos de seguridad y medidas de seguridad asociadas.

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
ISO/TS 15638	Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV)	ISO	Marco para aplicaciones telemáticas colaborativas para vehículos comerciales de carga regulados (TARV).
ISO/TR 12859	Intelligent transport systems — System architecture — Privacy aspects in ITS standards and systems	ISO	Brinda pautas generales a los desarrolladores de estándares e ITS sobre aspectos de privacidad de datos y requisitos legislativos asociados para el desarrollo y revisión de estándares y sistemas de ITS.
ETSI TS 102940	Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management	ETSI	Especifica una arquitectura de seguridad para las comunicaciones de ITS.
ETSI TS 102941	Intelligent Transport Systems (ITS); Security; Trust and Privacy Management	ETSI	Identifica el establecimiento de confianza y la gestión de la privacidad necesarios para respaldar la seguridad en un entorno ITS y las relaciones que existen entre las propias entidades y los elementos de la arquitectura de referencia ITS definida en ETSI EN 302 665.
ETSI TS 102942	Intelligent Transport Systems (ITS); Security; Access Control	ETSI	Especifica los servicios de autenticación y autorización para evitar el acceso no autorizado a los servicios ITS.También fija medidas para garantizar el nivel requerido de seguridad y privacidad para la comunicación de mensajes ITS.

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
ETSI TS 102943	Intelligent Transport Systems (ITS); Security; Confidentiality services	ETSI	Especifica los servicios para garantizar que la confidencialidad de la información enviada hacia y desde una estación de ITS se pueda mantener a un nivel que sea aceptable para los usuarios de la estación.

5.2.5. Vehículos terrestres

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
SAE J3101	Hardware Protected Security for Ground Vehicles	SAE	Conjunto común de requisitos en funciones asistidas por *hardware* para facilitar las aplicaciones de seguridad mejorada, con el fin de lograr un sistema ideal para la protección de *hardware* para aplicaciones de vehículos terrestres.
SAE J3061	Cybersecurity Guidebook for Cyber- Physical Vehicle Systems	SAE	Brinda orientación sobre la seguridad cibernética de los vehículos. Fue elaborado a partir de prácticas existentes que se están implementando o informando en la industria, el Gobierno y los documentos de conferencias, y se amplió a partir de ellas.
ISO/SAE 21434:2021	Road vehicles — Cybersecurity engineering	ISO	Especifica los requisitos de ingeniería para la gestión de riesgos de ciberseguridad con respecto al concepto, desarrollo de productos, producción, operación, mantenimiento y desmantelamiento de sistemas eléctricos y electrónicos (E/E) en vehículos de carretera, incluidos sus componentes e interfaces.
SAE J3138	Diagnostic Link Connector Security	SAE	Describe algunas de las acciones que deben tomarse para ayudar a garantizar la operación segura del vehículo en caso de que cualquier dispositivo conectado (equipo de prueba externo, dispositivo de recopilación de datos conectado) se haya visto comprometido por una fuente externa al vehículo. En particular, describe aquellas acciones específicamente relacionadas con los servicios de diagnóstico estandarizados SAE J1979, ISO 15765, e ISO 14229.

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
ISO 26262	Road vehicles — Functional safety	ISO	Aplicable a los sistemas relacionados con la seguridad que incluyen uno o más sistemas eléctricos o electrónicos (E/E) instalados en camionetas de producción en serie con una masa bruta máxima del vehículo de hasta 3500 kg.
SAE J3101	Hardware Protected Security for Ground Vehicles	SAE	Describe cómo el entorno de seguridad protegido por *hardware* proporciona una plataforma para implementar el control de acceso al permitir la autenticación, la autorización y la revocación de acceso de forma segura.
ISO/SAE 21434:2021	ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering	ISO	Especifica los requisitos de ingeniería para la gestión de riesgos de ciberseguridad con respecto al concepto, desarrollo de productos, producción, operación, mantenimiento y desmantelamiento de sistemas eléctricos y electrónicos (E/E) en vehículos de carretera, incluidos sus componentes e interfaces.

5.2.6. Sistemas industriales

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
IEC 61443	Seguridad de los sistemas de automatización y control industrial (IACS)	IEC	Serie de normas cuyo objetivo principal es facilitar el tratamiento de las vulnerabilidades de los Industrial and Automation Control Systems (IACS) frente a ataques informáticos y la aplicación de medidas que las mitiguen. Desde sus inicios, su propósito ha sido establecer un nexo entre la ciberseguridad y los IACS, definiendo una serie de requisitos mínimos para lograr niveles de seguridad cada vez más rigurosos que ayuden a mejorar la seguridad en entornos industriales.
SP 800-82 Rev. 2	Guide to ICS Security	NIST	Brinda orientación sobre cómo proteger los ICS, incluidos los SCADA, los Sistemas de Control Distribuido (DCS) y otras configuraciones de sistemas de control, como los Controladores Lógicos Programables (PLC), mientras aborda sus requisitos únicos de rendimiento, confiabilidad y seguridad.

5.2.7. Productos IT

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
UNE-EN ISO/IEC 15408-1:2020	It — Security Techniques — Evaluation Criteria for It Security: Part 1: Introduction and general model (15408-1). Part 2: Security functional requirements (15408-2) Part 3: Security assurance requirements (15408-3)	ISO	Estándar que contiene un conjunto común de requisitos para las funciones de seguridad de los productos y sistemas de IT y para las medidas de aseguramiento que se les aplican durante una evaluación de seguridad.

5.2.8. Infraestructuras críticas

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
NIST Framework	NIST Framework	NIST	Marco que sirve como base para la gestión de riesgos de ciberseguridad en infraestructuras críticas, basado en estándares de la industria ya aceptados, como NIST SP 800-53 Rev.4, ISO/IEC 27001:2013, COBIT 5, CIS CSC, entre otros.

5.2.9. Organizaciones

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
ISO/IEC 2700x Serie	Information Security Management	ISO / IEC	Contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

CÓDIGO	TÍTULO	AUTOR	DESCRIPCIÓN
ISO/IEC TR 18044	Information technology — Security techniques — Information security incident management	ISO / IEC	Informe técnico que contiene lineamientos generalmente aceptados y principios generales para la gestión de incidentes de seguridad de la información en una organización.
ISO 22301:2019	Security and resilience — Business continuity management systems — Requirements	ISO	Especifica los requisitos para implementar, mantener y mejorar un sistema de gestión, además de proteger, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de las interrupciones cuando surjan.

5.3. Anexo III. Modelo de entrevista con entidades públicas

5.3.1. Contexto de la entidad

En este punto, interesa conocer la concientización de la entidad entrevistada en materia de ciberseguridad en el momento actual y si se está realizando alguna acción en concreto sobre este tema en los proyectos que se gestionan.

1. ¿Incluyen aspectos sobre el riesgo cibernético como uno de los elementos importantes que considerar en el ámbito del transporte?

2. ¿Cómo ven el nivel de atención y gestión de este tipo de riesgo por parte de las empresas del sector?

3. ¿Han observado en los últimos años algún cambio en este sentido derivado de eventos internacionales importantes (tales como la pandemia de covid-19 o ciertos conflictos)?

5.3.2. Medidas legales / jurídicas

La regulación sobre ciberseguridad se basa en principios que deben respetar los interesados, que forman parte de la aplicación de leyes sobre aspectos tales como protección de datos, notificación de infracciones, requisitos de certificación/normalización, aplicación de medidas de ciberseguridad, criterios para auditorías de ciberseguridad, protección de privacidad, etc.

1. **Legislación o reglamentos sobre ciberseguridad**

   1.1. ¿Sabe si existen leyes o reglamentos sobre ciberseguridad en materia de...

   - protección de datos personales o de privacidad?
   - notificación de infracciones/incidentes de datos?
   - requisitos para auditorías de ciberseguridad?
   - aplicación de normas, marcos o estándares internacionales (de organizaciones tales como ISO, IEC, NIST, etc.)?
   - provisión de productos electrónicos certificados para sectores críticos (¿por ejemplo, productos IoT, ITS, etc.?
   - utilización de firmas digitales en servicios y aplicaciones gubernamentales, por ejemplo, para la digitalización de ciertos trámites en la cadena logística, como aduanas?
   - identificación y protección de infraestructuras esenciales a nivel nacional sobre las que puedan sustentarse los servicios de transporte, considerados como servicios críticos en muchos países?

Proporcione información sobre prácticas idóneas/logros/avances en su organización/país en materia de esferas jurídicas asociadas a actividades que se lleven a cabo, o que se hayan realizado anteriormente, con respecto a la ciberseguridad.

5.3.3. Medidas técnicas de respuesta

Discusión sobre la coordinación y respuesta ante incidentes y la existencia de CERT que tengan la responsabilidad de coordinar y dar apoyo a las intervenciones en caso de eventos o incidentes de seguridad, así como otros aspectos de medidas técnicas implementadas para la gestión de la seguridad.

1. **A nivel de planificación de respuesta ante incidentes**

   1.1. ¿Exige la definición de un plan de seguridad del operador o un plan de contingencia o respuesta ante incidentes en la operación de las infraestructuras de transporte que gestiona, sea de forma directa o a través de un concesionario?

2. **CERT nacionales/gubernamentales**

   2.1. ¿Sabe si existen CERT nacionales o gubernamentales?

   2.2. ¿Qué tipo de servicios o acciones que sean de su interés realiza (o debería realizar) su CERT nacional? Por ejemplo, ¿sabe si su CERT nacional o gubernamental...

   - prepara y lleva a cabo actividades de sensibilización en materia de ciberseguridad?
   - realiza periódicamente ejercicios de ciberseguridad, como cibersimulacros?
   - emite avisos públicos?

   2.3. ¿Cómo se relaciona con los CERT nacionales o gubernamentales?

3. **CERT sectoriales**

   3.1. ¿Hay en su país CERT sectoriales específicos para infraestructuras críticas o de transporte?

   3.2. Sus CERT sectoriales: ¿qué servicios ofrecen que sean de su interés? Por ejemplo,

   - ¿preparan y llevan a cabo actividades de sensibilización específicas para ese sector?
   - ¿participan activamente en los cibersimulacros nacionales?
   - ¿dan a conocer los incidentes acaecidos en el sector?

3.3. ¿Están coordinados los CERT entre ellos? ¿Tienen algún marco común de actividad?

Proporcione información sobre prácticas idóneas/logros/avances en su país en materia de esferas técnicas asociadas a actividades que se lleven a cabo, o que se hayan realizado anteriormente, con respecto a la ciberseguridad (utilice el recuadro de observaciones para detallar la(s) práctica(s) e incluir enlaces para su demostración).

5.3.4. Medidas organizativas

Discusión sobre la definición de políticas para fomentar la ciberseguridad como una de las prioridades nacionales, las agencias nacionales o los responsables de llevarlas adelante, así como los mecanismos para comprobar que las medidas definidas se estén llevando a cabo (auditorías o similares).

1. **Estrategia en materia de ciberseguridad**

Estrategia a nivel nacional:

1.1. ¿Sabe si su país dispone de una estrategia/política nacional de ciberseguridad? Si es así, ¿sabe si...

- comprende la protección de infraestructuras esenciales nacionales, incluidas las del sector de transporte?
- hace referencia a la resiliencia de ciberseguridad nacional?

1.2. ¿Han participado o se les ha consultado para la definición de esta estrategia?

1.3. ¿Sabe si existe un plan de acción/hoja de ruta definido para la implementación de la ciberseguridad a nivel nacional?

Estrategia a nivel de su organización:

1.4. En el caso de su organización en concreto, ¿tienen un plan de acción/hoja de ruta definido para incluir la ciberseguridad en los proyectos que gestionan?

2. **Responsabilidades en materia de ciberseguridad**

Responsables a nivel nacional:

2.1. ¿Sabe si existe una agencia responsable de la coordinación de la ciberseguridad a nivel nacional?

- ¿Sabe si esa agencia se ocupa de la protección de las infraestructuras de información esenciales a nivel nacional?
- ¿Hay alguna especialmente orientada al sector del transporte?

- ¿Cómo se relaciona con ella? ¿Qué servicios le ofrece?

Responsables a nivel de su organización:

2.2. En su organización, ¿existe algún responsable de los aspectos de ciberseguridad a nivel interno? ¿Y con los concesionarios?

3. **Medición de la ciberseguridad**

3.1. ¿Se realizan auditorías de ciberseguridad en su organización?

3.2. ¿Sabe si se realizan este tipo de auditorías en otras organizaciones?

3.3. ¿Utiliza algún sistema de medición para la evaluación de los ciberriesgos en su organización o en los proyectos que adjudican a las concesionarias?

3.4. ¿Realizan mediciones para evaluar el nivel de desarrollo de la ciberseguridad en los concesionarios o proveedores de soluciones?

Proporcione información sobre prácticas idóneas/logros/avances en su organización/país en materia de esferas técnicas asociadas a actividades que se lleven a cabo, o se hayan realizado anteriormente, con respecto a la ciberseguridad (utilice el recuadro de observaciones para detallar la(s) práctica(s) e incluir enlaces para su demostración).

5.3.5. Medidas de concienciación y capacitación

La sensibilización, tanto de los usuarios como del personal, requiere difundir mensajes sobre comportamientos seguros. En el sector del transporte puede ser especialmente relevante ofrecer campañas de sensibilización a ciertos segmentos específicos de la cadena de valor del transporte y la logística que pueden estar compuestos por micropymes o autónomos. Además, puede ser necesario disponer de proveedores capacitados de productos y servicios de ciberseguridad para el segmento del transporte en concreto.

1. **Campañas y concientización sobre ciberseguridad para usuarios y cadena de suministro del transporte**

1.1. ¿Llevan a cabo campañas de sensibilización para entidades de la cadena de suministro en general y en sectores específicos (por ejemplo, pymes, proveedores de servicios, concesionarios, etc.)?

1.2. ¿Se realizan campañas públicas de sensibilización para la sociedad y la población en general como usuarios de las infraestructuras de transporte?

2. **Formación para profesionales en materia de ciberseguridad**

2.1. ¿Su organización realiza o apoya la realización de cursos de formación en ciberseguridad? ¿Alguno específico para los responsables de los aspectos de seguridad?

2.2. ¿Han desplegado o desarrollado un programa de acreditación para ciertos profesionales de la ciberseguridad en su organización?

2.3. ¿Sabe si existen programas/formaciones/cursos sectoriales nacionales para profesionales de la ciberseguridad?

3. Programas de investigación y desarrollo en ciberseguridad

3.1. ¿Sabe si se realizan actividades de I+D en materia de ciberseguridad en su país? Por ejemplo,

- ¿hay programas de I+D específicos en ciberseguridad?
- ¿participan las instituciones de enseñanza superior, como instituciones académicas y universidades, en las actividades de I+D?
- ¿existen programas de I+D en ciberseguridad que prioricen la participación de determinados sectores (infraestructuras críticas, transporte, etc.)?
- ¿sabe cuál es el presupuesto de I+D que se dedica a ciberseguridad sobre el presupuesto total?

3.2. Su organización, ¿tiene definida una estrategia de I+D en materia de ciberseguridad? ¿Participa en proyectos de I+D? ¿Cuál es el porcentaje de su presupuesto de I+D que dedica a ciberseguridad sobre el presupuesto total?

4. Industria nacional de la ciberseguridad

4.1. ¿Existen proveedores de servicios de ciberseguridad (por ejemplo, SOC) que presten servicios especializados a sectores críticos, industriales o de transporte?

4.2. ¿Existe una industria de la ciberseguridad que ofrezca soluciones de ciberseguridad específicas o especializadas para su segmento (nacional o internacional)?

5. Mecanismos estatales de incentivos

5.1. ¿Existen mecanismos para fomentar la capacitación en ciberseguridad? ¿Los consideraría interesantes o esenciales para su organización?

5.2. ¿Existen mecanismos para el desarrollo de la industria de ciberseguridad? ¿Los consideraría interesantes o esenciales para su organización?

Proporcione información sobre prácticas idóneas/logros/avances en su país en materia de medidas de capacitación asociadas a actividades que se lleven a cabo, o se hayan realizado anteriormente, con respecto a la ciberseguridad (utilice el recuadro de observaciones para detallar la(s) práctica(s) e incluir enlaces para su demostración).

5.3.6. Medidas de cooperación

En ocasiones se establecen acuerdos o alianzas (nacionales o sectoriales) destinadas a compartir información y recursos sobre ciberseguridad. Pueden involucrar al Gobierno nacional, Gobiernos extranjeros, entidades regionales u organizaciones internacionales. Los acuerdos incluyen aspectos como, por ejemplo, cooperación o intercambio de información, conocimientos de expertos, tecnología, amenazas y otros recursos.

1. **Acuerdos con el sector privado**

   1.1. ¿Tiene su Gobierno acuerdos con empresas locales? ¿Tiene acuerdos con organizaciones del sector del transporte (asociaciones, clústeres, empresas referentes, proveedores de servicios para la administración, etc.)?

   1.2. ¿Ha concluido su Gobierno acuerdos con empresas extranjeras ubicadas en el país?

   1.3. ¿Se incluyen requisitos específicos en materia de ciberseguridad en los contratos de la ANI con los concesionarios o proveedores de soluciones y servicios?

2. **Acuerdos o colaboración con otros órganos estatales**

   2.1. ¿Existen acuerdos/alianzas con otros órganos estatales en materia de ciberseguridad? ¿Colaboran en los comités o grupos de trabajo que establecen medidas de ciberseguridad específicas para el sector del transporte (tales como ministerios o secretarías de TIC, seguridad y defensa o transporte)?

3. **Acuerdos bilaterales o multilaterales de cooperación en materia de ciberseguridad dentro del país o con otros países**

   3.1. ¿Se han establecido acuerdos bilaterales o multilaterales de cooperación en materia de ciberseguridad con otras entidades? Si es así:

   - ¿Con qué tipo de entidades: organizaciones del sector del transporte, como asociaciones, clústeres, empresas referentes, proveedores, etc.?
   - ¿Qué tipo de cuestiones incluyen: compartición de información, de recursos, de capacitación, etc.?

Proporcione información sobre prácticas idóneas/logros/avances en su país en materia de medidas de cooperación asociadas a actividades que se lleven a cabo, o que se hayan realizado anteriormente, con respecto a la ciberseguridad (utilice el recuadro de observaciones para detallar la(s) práctica(s) e incluir enlaces para su demostración).

Referencias bibliográficas

A., Maxime, Livia Tibirna y Threat & Detection Research Team. 2023. The Transportation sector cyber threat overview. *Sekoia.io Blog*. 12 de septiembre de 2023. https://blog.sekoia.io/the-transportation-sector-cyber-threat-overview/.

Agencia Reguladora del Transporte Ferroviario. 2023. *Pulso del Sistema Ferroviario Mexicano - Operativo Diciembre 2022*. Gobierno de México. 31 de enero de 2023. https://www.gob.mx/artf/documentos/pulso-del-sector-ferroviario-2023.

Airport Cooperative Research Program (ACRP). 2012. *Information Technology Systems at Airports - A Primer*. https://doi.org/10.17226/14622.

Altaf, Amna, Eylem Thron, Huseyin Dogan, Shamal Faily y Alexios Mylonas. 2019. Evaluating the Impact of Cyber Security and Safety with Human Factors in Rail Using Attacker Personas. *ASPECT*. (PDF) Evaluating the Impact of Cyber Security and Safety with Human Factors in Rail Using Attacker Personas

Asamblea general de la OEA. 2004. *Estrategia de Seguridad Cibernética (Resolución)*. Organización de los Estados Americanos (OEA).

Associated Press. 2022. Cyberattack cripples Puerto Rico toll collection system. *APNews*, 5 de abril de 2022. https://apnews.com/article/business-caribbean-puerto-rico-de668a1b604dcd9748da65fec57dcdf6.

Baltic and International Maritime Council (BIMCO), Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping , International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) y World Shipping Council (WSC). 2020. *The Guidelines on Cyber Security Onboard Ships*. https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.

Banco Interamericano de Desarrollo y Organización de los Estados Americanos. 2020. *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*. Washington: Inter-American Development Bank. https://doi.org/10.18235/0002513.

Banerd, Walker. 2018. Data Breach of the Month: Rail Europe North America. *D3 Security*, 11 de junio de 2018. https://d3security.com/blog/data-breach-of-the-month-rail-europe-north-america/.

Barleta, Eliana P. y Sánchez, Ricardo J. 2022. *Informe Portuario 2021: las primeras señales de recuperación en el transporte marítimo internacional vía contenedores de América Latina.* Facilitación, Comercio y Logística en América Latina y el Caribe / FAL, 391. https://repositorio.cepal.org/server/api/core/bitstreams/0f06eb0d-d9b0-4ac5-9dd6-aadd491637d8/content.

Bateman, Tom. 2013. Police warning after drug traffickers' cyber-attack. *BBC News*, 16 de octubre de 2013. https://www.bbc.com/news/world-europe-24539417.

Bischoff, Paul. 2025. "Ransomware gang says it hacked the Malaysia's Kuala Lumpur International Airport". *Comparitech*, abril 8. https://www.comparitech.com/news/ransomware-gang-says-it-hacked-the-malaysias-kuala-lumpur-international-airport/

Boyes, Hugh, Roy Isbell y Alexandra Luck. 2020. Cyber security for ports and port systems. Good Practice Guide. Institution of Engineering and Technology. https://assets.publishing.service.gov.uk/media/5e284eefe5274a6c3ee68fcd/cyber-security-for-ports-and-port-systems-code-of-practice.pdf.

Calatayud, Agustina, Carolina Benítez, Juan Manuel Leaño, Roberto Agosta, Frédéric Blas, Cynthia Goytia y Soledad Guilera, et al. 2020. *Vehículos autónomos: Una revisión bibliográfica sobre su impacto en la movilidad de las ciudades de la región.* http://dx.doi.org/10.18235/0002491.

CBC News. 2020. "Ransomware attack led to 3 days of transit payment problems, TransLink says". *CBC Radio Canada (British Columbia)*, diciembre 3. https://www.cbc.ca/news/canada/british-columbia/translink-debit-credit-payment-down-1.5826868

Centro de Ciberseguridad Industrial. 2021. *Comparativa de las estrategias nacionales de ciberseguridad en Latinoamérica.* https://www.cci-es.org/activities/comparativa-de-las-estrategias-nacionales-de-ciberseguridad-en-latinoamerica/.

Comité Interamericano Contra el Terrorismo (CICTE) y Organización de los Estados Americanos (OEA). 2012. *Fortalecimiento de la Seguridad Cibernética en las Américas.*

Council of Europe. 2023. Chart of signatures and ratifications of Treaty 185 - Convention on cybercrime. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

Crotte, Amado, Carina Arvizu, Carlos Mojica e Isabel Granada. 2017. *Apoyo al desarrollo de Sistemas Inteligentes de Transporte (ITS).* Inter-American Development Bank. https://publications.iadb.org/es/publicacion/14066/apoyo-al-desarrollo-de-sistemas-inteligentes-de-transporte-its.

CSIRT Americas Network. s. f. CSIRT Americas. Accedido 29 de octubre de 2023. https://csirtamericas.org/es.

Cybersecurity Infrastructure Security Agency (CISA). s. f.-a. *Cross-Sector Cybersecurity Performance Goals.* Accedido 29 de octubre de 2023. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

———. s. f.-b. *Transportation Systems Sector.* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector.

———. s. f.-c. *Industrial Control Systems.* https://www.cisa.gov/topics/industrial-control-systems.

Cyware Hacker News. 2020. Cyber Incidents Affecting Railways - A Threat to Customer Data. *Cyware Alerts,* 18 de mayo de 2020. Cyber Incidents Affecting Railways - A Threat to Customer Data | Cyware Alerts - Hacker News.

Departamento Nacional de Planeación. 2023. *Estrategia Nacional Digital 2023–2026.* Bogotá: Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Desarrollo%20Digital/EVENTOS/END_Colombia_2023_2026.pdf.

Díaz, Rodrigo Mariano. 2021. Estado de la ciberseguridad en la logística de América Latina y el Caribe. *Desarrollo Productivo,* 228. https://www.cepal.org/es/publicaciones/47240-estado-la-ciberseguridad-la-logistica-america-latina-caribe.

Digital Container Shipping Association. 2020. *Digital Container Shipping Association DCSA Implementation Guide for Cyber Security on Vessels v1.0.* https://dcsa.org/wp-content/uploads/2020/03/DCSA-Implementation-Guideline-for-BIMCO-Compliant-Cyber-Security-on-Vessels-v1.0.pdf.

Di Paula Ambrissi, Rodrigo. 2022. Kaspersky registra 4 mil ataques de ransomware por día en América Latina. *Cointelegraph,* 17 de diciembre de 2022. https://es.cointelegraph.com/news/kaspersky-records-4-000-ransomware-attacks-per-day-in-latin-america.

Dissent. 2021a. CA: Cyberattack targets Santa Clara Valley Transportation Authority. *DataBreaches.net,* 22 de abril de 2021. https://www.databreaches.net/ca-cyberattack-targets-santa-clara-valley-transportation-authority/.

———. 2021b. Spirit Airlines hit by Nefilim ransomware – Report. *DataBreaches.net,* 5 de abril de 2021. https://www.databreaches.net/spirit-airlines-hit-by-nefilim-ransomware-report/.

Drozhzhin, Alex. 2015. Black Hat USA 2015: The full story of how that Jeep was hacked. Kaspersky, 6 de agosto de 2015. https://www.kaspersky.es/blog/blackhat-jeep-cherokee-hack-explained/6552/.

European Cyber Security Organization (ECSO). 2020. Transportation Sector Report: Cyber security for road, rail, air, and sea WG3 I Sectoral Demand. www.ecs-org.eu.

European Parliament y European Council. 2008. Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. Council of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114.

———. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural people with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). European Parliament. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

European Union Agency for Cybersecurity (ENISA). 2016a. *Cyber Security and Resilience of Intelligent Public Transport. Good Practices and Recommendations*. https://www.enisa.europa.eu/publications/good-practices-recommendations.

———. 2016b. *Securing Smart Airports*. https://www.enisa.europa.eu/publications/securing-smart-airports.

———. 2017. *Cyber Security and Resilience of Smart Cars. Good Practices and Recommendations*. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.

———. 2019. *Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector*. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector.

———. 2020a. *Guidelines - Cyber Risk Management for Ports*. https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports.

———. 2020b. *Railway Cybersecurity: Security Measures in the Railway Transport Sector*. https://www.enisa.europa.eu/publications/railway-cybersecurity.

———. 2021. *Railway Cybersecurity: Good Practices in Cyber Risk Management*. https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management.

———. 2025. *ENISA Threat Landscape*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

———. s. f. *ENISA Mandate and Regulatory Framework*. ENISA Mandate and Regulatory Framework | ENISA.

Eurostat. 2022. *Statistics - Goods transported by rail*. https://ec.europa.eu/eurostat/databrowser/view/rail_go_total/default/table?lang=en.

Exec. Order 13636. 78 FR 11739- Improving Critical Infrastructure Cybersecurity. United States Government. Federal Register :: Improving Critical Infrastructure Cybersecurity

Fisher, Mary Kate y Catherine Gamper. 2017. *Marco de evaluación de políticas sobre la gobernanza de la resiliencia de las infraestructuras críticas en América Latina*. Banco Interamericano de Desarrollo. https://doi.org/10.18235/0000819.

Forbes Staff. 2023. Ataques de ransomware en Latinoamérica aumentaron en un 38%. *Forbes Chile,* 30 de marzo de 2023. https://forbes.cl/tecnologia/2023-03-30/ataques-ransomware-latinoamerica-ciberseguridad.

FRAME Forum. 2023. *FRAME Architecture*. https://frame-online.eu/frame-architecture/.

García Zaballos, Antonio e Inkyung Jeun. 2016. *Best Practices for Critical Information Infrastructure Protection (CIIP): Experiences from Latin America and the Caribbean and Selected Countries.* Banco Interamericano de Desarrollo. https://publications.iadb.org/en/best-practices-critical-information-infrastructure-protection-ciip-experiences-latin-america-and.

Glover, Claudia. 2023. "Japan's Port of Nagoya paralysed in LockBit's latest ransomware rampage". Tech Monitor, julio 5. https://www.techmonitor.ai/technology/cybersecurity/port-of-nagoya-cyberattack-lockbit-ransomware?cf-view&cf-closed.

Gómez-Lobo, Andrés, Santiago Sánchez González, Vileydy González Mejía y Agustina Calatayud 2022. *Aglomeración y congestión en América Latina*. https://doi.org/10.18235/0003984

Gompel, Marieke Van. 2017. WannaCry virus was 'wake-up call' for railway industry. *RailTech.com,* 2017. https://www.railtech.com/digitalisation/2017/12/11/wannacry-virus-was-wake-up-call-for-railway-industry/?gdpr=accept&gdpr=accept.

Greenberg, Andy. 2020. Dutch Hackers Found a Simple Way to Mess with Traffic Lights. *Wired,* 5 de Agosto de 2020. https://www.wired.com/story/hacking-traffic-lights-netherlands/.

Hackett, Robert. 2017. Petya Ransomware: Everything to Know About Cyber Attacks. *Fortune,* 27 de junio de 2017. https://fortune.com/2017/06/27/petya-ransomware-cyber-attack/.

Hay Newman, Lily. 2023. The Shocking Data on Kia and Hyundai Thefts in the US. *Wired,* 23 septiembre de 2023. https://www.wired.com/story/kia-hyundai-car-thefts-us-security-roundup/.

Hurst, Allison. 2021. Hackers asked TransLink for $7.5 million in December ransomware attack. *CTV News,* 15 de abril de 2021. Printed ransom note asked TransLink for $7.5 million in December cyberattack

INCIBE-CERT. 2021. Un ciberataque a Transnet provoca un colapso logístico. Instituto Nacional de Ciberseguridad, 22 de julio de 2021. https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/ciberataque-transnet-provoca-colapso-logistico.

INFOSYS. 2020. *Cybersecurity for Transport and Logistics Industry*. https://www.infosys.com/services/cyber-security/documents/transport-logistics-industry.pdf.

Intel471. 2021. Cybercrime in the transportation industry. *Intel471*, 14 de julio de 2021. https://intel471.com/blog/how-cybercriminals-create-turbulence-for-the-transportation-industry.

International Maritime Organization. s. f. *Cooperación técnica: Región de América Latina y el Caribe*. Accedido 29 de octubre de 2023. https://www.imo.org/es/OurWork/TechnicalCooperation/Paginas/LAC.aspx.

Jefatura de Gabinete de Ministros de Argentina. 2026. *Normativa - Ciberseguridad. Buenos Aires: Gobierno de Argentina*. https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa.

Kaspersky. 2023. Brasil, Ecuador y México se encuentran en el Top3 de los países más atacados - Experto advierte que estos ataques se han vuelto más dirigidos y rentables. *Kaspersky Lab,* 30 de agosto de 2023. https://latam.kaspersky.com/about/press-releases/2023_empresas-latinoamericanas-reciben-un-promedio-de-dos-ataques-de-ransomware-por-minuto-senala-kaspersky.

Kleinman, Zoe. 2020. Rail station wi-fi provider exposed traveler data. *BBC News,* 2 de marzo de 2020. https://www.bbc.com/news/technology-51682280.

Kosévich, Ekaterina Yu. 2020. Estrategias de seguridad cibernética en los países de América Latina. *Iberoamerica Journal,* 1: 137-59. https://doi.org/10.37656/s20768400-2020-1-07.

National Institute of Standards and Technology (NIST). 2018. Framework for Improving Critical Infrastructure Cybersecurity. https://doi.org/10.6028/NIST.CSWP.04162018.

Newbill, Colleen M. 2019. Defining Critical Infrastructure for a Global Application. *Indiana Journal of Global Legal Studies,* 26 (2). https://www.repository.law.indiana.edu/ijgls/vol26/iss2/11.

OAG. s. f. Megahubs 2023 | Most Connected Airports in the World. Accedido 29 de octubre de 2023. https://www.oag.com/megahub-airports-2023.

Organización de Aviación Civil Internacional (ICAO). 2019. Estrategia de ciberseguridad de la aviación. https://www.icao.int/sites/default/files/Meetings/a42/Documents/AVIATION-CYBERSECURITY-STRATEGY.SP_.pdf.

———. 2022. *Plan de acción de ciberseguridad*. https://www.icao.int/aviationcybersecurity/Documents/CYBERSECURITY%20ACTION%20PLAN%20-%20Second%20edition.SP.pdf.

———. s. f. Guidance Material on Aviation Cybersecurity. Accedido 24 de octubre de 2023. https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx.

Organización de los Estados Americanos (OEA). s. f. CICTE: Comité Interamericano contra el Terrorismo. Accedido 29 de octubre de 2023. https://www.oas.org/es/sms/cicte/.

Osborne, Charlie. 2018. NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs. *ZDNET,* 26 de enero de 2018. https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/.

OWASP GenAI Security Project. 2025. Top 10 2025 de riesgos y mitigaciones para LLMs y aplicaciones de IA Generativa. OWASP GenAI Security Project, 12 de marzo de 2025. https://genai.owasp.org/resource/top-10-2025-de-riesgos-y-mitigaciones-para-llms-y-aplicaciones-de-ia-generativa/.

Page, Carly. 2022. Car rental giant Sixt hit by cyberattack, customers told to expect delays. TechCrunch, 4 de mayo de 2022. https://techcrunch.com/2022/05/04/car-rental-sixt-cyberattack-delays/.

People's Republic of China. 2018. *Cybersecurity Law of the People's Republic of China (translation).* Standing Committee of the National People's Congress. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

PierNext. 2021. Colaboración y resiliencia contra los cibertaques. *PierNext,* 10 de agosto de 2021. https://piernext.portdebarcelona.cat/gobernanza/resiliencia-y-colaboracion-la-mejor-defensa-de-los-puertos-contra-los-ciberataques/.

Porrúa, Miguel, Guillermo Moncayo, Santiago Paz, Ariel Nowersztern, Jorge Fernando Bejarano, María Florencia Baudino, Maria Paula Bordese, Kerry-Ann Barret, Carlos Eduardo Baena, Mariana Jaramillo, Orlando Garces y Agustín Isidro. 2025. 2025 *Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean.* Banco Interamericano de Desarrollo. https://doi.org/10.18235/0013872.

Ransomware attack on Swissport causes delay at Zurich Airport. s. f. Accedido 3 de diciembre de 2023. https://www.airport-technology.com/news/ransomware-attack-swissport-zurich-airport/.

Republic of Singapore. 2018. *Cybersecurity Act 2018.* Parliament of Singapore. https://sso.agc.gov.sg/Acts-Supp/9-2018/.

Robertson, Jordan y Michael Riley. 2015. The Mob's IT Department. *Bloomberg Businessweek,* 7 de Julio de 2015. https://www.bloomberg.com/graphics/2015-mob-technology-consultants-help-drug-traffickers/.

Robbins, Arryn, Ebben W. Daggett y Michael Houst. 2026. AI doesn't 'see' the way that you do, and that could be a problem when it categorizes objects and scenes. The Conversation, 11 de marzo de 2026. https://theconversation.com/ai-doesnt-see-the-way-that-you-do-and-that-could-be-a-problem-when-it-categorizes-objects-and-scenes-271481.

SAE International. 2021. J3016_202104: *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. https://www.sae.org/standards/content/j3016_202104/.

Shoorbaje, Zaid. 2017. FedEx attributes $300 million loss to NotPetya ransomware attack. *CyberScoop,* 20 de septiembre de 2017. https://cyberscoop.com/fedex-attributes-300-million-loss-notpetya-attack/.

Tabak, Nate. 2017. Minnesota trucking company hit in 2nd ransomware attack. *Freight Waves,* 2017. https://www.freightwaves.com/news/minnesota-trucking-company-hit-in-2nd-ransomware-attack.

———. 2020. 5 defining cyberattacks on trucking and logistics in 2020. *Freight Waves,* 28 de diciembre de 2020. https://www.freightwaves.com/news/5-defining-cyberattacks-on-trucking-and-logistics-in-2020.

U.S. Department of Homeland Security. 2023. FY 2023 *Transit Security Grant Program Fact Sheet*. European Union Agency for Cybersecurity. https://www.fema.gov/grants/preparedness/transit-security/fy-23-fact-sheet.

———. s. f. *Surface Transportation Cybersecurity Toolkit | Transportation Security Administration*. Accedido 29 de octubre de 2023. https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit.

U.S. Department of Transportation. 2023. *Architecture Overview. Architecture Reference for Cooperative and Intelligent Transportation*. https://www.arc-it.net/html/architecture/architecture.html.

———. s. f.-a. *ITS Cybersecurity Research Program*. Accedido 29 de octubre de 2023. Cybersecurity | ITS Joint Program Office

———. s. f.-b. *Service Packages. Architecture Reference for Cooperative and Intelligent Transportation*. Accedido 29 de octubre de 2023. https://www.arc-it.net/html/servicepackages/servicepackages-areaspsort.html.

U.S. General Services Administration. s. f. *Cybersecurity framework*. Accedido 24 de octubre de 2023. https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/technology-products-and-services/it-security/cybersecurity-framework.

Vallance, Chris. 2023. MOVEit hack: Media watchdog Ofcom latest victim of mass hack. *BBC News,* 12 de junio de 2023. https://www.bbc.com/news/technology-65877210.

Vergara Cobos, E. 2024. *Cybersecurity Economics for Emerging Markets*. https://doi.org/10.1596/978-1-4648-2120-2

WAQAS. 2016. 24 Funny, Upsetting and Shocking Hacked Traffic Signs. *HackRead,* 7 de agosto de 2016. https://www.hackread.com/24-hacked-traffic-sigh-boards/.

What is a Security Operations Center (SOC)? | IBM. s. f. Accedido 17 de enero de 2024. https://www.ibm.com/topics/security-operations-center.

White House. 2021. *National Security Memorandum / NSM-22 on Improving Cybersecurity for Critical Infrastructure Control Systems.* U.S. Government. National Security Memorandum on Critical Infrastructure Security and Resilience - United States Department of State