Comisión Europea

Conjunto de herramientas de ciberseguridad para el transporte

Introducción

La Dirección General de Movilidad y Transportes de la Comisión Europea (DG MOVE) ha encargado el desarrollo de este conjunto de herramientas para mejorar la sensibilización y la preparación de las partes interesadas del transporte frente a las ciberamenazas. Proporciona información para comprender las ciberamenazas y mitigar sus efectos en los servicios, los sistemas y las operaciones de transporte. Este conjunto de herramientas ofrece dos vías de sensibilización que corresponden a distintos perfiles:

- La generalidad del personal de transporte (con información y orientación generales)

- Los responsables de la toma de decisiones en el transporte en materia de ciberseguridad.

Los hipervínculos conectan las distintas partes que forman el conjunto de herramientas para facilitar la navegabilidad.

Las prácticas mencionadas en este conjunto de herramientas son de carácter meramente informativo. Las recomendaciones que se formulan no son vinculantes ni obligatorias. Además, este conjunto de herramientas no representa los puntos de vista formales de la Comisión Europea y no pretende proporcionar medios para el cumplimiento de la legislación vigente o futura de la UE.

Perfiles de sensibilización en materia de ciberseguridad

Perfil I: personal de transporte. La primera vía se dirige a todo el personal que trabaja en organizaciones de transporte. Proporciona información para comprender mejor las ciberamenazas más comunes contra el transporte. Además, ofrece información sobre cómo hacer frente a posibles ciberamenazas, incluida la determinación, notificación y mitigación de las mismas mediante buenas prácticas en materia de ciberseguridad.

Perfil II: Responsables de la toma de decisiones en materia de ciberseguridad en el transporte. La segunda vía se dirige al personal responsable de la toma de decisiones en materia de ciberseguridad en las organizaciones de transporte. Destaca buenas prácticas adaptadas a los diferentes modos de transporte. En particular, ofrece buenas prácticas para determinar, proteger, detectar y responder a las ciberamenazas emergentes dirigidas a las organizaciones de transporte.

Comisión Europea

Conjunto de herramientas de ciberseguridad para el transporte

Panorama sobre amenazas para el transporte

Ciberamenazas emergentes que afectan a los modos de transporte

Perfiles de sensibilización en materia de ciberseguridad

Vías alternativas de sensibilización en materia de ciberseguridad correspondientes a los diferentes perfiles de transporte

Comisión Europea

Panorama de amenazas para el transporte

El panorama de ciberamenazas es dinámico y evoluciona continuamente. No obstante, es posible determinar las ciberamenazas a las que se enfrentan todos los modos de transporte.

Comisión Europea

Agentes de riesgo

Personas u organizaciones que pueden afectar a la seguridad y la protección de los servicios y sistemas de transporte

Ciberamenazas emergentes

Ciberamenazas seleccionadas que puedan afectar a la seguridad y la protección de los servicios y sistemas de transporte

Agentes de riesgo

Los personas o las organizaciones 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.

Los agentes malintencionados más importantes que se dirigen deliberadamente contra las organizaciones de transporte son los **ciberdelincuentes**, las **personas con información privilegiada**, los Estados-nación y los **grupos patrocinados por el Estado**.
Existen adversarios, como los **ciberdelincuentes**, que llevan a cabo campañas de ataques masivos y suelen participar en el juego a cambio de recompensas económicas.

Las **personas con información privilegiada** conocen las singularidades de las organizaciones para las que trabajan y a menudo son muy conscientes de las sutiles vulnerabilidades en materia de seguridad. Estas personas con información privilegiada pueden ser empleados, proveedores y contratistas individuales descontentos.
A medida que se intensifican las tensiones geopolíticas mundiales, los **Estados-nación** y los **grupos patrocinados por el Estado** persiguen objetivos estratégicos a largo plazo. Suelen tratar de ocultarse en las profundidades de los sistemas de las organizaciones y recabar información sensible. Una vez que se instalan en los sistemas, los atacantes patrocinados por el Estado intentan alcanzar una posición que pueda provocar los peores daños posibles.

Los agentes no malintencionados son **personas con información privilegiada** que, de forma involuntaria o accidental, pueden llevar a cabo acciones que den lugar a incidentes de ciberseguridad y, en el peor de los casos, a ciberincidentes que afecten a la seguridad y la protección de los servicios de transporte.

Ciberamenazas emergentes

Existen varias ciberamenazas dirigidas contra el transporte: **ataque distribuido de denegación de servicio**, **denegación de servicio**, robo de datos, difusión de programas maliciosos, ***phishing***, manipulación de *software*, **acceso no autorizado**, ataques destructivos, falsificación o elusión del proceso de decisión del operador de seguridad, suplantación de identidad, abuso de los privilegios de acceso, **ingeniería social**, desfiguración, escucha informática, uso indebido de activos y manipulación de *hardware*.

Sobre la base de una amplia investigación bibliográfica de documentación disponible públicamente y entrevistas con expertos, las ciberamenazas emergentes más acuciantes que afectan al transporte son las siguientes: programas maliciosos, ataque (distribuido) de denegación de servicio, acceso no autorizado y robo y manipulación de *software*.

Comisión Europea

Amenaza n.º 1: Programas maliciosos

Software malicioso que puede afectar a personas u organizaciones de todos los modos de transporte

Amenaza n.º 2: Ataque (distribuido) de denegación de servicio

Ataques de ciberseguridad que impiden el acceso de las personas o de la organización a los servicios y a los recursos

Amenaza n.º 3: Acceso no autorizado y robo

Acceso, apropiación y explotación no autorizados de activos estratégicos

Amenaza n.º 4: Manipulación de software

Ataques de ciberseguridad dirigidos contra *software* con el fin de modificar su comportamiento y realizar ataques específicos

Amenaza n.º 1: Programas maliciosos

Los programas maliciosos consisten en software malicioso, que puede incluir diferentes tipos de aplicaciones informáticas, como virus, troyanos, gusanos, programas de secuestro, mineros de criptomonedas o cualquier *software* que pueda tener efectos adversos en organizaciones o personas en todos los modos de transporte.

La mitigación de la difusión de programas maliciosos diseñados para dañar intencionadamente ordenadores, servidores, clientes, redes, o todos ellos, es una de las principales prioridades de la ciberseguridad en todos los modos de transporte. Un vector típico de ataque puede implicar correos electrónicos de *phishing* dirigidos contra empleados. Otros vectores de ataque pueden implicar estrategias de ingeniería social diferentes y sofisticadas, como conectar una memoria USB a un puerto libre (por ejemplo, para cargar un teléfono móvil). Al pulsar hipervínculos en correos electrónicos sospechosos o abrir archivos adjuntos, el usuario puede estar instalando programas maliciosos sin saberlo.

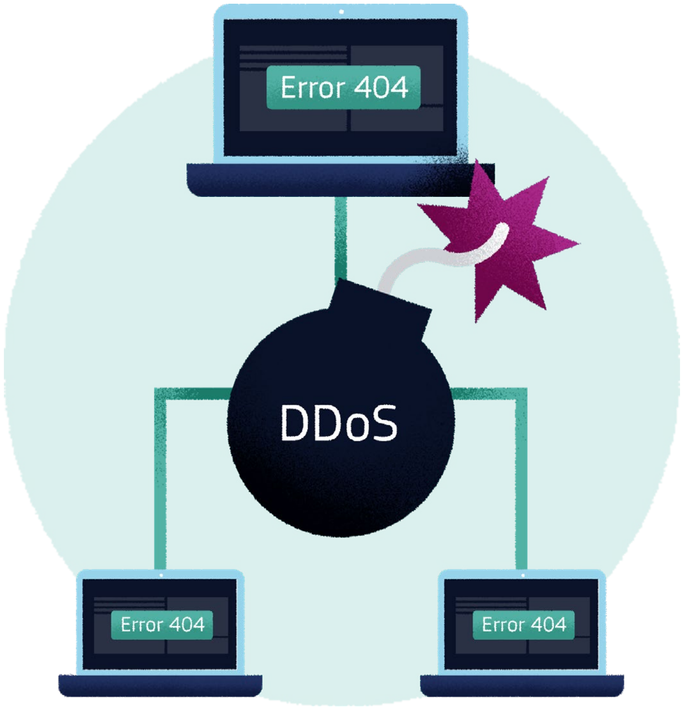
Por ejemplo, el ciberataque WannaCry con programas de secuestro afectó a más de 150 países e infectó a más de 230 000 sistemas. Se trataba de un programa de secuestro que normalmente se propaga a través de correos electrónicos de *phishing* que contienen archivos adjuntos o hipervínculos malintencionados. Este tipo de ataque explota de forma malintencionada la ingeniería social para inducir a error a los usuarios del sistema en la instalación (o la activación) de programas maliciosos específicos.

Amenaza n.º 2: Ataque (distribuido) de denegación de servicio

Los ataques distribuidos de denegación de servicio y los ataques de denegación de servicio afectan a la disponibilidad y accesibilidad de los datos, los servicios, los sistemas y otros recursos. La duración de estos tipos de ataques puede variar y pueden dirigirse a más de un servicio o sistema al mismo tiempo. Los ataques distribuidos de denegación de servicio emplean múltiples sistemas (o canales de ataque) para sobrecargar con solicitudes servicios o sistemas de telecomunicaciones interceptados. Los ataques con éxito afectan a las capacidades del servicio y del sistema para hacer frente a solicitudes imprevistas de volumen. Esto da lugar a la denegación de acceso a servicios y recursos.

Obsérvese que los servicios y sistemas afectados pertenecientes a organizaciones de transporte también pueden utilizarse para llevar a cabo ataques distribuidos de denegación de servicio y ataques de denegación de servicio dirigidos a sistemas específicos en operaciones u otras organizaciones.

Por ejemplo, los sistemas de información corporativos (como ordenadores y dispositivos personales) pueden recibir ataques para acceder a tecnologías operativas, que pueden estar conectadas a internet, o acceder a redes para transferir datos operativos. Las conexiones entre diferentes sistemas y redes (como las redes corporativas, las tecnologías operativas y los accesos de mantenimiento remoto) pueden representar vulnerabilidades explotables para la realización de ataques distribuidos de denegación de servicio y ataques de denegación de servicio a servicios y sistemas estratégicos de transporte. Por ejemplo, estos ataques pueden explotar protocolos comunes de red y comunicación, como el Web Services Dynamic Discovery (WS-Discovery), que los dispositivos del IdC pueden utilizar para descubrir automáticamente cada nodo de las redes de área local (LAN). Si los dispositivos del IdC presentan vulnerabilidades, los atacantes pueden aprovecharlas para descubrir otros dispositivos conectados y llevar a cabo ataques distribuidos de denegación de servicio y ataques de denegación de servicio.



Amenaza n.º 3: Acceso no autorizado y robo

Los agentes de riesgo pueden querer obtener acceso lógico o físico sin permiso a una red, sistema, aplicación, datos u otro recurso con el fin de llevar a cabo actividades malintencionadas, como el robo de datos o recursos sensibles (también los recursos físicos).
Las amenazas de acceso no autorizado y robo se dirigen a activos confidenciales y con derecho de propiedad registrado (en particular, las identidades personales, las credenciales de cuentas privilegiadas, los sistemas y otros tipos de información confidencial y con derecho de propiedad registrado). Estas amenazas pueden aprovecharse de las vulnerabilidades de los sistemas, así como de personas que no saben que están desvelando datos sensibles, como credenciales (por ejemplo, nombre de usuario, contraseña, etc.) o datos personales (por ejemplo, correo electrónico, número de identificación personal, etc.).

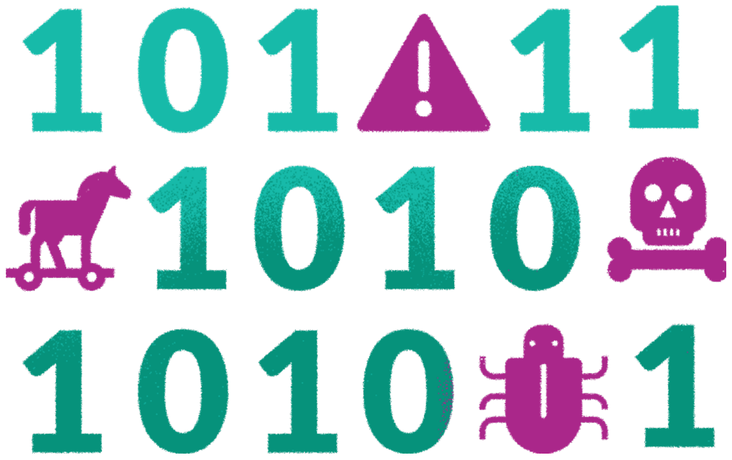
En relación con el acceso no autorizado, la usurpación de identidad es el uso ilícito de datos personales o identificadores únicos para suplantar a personas o servicios y sistemas con el fin de acceder a recursos privados o con derecho de propiedad registrado (por ejemplo, recursos financieros y físicos). Estas ciberamenazas también pueden dirigirse a activos físicos de todos los modos de transporte.

Amenaza n.º 4: Manipulación de software

Las malas configuraciones y las manipulaciones del *software* y de los sistemas o componentes relacionados pueden tener una repercusión directa en la posición de seguridad de los servicios y sistemas de transporte.

Los ataques de ciberseguridad que aprovechan las manipulaciones del *software* modifican la configuración de este o afectan a la integridad de los datos con el fin de cambiar el comportamiento de los sistemas y servicios. Los atacantes pueden manipular intencionadamente el *software* (o parte del mismo) con el fin de obtener ventajas (por ejemplo, obtener acceso no autorizado, impedir el acceso de personas o sistemas legítimos a los recursos necesarios, recopilar información sensible, cambiar los comportamientos funcionales, etc.) sobre activos sensibles.

Por ejemplo, los atacantes pueden dirigirse a los canales de comunicación de los fabricantes para cargar actualizaciones de programas maliciosos en servicios y sistemas en las operaciones (también las tecnologías operativas). Un agente de riesgo utiliza credenciales de autorización comprometidas para acceder a una interfaz de red de mantenimiento remoto seguro con el fin de instalar *software* manipulado y comprometer aún más otros servicios y sistemas accesibles. El agente de riesgo instala *software* manipulado que compromete aún más los servicios o sistemas de telecomunicaciones interceptados, o que ataca otros servicios o sistemas conectados.



Comisión Europea

Perfiles de sensibilización en materia de ciberseguridad

Comisión Europea

1

Perfil I: Generalidad del personal de transporte

La primera vía se dirige a todo el personal de las organizaciones de transporte, desde el personal encargado de las operaciones hasta el personal administrativo. Esta vía ofrece orientaciones para una mayor comprensión de las ciberamenazas más comunes, así como para una mayor sensibilización ante estas. Además, ofrece información sobre cómo hacer frente a posibles ciberamenazas, como la determinación, notificación y mitigación de estas. Esta vía es común a todos los modos de transporte.

2

Perfil II: Responsables de la toma de decisiones en materia de ciberseguridad en el transporte

La segunda vía se dirige al personal responsable de la toma de decisiones en materia de seguridad o ciberseguridad en las organizaciones de transporte. Esta vía ofrece buenas prácticas adaptadas a los diferentes modos de transporte. Ofrece buenas prácticas para determinar, proteger, detectar y responder a las ciberamenazas emergentes dirigidas a las organizaciones de transporte.

Comisión Europea

Perfil I: Generalidad del personal de transporte

Esta vía se dirige a todo el personal de las organizaciones de transporte, desde el personal encargado de las operaciones hasta el personal administrativo. Ofrece orientaciones para una mayor comprensión de las ciberamenazas más comunes, así como para una mayor sensibilización ante estas. Además, ofrece información sobre cómo hacer frente a posibles ciberamenazas, como la determinación, notificación y mitigación de estas.
Esta vía ofrece prácticas recomendadas y consejos útiles, que son pertinentes **en todos los modos de transporte**.

Comisión Europea

Buenas prácticas contra los programas maliciosos

Puede ayudar a proteger a su organización siguiendo buenas prácticas para **detectar programas maliciosos e impedir su difusión**, tales como:

- ***Seguir políticas de seguridad***, *como el escaneado de soportes de almacenamiento y archivos en busca de virus, evitar la apertura y el envío a través de correo electrónico de determinados tipos de archivos (por ejemplo, archivos ejecutables de tipo .exe, .bat, .com, etc.), instalar únicamente software autorizado, garantizar que el software (incluido el antivirus) esté actualizado y funcione correctamente, y otras políticas*

- ***Hacer una copia de seguridad de sus datos*** *periódicamente en dispositivos o servicios de almacenamiento de datos seguros (y autorizados), que sean compatibles con mecanismos de cifrado para proteger la información en reposo y estén disponibles para los procedimientos de recuperación de datos*

- *Proteger con* ***medidas de seguridad*** *adecuadas (por ejemplo, contraseña, cifrado, etc.) todos los sistemas, incluidos los dispositivos móviles y terminales, y recordar bloquear (física y digitalmente) de forma segura todos los sistemas sin vigilancia*

- *Evitar abrir archivos adjuntos y hacer clic en hipervínculos incluidos en correos electrónicos inesperados y ventanas emergentes del navegador sospechosas con un cuerpo del texto extraño o procedentes de remitentes y dominios de internet desconocidos*

- *Evitar introducir en su ordenador* ***dispositivos extraíbles poco fiables o desconocidos***, *como memorias USB, discos duros y otros dispositivos de almacenamiento*

- *Evitar desactivar las medidas de seguridad contra programas maliciosos (por ejemplo, software antivirus, software de filtrado de contenidos, cortafuegos, etc.)*

- ***Actualizar periódicamente el*** **software** ***instalado*** *a las últimas versiones disponibles (que los responsables de la seguridad de la información o los administradores de sistemas pueden publicar con actualizaciones periódicas)*

- *Evitar utilizar cuentas y credenciales privilegiadas (por ejemplo, a nivel administrativo) para actividades y operaciones habituales*

- *Comunicar a los responsables de la seguridad de la información o a los administradores de sistemas cualquier correo electrónico sospechoso o comportamiento inesperado del sistema*

- *Centrar la atención en la seguridad de la información en el trabajo rutinario diario con el fin de reconocer los problemas de seguridad informática y responder en consecuencia.*

Buenas prácticas contra los ataques (distribuidos) de denegación de servicio

Puede ayudar a proteger a su organización mediante la detección de ataques **distribuidos de denegación de servicio** y de **denegación de servicio**. Debe ponerse inmediatamente en contacto con sus equipos de seguridad e informática si detecta o experimenta alguno de los siguientes indicadores de posibles ataques distribuidos de denegación de servicio y de denegación de servicio en sus servicios o sistemas:

- *Aumento de las solicitudes que consumen capacidad de red (lo que se percibe como servicios y respuestas lentos), lo que da lugar a fallos en el servicio o en el sistema debido a la sobrecarga*

- *Aumento de la demanda de uso de recursos de memoria sin una razón evidente*

- ***Comportamientos inesperados de servicios y sistemas**, fallos frecuentes del sistema y mensajes de errores extraños debidos al consumo malintencionado de recursos computacionales o conexiones de red*

- ***Peor rendimiento** de los dispositivos, ejecuciones largas para tareas triviales y actividades perceptibles (por ejemplo, ventilador ruidoso mientras los dispositivos funcionan lentamente)*

- ***Conexiones inesperadas a internet o pérdida de conexiones** a servicios y sistemas*

- *Sutiles cambios de comportamiento en los controles o tecnologías de funcionamiento que den lugar a daños físicos*

- *Denegación de acceso a cuentas privilegiadas o administrativas para bloquear la recuperación de los procedimientos de respuesta a incidentes.*

Buenas prácticas contra el acceso no autorizado y el robo

Con el fin de evitar ataques con acceso no autorizado y robo, es necesario seguir principios como la «necesidad de conocer» y la «seguridad y privacidad por defecto», que subrayan que solo deben acceder a los activos sensibles y confidenciales (en especial los datos personales y sensibles, los sistemas de transporte, etc.) quienes tengan derecho a acceder a ellos para el ejercicio de sus funciones. Puede ayudar a proteger a su organización siguiendo buenas prácticas para detectar e impedir el acceso no autorizado y el robo, tales como:

- *Seguir las políticas organizativas de seguridad*

- *Evitar compartir y publicar credenciales y datos personales en línea, también las imágenes que puedan contener dicha información*

- *Evitar utilizar o transmitir credenciales y datos personales (y otros datos sensibles) en redes, dispositivos o servicios web poco fiables y no seguros (por ejemplo, sitios web que utilizan protocolos o direcciones no seguros, http://, en lugar de seguros, https://)*

- ***Nunca revelar a nadie sus credenciales** (por ejemplo, nombre de usuario y contraseña), ni siquiera por correo electrónico o por teléfono*

- *Proteger los datos sensibles introducidos mediante un teclado o mostrados en pantallas (incluso en los dispositivos móviles) de personas no autorizadas, instalar pantallas de privacidad y evitar trabajar desde lugares públicos con dispositivos privados, así como evitar dejar cualquier dispositivo desbloqueado y sin vigilancia*

- ***Utilizar contraseñas complejas** (por ejemplo, contraseñas suficientemente largas que combinen caracteres alfanuméricos y especiales) que cumplan las políticas de seguridad organizativas pertinentes para impedir el acceso no autorizado*

- ***Cambiar las contraseñas por defecto** de los sistemas y dispositivos conectados (por ejemplo, impresoras, encaminadores, cámaras, cerraduras inteligentes, etc.)*

- *Evitar utilizar las mismas credenciales (por ejemplo, nombre de usuario y contraseña) para múltiples servicios y sistemas, y evitar utilizar las mismas credenciales para servicios y sistemas que requieran cuentas privilegiadas*

- *Enviar contraseñas y claves para los archivos protegidos transferidos (por ejemplo, archivos ZIP) solo a través de un canal fuera de banda (por ejemplo, SMS a través de GSM y llamadas telefónicas) y nunca por correo electrónico*

- ***Activar la autenticación de doble factor** o la autenticación multifactor, si es posible.*

Buenas prácticas contra la manipulación de *software*

Puede ayudar a proteger a su organización siguiendo buenas prácticas para detectar y prevenir la manipulación de *software*, tales como:

- *Evitar la instalación de software poco fiable en sistemas y dispositivos (también ordenadores personales, servidores, periféricos, dispositivos de red, teléfonos inteligentes, etc.)*

- *Instalar siempre software y actualizaciones procedentes de fuentes y sitios web oficiales (por ejemplo, productores, repositorios corporativos, etc.)*

- *Evitar la descarga de software y aplicaciones (y de cualquier archivo) de fuentes ilegales*

- *Desinstalar software innecesario o no utilizado recientemente y desactivar conexiones innecesarias (por ejemplo, protocolos y servicios de red), en particular, el acceso a servicios remotos (por ejemplo, servicios de almacenamiento en la nube)*

- *Escanear cualquier software o dispositivo de almacenamiento con un antivirus fiable y actualizado*

- *Descargar software industrial seguro (por ejemplo, actualizaciones, parches, nuevos productos, etc.) de proveedores de confianza utilizando el principio white station*

- *Actualizar todo el software instalado de conformidad con las políticas y prácticas organizativas.*

Comisión Europea

Perfil II: Responsables de la toma de decisiones en materia de ciberseguridad en el transporte

Esta vía se dirige al personal responsable de la toma de decisiones en materia de seguridad o ciberseguridad en las organizaciones de transporte. Destaca buenas prácticas adaptadas a los diferentes modos de transporte. En particular, ofrece buenas prácticas para determinar, proteger, detectar y responder a las ciberamenazas emergentes.

Comisión Europea

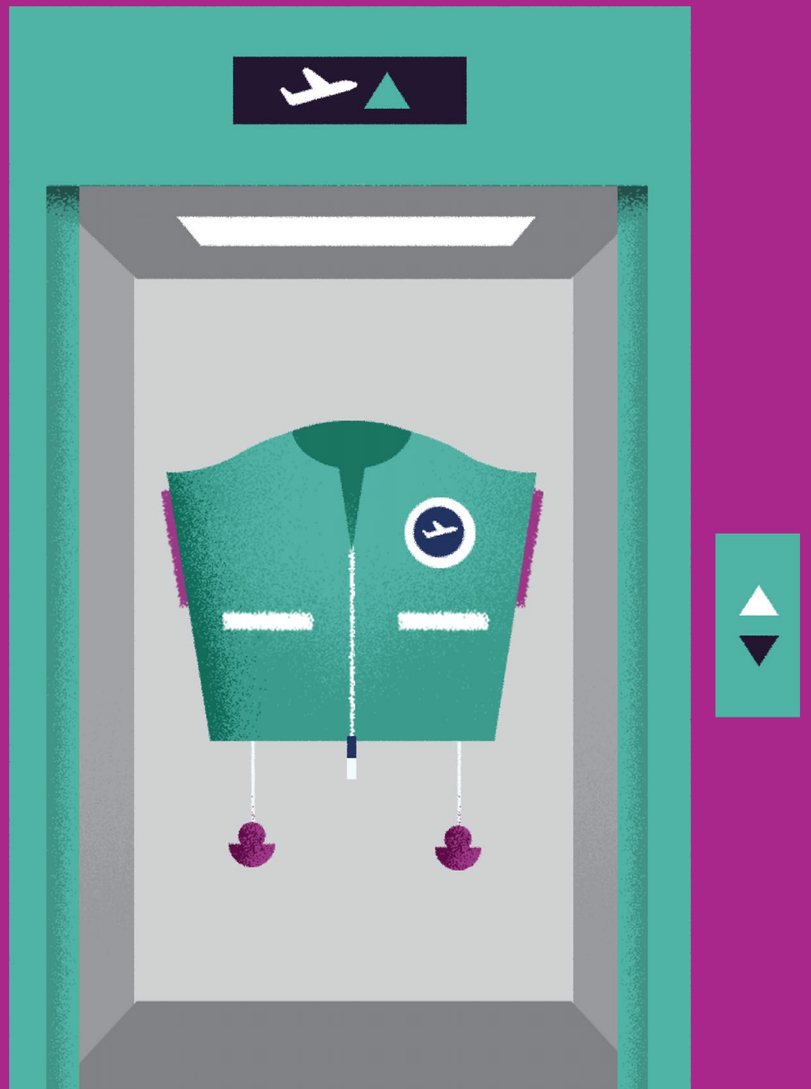
Buenas prácticas de ciberseguridad adaptadas al transporte aéreo

Buenas prácticas de ciberseguridad adaptadas al transporte terrestre

Buenas prácticas de ciberseguridad adaptadas al transporte marítimo

Comisión Europea

Buenas prácticas y medidas de seguridad adaptadas al transporte aéreo



Gobernanza

Las organizaciones de aviación necesitan una comprensión clara de las amenazas emergentes a fin de definir políticas y procesos de gestión que rijan sus enfoques con el fin de mejorar la ciberseguridad de los servicios y sistemas en las operaciones, incluidas las tecnologías de la información y las tecnologías operativas.

Las buenas prácticas para organizaciones de cualquier tamaño implican:

- Garantizar que los altos directivos informen sobre las preocupaciones en materia de ciberseguridad a los ejecutivos y los consejos, que pueden tomar decisiones con conocimiento de causa sobre la asignación de recursos

- Designar un cargo de alto nivel responsable de la ciberseguridad y la seguridad física, con responsabilidades generales de gestión para la seguridad de las tecnologías de la información y las tecnologías operativas, pero sin participación en las operaciones con el fin de evitar conflictos de intereses

- Definir claramente las funciones, responsabilidades, competencias y autorizaciones relacionadas con la ciberseguridad y comunicarlas y acordarlas con el personal pertinente, en particular en el caso de los miembros de los equipos de respuesta a emergencias informática (CERT)

- Garantizar la gobernanza de la ciberseguridad a lo largo de toda la cadena de prestación de servicios de seguridad, incluidas las interfaces físicas y digitales, desde los fabricantes e instaladores de tecnología hasta los proveedores de seguridad

- Acordar actividades y controles, en particular, las responsabilidades compartidas, para gestionar los riesgos de ciberseguridad, y garantizar que estas responsabilidades se mantengan a lo largo de toda la vida útil (por ejemplo, mediante acuerdos de servicios) de las soluciones y servicios de seguridad

- Definir mecanismos de gobernanza (por ejemplo, políticas) para cumplir las obligaciones derivadas de los reglamentos y las directivas pertinentes, como, por ejemplo, el Reglamento 2018/1139 sobre normas comunes en el ámbito de la aviación civil y el Reglamento de Ejecución 2017/373 de la Comisión por el que se establecen requisitos comunes para los proveedores de servicios de gestión del tránsito aéreo/navegación aérea y otras funciones de la red de gestión del tránsito aéreo y su supervisión, así como la Directiva SRI (Directiva 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información).

Ejemplos de servicios y sistemas en el transporte aéreo: Ejemplos de tecnologías de la información son aquellas a las que tienen acceso los empleados (por ejemplo, ordenadores personales, teléfonos móviles, periféricos de oficina, etc.), así como los pasajeros (por ejemplo, encaminadores y conexiones wifi públicos, etc.). Ejemplos de equipos operativos son los Sistemas de Supervisión para el Control y la Obtención de Datos (SCADA), los sistemas de calefacción, ventilación y aire acondicionado (HVAC), los puntos de control de seguridad para el equipaje de mano, los sistemas de gestión de equipajes, el control de acceso, el seguimiento, la vigilancia, la respuesta a las alarmas, la tecnología de control, los sistemas de control de la iluminación de los aeródromos, los sistemas y sensores de radar, los sistemas de posicionamiento global (GPS), los sistemas de gestión del tránsito aéreo (ATM), los sistemas de comunicaciones, navegación y vigilancia (CNS), los sistemas de información aeronáutica, los sistemas meteorológicos, los sistemas de los centros de operaciones de seguridad, los sistemas a bordo de las aerolíneas, etc.

Comisión Europea

Determinación de las ciberamenazas

Gestión de riesgos: Las organizaciones de aviación deben adoptar las medidas adecuadas para determinar, evaluar y comprender los riesgos de ciberseguridad para los sistemas de red y de información que apoyan las operaciones de las funciones esenciales.

Esto requiere un enfoque organizativo global de la gestión de riesgos, que incluya:

- *Garantizar una visión general clara de los distintos sistemas de hardware y software desplegados para la prestación de diferentes servicios. En el contexto de la aviación, estos sistemas incluyen tecnologías de la información y tecnologías operativas*

- *Realizar **evaluaciones de riesgos en materia de ciberseguridad**, que tengan en cuenta las amenazas emergentes, las vulnerabilidades conocidas y los datos operativos en relación con los sistemas en el ámbito de aplicación. Organizaciones como el Equipo Europeo de Respuesta a Emergencias Informáticas de Gestión del Tránsito Aéreo (EATM-CERT) y el Centro de puesta en común y análisis de la información sobre aviación (A-ISAC) pueden proporcionar información sobre las amenazas que afectan al transporte aéreo*

- *Garantizar que las evaluaciones de riesgos también cubran los riesgos relacionados con las actividades cotidianas del personal (por ejemplo, uso de redes sociales, uso de dispositivos personales, tratamiento de datos, intercambio de información, etc.)*

- *Determinar y aplicar medidas y planes de tratamiento de riesgos para mitigar los riesgos de ciberseguridad*

- *Aplicar un **Sistema de Gestión de la Seguridad de la Información** (SGSI) global y un **Sistema de Gestión de la Información Privada** (SGIP) armonizados con otros sistemas de gestión. Estos sistemas de gestión (es decir, el SGSI y el SGIP) implican la aplicación de controles de seguridad (así como de protección de datos y privacidad) con el fin de mitigar y prevenir las amenazas emergentes que afectan a la seguridad de los servicios y sistemas de aviación (también sus datos)*

- *Tener en cuenta cualquier limitación relacionada con **la gestión de activos y la planificación de recursos** (es decir, las limitaciones que pueden afectar a la entrega, el mantenimiento y el apoyo de sistemas críticos para el funcionamiento de las funciones esenciales en el transporte aéreo).*

Ejemplos de marcos de gestión de riesgos: Diferentes marcos (por ejemplo, las normas de la familia ISO/IEC 27000, el marco de ciberseguridad del NIST, el marco MITRE ATT&CK, la norma BSI IT-Grundschutz, etc.) pueden servir de base y sustentar un enfoque de gestión de riesgos adaptado para el transporte aéreo. Organizaciones internacionales como la IATA y la OACI proporcionan orientaciones para las evaluaciones de riesgos en materia de ciberseguridad. La ENISA, la AESA, Eurocontrol y el Consejo Internacional de Aeropuertos (ACI), entre otros, destacan las buenas prácticas para garantizar la seguridad de los aeropuertos, los proveedores de gestión del tráfico aéreo y otras organizaciones de aviación. La empresa común SESAR coordina y concentra todas las actividades de investigación y desarrollo (I+D) de la UE en materia de gestión del tránsito aéreo y abarca también aspectos de la seguridad y la protección.

Comisión Europea

Protección contra las ciberamenazas

Las organizaciones de transporte aéreo deben aplicar medidas de seguridad adecuadas y proporcionadas para proteger sus redes y sistemas de información, en particular, las tecnologías de la información y las tecnologías operativas, frente a los ciberataques. Entre las medidas de seguridad se incluyen:

- ***Políticas y procesos de seguridad:*** *definir, aplicar, comunicar y hacer cumplir políticas y procesos adecuados que definan un enfoque global para la seguridad de los sistemas y datos que apoyen las operaciones de las funciones esenciales de la aviación. Estas políticas y procedimientos de seguridad (por ejemplo, las políticas de contraseña y almacenamiento) deben abarcar también los parches y la gestión de la vulnerabilidad de los sistemas de hardware y software (también las tecnologías de la información y las tecnologías operativas), la gestión de incidentes, así como la protección de los sistemas y de las redes.*

- ***Gestión de la identidad y del acceso:*** *comprender, documentar y gestionar el acceso a las redes y los sistemas de información (también las tecnologías de la información y las tecnologías operativas) que apoyan el funcionamiento de las funciones esenciales en el transporte aéreo. Los usuarios (o funciones automatizadas) que pueden acceder a los datos o sistemas están debidamente verificados, autenticados y autorizados. Esto también debe tener en cuenta las diferentes funciones y responsabilidades de las cuentas normales y privilegiadas.*

- ***Seguridad de los datos y sistemas:*** *proteger los datos (almacenados y transmitidos electrónicamente), las redes críticas y los sistemas de información (incluidas las tecnologías de la información y las tecnologías operativas) de los ciberataques. Teniendo en cuenta un enfoque basado en el riesgo, las organizaciones deben aplicar medidas de seguridad para limitar de manera efectiva las oportunidades de que los atacantes pongan en peligro los datos, las redes y los sistemas. Estas medidas de seguridad también deben incluir la adopción de protocolos de cifrado y de comunicación segura con el fin de proteger la información en reposo y en tránsito de las ciberamenazas resultantes de ataques de repetición. Además, es necesario combinar estas medidas con medidas de seguridad física para proteger el acceso a los sistemas (por ejemplo, los sistemas deben estar ubicados en espacios confinados con acceso restringido).*

- ***Resiliencia de las redes y los sistemas:*** *aumentar la resiliencia de las redes y los sistemas (también las tecnologías de la información y las tecnologías operativas) mediante su diseño y aplicación (y el de sus procedimientos operativos) con el fin de resistir y mitigar la repercusión de los ciberataques. Algunos ejemplos de soluciones de diseño y aplicación que refuerzan la resiliencia son: funciones esenciales verificadas formalmente, redundancia de sistemas y redes, segregación de redes (en particular, segregación de las tecnologías de la información y las tecnologías operativas), medidas de seguridad multinivel y muchas otras. Obsérvese que, desde el punto de vista de la seguridad de la información, los ámbitos de seguridad que aplican la segregación de redes y sistemas pueden ofrecer soluciones de seguridad adecuadas. Sin embargo, las necesidades operativas (por ejemplo, actividades de mantenimiento, transferencia de datos, etc.) de los sistemas pueden requerir la derivación o conexión de diferentes ámbitos de seguridad (por ejemplo, sistemas y redes segregados), incluida la conexión de las tecnologías de la información y las tecnologías operativas.*

Detección de las ciberamenazas

Las organizaciones deben garantizar que las medidas de seguridad sigan siendo eficaces y detectar cualquier incidente de ciberseguridad que afecte o pueda afectar a los controles de seguridad, así como a los servicios y sistemas esenciales. A fin de detectar las ciberamenazas, las medidas de seguridad pertinentes son las siguientes:

■ ***Supervisión de la seguridad:*** *supervisar el estado de seguridad de las redes y los sistemas de información, también las tecnologías de la información y las tecnologías operativas, que apoyan el funcionamiento de las funciones esenciales en los servicios de transporte aéreo. Para apoyar la supervisión de la seguridad, los datos que se tienen en cuenta son, por ejemplo:*

- *registros de seguridad*
- *registros de detección de virus*
- *registros de detección de intrusiones*
- *registros de identificación, autenticación y autorización*
- *registros de sistemas y servicios*
- *registros de tráfico de la red*
- *registros de tratamiento de datos*

■ ***Descubrimiento de incidentes de seguridad:*** *detectar las actividades malintencionadas (es decir, incidentes de seguridad) que afecten o puedan afectar a la seguridad de las redes y los sistemas de información (también las tecnologías de la información y las tecnologías operativas) que apoyan el funcionamiento de las funciones esenciales en los servicios de transporte aéreo.*

Estas medidas pueden requerir la adopción de tecnologías específicas (por ejemplo, gestión de información e incidentes en materia de seguridad, sistema de detección de intrusiones, sistema de prevención de intrusiones, etc.) y la creación de un centro de operaciones de seguridad o equivalente. Es decir, desarrollar medios para detectar, analizar, responder y recuperarse de los ciberataques a escala local.

Los equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT), los CERT sectoriales (por ejemplo, el Equipo Europeo de Respuesta a Emergencias Informáticas de Gestión del Tránsito Aéreo, EATM-CERT), Eurocontrol, los CERT comerciales de aerolíneas y el Centro de puesta en común y análisis de la información sobre aviación (A-ISAC) pueden proporcionar inteligencia sobre amenazas que sirva de base para las tareas de seguimiento y descubrimiento en el ámbito de la seguridad.

Planificación de la respuesta y de la recuperación

Las organizaciones deben definir, aplicar y probar procedimientos de gestión de incidentes que tengan por objeto garantizar la continuidad de las actividades de los servicios y sistemas en caso de incidentes de ciberseguridad. Las medidas de mitigación tienen por objeto contener o limitar la repercusión de los incidentes de ciberseguridad.

La planificación de la respuesta y de la recuperación debe tener en cuenta las medidas de seguridad, que limiten el efecto de ataques específicos de ciberseguridad, tales como:

- *Coordinación y colaboración con los CSIRT nacionales, los CERT (públicos y comerciales) y los ISAC durante los incidentes de ciberseguridad, la coordinación de incidentes y las crisis a escala paneuropea*

- *Intercambio de información con otras organizaciones, en particular, los proveedores de la cadena de suministro de servicios de aviación*

- *Realización de **ejercicios periódicos de ciberataque** (coordinación técnica, así como de simulaciones teóricas) para evaluar las medidas y los procedimientos de seguridad, así como la resiliencia de la organización para hacer frente a incidentes de ciberseguridad*

- *Acceso a lugares de almacenamiento en archivo permanente o de respaldo en caso de que la integridad y disponibilidad del almacenamiento de datos se encuentre en peligro*

- ***Manuales de estrategia en materia de seguridad** con procedimientos detallados para gestionar los incidentes de ciberseguridad y devolver los servicios y sistemas a las condiciones operativas normales*

- *Reorientar el tráfico de la red a servicios redundantes durante los ataques de denegación de servicio*

- *Procedimientos manuales para operar con servicios y sistemas en modos de funcionamiento degradados*

- *Definir procedimientos para hacer frente a las violaciones de la seguridad de los datos, en particular, los procedimientos para tratar las violaciones de la seguridad de los datos que afecten a datos personales de conformidad con el Reglamento General de Protección de Datos (RGPD) y cualquier otro reglamento o directiva sectorial pertinente*

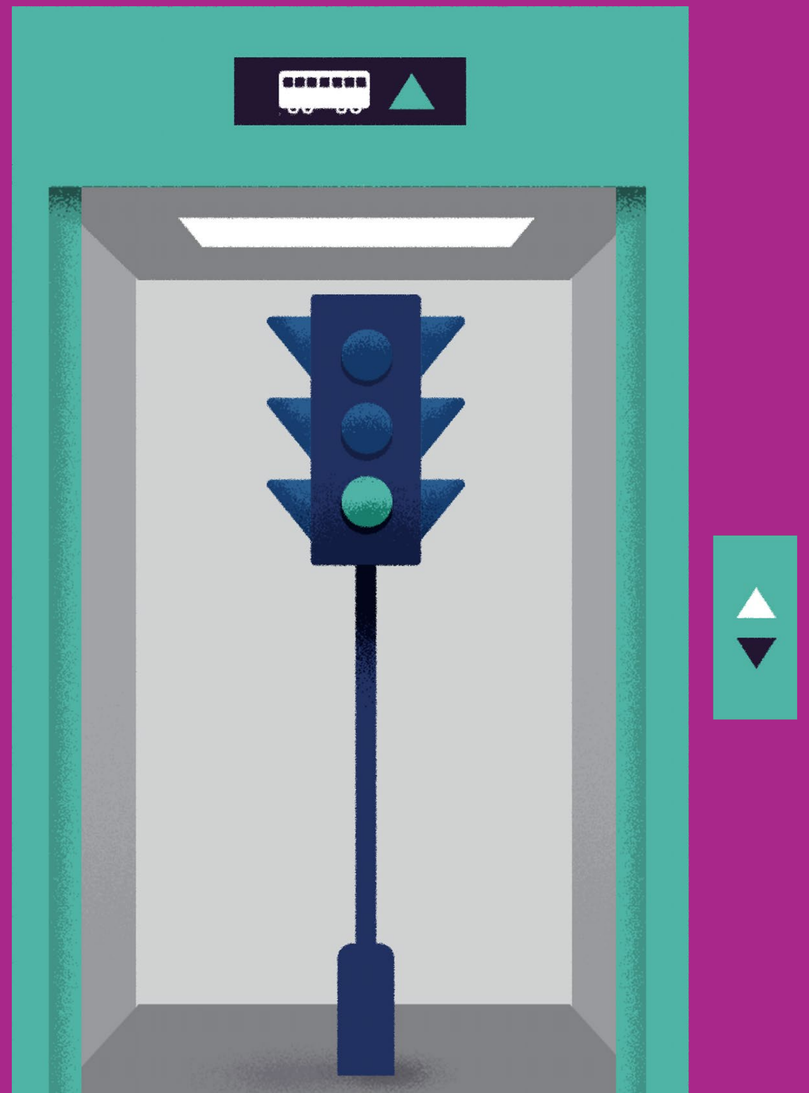
- *Adquirir **seguros cibernéticos** para compensar parcialmente el riesgo asociado a los incidentes de ciberseguridad graves*

- *Contratar un servicio de respuesta a incidentes con una o más empresas especializadas para obtener más capacidad y conocimientos especializados*

- *Definir procedimientos para **compartir información sobre incidentes de ciberseguridad** con las partes interesadas pertinentes, incluidos los procedimientos de notificación de incidentes de conformidad con la Directiva SRI (Directiva 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión).*

Comisión Europea

Buenas prácticas y medidas de seguridad adaptadas al transporte terrestre



Gobernanza

Las organizaciones de transporte terrestre (ferroviario y por carretera) necesitan una comprensión clara de las amenazas emergentes a fin de definir políticas y procesos de gestión que rijan sus enfoques con el fin de mejorar la ciberseguridad de los servicios y sistemas en las operaciones, en particular, las tecnologías de la información y las tecnologías operativas.

Las buenas prácticas para organizaciones de cualquier tamaño implican:

- *Garantizar que los altos directivos informen sobre las preocupaciones en materia de ciberseguridad a los ejecutivos y los consejos, que pueden tomar decisiones con conocimiento de causa sobre la asignación de recursos*

- *Designar un cargo de alto nivel responsable de la ciberseguridad y la seguridad física, con responsabilidades generales de gestión para la seguridad de las tecnologías de la información y las tecnologías operativas, pero sin participación en las operaciones con el fin de evitar conflictos de intereses*

- *Definir claramente las funciones, responsabilidades, competencias y autorizaciones relacionadas con la ciberseguridad y comunicarlas y acordarlas con el personal pertinente. Esto es necesario, en particular, para los miembros de los equipos de respuesta a emergencias informática (CERT)*

- *Garantizar la gobernanza de la ciberseguridad a lo largo de toda la cadena de prestación de servicios de seguridad, incluidas las interfaces físicas y digitales, desde los fabricantes e instaladores de tecnología hasta los proveedores de seguridad*

- *Acordar actividades y controles, en particular, las responsabilidades compartidas, para gestionar los riesgos de ciberseguridad, y garantizar que estas responsabilidades se mantengan a lo largo de toda la vida útil (por ejemplo, mediante acuerdos de servicios) de las soluciones y servicios de seguridad*

- *Definir mecanismos de gobernanza (por ejemplo, políticas) para cumplir las obligaciones derivadas de los reglamentos y las directivas pertinentes. Esto incluye un amplio conjunto de políticas que abarcan los modos de transporte específicos, así como diferentes tipos de partes interesadas (por ejemplo, fabricantes de vehículos y sistemas ferroviarios), así como la Directiva SRI (Directiva 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información).*

Comisión Europea

Ejemplos de servicios y sistemas en el transporte terrestre: Ejemplos de tecnologías de la información son aquellas a las que tienen acceso los empleados (por ejemplo, ordenadores personales, teléfonos móviles, periféricos de oficina, etc.), así como los pasajeros (por ejemplo, encaminadores y conexiones wifi públicos, etc.). Ejemplos de equipos operativos son los Sistemas de Supervisión para el Control y la Obtención de Datos (SCADA), los sistemas de calefacción, ventilación y aire acondicionado (HVAC), los sistemas de posicionamiento global (GPS), el control de acceso, el seguimiento, la vigilancia, la respuesta a las alarmas y la tecnología de control. Los sistemas específicos para el transporte ferroviario son, por ejemplo: operativos (sistemas de control y mando), incluidos los sistemas de señalización, el Sistema Europeo de Gestión del Tráfico Ferroviario (ERTMS), los sistemas instalados en los trenes, los sistemas de mantenimiento, etc.

Comisión Europea

Determinación de las ciberamenazas

Gestión de riesgos: Las organizaciones de transporte terrestre deben adoptar las medidas adecuadas para determinar, evaluar y comprender los riesgos de ciberseguridad para los sistemas de red y de información que apoyan las operaciones de las funciones esenciales. Esto requiere un enfoque organizativo global de la gestión de riesgos, que incluya:

- *Garantizar una visión general clara de los distintos sistemas de hardware y software desplegados para la prestación de diferentes servicios. En el contexto del transporte terrestre, estos sistemas incluyen tecnologías de la información y tecnologías operativas*

- *Realizar **evaluaciones de riesgos de ciberseguridad**, que tengan en cuenta las amenazas emergentes, las vulnerabilidades conocidas y los datos operativos en relación con los sistemas en el ámbito de aplicación. Ejemplos de sistemas en los modos de transporte terrestre son: sistemas de pago, sistemas de red y de comunicación (por ejemplo, internet, radiocomunicaciones, wifi, etc.), equipos a bordo, centros de control operativo, sistemas de gestión de identidades, sistemas de seguridad, etc. En el caso de las infraestructuras ferroviarias, algunos ejemplos de sistemas son: subsistemas de material rodante, de explotación y gestión del tráfico, subsistemas de control-mando y señalización a bordo y en tierra, etc.*

- *Garantizar que las evaluaciones de riesgos también cubran los riesgos relacionados con las actividades cotidianas del personal (por ejemplo, el uso de las redes sociales, el uso de dispositivos personales, el tratamiento de datos, el intercambio de información, etc.)*

- *Determinar y aplicar medidas y planes de tratamiento de riesgos para reducir los riesgos de ciberseguridad. Por ejemplo, aplicar un **Sistema de Gestión de la Seguridad de la Información (SGSO)** global y un **Sistema de Gestión de la Información Privada** (SGIP) armonizados con otros sistemas de gestión. Estos sistemas de gestión (es decir, el SGSO y el SGIP) implican la aplicación de controles de seguridad (así como de protección de datos y privacidad) con el fin de mitigar y prevenir las amenazas emergentes que afectan a la seguridad de los servicios y sistemas de transporte terrestre (también sus datos)*

- *Tener en cuenta cualquier limitación relacionada con **la gestión de activos y la planificación de recursos** (es decir, las limitaciones que pueden afectar a la entrega, el mantenimiento y el apoyo de sistemas críticos para el funcionamiento de las funciones esenciales en el transporte terrestre).*

Ejemplos de marcos de gestión de riesgos: Diferentes marcos (por ejemplo, las normas de la familia ISO/IEC 27000, el marco de ciberseguridad del NIST, el marco MITRE ATT&CK, la norma BSI IT-Grundschutz, etc.) pueden servir de base y sustentar un enfoque de gestión de riesgos adaptado para el transporte por carretera y ferroviario. Organizaciones como ENISA definen buenas prácticas para la ciberseguridad de los vehículos inteligentes y del transporte público inteligente, que sirven de base para los fabricantes y las asociaciones de la industria (por ejemplo, la Asociación de Fabricantes Europeos de Automóviles, ACEA). En el transporte ferroviario, la Agencia Ferroviaria de la Unión Europea (AFE) define las especificaciones técnicas de interoperabilidad (ETI) que deben cumplir cada subsistema o parte de subsistema para satisfacer los requisitos esenciales y garantizar la interoperabilidad del sistema ferroviario de la Unión Europea. La empresa común Shift2Rail también impulsa iniciativas y proyectos innovadores (en particular, la ciberseguridad) para el transporte ferroviario.

Protección contra las ciberamenazas

Las organizaciones de transporte terrestre deben aplicar medidas de seguridad adecuadas y proporcionadas para proteger sus redes y sistemas de información, en particular, las tecnologías de la información y las tecnologías operativas, frente a los ciberataques. Entre las medidas de seguridad se incluyen:

- ***Políticas y procesos de seguridad:*** *definir, aplicar, comunicar y hacer cumplir políticas y procesos adecuados que definan un enfoque global para la seguridad de los sistemas y datos que apoyen las operaciones de las funciones esenciales en los modos de transporte terrestre. Estas políticas y procedimientos de seguridad (por ejemplo, las políticas de contraseña y almacenamiento) deben abarcar también los parches y la gestión de la vulnerabilidad de los sistemas de hardware y software (también las tecnologías de la información y las tecnologías operativas), la gestión de incidentes, así como la protección de los sistemas y de las redes.*

- ***Gestión de la identidad y del acceso:*** *comprender, documentar y gestionar el acceso a las redes y los sistemas de información (en particular, las tecnologías de la información y las tecnologías operativas) que apoyan el funcionamiento de las funciones esenciales en los modos de transporte terrestre. Los usuarios (o funciones automatizadas) que pueden acceder a los datos o sistemas están debidamente verificados, autenticados y autorizados. Esto también debe tener en cuenta las diferentes funciones y responsabilidades de las cuentas normales y privilegiadas.*

- ***Seguridad de los datos y sistemas:*** *proteger los datos (almacenados y transmitidos electrónicamente), las redes críticas y los sistemas de información (incluidas las tecnologías de la información y las tecnologías operativas) de los ciberataques. Teniendo en cuenta un enfoque basado en el riesgo, las organizaciones deben aplicar medidas de seguridad para limitar de manera efectiva las oportunidades de que los atacantes pongan en peligro los datos, las redes y los sistemas. Estas medidas de seguridad también deben incluir la adopción de protocolos de cifrado y de comunicación segura con el fin de proteger la información en reposo y en tránsito de las ciberamenazas resultantes de ataques de repetición. Además, es necesario combinar estas medidas con medidas de seguridad física para proteger el acceso a los sistemas (por ejemplo, los sistemas deben estar ubicados en espacios confinados con acceso restringido). Esto es muy importante para los sistemas que pueden tener un impacto en la seguridad de la vida humana.*

- ***Resiliencia de las redes y los sistemas:*** *aumentar la resiliencia de las redes y los sistemas (también las tecnologías de la información y las tecnologías operativas) mediante su diseño y aplicación (y el de sus procedimientos operativos) con el fin de resistir y mitigar la repercusión de los ciberataques. Algunos ejemplos de soluciones de diseño y aplicación que refuerzan la resiliencia son: funciones esenciales verificadas formalmente, redundancia de sistemas y redes, segregación de redes (en particular, segregación de las tecnologías de la información y las tecnologías operativas), medidas de seguridad multinivel y muchas otras. Obsérvese que, desde el punto de vista de la seguridad de la información, los ámbitos de seguridad que aplican la segregación de redes y sistemas pueden ofrecer soluciones de seguridad adecuadas. Sin embargo, las necesidades operativas (por ejemplo, actividades de mantenimiento, transferencia de datos, etc.) de los sistemas pueden requerir la derivación o conexión de diferentes ámbitos de seguridad (por ejemplo, sistemas y redes segregados), incluida la conexión de las tecnologías de la información y las tecnologías operativas.*

Comisión Europea

Detección de las ciberamenazas

Las organizaciones deben garantizar que las medidas de seguridad sigan siendo eficaces y detectar cualquier incidente de ciberseguridad que afecte o pueda afectar a los controles de seguridad, así como a los servicios y sistemas esenciales. A fin de detectar las ciberamenazas, las medidas de seguridad pertinentes son las siguientes:

- ***Supervisión de la seguridad:*** *supervisar el estado de seguridad de las redes y los sistemas de información, también las tecnologías de la información y las tecnologías operativas, que apoyan el funcionamiento de las funciones esenciales en los modos de transporte terrestre. Esto es necesario para detectar posibles amenazas a la seguridad y hacer un seguimiento de la eficacia permanente de las medidas de protección de la seguridad. Para apoyar la supervisión de la seguridad, los datos que se tienen en cuenta son, por ejemplo:*

  - *registros de seguridad*
  - *registros de detección de virus*
  - *registros de detección de intrusiones*
  - *registros de identificación, autenticación y autorización*
  - *registros de sistemas y servicios*
  - *registros de tráfico de la red*
  - *registros de tratamiento de datos*

- ***Descubrimiento de incidentes de seguridad:*** *detectar actividades malintencionadas (es decir, incidentes de seguridad) que afecten o puedan afectar a la seguridad de las redes y los sistemas de información (en particular, las tecnologías de la información y las tecnologías operativas) que apoyan el funcionamiento de las funciones esenciales.*

  Estas medidas pueden requerir la adopción de tecnologías específicas (por ejemplo, gestión de información e incidentes en materia de seguridad, sistema de detección de intrusiones, sistema de prevención de intrusiones, etc.) y la creación de un centro de operaciones de seguridad o equivalente. Es decir, desarrollar medios para detectar, analizar, responder y recuperarse de los ciberataques a escala local.
  Los equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT), los CERT sectoriales y comerciales o los operadores de infraestructuras viarias y ferroviarias, y el Centro europeo de puesta en común y análisis de la información ferroviaria (ER-ISAC) pueden proporcionar inteligencia sobre amenazas que sirva de base para las tareas de seguimiento y descubrimiento en el ámbito de la seguridad.

Comisión Europea

Planificación de la respuesta y de la recuperación

Las organizaciones deben definir, aplicar y probar procedimientos de gestión de incidentes que tengan por objeto garantizar la continuidad de las actividades de los servicios y sistemas en caso de incidentes de ciberseguridad.

La planificación de la respuesta y de la recuperación debe tener en cuenta las medidas de seguridad, que limiten el efecto de ataques específicos de ciberseguridad, tales como:

- *Coordinación y colaboración con los CSIRT nacionales, los CERT (públicos y comerciales) y los ISAC durante los incidentes de ciberseguridad, la coordinación de incidentes y las crisis a escala paneuropea*

- *Intercambio de información con otras organizaciones, en particular, los proveedores de la cadena de suministro de servicios de transporte terrestre*

- *Realización de **ejercicios periódicos de ciberataque** (coordinación técnica, así como de simulaciones teóricas) para evaluar las medidas y los procedimientos de seguridad, así como la resiliencia de la organización para hacer frente a incidentes de ciberseguridad*

- *Acceso a lugares de almacenamiento en archivo permanente o de respaldo en caso de que la integridad y disponibilidad del almacenamiento de datos se encuentre en peligro*

- ***Manuales de estrategia en materia de seguridad** con procedimientos detallados para gestionar los incidentes de ciberseguridad y devolver los servicios y sistemas a las condiciones operativas normales*

- *Reorientar el tráfico de la red a servicios redundantes durante los ataques de denegación de servicio*

- *Procedimientos manuales para operar con servicios y sistemas en modos de funcionamiento degradados*

- *Definir procedimientos para hacer frente a las violaciones de la seguridad de los datos, en particular, los procedimientos para tratar las violaciones de la seguridad de los datos que afecten a datos personales de conformidad con el Reglamento General de Protección de Datos (RGPD) y cualquier otro reglamento o directiva sectorial pertinente*

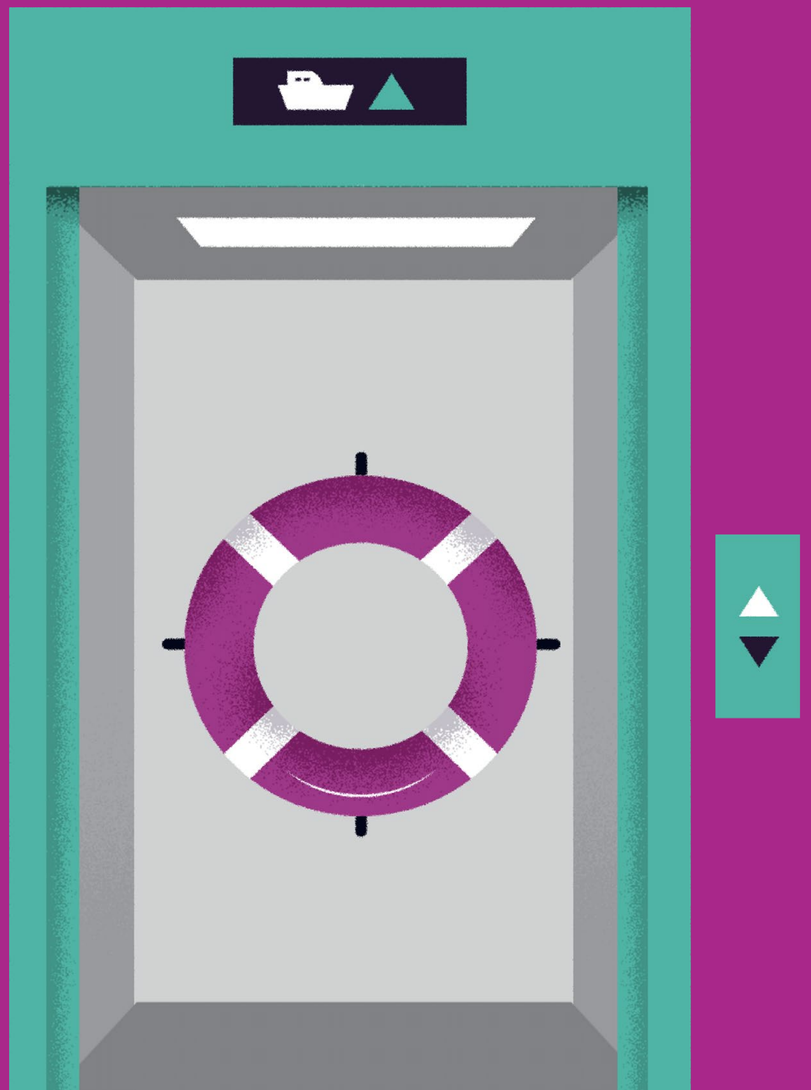
- *Adquirir **seguros cibernéticos** para compensar parcialmente el riesgo asociado a los incidentes de ciberseguridad graves*

- *Contratar un servicio de respuesta a incidentes con una o más empresas especializadas para obtener más capacidad y conocimientos especializados*

- *Definir procedimientos para compartir información sobre incidentes de ciberseguridad con las partes interesadas pertinentes, en especial, los procedimientos de notificación de incidentes de conformidad con la Directiva SRI (Directiva 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión).*

Comisión Europea

Buenas prácticas y medidas de seguridad adaptadas al transporte marítimo



Gobernanza

Las organizaciones de transporte marítimo necesitan una comprensión clara de las amenazas emergentes a fin de definir políticas y procesos de gestión que rijan sus enfoques con el fin de mejorar la ciberseguridad de los servicios y sistemas en las operaciones, en particular, las tecnologías de la información y las tecnologías operativas.

Las buenas prácticas para organizaciones de cualquier tamaño implican:

- *Garantizar que los altos directivos informen sobre las preocupaciones en materia de ciberseguridad a los ejecutivos y los consejos, que pueden tomar decisiones con conocimiento de causa sobre la asignación de recursos*

- *Designar un cargo de alto nivel con responsabilidades generales de gestión para la seguridad de las tecnologías de la información y las tecnologías operativas. Este cargo debe rendir cuentas de la ciberseguridad y la seguridad física*

- *Definir claramente las funciones, responsabilidades, competencias y autorizaciones relacionadas con la ciberseguridad, definir los niveles de autoridad y las líneas de comunicación entre el personal de tierra y de a bordo y entre ellos, y acordarlos con el personal pertinente. Esto es necesario, en particular, para los miembros de los equipos de respuesta a emergencias informáticas (CERT). El personal con funciones relacionadas con la legislación de la UE en materia de protección y seguridad marítimas, como los oficiales de protección de las instalaciones portuarias, los oficiales de protección portuaria, los oficiales de protección de las empresas o la persona designada en tierra y el capitán a bordo, debe estar familiarizado, como mínimo, con las medidas de ciberseguridad adoptadas por la organización*

- *Garantizar la gobernanza de la ciberseguridad a lo largo de toda la cadena de prestación de servicios de seguridad, incluidas las interfaces físicas y digitales, desde los fabricantes e instaladores de tecnología hasta los proveedores de seguridad*

- *Acordar actividades y controles, en particular, las responsabilidades compartidas, para gestionar los riesgos de ciberseguridad, y garantizar que estas responsabilidades se mantengan a lo largo de toda la vida útil (por ejemplo, mediante acuerdos de servicios) de las soluciones y servicios de seguridad*

- *Definir mecanismos de gobernanza (por ejemplo, políticas) para cumplir las obligaciones derivadas de los reglamentos y las directivas pertinentes, por ejemplo, el Reglamento 2019/1239 por el que se crea un entorno europeo de ventanilla única marítima (EMSWe), el Reglamento 725/2004 relativo a la mejora de la protección de los buques y las instalaciones portuarias, la Directiva 2005/65/CE sobre mejora de la protección portuaria y el Reglamento (CE) n.º 336/2006 sobre la aplicación del Código internacional de gestión de la seguridad (CGS), y la Resolución A.741 (18) por la que se aprueba el Código internacional de gestión de la seguridad operacional del buque y la prevención de la contaminación. En este contexto, también es pertinente mencionar el entorno común de intercambio de información (CISE), una iniciativa de la UE destinada a hacer interoperables los sistemas de vigilancia europeos y de los Estados miembros para que todas las autoridades afectadas tengan acceso a la información clasificada y no clasificada que necesitan para llevar a cabo misiones en el mar.*

Ejemplos de servicios y sistemas en el transporte marítimo: Ejemplos de tecnologías de la información son aquellas a las que tienen acceso los empleados (por ejemplo, ordenadores personales, teléfonos móviles, periféricos de oficina, etc.), así como los pasajeros (por ejemplo, encaminadores y conexiones wifi públicos, etc.). Ejemplos de tecnologías operativas son los Sistemas de Supervisión para el Control y la Obtención de Datos (SCADA), los sistemas de calefacción, ventilación y aire acondicionado (HVAC), los sistemas de posicionamiento global (GPS), el control de acceso, el seguimiento, la vigilancia, la respuesta a las alarmas y la tecnología de control, los sistemas de navegación a bordo, SafeSeaNet, los sistemas del puente, los sistemas de manipulación y gestión de la carga, los sistemas de gestión y control de la potencia de la propulsión y la maquinaria, los sistemas de control de acceso, los sistemas de servicio y gestión de pasajeros, las redes públicas disponibles para los pasajeros, los sistemas administrativos y de bienestar de la tripulación, los sistemas de comunicación, etc.

Determinación de las ciberamenazas

Gestión de riesgos: Las organizaciones marítimas deben adoptar las medidas adecuadas para determinar, analizar, evaluar y comunicar los riesgos de ciberseguridad, y aceptarlos, evitarlos, transferirlos o reducirlos a un nivel aceptable. Esto requiere un enfoque organizativo global de la gestión de riesgos, que incluya:

- *Garantizar una visión general clara de los distintos sistemas de hardware y software desplegados para la prestación de diferentes servicios. En el contexto del transporte marítimo, estos sistemas incluyen las tecnologías de la información y las tecnologías operativas, y cómo estos sistemas conectan e integran el lado terrestre, incluidas las autoridades públicas, las terminales marítimas y los estibadores*

- *Determinar y evaluar las principales operaciones a bordo de buques, que son vulnerables a los ciberataques, y realizar evaluaciones de riesgos en materia de ciberseguridad (también la evaluación de los posibles efectos operativos y la probabilidad de que ocurran), que deben tener en cuenta las amenazas emergentes, las vulnerabilidades conocidas y los datos operativos en relación con los sistemas en el ámbito de aplicación. Si procede, establecer un vínculo con las evaluaciones de protección realizadas para los buques, las instalaciones portuarias y los puertos, tal como establece la legislación de la UE en materia de protección marítima. En ellos se determinan las posibles amenazas para la protección de las infraestructuras portuarias y las deficiencias en materia de protección. Además, organizaciones marítimas como la Organización Marítima Internacional (OMI) y las ISAC marítimas pueden proporcionar información sobre las amenazas que afectan al transporte marítimo.*

- *Garantizar que las evaluaciones de riesgos también cubran los riesgos relacionados con las actividades cotidianas del personal (por ejemplo, el uso de las redes sociales, el uso de dispositivos personales, el tratamiento de datos, el intercambio de información, etc.)*

- *Determinar y aplicar medidas y planes de tratamiento de riesgos para mitigar los riesgos de ciberseguridad. Por ejemplo, aplicar un Sistema Global de Gestión de la Seguridad de la Información y un Sistema de Gestión de la Información Privada armonizados con otros sistemas de gestión como los sistemas de gestión de la seguridad (SGS), de conformidad con el Código internacional de gestión de la seguridad (CGS). Estos sistemas de gestión (es decir, el SGSI y el SGIP) implican la aplicación de controles de seguridad (así como de protección de datos y privacidad) con el fin de mitigar y prevenir las amenazas emergentes que afectan a la seguridad de los servicios y sistemas marítimos (en particular, sus datos)*

- *Tener en cuenta cualquier limitación relacionada con* ***la gestión de activos y la planificación de recursos*** *(es decir, las limitaciones que pueden afectar a la entrega, el mantenimiento y el apoyo de sistemas críticos para el funcionamiento de las funciones esenciales en el transporte marítimo). En cuanto a las evaluaciones, hágase referencia, cuando proceda, a los requisitos del Código CGS, los sistemas de gestión de la seguridad (SGS) y los planes de protección realizados de conformidad con la legislación de la UE en materia de seguridad y protección marítima.*

Ejemplos de marcos de gestión de riesgos: Diferentes marcos (por ejemplo, el Código CGS o normas de la familia ISO/IEC 27000, el marco de ciberseguridad del NIST, el marco MITRE ATT&CK, la norma BSI IT-Grundschutz, etc.) pueden servir de base y sustentar un enfoque de gestión de riesgos adaptado para el transporte marítimo. El marco de ciberseguridad del NIST también se ha adaptado para abordar la ciberseguridad de la transferencia marítima de líquidos a granel, las operaciones mar adentro y las operaciones de buques de pasaje. Del mismo modo, la Conferencia Marítima Internacional y del Báltico (CMIB) ha publicado el documento «The Guidelines on Cyber Security Onboard Ships» [«Directrices sobre ciberseguridad a bordo de los buques», documento en inglés] y la Organización Marítima Internacional (OMI) ha publicado el documento «Directrices sobre la gestión de los riesgos cibernéticos marítimos» (MSC-FAL.1/Circ.3). La ENISA ha llevado a cabo varios estudios relacionados con las buenas prácticas en materia de ciberseguridad marítima, en particular, la ciberseguridad portuaria. La AESM presta servicios a la comunidad marítima, entre ellos cursos de sensibilización en materia de ciberseguridad. Determinadas normas (por ejemplo, IEC 61162-460:2018 sobre protección y seguridad de los materiales y sistemas de navegación y radiocomunicación marítimos, ISO 16425:2013 sobre buques y tecnología marina, IEC 62443-4-1:2018 sobre seguridad de los sistemas de automatización y control industrial, etc.) definen también requisitos específicos de protección y seguridad para los sistemas y redes de transporte marítimo.

Protección contra las ciberamenazas

Las organizaciones de transporte marítimo deben aplicar medidas de seguridad adecuadas y proporcionadas para proteger sus redes y sistemas de información, en particular, las tecnologías de la información y las tecnologías operativas. Entre las medidas de seguridad se incluyen:

- ***Políticas y procesos de seguridad:*** *definir, aplicar, comunicar y hacer cumplir políticas y procesos adecuados que definan un enfoque global para la seguridad de los sistemas y datos que apoyen las operaciones de las funciones esenciales en el transporte marítimo. Las medidas de seguridad (en particular, las medidas de seguridad cibernética y física) deben incluirse en los planes pertinentes, como el sistema de gestión de la seguridad (SGS) y el plan de protección del buque. Estas políticas y procedimientos de seguridad (por ejemplo, las políticas de contraseña y almacenamiento) deben abarcar también los parches y la gestión de la vulnerabilidad de los sistemas de hardware y software (también las tecnologías de la información y las tecnologías operativas), la gestión de incidentes, así como la protección de los sistemas y de las redes.*

- ***Gestión de la identidad y del acceso:*** *comprender, documentar y gestionar el acceso a las redes y los sistemas de información (en particular, las tecnologías de la información y las tecnologías operativas) que apoyan el funcionamiento de las funciones esenciales en el transporte marítimo. Los usuarios (o funciones automatizadas) que pueden acceder a los datos o sistemas están debidamente verificados, autenticados y autorizados. Esto también debe tener en cuenta las diferentes funciones y responsabilidades de las cuentas normales y privilegiadas.*

- ***Seguridad de los datos y sistemas:*** *proteger los datos (almacenados y transmitidos electrónicamente), las redes críticas y los sistemas de información (incluidas las tecnologías de la información y las tecnologías operativas) de los ciberataques. Teniendo en cuenta un enfoque basado en el riesgo, las organizaciones deben aplicar medidas de seguridad para limitar de manera efectiva las oportunidades de que los atacantes pongan en peligro los datos, las redes y los sistemas. Estas medidas de seguridad también deben incluir la adopción de protocolos de cifrado y de comunicación segura con el fin de proteger la información en reposo y en tránsito de las ciberamenazas resultantes de ataques de repetición. Además, es necesario combinar estas medidas con medidas de seguridad física para proteger el acceso a los sistemas (por ejemplo, los sistemas deben estar ubicados en espacios confinados con acceso restringido). Esto es muy importante para los sistemas que pueden repercutir en la seguridad de la vida humana (por ejemplo, los sistemas de navegación y radiocomunicación de las categorías II y III).*

- ***Resiliencia de las redes y los sistemas:*** *aumentar la resiliencia de las redes y los sistemas (también las tecnologías de la información y las tecnologías operativas) mediante su diseño y aplicación (y el de sus procedimientos operativos) con el fin de resistir y mitigar la repercusión de los ciberataques. Algunos ejemplos de soluciones de diseño y aplicación que refuerzan la resiliencia son: funciones esenciales verificadas formalmente, redundancia de sistemas y redes, segregación de redes (en particular, segregación de las tecnologías de la información y las tecnologías operativas), medidas de seguridad multinivel y muchas otras. Obsérvese que, desde el punto de vista de la seguridad de la información, los ámbitos de seguridad que aplican la segregación de redes y sistemas pueden ofrecer soluciones de seguridad adecuadas. Sin embargo, las necesidades (por ejemplo, actividades de mantenimiento, transferencias de datos, etc.) de los sistemas (por ejemplo, Maritime Autonomous Surface Ships – MASS) pueden requerir la derivación o conexión de diferentes ámbitos de seguridad (por ejemplo, sistemas y redes segregados), en particular, la conexión de las tecnologías de la información y las tecnologías operativas.*

Detección de las ciberamenazas

Las organizaciones deben garantizar que las medidas de seguridad sigan siendo eficaces y detectar cualquier incidente de ciberseguridad que afecte o pueda afectar a los controles de seguridad, así como a los servicios y sistemas esenciales. A fin de detectar las ciberamenazas, las medidas de seguridad pertinentes son las siguientes:

- ***Supervisión de la seguridad:*** *supervisar el estado de seguridad de las redes y los sistemas de información, también las tecnologías de la información y las tecnologías operativas, que apoyan el funcionamiento de las funciones esenciales en los servicios de transporte marítimo. Esto es necesario para detectar posibles amenazas a la seguridad y hacer un seguimiento de la eficacia permanente de las medidas de protección de la seguridad. Para apoyar la supervisión de la seguridad, los datos que se tienen en cuenta son, por ejemplo:*

  - *registros de seguridad*
  - *registros de detección de virus*
  - *registros de detección de intrusiones*
  - *registros de identificación, autenticación y autorización*
  - *registros de sistemas y servicios*
  - *registros de tráfico de la red*
  - *registros de tratamiento de datos*

- ***Descubrimiento de incidentes de seguridad:*** *detectar actividades malintencionadas (es decir, incidentes de seguridad) que afecten o puedan afectar a la seguridad de las redes y los sistemas de información (en particular, las tecnologías de la información y las tecnologías operativas) que apoyan el funcionamiento de las funciones esenciales en los servicios de transporte marítimo.*

Estas medidas pueden requerir la adopción de tecnologías específicas (por ejemplo, gestión de información e incidentes en materia de seguridad, sistema de detección de intrusiones, sistema de prevención de intrusiones, etc.) y la creación de un centro de operaciones de seguridad o equivalente. Es decir, desarrollar medios para detectar, analizar, responder y recuperarse de los ciberataques a escala local.

Los equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT), los CERT sectoriales y los CERT comerciales de los operadores marítimos y los ISAC marítimos pueden proporcionar inteligencia sobre amenazas que sirva de base para las tareas de seguimiento y descubrimiento en el ámbito de la seguridad.

Comisión Europea

Planificación de la respuesta y de la recuperación

Las organizaciones deben definir, aplicar y probar procedimientos de gestión de incidentes que tengan por objeto garantizar la continuidad de las actividades de los servicios y sistemas en caso de incidentes de ciberseguridad.
La planificación de la respuesta y de la recuperación debe tener en cuenta medidas de seguridad, que limiten el efecto de ataques específicos de ciberseguridad, tales como:

- *Reorientar el tráfico de la red a servicios redundantes durante los ataques de denegación de servicio*

- *Definir procedimientos manuales para operar con servicios y sistemas en modos de funcionamiento degradados*

- *Establecer programas de ejercicios y prácticas (por ejemplo, ejercicios de coordinación técnica, de simulaciones teóricas y de respuesta) para responder a los ciberataques y las situaciones de emergencia, así como para evaluar las medidas de seguridad, los procedimientos y la resiliencia organizativa para hacer frente a incidentes de ciberseguridad*

- *Tener acceso a lugares de almacenamiento en archivo permanente o de respaldo en caso de que la integridad y disponibilidad del almacenamiento de datos se encuentre en peligro*

- *Establecer líneas de coordinación y colaboración con los CSIRT nacionales, los CERT (públicos y comerciales) y los ISAC durante los incidentes de ciberseguridad, la coordinación de incidentes y las crisis a escala paneuropea*

- *Intercambiar información con otras organizaciones, en particular, los proveedores de la cadena de suministro de servicios en el transporte marítimo*

- *Establecer manuales de estrategia en materia de seguridad con procedimientos detallados para gestionar los incidentes de ciberseguridad y devolver los servicios y sistemas a las condiciones operativas normales*

- *Definir procedimientos para hacer frente a las violaciones de la seguridad de los datos, en particular, los procedimientos para tratar las violaciones de la seguridad de los datos que afecten a datos personales de conformidad con el Reglamento General de Protección de Datos (RGPD) y cualquier otro reglamento o directiva sectorial pertinente*

- *Adquirir seguros cibernéticos para compensar parcialmente el riesgo asociado a incidentes de ciberseguridad graves*

- *Contratar un servicio de respuesta a incidentes con una o más empresas especializadas para obtener más capacidad y conocimientos especializados*

- *Definir procedimientos para compartir información sobre incidentes de ciberseguridad (en particular, casos de incumplimientos, accidentes y situaciones peligrosas) con las partes interesadas pertinentes, también los procedimientos de notificación de incidentes de conformidad con la Directiva SRI (Directiva 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión).*

La información y las opiniones expresadas en el presente informe son las del autor o autores y no reflejan necesariamente la posición oficial de la Comisión. La Comisión no garantiza la exactitud de los datos que figuran en el presente informe. Ni la Comisión ni ninguna persona que actúe en su nombre podrán ser consideradas responsables del uso que pudiera hacerse de la información que contiene.

Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2021

© Unión Europea, 2021
Reutilización autorizada, con indicación de la fuente bibliográfica y sin deformar, en ningún caso, el contenido o significado original de este documento. La Comisión Europea no es responsable de las consecuencias que pudieran derivarse de la reutilización de esta publicación. La política de reutilización de los documentos de la Comisión Europea se rige por la Decisión 2011/833/UE de la Comisión, de 12 de diciembre de 2011, relativa a la reutilización de los documentos de la Comisión (DO L 330 de 14.12.2011, p. 39).

Para cualquier uso o reproducción de elementos que no sean propiedad de la Unión Europea, podrá ser necesario solicitar la autorización directamente de los respectivos titulares de derechos.

Print	ISBN 978-92-76-40465-1	doi:10.2832/551586	MI-05-21-230-ES-C
PDF	ISBN 978-92-76-40482-8	doi:10.2832/371294	MI-05-21-230-ES-N

Oficina de Publicaciones
de la Unión Europea