Ciberseguridad en la automatización a bordo a través de sistemas digitales integrados en redes internas y externas

LUIS ENRIQUE SÁNCHEZ CRESPO
JOSÉ RAMÓN ALVAREZ
GRUPO COMISMAR

Las amenazas de ciberseguridad, no son un problema puntual o temporal que vaya a desaparecer, sino que es un factor continuo, que se irá incrementando y con el que las compañías tienen que aprender a convivir.

Por todo ello las compañías, desde su nivel superior, deben tomar conciencia de este nuevo riesgo para la explotación de sus buques y situar la ciberseguridad en su agenda de forma prioritaria.

1. ¿POR QUÉ NECESITAMOS GESTIONAR LA CIBERSEGURIDAD DE NUESTROS BARCOS?

La información se ha convertido en un activo crítico en todo tipo de organizaciones y el sector marítimo no es una excepción. La protección frente a posibles ciberamenazas que pudiesen sufrir los buques es en la actualidad imprescindible en un entorno donde la información es muy vulnerable frente a ataques premeditados.

Un caso claro de esto se pudo vivir en el año 2017, cuando el virus Petya (*malware* de tipo *ransomware*) afectó a la naviera Maersk al causar congestión en casi 80 puertos, con un coste estimado de 255 millones de euros, además del daño reputacional, siendo este solo un ejemplo más de lo que hoy está pasando en un sector cada vez más vulnerable.

Para conseguir frenar este y otros casos, es importante que la gestión de los ciberriesgos y la ciberseguridad sea específica para cada compañía y cada buque, aunque tomando como referencia varias guías ya elaboradas para el sector entre las que se pueden destacar las siguientes

- MSC.428(98): Gestión de Riesgos Cibernéticos en SGS.
- MSC-FAL 1/Circ.3: Orientaciones en la Gestión de Riesgos Cibernéticos
- The Guidelines on Cybersecurity on board ships V.3.0. ICS/ BIMCO/ OCIMF/ CLIA/ INTERCARGO/ INTERTANKO.

También podrían servir de referencia la ISO 27001:1 de Sistemas de Gestión de Seguridad de la Información, así como el Esquema Nacional de Seguridad, o incluso las normativas que se están aplicando en sectores como las Infraestructuras Criticas.

En un contexto tan complejo y con un riesgo creciente, es necesario que las compañías marítimas aceleren y prioricen la gestión de la ciberseguridad con el objetivo de asegurar el cumplimiento de la legislación aplicable y la continuidad del negocio, demostrando:

- Que sus activos vinculados a la información han sido adecuadamente identificados, valorados y catalogados. Es decir, que la compañía es consciente de cuáles son sus activos de valor y que dimensiones de estos activos (confidencialidad, integridad, disponibilidad) pueden ser objeto de ataques.
- Que conocen las amenazas que pueden afectar a estos activos, y son conscientes de su probabilidad de ocurrencia y el potencial impacto que tendrían.
- Y finalmente que han implementado los controles necesarios para evitar que esas amenazas puedan aprovechar una vulnerabilidad en esos controles para impactar en sus activos de valor.

Es decir, que son conscientes de sus ries-

gos, lo que permitirá establecer un plan de acciones correctivas y preventivas que sean implantadas, auditadas y revisadas, al objeto de asegurar su eficacia para minimizar los riesgos detectados; todo ello dentro de un sistema de gestión en el ámbito de la seguridad (*safety* - Código ISM) y de la protección (*security* - Código ISPS).

2. ¿ES NECESARIO EFECTUAR UNA EVALUACIÓN DE RIESGOS?

En COMISMAR consideramos que no se puede llevar a cabo adecuadamente una gestión de los riesgos sin una evaluación previa de los mismos, y sin haber identificado los activos de valor. Esta evaluación puede tener aspectos comunes para todos los buques de una compañía, pero luego se debe particularizar en cada caso.

En una primera fase es necesario elaborar un catálogo de activos que permita identificar cuáles son los activos críticos y su *«valor»*.

Posteriormente, se calcula su vulnerabilidad ante las amenazas, factor que puede depender de varios factores entre los que podemos destacar:

- Cultura de la seguridad en el personal de la compañía y en la tripulación.
- Responsabilidades definidas para los sistemas de Tecnologías de la Información (IT) y Tecnologías de Operación (OT).
- Niveles de automatización e integración de sistemas digitalizados a bordo.
- Ubicación de los sistemas como sistema autónomo, conectado a Internet, en una red controlada o en una red no controlada.
- Interfaces y comunicaciones del buque con Compañía, Fletadores, Cargadores, Receptores, Transitarios, Terminales, Agencia de Reclutamiento, SS.CC., Aseguradores, Agencias de Vetting, etc.
- Controles existentes y su nivel de implementación.
- Disponibilidad de medidas y sistemas de seguridad que depende de tecnologías de información y control.

El objetivo de la evaluación de riesgos es establecer un punto de partida y una estrategia para la gestión de las ciberamenazas. Reducir el ciberriesgo a niveles aceptables debería ser el objetivo principal de la estrategia de ciberseguridad de la compañía.

3. ¿EL SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD DEBE ESTAR DOCUMENTADO?

De acuerdo con MSC.428(98) de 16 Junio 2017 (Gestión de Riesgos Cibernéticos en el Sistema de Gestión de Seguridad) se deben tener en cuenta y documentar esta gestión antes de la primera renovación del DOC (Documento de Cumplimiento del Código ISM) a partir del año 2021.

El objetivo de la evaluación de riesgos es establecer un punto de partida y una estrategia para la gestión de las ciberamenazas

Esto va a implicar la necesidad de elaborar realizar Instrucciones de Trabajo, Listas de Comprobación, Formatos y sus correspondientes Registros, para integrar bien en el SGS (Sistema de Gestión de la Seguridad - Código ISM) y/o en el PPB (Código ISPS).

Los planes y procedimientos de la compañía para la gestión de los ciberriesgos deberían ser complementarios y estar alineados con los existentes para la gestión de la seguridad/protección, requeridos por los códigos ISPS e ISM.

Los controles procedimentales mencionados en la guía de BIMCO/ICS, se refieren a los planes y procedimientos para el uso de los sistemas de a bordo por la tripulación. Algunos ejemplos mencionados son:

- Formación y concienciación.
- Mantenimiento de software y actualizaciones.
- Actualizaciones de antivirus y herramientas *anti-malware*.
- Uso de privilegios de administrador.
- Control de medios físicos removibles.
- Desinstalación de equipos, programas y aplicaciones; incluyendo la destrucción de datos.
- Servicio técnico de personal de tierra y planes de contingencia.

Estos procedimientos deberían ampliar su alcance a la oficina ya que desde allí se gestiona también la información del buque.

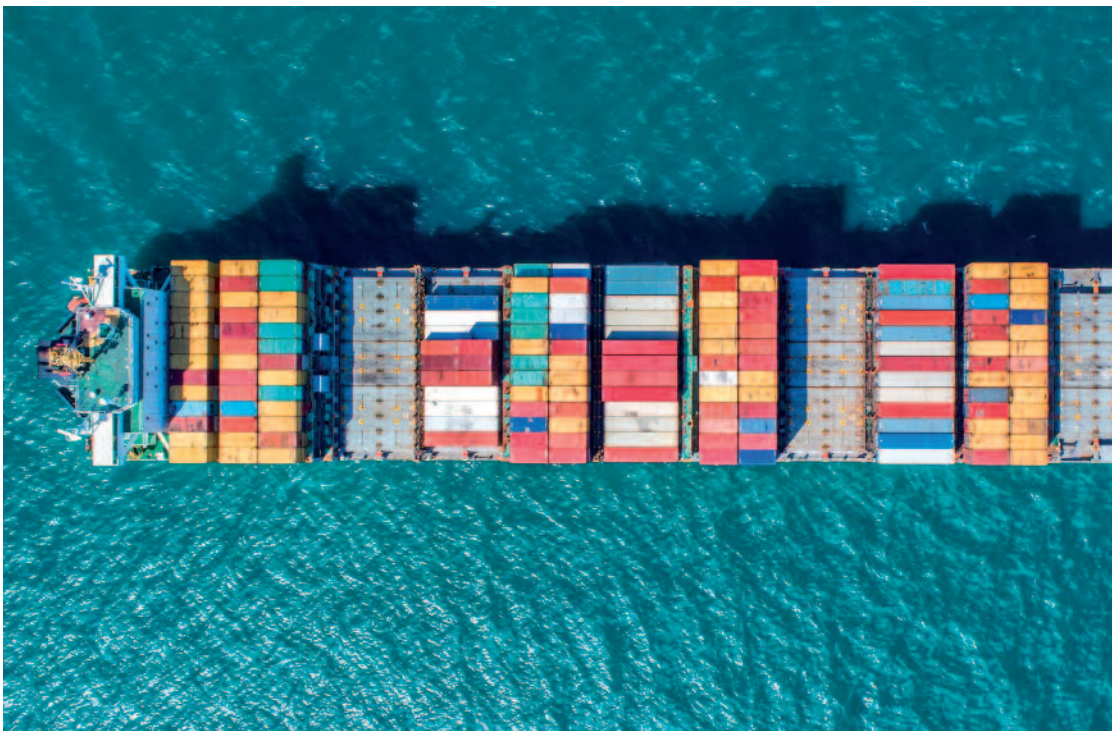
4. ¿SE DEBE DISPONER DE PLANES DE CONTINGENCIA FRENTE A CUALQUIER INCIDENTE?

Cuando las medidas preventivas no hayan sido suficientes para limitar los riesgos hasta un nivel aceptable, en COMISMAR recomendamos elaborar planes de respuesta para diferentes escenarios como por ejemplo:

- En caso de ataque que implique manipulación o parada de los sistemas de navegación del buque.
- En caso de ataque que implique manipulación o parada de los sistemas de control de propulsión, sistemas auxiliares u otros sistemas críticos.
- Para verificar la integridad de los datos en caso de sospecha de ataque.
- Para gestionar los incidentes de secuestro de datos o *ransomware*.
- Para casos en que en los buques se pierden datos de tierra.

Cuando se descubre un ciberincidente, es importante que todo el personal relevante sepa cómo actuar y el procedimiento que debe seguir. Para ello, es necesario que todos los años se realice una prueba parcial dentro del plan de contingencia que permita ir validando de forma progresiva el cumplimiento del plan.

Es crucial que los planes de contingencia y la información relacionada, estén disponibles a bordo en formato no electrónico ya que algunos ciber-incidentes pueden implicar la destrucción de datos y la parada de sistemas y enlaces de comunicación.



5. ¿CUÁLES SON LOS PRINCIPALES CONTROLES TECNOLÓGICOS PARA LA PROTECCIÓN DE SISTEMAS DIGITALIZADOS?

Los controles técnicos relevantes para la ciberseguridad, y que serían aplicables tanto a bordo como en oficina son los siguientes:

- Limitación y control de puertos de red, protocolos y servicios.
- Configuración de dispositivos de red como cortafuegos, enrutadores y conmutadores.
- Configuración segura de *hardware* y *software*.
- Protección de navegación web y correo electrónico.
- Comunicaciones por satélite y radio.
- Defensas contra el *malware*.
- Capacidad de recuperación de datos.
- Control de redes inalámbricas.
- Seguridad en las aplicaciones (gestión de parches).
- Diseño de red seguro.
- Seguridad física de la información. Zonas restringidas
- Defensas perimetrales. IPS e IDS.

6. ¿QUE SISTEMAS IT/OT SON LOS MÁS SENSIBLES A BORDO?

Al enfrentarnos a un ciberataque, debemos ser conscientes de cuáles son los principales activos dentro de los buques objeto del ataque. Los sistemas del buque que pueden ser comprometidos por un ciber-ataque incluyen:

- Sistemas de Control en el puente. (Sistema Integrado de Navegación, Sistema integrado de Control de Máquinas, Centralita C.I., Paneles de función puertas C.I., rampas y portas de acceso, puertas estancas, sistema de megafonía, etc.
- Equipos de navegación: ARPA, ECDIS, GNSS, AIS, VDR.
- Comunicaciones: GMDSS, Sat.com comerciales y de acceso al pasaje, etc.
- Gestión de la carga. Programas de cálculo de carga, estabilidad y esfuerzos estructurales, enlace con la terminal para programar *slots* de estiba, lista de MM.PP. y documentación de carga.
- Sistemas de control de propulsión, maquinaria y electricidad.
- Sistemas de control de accesos. CCTV, IDS, tarjetas acceso zonas restringidas.
- Sistemas de gestión del pasaje. Listas de pasajeros, tarjetas de embarque, tarjetas de acceso a camarotes, etc.
- Redes públicas para el pasaje. Acceso WI-FI.
- Sistemas administrativos. Programas de gestión y mantenimiento con la compañía.
- Redes y sistemas de entretenimiento de la tripulación y pasaje. Ordenadores, servidores, routers, antivirus, cortafuegos, etc.

7. ¿ESTÁ NUESTRA TRIPULACIÓN PREPARADA PARA PREVENIR Y ACTUAR ANTE CIBERATAQUES?

Los usuarios de las IT y OT que soportan la navegación y sistemas de control de los buques, deberían ser conscientes de los riesgos en ciber-seguridad y tener formación específica para su identificación y gestión.

Esta formación debe cubrir a todo el personal de la compañía en tierra (principalmente directores de flota, persona designada en tierra (PDT), oficial de la compañía para la protección del buque (OCPM), inspectores y técnicos informáticos) y a bordo (tripulaciones).

En COMISMAR estamos seguros de que se deben incluir en el programa de formación los aspectos relativos a la ciberseguridad, incidiendo en las medidas de protección e identificación de amenazas y los planes de contingencia para minimizar daños y restaurar sistemas.

8. ¿COMO AFECTA LA CIBERSEGURIDAD A LOS SISTEMAS DE AUTOMATIZACIÓN Y CONTROL?

En los buques en servicio hay muchos parámetros que tienen que estar controlados y monitorizados: temperaturas, presiones, niveles de tanques, así como el control del funcionamiento de motores principales, generadores y todo tipo de maquinaria auxiliar.

Es un objetivo constante en el diseño y construcción de buques mejorar la eficiencia y fiabilidad de los sistemas, reducir el número de personas a bordo y mejorar las condiciones de trabajo de los tripulantes (instalaciones más seguras, reduc-

ción de tiempos de trabajo, ahorro de costes de mantenimiento, mejorar la eficacia y limpieza de los sistemas, etc.).

Esto se lleva a cabo de manera cada vez más avanzada mediante sistemas automatizados que facilitan la monitorización y control de la mayoría de los sistemas y elementos del buque y favorecen el concepto de *«máquina desatendida»* y *«buque autónomo».*

Debido a la flexibilidad que supone conectar los dispositivos mediante redes de comunicación digital, es fácil integrarlos en redes de rango superior o incluso en internet, lo que supone un problema de seguridad en el acceso a los dispositivos y a la información de la redes internas y externas.

Cuando usuarios ajenos a la gestión del buque tienen acceso a redes desde el exterior, los problemas de seguridad se plantean en tres aspectos:

- La seguridad del perímetro: protección frente a ataques del exterior, generalmente utilizando cortafuegos (*firewalls*).
- La seguridad en el canal: protección de los datos frente a escuchas mediante criptografía.
- La seguridad de acceso, que contempla tres aspectos: la identificación del usuario, la autorización del acceso y la auditoría de las operaciones realizadas por el usuario.

El problema de seguridad puede aparecer también dentro del mismo buque, en su red interna, provocado bien por los propios tripulantes, o porque la barrera del cortafuegos ha sido insuficiente y se ha sufrido el ataque de un pirata informático. En este caso es importante el uso de técnicas como la segmentación de redes, mediante el uso de conmutadores con características de seguridad (VLANs, monitorización de puertos, etc); el uso de sistemas de monitorización del tráfico de red y la mejora de la seguridad de los servidores (adquisición y actualización de aplicaciones, antivirus, administración de cuentas de usuario, etc)

Los buques modernos actuales disponen de sistemas SCADA (*Supervisory Control and Data Acquisition* o Supervisión, Control y Adquisición de datos) como aplicación de *software* que se sitúa en un nivel de supervisión y explotación de los procesos. Como aplicación de control del funcionamiento de la maquinaria a bordo, se comunica con los sensores dispuestos en la misma y ofrece información al oficial, permitiéndole tomar decisiones sobre su régimen de funcionamiento; sirviendo por tanto, cómo elemento HMI (*Human Machine Interface*/Interfaz Hombre Máquina). Está diseñado para sustituir los paneles de control físicos repletos de mandos, luces e indicadores, por pantallas con gráficos y elementos interactivos a través de controles (cámara máquinas, control de carga y lastre, etc.) mediante ordenadores personales con sistema operativo Windows, aunque su uso se está extendiendo a dispositivos móviles, como tabletas y teléfonos móviles.

9. CONCLUSIONES Y RECOMENDACIONES

La gestión de la seguridad de la información tiene muchas similitudes con otros sistemas de gestión implantados actualmente a bordo, que pueden facilitar la implantación de estos estándares.

Inicialmente se debe efectuar un estudio completo de la situación de partida en oficina y a bordo, analizando las posibles amenazas y vulnerabilidades, evaluando los riesgos resultantes y estableciendo las medidas preventivas a tomar para minimizar su probabilidad e impacto.

La gestión debe basarse en el aumento de la resiliencia, es decir la resistencia de los sistemas a ser atacados y su respuesta y recuperación tras un incidente.

Se debe aplicar el ciclo de mejora continua PDCA (Planear >> Hacer >> Verificar >> Actuar >>) asegurando de esta manera la continua revisión y evolución en el tiempo y la adaptación a la gestión del cambio constante de maquinaria, equipos y sistemas a bordo. Con el ciclo PDCA conseguimos un reforzamiento constante y evolutivo a lo largo del tiempo de la seguridad, lo que se traduce en un aumento continuo de la resiliencia del sistema.

Las amenazas de ciber seguridad, no son un problema puntual o temporal que vaya a desaparecer, sino que es un factor continuo, que se irá incrementando y con el que las compañías tienen que aprender a convivir.

Por todo ello las compañías, desde su nivel superior, deben tomar conciencia de este nuevo riesgo para la explotación de sus buques y situar la ciberseguridad en su agenda de forma prioritaria.