S2 GRUPO
Anticipando un mundo ciberseguro

CASO DE ÉXITO

Sector Naval

Ciberseguridad para hacer frente a los **desafíos** presentes y futuros.

01

Breve presentación de la empresa

Nuestro cliente es un importante astillero nacional dedicado a la **construcción de barcos**.

Recibe importantes **encargos** para la construcción de barcos de todo tipo: pesqueros, de recreo, investigación, etc.

Ha recibido recientemente un encargo donde su cliente le pide que el barco en construcción cumpla con las recientes **exigencias** de ciberseguridad que exige la normativa internacional.

En el diseño y construcción del nuevo barco se deben de incorporar las medidas necesarias para cumplir con éxito con los requerimientos de ciberseguridad de la Organización Marítima Internacional **(OMI – IMO)** que serán certificados por una empresa acreditada una vez el buque esté construido.

02

Descripción de la problemática/reto

Estos requerimientos sobre la gestión de riesgos **cibernéticos** son de reciente aplicación y nuestro cliente no tiene **experiencia** sobre las implicaciones que estas exigencias tienen en el proceso de construcción del buque.

La resolución **MSC 428(98)** “Gestión de los riesgos cibernéticos marítimos en los sistemas de gestión de la seguridad” y la circular **MSC-FAL.1/Circ.3** “Directrices sobre la gestión de los riesgos cibernéticos marítimos” exigen que los responsables “adopten las medidas necesarias para salvaguardar el transporte marítimo de las amenazas y vulnerabilidad actuales y emergentes relacionadas con la digitalización, la integración y automatización de los procedimientos y sistemas del transporte marítimo

Para ello se han venido desarrollando diferentes metodologías por las empresas del sector dónde **se adoptan los criterios de la norma internacional IEC 62443 para el análisis de riesgos y la segmentación de las redes de comunicación de los barcos.**

Se trata de un ámbito dónde el astillero no tiene experiencia y requiere de nuestra asistencia especializada para incorporar las medidas que le permitan **cumplir estos requerimientos y superar la certificación final del barco.**

03

Descripción de la actuación realizada

Se realiza un servicio de **consultoría** con el acompañamiento durante todo el proceso de construcción para comprobar las características de **ciberseguridad** de los diferentes elementos e instalaciones del barco. Además de un análisis de las zonas y conductos de los diferentes sistemas y sus riesgos asociados. Por último se realizan unas **pruebas técnicas** de evaluación.

GRUPO
Anticipando un mundo ciberseguro

1

Se recopilan y comprueban las **características técnicas** de **ciberseguridad** de los diferentes componentes con la relación de proveedores contratados: sistemas de propulsión, comunicaciones, navegación, lastrado, estanqueidad, lastrado, generación de energía….

2

Se realiza un análisis de la interconexión de los diferentes sistemas y los riesgos asociados de acuerdo con el **estándar internacional IEC 62443**. Para garantizar un nivel general de seguridad **"Essential +"** se realiza una serie de recomendaciones que garanticen un nivel de protección adecuado.

3

En las últimas **etapas de construcción** del barco ya prácticamente terminado se desplaza al astillero un equipo disciplinar para la realización de una serie de **pruebas técnicas del nivel de seguridad de las redes de** comunicaciones del buque.

DNV-GL

CLASS PROGRAMME

Type approval

DNVGL-CP-0231 Edition January 2018

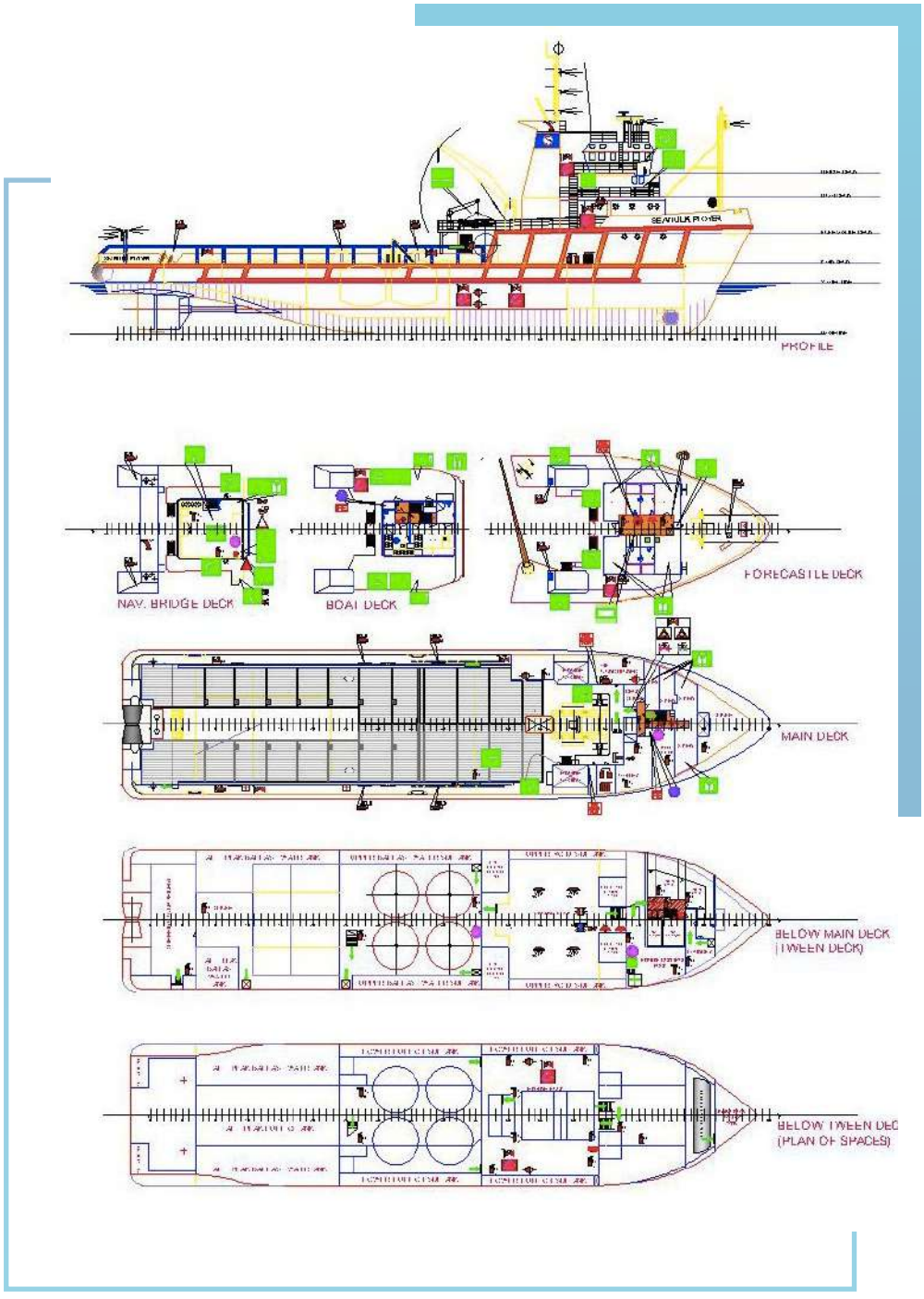
Cyber security capabilities of control system components

DNV GL AS

04

Beneficios obtenidos

Como resultado de las acciones realizadas el cliente obtiene una **serie de beneficios**:



El cliente tiene la seguridad de que cada uno de los diferentes componentes del proyecto **cumplen con las especificaciones mínimas de ciberseguridad que les son exigibles**. De este modo, se **evitan posibles sobrecostes** ocasionados por la instalación de sistemas de características inadecuadas.

Dispondrá de un **AA.RR. según la arquitectura de los diferentes sistemas de barco, su nivel de riesgo y sus interconexiones**. Pudiendo adoptar las medidas necesarias para garantizar el nivel de seguridad general requerido.

Dispone de un informe con el resultado de la evaluación de seguridad del barco terminado que garantiza el Security Level requerido y facilita la obtención de la **certificación correspondiente por una empresa acreditada.**

S2 GRUPO

Anticipando un mundo
ciberseguro

MADRID
Avda de Manoteras 46
BIS 6ºC
28050 Madrid
T (34) 902 882 992

BARCELONA
Llull, 321
08019 Barcelona
T (34) 933 030 060

VALENCIA CERT
Ramiro de Maeztu, 7
46022 Valencia
T (34) 963 110 300
F (34) 963 106 086

VALENCIA HQ
Doctor Juan Regla, 6
46010 Valencia
T (34) 960 010 105

SEVILLA
C/Gonzalo Jiménez de
Quesada 2, Planta 18
41092 Sevilla
T (34) 902 882 992

SAN SEBASTIAN
Juan Fermín Gilisagasti
nº 2 (Zuatzu)
Edificio Pi@ Oficina 121
Donostia 20018
T (34) 902 882 992

SANTIAGO DE CHILE
Calle Padre Mariano N° 82
of. 1102, Providencia,
T (56) 9 9440 4365

MÉXICO D.F.
Monte Athos 420
CDMX 11000
T (52) 55 5035 7868

BOGOTÁ
Carrera 14, nº 98-51,
Oficina 701
T (571) 745 74 39

BRUSELAS
Rue belliard,20.
1040
T (32) (0) 474 532 974

LISBOA
Avda do Brasil, nº1,
1749-008 Lisboa
T (351) 217 923 729

Síguenos en: • @s2grupo • s2grupo.es