



**PROGRAMA FORMATIVO DE LA ESPECIALIDAD FORMATIVA
ESPECIALISTA EN CIBERSEGURIDAD EN EL TRANSPORTE
MARITIMO
IFCT141PO**

PROGRAMAS DE FORMACIÓN DIRIGIDOS PRIORITARIAMENTE A TRABAJADORES OCUPADOS

Noviembre 2018

**PROGRAMA DE LA ESPECIALIDAD FORMATIVA:
ESPECIALISTA EN CIBERSEGURIDAD EN EL TRANSPORTE MARITIMO**

DATOS GENERALES DE LA ESPECIALIDAD FORMATIVA

1. Familia Profesional: INFORMÁTICA Y COMUNICACIONES

Área Profesional: SISTEMAS Y TELEMÁTICA

2. Denominación: ESPECIALISTA EN CIBERSEGURIDAD EN EL TRANSPORTE MARITIMO

3. Código: **IFCT141PO**

4. Objetivo General: Adquirir unas bases muy sólidas y actualizadas que permitan profundizar en conocimientos avanzados en Ciberseguridad, así como diseñar un plan de seguridad para un entorno de comunicaciones corporativo y activar sobre una red de comunicaciones los sistemas que permitan establecer los niveles de seguridad adecuados y fiables.

5. Número de participantes: Según normativa, el número máximo de participantes en modalidad presencial es de 30.

6. Duración:

Horas totales: 80

Modalidad: Presencial

Distribución de horas:

Presencial:..... 80

Teleformación:..... 0

7. Requisitos mínimos de espacios, instalaciones y equipamiento:

7.1 Espacio formativo:

AULA POLIVALENTE:

El aula contará con las instalaciones y equipos de trabajo suficientes para el desarrollo de la acción formativa.

- Superficie: El aula deberá contar con un mínimo de 2m² por alumno.
- Iluminación: luz natural y artificial que cumpla los niveles mínimos preceptivos.
- Ventilación: Climatización apropiada.
- Acondicionamiento eléctrico de acuerdo a las Normas Electrotécnicas de Baja Tensión y otras normas de aplicación.
- Aseos y servicios higiénicos sanitarios en número adecuado.
- Condiciones higiénicas, acústicas y de habitabilidad y seguridad, exigidas por la legislación vigente.
- Adaptabilidad: en el caso de que la formación se dirija a personas con discapacidad dispondrá de las adaptaciones y los ajustes razonables para asegurar la participación en condiciones de igualdad.
- PRL: cumple con los requisitos exigidos en materia de prevención de riesgos laborales

Cada espacio estará equipado con mobiliario docente adecuado al número de alumnos, así mismo constará de las instalaciones y equipos de trabajo suficientes para el desarrollo del curso.

7.2 Equipamientos:

Se contará con todos los medios y materiales necesarios para el correcto desarrollo formativo.

- Pizarra.
- Rotafolios.
- Material de aula.
- Medios audiovisuales.
- Mesa y silla para formador/a.
- Mesas y sillas para alumnos/as.
- Hardware y Software necesarios para la impartición de la formación.
- Conexión a Internet.

Se entregará a los participantes los manuales y el material didáctico necesarios para el adecuado desarrollo de la acción formativa

Las instalaciones y equipamientos deberán cumplir con la normativa industrial e higiénico sanitaria correspondiente y responderán a medidas de accesibilidad universal y seguridad de los participantes. En el caso de que la formación se dirija a personas con discapacidad se realizarán las adaptaciones y los ajustes razonables para asegurar su participación en condiciones de igualdad.

8. Requisitos necesarios para el ejercicio profesional:

(Este epígrafe sólo se cumplimentará si existen requisitos legales para el ejercicio de la profesión)

9. Requisitos oficiales de los centros:

(Este epígrafe sólo se cumplimentará si para la impartición de la formación existe algún requisito de homologación / autorización del centro por parte de otra administración competente.

10. CONTENIDOS FORMATIVOS:

1. ESTADO ACTUAL DE LA SEGURIDAD MARÍTIMA Y LA SEGURIDAD EN INSTALACIONES PORTUARIAS.
2. GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN
 - 2.1. Segregación eficaz y segura de las redes del buque.
 - 2.2. Gestión de la seguridad cibernética durante las escalas en puerto y en las comunicaciones con tierra.
3. PRINCIPIOS DE BUEN GOBIERNO DE LA INFORMACIÓN (POLÍTICAS, LEGISLACIÓN Y CUMPLIMIENTO).
 - 3.1. Elaboración de planes y procedimientos para la gestión de los riesgos cibernéticos e integración en el sistema de gestión de la compañía para cumplimiento del Código Internacional de Gestión de la Seguridad (Código ISM).
 - 3.2. Elaboración de planes y procedimientos para la gestión de los riesgos cibernéticos e integración en sistema de gestión de la compañía para cumplimiento del Código Internacional de Protección del Buque e Instalaciones Portuarias (Código ISPS).
4. CONTROLES DE GESTIÓN Y AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN.
 - 4.1. Identificación de los sistemas, equipos, datos y capacidades críticos (que pondrían en riesgo las operaciones y la seguridad del buque en caso de que se interrumpiese su funcionamiento).
 - 4.2. Definición de una estrategia específica de protección de los sistemas críticos del buque, función de su tipo, sistema de a bordo, áreas de navegación, tráfico, etc.
5. GESTIÓN DEL RESPONSABLE DE CIBERSEGURIDAD – PROYECTOS Y OPERACIONES.
 - 5.1. Formación, funciones y responsabilidades que deben conocer todos los miembros de la tripulación.
 - 5.2. Definición del personal clave. Formación complementaria.
 - 5.3. Oficial encargado de la ciberseguridad a bordo.
 - 5.4. Gestión, tanto en tierra como a bordo.
6. MEDIDAS TÉCNICAS DE SEGURIDAD DE LA INFORMACIÓN.
 - 6.1. Medidas técnicas para protegerse contra un incidente cibernético a bordo, asegurando la continuidad de las operaciones del buque.
 - 6.2. Medidas de protección relacionadas con los procedimientos del buque que proporcionen una capacidad de resistencia (resiliencia) contra incidentes cibernéticos.
 - 6.3. Planes de contingencia, ejercicios prácticos en diversos escenarios
 - 6.3.1. Pérdida de disponibilidad de equipos electrónicos de navegación o de la integridad de los datos relacionados con la navegación.
 - 6.3.2. Pérdida de disponibilidad o integridad de fuentes de datos externas, que incluya, pero no se limite al Sistema Global de Navegación por Satélite, GNSS.
 - 6.3.3. Pérdida de conectividad esencial con tierra, que incluya, pero no se limite, a la disponibilidad del Sistema Global de Comunicaciones, GMDSS.
 - 6.3.4. Pérdida de disponibilidad de sistemas de control, que incluya los medios de propulsión, auxiliares y otros equipos críticos, y la pérdida de integridad de la gestión y control de datos.
 - 6.3.5. Un ataque de ransomware (programa malicioso que encripta los datos de los sistemas hasta que el distribuidor descifra la información) o un incidente de denegación o servicio.
7. PLANIFICACIÓN Y GESTIÓN DE RECURSOS.