PROGRAMA FORMATIVO DE LA ESPECIALIDAD FORMATIVA

CONCIENCIACION EN CIBERSEGURIDAD EN EL TRANSPORTE MARITIMO

IFCT138PO

PROGRAMAS DE FORMACIÓN DIRIGIDOS PRIORITARIAMENTE A TRABAJADORES OCUPADOS

5 de abril de 2018

PROGRAMA DE LA ESPECIALIDAD FORMATIVA:

CONCIENCIACION 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: CONCIENCIACION EN CIBERSEGURIDAD EN EL TRANSPORTE MARITIMO

3. Código: **IFCT138PO**

4. Objetivo General: Identificar amenazas actuales a la Ciberseguridad que puedan materializarse en ataques, especialmente aquellas que tengan mayor incidencia en los sistemas de tecnologías de la información en el transporte marítimo, o de interconexión con infraestructuras portuarias, para poder aplicar las medidas, tanto técnicas como organizativas, que se pueden adoptar en el desarrollo de las operaciones de trabajo para asegurar los primeros niveles de seguridad.

5. Número de participantes: **-**

6. Duración:

Horas totales: 16 Modalidad: Presencial

Distribución de horas:

Presencial:..... 16

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 el equipamiento suficiente para el desarrollo de la acción formativa.
- Pizarra.
- Rotafolios.
- Material de aula.
- Medios audiovisuales.
- Mesa y silla para formador.
- Mesa y silla para alumnos.
- 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. INTRODUCCIÓN Y CONCEPTOS DE CIBERSEGURIDAD.
1.1. Las tecnologías de la información en el buque (Ship information Technology, IT).
1.2. Uso de tecnologías operacionales a bordo (Ship Operational Technology, OT).
2. TENDENCIAS EMERGENTES EN SEGURIDAD.
2.1. Ejemplos de casos recientes de ciberataques en sector marítimo y sus efectos.
3. ECUACIÓN DEL RIESGO: VULNERABILIDADES, AMENAZAS E IMPACTO.
3.1. Vulnerabilidades en la interfaz buque – tierra.
3.2. Sistemas del buque que dependen de la digitalización, integración y automatización
3.2.1. Sistemas de gestión de la carga, incluidas las mercancías peligrosas. Sistemas de control de lastre del buque.
3.2.2. Equipos de navegación y comunicaciones en el puente: ordenadores, cartas náuticas electrónicas (ECDIS), Sistema Mundial de Navegación por Satélite (GNSS), sensores esenciales para la operación del buque.
3.2.3. Equipos relacionados con la propulsión, generación de energía eléctrica, gestión de las máquinas y control de suministro eléctrico a bordo.
3.2.4. Control de acceso al buque: de pasajeros, de la carga y de tripulaciones, inspectores, administración, etc.
3.2.5. Redes públicas a bordo para pasajeros.
4. TIPOS DE AMENAZAS Y ATAQUES A LA SEGURIDAD DE LA INFORMACIÓN.
4.1. El factor humano.
4.2. La seguridad cibernética del buque (safety).
4.3. La protección cibernética del buque (security).
4.4. Piratería cibernética contra buques e instalaciones portuarias.
5. APT – AMENAZAS AVANZADAS PERSISTENTES.
6. ESTUDIO DE CASO DE ATAQUE.
7. INGENIERÍA SOCIAL.
8. MEDIDAS DE SEGURIDAD Y PROTECCIÓN.
8.1. Obligaciones de protección cibernética incluidas en el Código Internacional de Protección del Buque e Instalaciones Portuarias (Código ISPS).
8.2. Obligaciones de protección cibernética incluidas en el Código Internacional de Gestión de la Seguridad (Código ISM).