# Curso Ciberseguridad para Operaciones Portuarias e Infraestructura Crítica

| | |
|---|---|
| **SKU** | 5098 |
| **Modalidad** | 100% Online Asincrónica |
| **Duración** | 100 horas |
| **Dirigido a** | Trabajadores portuarios, equipos operativos, supervisores, administrativos marítimos, personal de seguridad y coordinación logística. |

El **Curso Ciberseguridad para Operaciones Portuarias e Infraestructura Crítica** entrega herramientas prácticas para comprender, aplicar y mejorar procesos relacionados con las operaciones portuarias, seguridad marítima, gestión documental, prevención de riesgos y continuidad operacional. Está diseñado para fortalecer competencias laborales mediante contenidos claros, actividades aplicadas y orientación a situaciones reales del sector.

## Unidad 1. Fundamentos y contexto del curso

- **Conceptos esenciales.** Reconoce los principios, términos y criterios básicos asociados a ciberseguridad para operaciones portuarias e infraestructura crítica.
- **Marco de aplicación.** Comprende la importancia del tema en el trabajo diario, la atención de usuarios, la gestión institucional y la toma de decisiones.
- **Roles y responsabilidades.** Identifica funciones, actores relevantes y buenas prácticas para actuar con orden, responsabilidad y criterio técnico.

## Unidad 2. Procedimientos, herramientas y buenas prácticas

- **Procesos principales.** Analiza etapas, documentos, protocolos, registros y criterios de gestión vinculados al contenido del curso.
- **Aplicación práctica.** Desarrolla ejercicios, ejemplos y situaciones tipo para aplicar los contenidos en contextos laborales o comunitarios.

- **Uso de información.** Interpreta antecedentes, datos, evidencias o requerimientos para apoyar decisiones oportunas y fundamentadas.

### Unidad 3. Gestión de riesgos, calidad y mejora continua

- **Prevención de errores.** Reconoce riesgos frecuentes, malas prácticas, brechas de comunicación y medidas preventivas.
- **Calidad de servicio.** Aplica criterios de atención, trazabilidad, coordinación y mejora de procesos según las necesidades del sector.
- **Comunicación efectiva.** Presenta información de manera clara, ética y comprensible para usuarios, equipos de trabajo o partes interesadas.

### Unidad 4. Aplicación final y transferencia al puesto de trabajo

- **Casos integradores.** Resuelve situaciones asociadas a ciberseguridad para operaciones portuarias e infraestructura crítica utilizando criterios técnicos, normativos y prácticos.
- **Plan de mejora.** Propone acciones concretas para aplicar los aprendizajes en su institución, equipo o contexto laboral.
- **Buenas prácticas.** Integra recomendaciones de orden, transparencia, seguridad, cumplimiento y responsabilidad profesional.

## Modalidad

Curso 100% online asincrónico, disponible en plataforma e-learning, con acceso a contenidos digitales, material descargable, actividades de aplicación y evaluaciones en línea.

## Duración

100 horas cronológicas.

## Dirigido a

Dirigido a trabajadores portuarios, equipos operativos, supervisores, administrativos marítimos,

personal de seguridad y coordinación logística.

## Metodología

La metodología considera lectura guiada, cápsulas explicativas, recursos descargables, ejercicios de análisis, revisión de casos y actividades orientadas a la transferencia de aprendizajes al puesto de trabajo.

## Evaluación

La evaluación considera actividades formativas, controles de comprensión y una evaluación final orientada a verificar la aplicación práctica de los contenidos desarrollados.

## Competencias de egreso

- Comprender conceptos fundamentales asociados a ciberseguridad para operaciones portuarias e infraestructura crítica.
- Aplicar procedimientos, herramientas y criterios prácticos según el enfoque del curso.
- Analizar información relevante para apoyar decisiones responsables y oportunas.
- Reconocer riesgos, errores frecuentes y buenas prácticas de gestión.
- Comunicar resultados, antecedentes o recomendaciones de manera clara y ordenada.