

CL3 PROTECCIÓN CIVIL PARA LA SOCIEDAD

CONVOCATORIAS HORIZONTE EUROPA
PROGRAMA DE TRABAJO 2026-2027

CL3 PROTECCIÓN CIVIL PARA LA SOCIEDAD

1. Abierto a todo el mundo
2. Gestión de emergencias
3. Riesgos climáticos
4. Transición verde
5. Riesgos NaTech
6. Riesgos de protección
7. Ciberriesgos





Puerto de A Coruña

Autoridad Portuaria de A Coruña

ABIERTO
a todo
el mundo

CL3 PROTECCIÓN CIVIL PARA LA SOCIEDAD

Destinos y convocatorias de interés, para principio y sin exhaustividad, para la Autoridad Portuaria de A Coruña



AXENCIA
GALEGA DE
INNOVACIÓN



MINISTERIO
DE CIENCIA, INNOVACIÓN
Y UNIVERSIDADES



AGENCIA
ESTATAL DE
INVESTIGACIÓN



HORIZON-CL3-2026-01-DRS-03/04

Gestión de emergencias en la zona de servicio

- Evaluación de riesgos de desastre
 - Desarrollar sistemas de prevención
- Desarrollo de nuevas tecnologías de prevención
 - Diseño de tecnologías TRL 7-8-9
 - Integración en los actuales planes de emergencia
 - Validación de las soluciones a los riesgos de desastre



HORIZON-CL3-2026-01-DRS-05

Resiliencia al cambio climático

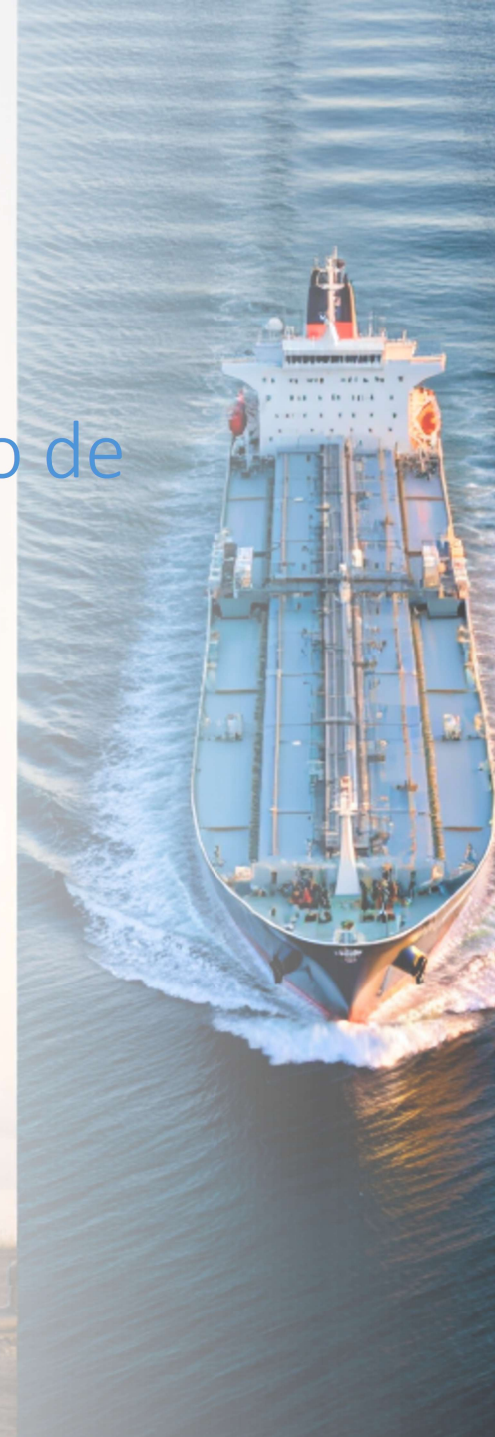
- Evaluación de riesgos climáticos
- Análisis de riesgos encadenados y acumulativos
- Análisis de riesgos encadenados
 - Fenómenos adversos → paradas operativas
 - Fenómenos adversos → accidente → impacto ambiental
 - Fenómenos adversos → toma de decisiones estratégicas
- Herramientas de previsión de riesgos climáticos
- Medidas de adaptación a los riesgos climáticos

HORIZON-CL3-2026-01-INFRA-02

Transición verde: producción y almacenamiento de nuevos combustibles renovables

En los próximos 10 o 15 años vamos a asistir a la paulatina disminución de la expedición de los combustibles fósiles convencionales (fueloil, gasoil, gasolina, querosenos, propilenos, LPGs) y a un progresivo aumento de productos renovables (biocombustibles, aceites vegetales, HEFA, RFNBO, HVO, FAME, etc.)

- Identificación de nuevos riesgos debidos a nuevas tecnologías renovables
- Verificación de nuevas medidas de seguridad y respuesta



HORIZON-CL3-2026-01-INFRA-03

Resiliencia frente a accidentes naturales o tecnológicos

- Identificación de vulnerabilidades sistémicas
- Comprobación de las medidas de respuesta actuales
- Desarrollo de herramientas operacionales para la evaluación dinámica del riesgo y el apoyo a la toma de decisiones



HORIZON-CL3-2027-01-INFRA-01

Plan de protección portuario (Código ISPS)

- Sistema de control de accesos más robustos
 - Flujos de entradas y salidas
 - Respetuosos con la LOPD
 - combinación de vehículos y conductores, acompañante
 - limitación de uso de huellas dactilares u otros datos biométricos).
 - Con operadores/actores múltiples
- Sensorización de los vallados perimetrales para anticiparse a las intrusiones
- Nuevas tecnologías, nuevas amenazas (drones no colaborativos, tanto aéreos como submarinos)



Tipología de amenazas: ataques físicos, digitales y combinados

- Ataques físicos tradicionales
 - Incluyen sabotajes e intrusiones que afectan la infraestructura portuaria de manera directa y tangible.
- Ataques informáticos
 - Malware, ransomware e interrupciones digitales que comprometen sistemas esenciales en los puertos: gestión de atraques, sistemas de comunidad portuaria (PCS)...
- Amenazas combinadas
 - Ataques que mezclan métodos físicos y digitales para maximizar el daño y complicar la defensa. Necesidad de integrar PSIM y SIEM
- Defensas híbridas
 - Planes de protección integrales que incluyen elementos físicos (barreras, tornos, cámaras), ciberseguridad avanzada y respuesta coordinada: lo virtual puede “parar” lo físico
- Integración de la IA
 - Necesidad de aplicar la IA sobre un universo de datos híbridos: sensórica IoT, datos CCTV y CCAA, datos operativos...





Conclusiones



Puerto de A Coruña

Autoridad Portuaria de A Coruña



AXENCIA
GALEGA DE
INNOVACIÓN



MINISTERIO
DE CIENCIA, INNOVACIÓN
Y UNIVERSIDADES



AGENCIA
ESTATAL DE
INVESTIGACIÓN

