

MAPA DE DEMANDA TEMPRANA

LICITACIÓN	ACTUACIÓN	RETO TECNOLÓGICO	CARACTERÍSTICAS	PRESUPUESTO	FECHA
EXP. CPP001/22: SERVICIOS DE INVESTIGACIÓN Y DESARROLLO EN MATERIA DE CIBERSEGURIDAD	A1: Programas de I+D	<u>Iniciales:</u> <ul style="list-style-type: none"> Gestión de identidades digitales. Criptografía. Gestión de incidentes. Protección de datos e información. Protección de las comunicaciones. Detección y análisis de amenazas y vulnerabilidades. Simulación de incidentes. Otros retos en materia de ciberseguridad. 	<ul style="list-style-type: none"> Compra Pública Precomercial – Procedimiento competitivo de diálogo. Programas de entre 15 y 40M€. Coinversión privada. 2/3 años de ejecución. 	86,7 M€	Julio 2022
EXP. CPP002/22: SERVICIOS DE I+D+I EN MATERIA DE CIBERSEGURIDAD	A2: Soluciones PYMES A3: Sectores estratégicos A4: Sector público A5: Infraestructuras y equipos INCIBE A7: Pequeños proyectos altamente innovadores	R1. Lucha contra los <i>insiders</i> . R2. Criptografía avanzada resistente a ataques cuánticos. R3. Soluciones para la seguridad de datos y prevenir su uso malicioso. R4. Sistemas innovadores para la evaluación, cumplimiento normativo y certificación. R5. Gestión de identidades. R6. Ciberresiliencia de cadena de suministro. R7. Sistemas innovadores para el análisis de seguridad de dispositivos IoT. R8. Sistemas para la protección frente a ataques contra el espectro electromagnético. R9. Soluciones innovadoras en ciberseguridad para Redes 5G. R10. Ciberseguridad en el vehículo conectado. R11. Ciberdiagnóstico automatizado para pymes y autónomos. R12. Sistemas innovadores para el descubrimiento y análisis de servicios en internet. R13. Investigación a partir de entornos simulados (señuelos).	<ul style="list-style-type: none"> Compra Pública Precomercial. Contratos entre 0,3 y 1,5M€. Coinversión privada. 2/3 años de ejecución. 	137,2 M€	Octubre 2022

LICITACIÓN	ACTUACIÓN	RETO TECNOLÓGICO	CARACTERÍSTICAS	PRESUPUESTO	FECHA
		<p>R14. Detección víctimas ciberdelitos.</p> <p>R15. Detección de víctimas de <i>botnets</i> a través de técnicas innovadoras.</p> <p>R16. Sistemas para el seguimiento de cripto-transacciones.</p> <p>R17. Sistema de detección de SMS y mensajería instantánea fraudulenta y campañas asociadas.</p> <p>R18. Atribución de ciberamenazas mediante técnicas innovadoras.</p> <p>R19 – R30. Centros de operaciones de ciberseguridad sectoriales.</p>			