PROGRAMA 120A

DEFENSA. MECANISMO DE RECUPERACIÓN Y RESILIENCIA

1. DESCRIPCIÓN

La Comisión Europea ha pedido a los Estados miembros que destinen las ayudas del fondo de recuperación a un total de siete áreas que el Ejecutivo Comunitario ha identificado para una correcta absorción del dinero, a fin de asegurar la reconstrucción económica a corto plazo y garantizar un crecimiento sostenido en el futuro. Bruselas se centra en impulsar las energías renovables, la eficiencia energética en edificios, el transporte limpio, el despliegue de banda ancha de internet, la ampliación de la nube, la modernización de las Administraciones públicas y la actualización de los sistemas educativos nacionales.

Pese a estas directrices, las capitales deberán respetar también las recomendaciones económicas que Bruselas les hace cada año, en particular las de 2019 y 2020, centradas principalmente en el Pacto Verde y en el crecimiento sostenible. Es vital, explica la Comisión, que los Estados miembros impulsen "la capacidad de absorción de fondos de la UE a nivel nacional".

2. ACTIVIDADES

Para el ejercicio 2021, en función de los fondos disponibles, el Ministerio de Defensa pretende acometer parte del Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (PECIS).

Este Plan, aprobado por la Instrucción 33/2018, de 6 de junio, del Secretario de Estado de Defensa, es un instrumento de coordinación con el Eje Estratégico 5 de la Secretaría de Estado de Defensa, con el Plan de Acción del MDEF para la Transformación Digital (partes 1 y 2), y con el Plan de Actuación para la Seguridad de la Información del Ministerio. Consta de 6 Ejes Estratégicos (EE), cada uno de ellos con sus propios objetivos estratégicos.

De estos 6 Ejes Estratégicos, los que se pretende impulsar en el Ministerio de Defensa con la financiación del Mecanismo Europeo de Recuperación y Resiliencia son los siguientes:

- EE 1. Avanzar hacia una Única Infraestructura Integral de Información para la Defensa (I3D).

Para ello será necesaria la integración, convergencia y en su caso unificación de las infraestructuras CIS/TIC existentes en una misma infraestructura que permita una gestión más óptima de la información requerida por los usuarios.

La I3D será una red privada destinada a los servicios específicos de la defensa y seguridad nacional, para lo que estará dotada de los más altos estándares de calidad, disponibilidad, redundancia, seguridad y resiliencia.

La transición desde la situación actual hasta la prevista se llevará a cabo mediante la racionalización, consolidación y simplificación de los Centros Proceso de Datos, las Salas Técnicas y los servicios de información para su integración en la citada I3D, así como la racionalización y simplificación de Equipos y Servicios CIS/TIC de Usuario. Se establecerá la estructura de gestión de los CIS de la I3D y se definirá e implantará un modelo de gestión flexible, que combinará aspectos de múltiples marcos de referencia y normas, proporcionará un lenguaje común y homogéneo y contendrá orientaciones para mejorar la eficacia, la eficiencia y la seguridad de la información, en línea con las mejores prácticas existentes para los procesos funcionales y operativos específicos del Departamento.

Al igual que los medios anteriores que son permanentes, ha de asegurarse la racionalización y la plena integración de los medios CIS/TIC desplegables en la I3D en línea con el modelo objetivo establecido para los permanentes. Para despliegues, se debe definir un modelo único de Red de Misión Española que cuando se despliegue para operaciones nacionales, será conceptualmente una proyección de la I3D y habrá de verificar el modelo nacional de interoperabilidad. Ese mismo modelo de Red de Misión Española se desplegará en operaciones internacionales aplicando el concepto de redes federadas, por lo que el modelo nacional de interoperabilidad deberá satisfacer también las políticas, normas y estándares internacionales del ámbito de Redes Federadas de Misión.

- EE 3. Potenciar la utilización de sistemas normalizados, homogéneos e interoperables, con empleo preferente de productos ya desarrollados en el ámbito nacional o aliado, en convergencia con el proceso de transformación digital de la AGE e incorporando las estrategias, las políticas y las iniciativas de la OTAN y la UE.

Revisando integralmente las tareas, actividades y procesos del Departamento, para lograr una transformación digital, basada en la integración de las Capacidades y los Servicios CIS/TIC en dichas actividades y procesos.

Las múltiples misiones y cometidos del MDEF y las heterogéneas condiciones en las que se desarrolla la actividad del Departamento hacen imprescindible poder disponer en todo momento del acceso a los recursos de información relevantes, a fin de poder aprovechar la superioridad que una adecuada explotación de dichos recursos supone. Para ello es necesario contar con modelo de estandarización, normalización y de interoperabilidad, para asegurar que las distintas entidades que participan en el desarrollo de una misión o cometido pueden intercambiar información de manera fiable en todo momento y lugar.

- EE 4. Consolidar la Seguridad en los CIS/TIC, a través del fortalecimiento de las capacidades de prevención, detección y respuesta a ciberataques, en línea con la Política de Seguridad de la Información del MDEF y con la Estrategia de Ciberseguridad Nacional y de las organizaciones internacionales de las que España forma parte.

Con el fin de lograr una visión integral de la seguridad de la información, es imprescindible que al margen de las medidas técnicas establecidas y los servicios asociados se desarrollen una serie de actuaciones de coordinación y gestión complementarias para asegurar la protección de la información conforme a lo establecido en la Política CIS/TIC.

Uno de los elementos principales para asegurar la protección adecuada de la información del MDEF, es el cumplimiento del Esquema Nacional de Seguridad de la AGE. Esta ejecución se hará tomando en consideración los procesos y procedimientos de evaluación y adecuación que en este sentido se establecerán igualmente para la consecución del Plan de actuación para la Seguridad de la Información.

3. OBJETIVOS E INDICADORES DE SEGUIMIENTO

OBJETIVO	2019		2020		2021
	Presu-puestado	Ejecución	Presu-puestado	Ejecución Prevista	Presu-puestado
1. Órgano Central de la Defensa ***(Miles €)***	**0,00**	**0,00**	**0,00**	**0,00**	**25.000,00**

INDICADORES	2019		2020		2021
	Presu-puestado	Ejecución	Presu-puestado	Ejecución Prevista	Presu-puestado
Inversiones en:					
– Plan estratégico CIS (PECIS) ***(Miles €)***	0,00	0,00	0,00	0,00	25.000,00