RESUMEN EJECUTIVO

ANTECEDENTES

Entidad: Ministerio de Defensa.

Referencia: Supervisión a la implementación de los Planes de Contingencia Tecnológica.

Informe Nº: K3/GP419/L25-G1.

Objeto: Las acciones que se ejecutan por el Ministerio de Defensa para la implementación de su Plan de Contingencia Tecnológica.

Periodo supervisado: Información y actividades verificadas hasta el 23 de septiembre de 2025.

OBJETIVO Y ALCANCE

Objetivo de la Supervisión:

"Evaluar si las acciones para la implementación del Plan de Contingencia Tecnológica en el Ministerio de Defensa se ejecutan en el marco de los criterios de legalidad, calidad y/o oportunidad."

Alcance:

Se basó en el análisis de la documentación remitida por la entidad, enfocándose en la capacitación, la designación de responsables y la ejecución de pruebas al Plan de Contingencia Tecnológica. La supervisión se realizó bajo el "Procedimiento para el Ejercicio de la Supervisión" aprobado por Resolución N° CGE/014/2025.

RESULTADOS

La supervisión identificó que, aunque el Ministerio de Defensa cuenta con un Plan Institucional de Seguridad de la Información (PISI) aprobado y ha conformado formalmente su Comité de Seguridad de la Información (CSI), existen deficiencias en la implementación operativa. Se constató la ausencia de capacitaciones específicas sobre el plan, la falta de ejecución de pruebas integrales y una definición imprecisa de roles y responsabilidades.

K3/GP419/L25-G1

PRONUNCIAMIENTO

De la evaluación realizada, se establece que las acciones del Ministerio de Defensa presentan limitaciones respecto a los criterios de calidad y oportunidad. Si bien la entidad posee protocolos para cinco tipos de contingencias y realiza respaldos habituales de información crítica, estas medidas son insuficientes al no estar validadas mediante simulacros o pruebas integrales.

Se evidenció que las responsabilidades se asignan de manera genérica a cargos que no existen formalmente en la estructura organizacional, lo que genera ambigüedad y riesgo de dilución de responsabilidades ante un evento real. Asimismo, la postergación de las pruebas programadas y la falta de capacitación del personal involucrado impiden identificar debilidades en los procedimientos, lo que podría derivar en un incremento del tiempo de inactividad de los sistemas y afectar la continuidad de los servicios críticos y la Política de Seguridad y Defensa Nacional.

RECOMENDACIÓN GENERAL

Se recomienda a la Máxima Autoridad Ejecutiva del Ministerio de Defensa adoptar oportunamente las acciones preventivas o correctivas para la implementación de su Plan de Contingencia Tecnológica, en el marco de la normativa de Seguridad de la Información vigente. Además, se recomienda responder por escrito y con la debida fundamentación sobre las alertas reportadas en un plazo de 5 días hábiles computables a partir de la fecha de recepción del informe.