

RESUMEN EJECUTIVO

ANTECEDENTES

Entidad: Ministerio de Gobierno.

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

Informe N°: K3/GP450/L25-G1.

Objeto: Las acciones que se ejecutan por el Ministerio de Gobierno para la implementación de sus Planes de Contingencia Tecnológica.

Periodo supervisado: Información y actividades verificadas hasta el 26 de septiembre de 2025.

OBJETIVO Y ALCANCE

Objetivo de la Supervisión:

“Evaluar si las acciones para la implementación de los Planes de Contingencia Tecnológica en el Ministerio de Gobierno 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 y la información proporcionada sobre las actividades de implementación en curso. La supervisión se realizó bajo el “Procedimiento para el Ejercicio de la Supervisión” aprobado por Resolución N° CGE/014/2025.

RESULTADOS

La supervisión identificó deficiencias significativas, constatando que el Ministerio de Gobierno no cuenta con Planes de Contingencia Tecnológica (PCT) formalmente aprobados por la Máxima Autoridad Ejecutiva (MAE). Asimismo, se evidenció la ausencia de un manual de procedimientos para la gestión de contingencias y la falta de constitución formal del Comité de Seguridad de la Información (CSI) y del Responsable de Seguridad de la Información (RSI).

PRONUNCIAMIENTO

De la evaluación realizada, se establece que las acciones del Ministerio de Gobierno no aseguran una adecuada implementación bajo criterios de calidad y oportunidad. Si bien la Unidad de Sistemas ejecuta actividades técnicas como respaldos, monitoreo y revisiones de infraestructura, estas carecen de respaldo en normativa interna formalizada, lo que restringe su validez institucional y dificulta la asignación de responsabilidades y la ejecución de pruebas periódicas.

Se identificó que la coordinación ante incidentes se realiza de manera informal mediante comunicación directa entre el personal técnico, sin un esquema formal de roles y responsabilidades. Esta carencia de un marco normativo aprobado y de procedimientos documentados genera un riesgo crítico, ya que ante una contingencia, la entidad podría no disponer de una estructura institucional para coordinar respuestas efectivas, garantizando la continuidad de los servicios críticos y minimizando el impacto en la disponibilidad de la información.

RECOMENDACIÓN GENERAL

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