RESUMEN EJECUTIVO

ANTECEDENTES

Entidad: Servicio General de Identificación Personal (SEGIP).

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

Informe Nº: K3/GP375/Y25-G1.

Objeto: Las acciones emprendidas por el SEGIP para la implementación de su Plan de Contingencia Tecnológica.

Periodo supervisado: Información y actividades verificadas hasta el 04 de agosto de 2025.

OBJETIVO Y ALCANCE

Objetivo de la Supervisión:

"Evaluar si las acciones para la implementación del Plan de Contingencia Tecnológica en el SEGIP 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 el SEGIP, incluyendo los procedimientos para el respaldo de información (backup) y las actividades en curso para la implementación del plan. 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 el SEGIP no dispone de un Plan de Contingencia Tecnológica formalmente elaborado, aprobado e implementado. Asimismo, se constató la ausencia de procedimientos documentados para la atención de incidentes, falta de un cronograma de pruebas periódicas, inexistencia de programas de capacitación específica y la falta de aprobación formal por la Máxima Autoridad Ejecutiva (MAE) del procedimiento de generación de respaldos.

PRONUNCIAMIENTO

De la evaluación realizada, se establece que las acciones del SEGIP presentan deficiencias respecto a los criterios de calidad y oportunidad. Si bien la entidad ejecuta acciones operativas (respaldos de bases de datos, mantenimiento de infraestructura y conectividad redundante), estas se sustentan en buenas prácticas y guías preliminares en borrador, sin estar articuladas en un marco documental oficial que defina responsabilidades y procedimientos formales.

La carencia de un plan institucionalizado y de una estructura transversal con roles definidos genera riesgos críticos, considerando el rol del SEGIP en la administración de la base de datos de identificación personal del país. La ausencia de pruebas documentadas y de capacitación limita la capacidad de respuesta ante fallas, lo que podría derivar en interrupciones operativas prolongadas de servicios esenciales (emisión de CI y licencias), comprometiendo la disponibilidad, integridad y confidencialidad de la información institucional.

RECOMENDACIÓN GENERAL

Se recomienda a la Máxima Autoridad Ejecutiva del SEGIP adoptar oportunamente las acciones preventivas o correctivas para consolidar la elaboración, aprobación e implementación de su Plan de Contingencia Tecnológica. Asimismo, se recomienda emitir un pronunciamiento por escrito sobre las alertas reportadas en un plazo de 5 días hábiles computables a partir de la fecha de recepción del informe.