RESUMEN EJECUTIVO

ANTECEDENTES

Entidad: Universidad Mayor de San Andrés (UMSA).

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

Informe Nº: K3/GP645/S25-G1.

Objeto: Las acciones emprendidas por la Universidad Mayor de San Andrés para la implementación de su Plan de Contingencia Tecnológica.

Periodo supervisado: Información y actividades verificadas hasta el 13 de noviembre de 2025.

OBJETIVO Y ALCANCE

Objetivo de la Supervisión:

"Evaluar si las acciones para la implementación del Plan de Contingencia Tecnológica en la UMSA 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, entrevistas y la verificación de actividades en curso respecto a la implementación de Planes 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 la UMSA no cuenta con un Plan de Contingencia Tecnológica aprobado por la Máxima Autoridad Ejecutiva (MAE). Aunque la universidad dispone de un Plan Institucional de Seguridad de la Información (PISI) y un Responsable de Seguridad de la Información (RSI), se evidenció la ausencia del Comité de Seguridad de la Información (CSI) y la inexistencia de procedimientos formalizados, pruebas documentadas y programas de capacitación específicos para contingencias.

PRONUNCIAMIENTO

De la evaluación realizada, se establece que las acciones de la UMSA son insuficientes respecto a los criterios de calidad y oportunidad. Si bien se constató que la elaboración del plan (basado en la Norma ISO 22301:2019) está en curso y que se aplican prácticas operativas como respaldos diarios y pruebas de restauración trimestrales, estas se ejecutan de manera informal y no estandarizada.

La dependencia de canales de comunicación no oficiales (como WhatsApp, Telegram y Slack) para la gestión de incidentes y la falta de un marco normativo interno aprobado generan riesgos significativos. Estos incluyen la posible prolongación de tiempos de respuesta, la afectación a la disponibilidad de servicios críticos y la probabilidad de restauraciones incompletas o errores por falta de procedimientos documentados, lo que impide garantizar una continuidad operativa resiliente ante fallas tecnológicas o ciberataques.

RECOMENDACIÓN GENERAL

Se recomienda a la Máxima Autoridad Ejecutiva de la Universidad Mayor de San Andrés adoptar oportunamente las acciones preventivas y correctivas que correspondan para formalizar la aprobación e implementación de su Plan de Contingencia Tecnológica. Asimismo, se requiere que la entidad responda por escrito y con la debida fundamentación sobre las alertas reportadas en un plazo de 5 días hábiles tras la recepción del informe