Tipo de trabajo	**Auditoría Especial**		**Auditoría Regular**	**X**
Fecha trabajo	30/03/2026			
Proceso/Unidad Auditable	Modelo de Seguridad y Privacidad de la Información MSPI			
Equipo auditor	Ana Josefa Carreño Pérez			
Objetivo Auditoría	Evaluar el nivel de implementación del Modelo de Seguridad y Privacidad de la Información MSPI de la UMV, verificando el cumplimiento de los lineamientos del MinTIC, las políticas institucionales y los controles establecidos, con el fin de determinar la capacidad del modelo para proteger la confidencialidad, integridad y disponibilidad de la información.			
Alcance	Esta auditoría evaluó los riesgos y controles de los procedimientos, políticas, planes, manuales e instructivos relacionados con el MSPI desde el 01/01/2025 hasta el 15/11/2025 • Declaración de aplicabilidad • Mapa de riesgos proceso EGTI • Política General • Políticas específicas • Manual del SGSI • Política de administración del riesgo • Procedimiento Gestión de activos de Información • Plan de Seguridad y Privacidad de la información			

1. ASPECTOS RELEVANTES

1.1 Fortalezas	1. Cumplimiento del Plan de Seguridad de la Información proyectado para la vigencia 2025, reflejado en la ejecución de las actividades programadas y el logro de los productos esperados en los diferentes ejes estratégicos del MSPI. 2. Cumplimiento del plan de sensibilización en seguridad y privacidad de la información, mediante la ejecución de las actividades programadas y la implementación de estrategias de concientización orientadas a los funcionarios y contratistas lo cual ha contribuido a fortalecer la cultura organizacional en materia de seguridad de la información, promoviendo buenas prácticas.

	3. Se adelantó el proceso de actualización de instrumentos para la identificación de activos de información, y como parte de la segunda línea de defensa, el Oficial de Seguridad de la Información realizó el monitoreo de los riesgos de seguridad de la entidad, fortaleciendo la identificación, evaluación y seguimiento de los riesgos asociados a la información institucional. 4. Se actualizaron dos políticas específicas de seguridad de la información, se revisó y ajustó el procedimiento de gestión de incidentes, y se formuló la política de uso seguro de IA generativa. 5. Se realizó un análisis de vulnerabilidades a los portales de la entidad con el apoyo de la Alta Consejería Distrital de TIC. 6. Los auditados atendieron oportunamente las mesas de trabajo y remitieron la información solicitada.
1.2 Oportunidades de mejora	1. Establecer y formalizar de manera integral los roles, responsabilidades y líneas de autoridad del MSPI, asegurando su independencia funcional, adecuada segregación de funciones y articulación con las instancias de decisión, con el fin de mejorar la supervisión y la toma de decisiones estratégicas. 2. Actualizar y armonizar los instrumentos clave del modelo (política de seguridad, declaración de aplicabilidad, autodiagnóstico y mapas de riesgo), garantizando su alineación con la NTC ISO/IEC 27001:2022, los lineamientos del MinTIC y su coherencia interna, de manera que soporten efectivamente la gestión de riesgos y el cumplimiento normativo. 3. Definir e integrar indicadores de desempeño, mecanismos de monitoreo y controles de trazabilidad para los componentes del MSPI, que permitan evaluar su nivel de madurez, y fortalecer la mejora continua del sistema. 4. Establecer criterios claros para el diseño, documentación e implementación de los controles del MSPI, así como mecanismos periódicos de monitoreo y evaluación de su efectividad, que permitan verificar su adecuada ejecución, medir su desempeño frente a los riesgos identificados y

	asegurar su contribución a la mitigación de los riesgos de seguridad y privacidad de la información.
1.3 Conclusiones	**Diseño de controles** Se evaluaron 16 controles asociados al mapa de riesgos del proceso, evidenciando una concentración significativa en controles manuales y con niveles de madurez limitados: • 7 controles (44%) obtuvieron una calificación del 40%, al ser de naturaleza preventiva pero ejecutados de forma manual. • 7 controles (44%) alcanzaron una calificación del 30%, al corresponder a controles correctivos con ejecución manual. • 1 control (6%) obtuvo una calificación del 25%, por ser correctivo y manual, con debilidades adicionales en su diseño. • 1 control (6%) alcanzó una calificación del 50%, al ser preventivo y automático, evidenciando un mayor nivel de madurez y capacidad de aseguramiento. El 94% de los controles evaluados son manuales, asimismo, se observa una alta proporción de controles correctivos, lo que indica un enfoque reactivo en la gestión del riesgo. El diseño de los controles presenta un nivel de madurez bajo–medio, con predominancia de controles manuales y oportunidades de mejora en su diseño, automatización y enfoque preventivo. **Ejecución del control** Dieciséis (16) controles son eficaces y eficientes, en tanto se ejecutan conforme a su diseño, cuentan con evidencia suficiente de aplicación y contribuyen de manera adecuada a la mitigación de los riesgos asociados. Por su parte, seis (6) actividades clave relacionadas con la actualización, mantenimiento, seguimiento y monitoreo del MSPI son parcialmente eficaces y parcialmente eficientes, debido a debilidades en su implementación, consistencia en la ejecución y/o limitaciones en los mecanismos de seguimiento y medición, lo que reduce su capacidad para gestionar oportunamente las brechas identificadas. Finalmente, una (1) actividad clave se clasifica como no eficaz ni eficiente, dado que carece de indicadores definidos, lo que impide medir su desempeño, realizar seguimiento estructurado y evaluar su contribución al cumplimiento de los objetivos del MSPI. Si bien se evidencian avances en la implementación de controles, persisten debilidades en los componentes de medición, seguimiento y

	mejora continua, lo cual limita la madurez del MSPI y su capacidad para anticipar y mitigar riesgos de seguridad y privacidad de la información.

2. RESUMEN DE LOS RESULTADOS

Proceso/ unidad auditable	Procedimiento	Total	%
Modelo de Seguridad y Privacidad de la Información	Gobernanza y estructura organizacional	2	29%
	Marco normativo y documentación del sistema	3	43%
	Seguimiento, medición y mejora continua	1	14%
	Gestión de riesgos	1	14%
TOTAL GENERAL		**7**	**100%**

3. DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA

A continuación se relacionan la zona de riesgo de los hallazgos identificados en el ejercicio de auditoría:

Modelo de Seguridad y Privacidad de la Información MSPI	
	Hallazgo1. Debilidades en la gobernanza del MSPI Se evidenció que el rol de Oficial de Seguridad y Privacidad de la Información no se encuentra formalmente definido dentro de la estructura orgánica de la UAERMV. Las funciones asociadas a la seguridad de la información son asumidas por la Oficina de Tecnologías de la Información (OTI), con apoyo de un contrato de prestación de servicios que contempla algunas obligaciones relacionadas con dicho rol. Esta configuración limita la independencia, autoridad y visibilidad estratégica del responsable del MSPI y genera potenciales conflictos de interés, en la medida en que el mismo equipo encargado de implementar y operar las soluciones tecnológicas participa en el monitoreo y verificación del cumplimiento del modelo. Los sistemas son responsables también de monitorear el cumplimiento del Modelo.
	Hallazgo2. Debilidades en la estructura y contenido de la Política de Seguridad y Privacidad de la Información frente a los requisitos normativos y buenas prácticas (Secretaría General) Se evidenció que la Política de Seguridad y Privacidad de la Información (documento EGTI_DI-030_v1) no incorpora de manera integral los elementos mínimos requeridos para una política de seguridad de la información robusta. En particular, se identificaron vacíos en la definición explícita de seguridad de la información, la formulación de principios rectores, la asignación clara de responsabilidades a roles definidos del MSPI, el compromiso expreso con la mejora continua y la inexistencia de procedimientos para la gestión de exenciones y excepciones a la política y a los controles de seguridad.

	Hallazgo 3. Declaración de Aplicabilidad incompleta frente a los requisitos de la NTC ISO/IEC 27001:2022 (Secretaría General) Durante el ejercicio de auditoría se evidenció que la Declaración de Aplicabilidad (SoA) se encuentra estructurada conforme al Anexo A de la norma NTC ISO/IEC 27001:2022 e incluye el listado de los 93 controles; sin embargo, presenta deficiencias en su diligenciamiento, al no contener información clave como la descripción de cada control, la justificación para su inclusión o exclusión, el nivel de implementación, la descripción de la forma en que se implementa el control y el enlace o referencia a los procedimientos, políticas o controles operativos asociados.
	Hallazgo 4. Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información desactualizado frente a la NTC ISO/IEC 27001:2022 (Secretaría General) En el desarrollo de la auditoría se evidenció que el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) se encuentra elaborado con base en versiones anteriores de la NTC ISO/IEC 27001 y no incorpora los cambios, controles y enfoques establecidos en la versión 2022. En consecuencia, el instrumento no refleja de manera integral el nivel real de madurez del Sistema de Gestión de Seguridad de la Información (SGSI).
	Hallazgo 5. Debilidad en la definición de indicadores de desempeño para el seguimiento y medición del Modelo de Seguridad y Privacidad de la Información (Secretaría General) Durante el ejercicio de auditoría se evidenció que la entidad no cuenta con indicadores definidos, documentados e implementados para medir el desempeño, efectividad y nivel de madurez del Modelo de Seguridad y Privacidad de la Información (MSPI). No se identificaron indicadores asociados a la gestión de riesgos, implementación de controles, gestión de incidentes, cumplimiento normativo ni mejora continua, ni reportes periódicos que permitan evaluar su evolución y soporte para la toma de decisiones.
	Hallazgo 6. Inconsistencia en la gestión, actualización y trazabilidad de los mapas de riesgo del proceso EGTI (OTI) En la documentación allegada al equipo auditor se evidenció que, para el ejercicio de monitoreo cuatrimestral realizado por la Oficina Asesora de Planeación, se presentaron dos mapas de riesgo distintos correspondientes al proceso EGTI, sin soporte documental que respalde su actualización: • **I cuatrimestre:** 17 riesgos, 26 controles y 28 acciones. • **II cuatrimestre:** 13 riesgos, 28 controles y 27 acciones. No se identificó evidencia de solicitud formal de actualización, análisis técnico que sustente los cambios, actas de validación y aprobación, ni mecanismos de trazabilidad que expliquen la eliminación, incorporación o modificación de riesgos, controles y acciones entre ambos periodos.
	Hallazgo 7. Inconsistencia en la gestión, actualización y trazabilidad de los mapas de riesgo del proceso EGTI (OTI) En la documentación allegada al equipo auditor se evidenció que, para el ejercicio de monitoreo cuatrimestral realizado por la Oficina Asesora de Planeación, se presentaron dos mapas de riesgo distintos correspondientes al proceso EGTI, sin soporte documental que respalde su actualización: • **I cuatrimestre:** 17 riesgos, 26 controles y 28 acciones. • **II cuatrimestre:** 13 riesgos, 28 controles y 27 acciones. No se identificó evidencia de solicitud formal de actualización, análisis técnico que sustente los cambios, actas de validación y aprobación, ni mecanismos de trazabilidad que expliquen la eliminación, incorporación o modificación de riesgos, controles y acciones entre ambos periodos.

4. PLAN DE MEJORAMIENTO

El auditor radico informe final mediante radicado 20261600105913 con fecha 30 de marzo de 2026.

El auditado cuenta con 8 días hábiles para suscribir el plan de mejoramiento y remitirlo vía memorando a la Oficina de Control Interno. Una vez remitido se sube al aplicativo CHIE y se realizará seguimiento de manera periódica.

FIRMA DEL INFORME DE AUDITORÍA:		
FECHA DE APROBACIÓN:		
NOMBRE	**RESPONSABILIDAD**	**FIRMA**
Ana Lucia Bacares Toledo	Jefe Oficina de Control Interno	
Ana Josefa Carreño Pérez	Auditor Líder	